PACHA
Revista de Estudios Contemporáneos del Sur Global

Seguridad militar inteligente: integración de tecnologías emergentes y gobernanza contractual en la protección de infraestructuras estratégicas del Ejército Ecuatoriano

Smart military security: Integrating emerging technologies and contractual governance in the protection of strategic infrastructures of the Ecuadorian Army

Christian Germánico Espinoza Jaramillo, Diego Alexander Sotomayor Ortiz, Miguel Mauricio Viera Cisneros, Víctor Hugo Cano Morales

Resumen

La transformación de los sistemas de defensa en el siglo XXI exige que las instituciones militares integren tecnologías emergentes dentro de sus estructuras estratégicas, operativas y contractuales. Este artículo aborda la evolución hacia una "seguridad militar inteligente" en el contexto del Ejército Ecuatoriano, entendida como la articulación entre capacidades tecnológicas avanzadas —como la inteligencia artificial, la ciberdefensa, los sistemas ciberfísicos y la automatización logística— y una gobernanza contractual sólida, ética y eficiente. Desde un enfoque cualitativo y mediante una revisión documental especializada en bases académicas de alto impacto (JCR, Scopus, REDIB, Dialnet Metrics y ERIHPLUS), se analizan catorce ejes temáticos clave que permiten comprender tanto los avances como las limitaciones que enfrenta Ecuador en su transición hacia una defensa más moderna, resiliente y soberana. Los resultados muestran que, si bien existen señales positivas en la adopción de innovaciones tecnológicas, aún persisten importantes brechas en términos de planificación institucional, formación de talento humano, seguridad normativa y capacidad de integración interinstitucional. Se identifica la gobernanza contractual como un elemento crítico para asegurar que las inversiones tecnológicas respondan a intereses estratégicos del Estado y no generen dependencias perjudiciales. Además, se destaca la necesidad de adoptar una visión ética y multidisciplinaria que permita anticiparse a los dilemas propios de la automatización militar y la vigilancia digital. Finalmente, el estudio propone un conjunto de lineamientos para fortalecer la seguridad militar ecuatoriana mediante una estrategia de innovación gradual, contextualizada y soberana, destacando que la tecnología, sin un marco de gobernanza robusto, puede volverse tan vulnerable como aquello que busca proteger.

Palabras clave: Seguridad militar inteligente; Tecnologías emergentes; Gobernanza contractual; Infraestructuras estratégicas; Ejército Ecuatoriano

Christian Germánico Espinoza Jaramillo
Universidad de las Fuerzas Armadas, ESPE | Sangolquí | Ecuador | germanico5452@gmail.com
https://orcid.org/0009-0000-4958-5327
Diego Alexander Sotomayor Ortiz
Universidad de las Fuerzas Armadas, ESPE | Sangolquí | Ecuador | sotomayordiego76@gmail.com
Miguel Mauricio Viera Cisneros
Universidad de las Fuerzas Armadas, ESPE | Sangolquí | Ecuador | mmaurovc97@gmail.com
Víctor Hugo Cano Morales
Universidad de las Fuerzas Armadas, ESPE | Sangolquí | Ecuador | victorcanomorales@gmail.com

http://doi.org/10.46652/pacha.v6i19.466
ISSN 2697-3677
Vol. 6 No. 19 septiembre-diciembre 2025, e250466
Quito, Ecuador

Enviado: abril 01, 2025
Aceptado: agosto 03, 2025
Publicado: agosto 27, 2025
Publicación Continua

RELIGACIÓN CICSHAL
Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina

Abstract

The transformation of defense systems in the 21st century requires military institutions to integrate emerging technologies into their strategic, operational, and contractual structures. This article addresses the evolution toward "smart military security" in the context of the Ecuadorian Army, understood as the articulation between advanced technological capabilities—such as artificial intelligence, cyber defense, cyber-physical systems, and logistics automation—and solid, ethical, and efficient contractual governance. Using a qualitative approach and a specialized review of high-impact academic databases (JCR, Scopus, REDIB, Dialnet Metrics, and ERIHPLUS), fourteen key thematic areas are analyzed to understand both the advances and limitations Ecuador faces in its transition toward a more modern, resilient, and sovereign defense. The results show that, although there are positive signs in the adoption of technological innovations, significant gaps remain in terms of institutional planning, human talent training, regulatory security, and inter-institutional integration capacity. Contractual governance is identified as a critical element in ensuring that technological investments respond to the strategic interests of the state and do not create harmful dependencies. In addition, the study highlights the need to adopt an ethical and multidisciplinary vision that allows for the anticipation of dilemmas inherent to military automation and digital surveillance. Finally, the study proposes a set of guidelines to strengthen Ecuadorian military security through a strategy of gradual, contextualized, and sovereign innovation, emphasizing that technology, without a robust governance framework, can become as vulnerable as what it seeks to protect.

Keywords: Intelligent military security; Emerging technologies; Contractual governance; Strategic infrastructure; Ecuadorian Army

Introducción

En el contexto contemporáneo, marcado por una complejidad geopolítica creciente y amenazas híbridas que trascienden las fronteras físicas y digitales, la seguridad de las infraestructuras estratégicas ha adquirido un papel central en la estabilidad y soberanía de los Estados. En este escenario, las instituciones militares ya no pueden limitarse a enfoques convencionales de defensa; se enfrentan al desafío urgente de integrar tecnologías emergentes y marcos de gobernanza adaptativos que les permitan anticipar, prevenir y neutralizar riesgos con mayor precisión y eficiencia. Particularmente en América Latina, y de manera específica en Ecuador, este desafío se torna aún más crítico debido a la combinación de vulnerabilidades estructurales, amenazas transnacionales (como el narcotráfico y el crimen organizado) y una creciente dependencia de activos tecnológicos en sectores estratégicos como la energía, las telecomunicaciones y la infraestructura crítica.

La noción de "seguridad militar inteligente" emerge como una respuesta integral a este nuevo entorno de amenazas. Este enfoque propone no solo el uso de herramientas tecnológicas avanzadas —como inteligencia artificial, sistemas ciberfísicos, análisis predictivo y vigilancia automatizada— sino también la reestructuración de las relaciones contractuales entre el Estado, sus fuerzas armadas y actores privados especializados en tecnología y seguridad. Así, el concepto de gobernanza contractual adquiere protagonismo como mecanismo de articulación entre innovación, regulación, control estatal y soberanía, garantizando que las nuevas capacidades tecnológicas respondan a los intereses nacionales sin comprometer principios éticos ni la transparencia institucional.

Los antecedentes históricos del Ejército Ecuatoriano muestran una evolución desde modelos de defensa territorial hacia estrategias más flexibles e interinstitucionales. No obstante, la adopción efectiva de tecnologías emergentes aún enfrenta obstáculos significativos, como limitaciones presupuestarias, marcos jurídicos obsoletos y brechas de interoperabilidad entre sistemas civiles y militares. A pesar de estos desafíos, recientes iniciativas —como la digitalización de los procesos logísticos, la implementación de drones en vigilancia fronteriza y la cooperación internacional en ciberseguridad— evidencian un cambio de paradigma que merece ser analizado con mayor profundidad. La situación actual demanda entonces un abordaje académico que combine los enfoques de las ciencias militares, la economía política, la ingeniería de sistemas y el derecho contractual.

Este artículo tiene como objetivo analizar cómo la integración de tecnologías emergentes y mecanismos de gobernanza contractual pueden fortalecer la protección de infraestructuras estratégicas del Ejército Ecuatoriano, a partir de una revisión teórico-práctica, estudios de caso regionales, y un enfoque interdisciplinario que articula los ámbitos técnico, jurídico e institucional. Se busca no solo evaluar el estado actual de estas capacidades en Ecuador, sino también proponer lineamientos estratégicos y recomendaciones de política pública que impulsen una defensa más inteligente, eficiente y soberana.

Metodología

Este artículo se enmarca dentro de una investigación de naturaleza cualitativa, de tipo documental y enfoque interpretativo. La elección de este diseño metodológico responde a la necesidad de analizar en profundidad fenómenos complejos —como la integración tecnológica y la gobernanza contractual en el ámbito militar— cuyas dinámicas no pueden ser comprendidas adecuadamente mediante técnicas cuantitativas o de medición estadística tradicional. En su lugar, se opta por una estrategia que privilegia la comprensión contextual, el análisis crítico de fuentes especializadas y la construcción teórica a partir del contraste entre marcos conceptuales y experiencias prácticas relevantes.

La recopilación de información se realizó a través de una revisión sistemática de literatura académica indexada en las principales bases de datos científicas reconocidas a nivel internacional: Journal Citation Reports (JCR), Scopus, REDIB, Dialnet Metrics y ERIHPLUS. Esta selección garantiza tanto la actualidad como la rigurosidad de las fuentes utilizadas, y responde a la exigencia de utilizar al menos un 30% de referencias provenientes de publicaciones de alto impacto, tal como lo establecen los lineamientos editoriales del Congreso Internacional de Economía y Comercio.

El corpus documental incluye artículos científicos, libros especializados, documentos técnicos de organismos multilaterales, normativas nacionales e internacionales, y estudios de caso aplicados al sector defensa. Se priorizaron los trabajos publicados en los últimos diez años (2014-2024), especialmente aquellos que abordan temas relacionados con seguridad militar, tecnologías emergentes, ciberdefensa, gobernanza contractual y protección de infraestructuras críticas. Adi-

cionalmente, se incorporaron fuentes institucionales y marcos normativos del contexto ecuatoriano, con el fin de garantizar la pertinencia local del análisis.

El tratamiento de la información se llevó a cabo mediante análisis de contenido temático, con énfasis en la identificación de categorías recurrentes, patrones discursivos y tensiones conceptuales presentes en la literatura. Las unidades de análisis se organizaron en torno a tres ejes: (1) tecnologías emergentes aplicadas a la defensa y seguridad; (2) modelos de gobernanza y contratación en sistemas militares; y (3) gestión y protección de infraestructuras estratégicas. Este esquema permitió una triangulación teórica que contribuyó a enriquecer la interpretación de los hallazgos y a fundamentar sólidamente las propuestas derivadas.

Cabe destacar que, al tratarse de una investigación documental y no experimental, no se recurrió a técnicas de recolección de datos empíricos como encuestas o entrevistas. No obstante, se aplicaron criterios de exhaustividad, relevancia y validez para seleccionar las fuentes y asegurar la coherencia metodológica del estudio.

Resultados

Inteligencia Artificial en la Defensa Militar

La inteligencia artificial (IA) se ha convertido en un factor transformador en las operaciones militares, permitiendo procesar grandes volúmenes de datos y mejorar la toma de decisiones estratégicas. Según Garat González (2024), la IA contribuye a ordenar y dar coherencia al gran volumen de datos existentes, aliándose con la inteligencia humana para satisfacer las necesidades militares en un entorno competitivo y demandante.

En el contexto ecuatoriano, la incorporación de IA en las fuerzas armadas podría mejorar significativamente las capacidades operativas y estratégicas. Sin embargo, es crucial establecer marcos éticos y legales que regulen su uso, garantizando que las decisiones críticas no se deleguen completamente a sistemas autónomos sin supervisión humana.

Ciberdefensa y protección de infraestructuras críticas

La ciberdefensa es esencial para proteger las infraestructuras críticas del Estado, incluyendo las militares. Semanate y Recalde (2023), destacan que, ante la proliferación de amenazas cibernéticas, Ecuador ha promulgado políticas y estrategias enfocadas a garantizar un ciberespacio seguro.

A pesar de estos esfuerzos, persisten desafíos significativos en la implementación efectiva de medidas de ciberseguridad. Es necesario fortalecer las capacidades técnicas y humanas, así como fomentar una cultura de seguridad cibernética en todas las instituciones del Estado.

Gobernanza contractual en la adopción de tecnologías emergentes

La adopción de tecnologías emergentes en el ámbito militar no puede ser entendida únicamente como una cuestión técnica o presupuestaria; se trata, fundamentalmente, de un proceso político-estratégico que exige una gobernanza contractual sólida, transparente y orientada al interés público. La gobernanza contractual en defensa hace referencia al conjunto de normas, mecanismos y relaciones que regulan la adquisición, implementación, uso y supervisión de tecnologías a través de acuerdos entre el Estado y actores privados, nacionales o internacionales. Esta dimensión adquiere especial relevancia cuando se trata de tecnologías sensibles como inteligencia artificial, sistemas autónomos, sensores inteligentes, redes de comunicación militar o herramientas de ciberdefensa, cuyos impactos operativos y éticos son de alto alcance.

Según González Mosquera et al. (2022), es indispensable que las Fuerzas Armadas del Ecuador cuenten con un sistema institucional robusto que oriente sus procesos de innovación hacia áreas de conocimiento alineadas con sus misiones estratégicas y con la realidad geopolítica y territorial del país. Este sistema debe permitir una toma de decisiones informada, técnica y legalmente respaldada, reduciendo los márgenes de discrecionalidad en los procesos de contratación tecnológica. Además, debe garantizar la transparencia en los acuerdos, la trazabilidad de las decisiones y la rendición de cuentas a través de auditorías externas y mecanismos de control civil.

Implementar una gobernanza efectiva implica, por tanto, establecer marcos normativos claros que definan criterios mínimos para la contratación de tecnologías emergentes en defensa: origen de los proveedores, condiciones de seguridad, cláusulas de interoperabilidad, cumplimiento de estándares internacionales, obligaciones éticas y resguardos sobre la soberanía digital. Asimismo, debe existir una arquitectura de supervisión compuesta por organismos técnicos especializados capaces de evaluar el cumplimiento de los contratos no solo en términos financieros, sino en su impacto estratégico, operativo y social. En otras palabras, la gobernanza contractual no debe ser una tarea exclusivamente jurídica o administrativa, sino una función articuladora entre los objetivos de seguridad nacional, la ética tecnológica y la sostenibilidad institucional.

En el caso ecuatoriano, avanzar en esta dirección supone también revisar y modernizar los marcos legales existentes en materia de adquisiciones militares, defensa tecnológica y cooperación internacional, asegurando que estos respondan a las particularidades del nuevo entorno digital y militar. Solo a través de una gobernanza contractual bien diseñada y aplicada será posible garantizar que la integración de tecnologías emergentes refuerce, y no debilite, la autonomía estratégica del Estado y la eficacia operativa de sus Fuerzas Armadas.

Sistemas ciberfísicos en la seguridad nacional

Los sistemas ciberfísicos, que integran componentes físicos y computacionales, ofrecen capacidades avanzadas para la vigilancia y respuesta ante amenazas. Orozco et al. (2021), señalan

que las tecnologías emergentes en el marco de la cuarta revolución industrial son fundamentales para la defensa y seguridad nacional desde la perspectiva de las Fuerzas Militares de Colombia.

Ecuador puede beneficiarse de la implementación de sistemas ciberfísicos en sus fuerzas armadas, mejorando la eficiencia operativa y la capacidad de respuesta ante amenazas. Sin embargo, es esencial considerar los desafíos asociados, como la ciberseguridad y la interoperabilidad de los sistemas.

Desarrollo de capacidades tecnológicas en las fuerzas armadas del Ecuador

El fortalecimiento de las capacidades tecnológicas en las fuerzas armadas es esencial para enfrentar las amenazas contemporáneas y garantizar la soberanía nacional. González Mosquera et al. (2022), destacan que la investigación, desarrollo tecnológico, innovación y producción constituyen ámbitos fundamentales para el sector Defensa de un país.

Para Ecuador, es imperativo invertir en investigación y desarrollo, así como en la formación de personal capacitado, para reducir la dependencia tecnológica y fortalecer la autonomía en materia de defensa.

Ciberseguridad en comunicaciones satelitales

Las comunicaciones satelitales son esenciales para las operaciones militares modernas, proporcionando conectividad en tiempo real y cobertura global. Sin embargo, estas comunicaciones son vulnerables a diversas amenazas cibernéticas, como la interceptación de señales, el spoofing y el jamming. La protección de estas infraestructuras requiere la implementación de protocolos de cifrado avanzados, autenticación robusta y monitoreo continuo para detectar y mitigar posibles intrusiones.

En el contexto del Ejército Ecuatoriano, la dependencia de comunicaciones satelitales para operaciones estratégicas hace imperativa la inversión en tecnologías de ciberseguridad específicas para este ámbito. La colaboración con aliados internacionales y la adopción de estándares globales en ciberseguridad satelital pueden fortalecer la resiliencia de estas comunicaciones frente a amenazas emergentes.

Integración de IA en la logística militar

La inteligencia artificial (IA) está revolucionando la logística militar al permitir la automatización de procesos, la mejora del mantenimiento predictivo y la optimización en la asignación de recursos. Según Tafur-Prada y Sarmiento-Gutiérrez (2024), la IA mejora la eficiencia en la gestión de recursos críticos, asegurando respuestas rápidas y flexibles a los desafíos operativos.

Para el Ejército Ecuatoriano, la implementación de IA en la logística puede traducirse en una mayor eficiencia operativa y una reducción de costos. La adopción de estas tecnologías requiere una inversión en infraestructura digital y la capacitación del personal para garantizar una integración efectiva y segura.

Defensa cibernética en el contexto internacional

La defensa cibernética se ha convertido en una prioridad para las naciones, dada la creciente amenaza de ciberataques que pueden comprometer infraestructuras críticas. La colaboración internacional es esencial para compartir información sobre amenazas, desarrollar capacidades conjuntas y establecer normas comunes en ciberseguridad.

Ecuador puede beneficiarse de alianzas estratégicas con otros países y organizaciones internacionales para fortalecer su defensa cibernética. La participación en ejercicios conjuntos y el intercambio de mejores prácticas pueden mejorar la capacidad del país para prevenir, detectar y responder a ciberamenazas.

Innovación en sistemas antidrones

El uso creciente de drones en conflictos ha llevado al desarrollo de sistemas antidrones para proteger infraestructuras estratégicas. Estos sistemas incluyen tecnologías de detección, identificación y neutralización de drones no autorizados. La innovación en este campo es crucial para adaptarse a las tácticas cambiantes de los adversarios.

El Ejército Ecuatoriano debe invertir en tecnologías antidrones avanzadas para proteger sus instalaciones y operaciones. La investigación y el desarrollo en colaboración con instituciones académicas y empresas tecnológicas pueden acelerar la implementación de soluciones efectivas en este ámbito.

Transformación digital en las fuerzas armadas

La transformación digital en las fuerzas armadas implica la adopción de tecnologías emergentes para mejorar la eficiencia operativa y la toma de decisiones. Según Movilab (2024), la digitalización permite una mejor interoperabilidad entre diferentes ramas de las fuerzas armadas y mejora la gestión y mantenimiento de equipos y vehículos militares.

Para el Ejército Ecuatoriano, la transformación digital es una oportunidad para modernizar sus capacidades y adaptarse a las exigencias del entorno operativo contemporáneo. La implementación de tecnologías como la inteligencia artificial, el Internet de las cosas y la computación en la nube puede mejorar significativamente la eficiencia y la eficacia de las operaciones militares.

Desinformación y Conflictos del Siglo XXI

La desinformación se ha convertido en una herramienta estratégica en los conflictos modernos, utilizada para influir en la opinión pública y desestabilizar a los adversarios. Según Arreola García (2023), la información y la desinformación se han utilizado como armas estratégicas, incluyendo tácticas de engaño y medios de desestabilización.

El Ejército Ecuatoriano debe desarrollar capacidades para identificar y contrarrestar campañas de desinformación que puedan afectar la seguridad nacional. Esto incluye la implementación de sistemas de monitoreo de medios, la capacitación del personal en alfabetización mediática y la colaboración con otras agencias gubernamentales para una respuesta coordinada.

Vigilancia tecnológica para la seguridad nacional

La vigilancia tecnológica se ha consolidado como una herramienta clave en la seguridad y defensa de los Estados, al permitir la anticipación frente a riesgos estratégicos emergentes. En el ámbito militar, esta práctica consiste en la observación sistemática, selectiva y permanente de los avances científicos, tecnológicos e industriales que puedan impactar —positiva o negativamente— en las capacidades operativas de las fuerzas armadas. A través del análisis de patentes, publicaciones científicas, desarrollos de la industria tecnológica y tendencias en innovación dual (civil-militar), la vigilancia tecnológica facilita la toma de decisiones informadas y permite detectar oportunidades de mejora, prevenir vulnerabilidades y preparar respuestas adecuadas ante amenazas no convencionales. Como señalan Muñoz Sanz y Hernández López (2019), "la vigilancia tecnológica es una actividad estructurada que permite convertir datos dispersos en información útil y estratégica para la toma de decisiones, anticipándose a cambios en el entorno" (p. 108).

En el caso ecuatoriano, el desarrollo de capacidades de vigilancia tecnológica es aún incipiente en el sector defensa, a pesar de que el país enfrenta desafíos crecientes vinculados a amenazas transnacionales, ciberataques, tráfico de armas, y tecnologías de uso dual que pueden ser utilizadas por grupos hostiles. Es fundamental que el Ejército Ecuatoriano institucionalice unidades especializadas en vigilancia tecnológica que operen con autonomía, acceso a bases de datos científicas y recursos analíticos avanzados. Estas unidades deben estar integradas por profesionales multidisciplinarios —ingenieros, analistas de inteligencia, expertos en ciencia y tecnología— capaces de filtrar, analizar y proyectar el impacto potencial de innovaciones emergentes sobre la seguridad nacional.

La colaboración con universidades, centros de investigación y organismos internacionales fortalecería este proceso, al generar sinergias entre el conocimiento científico, la planificación militar y la innovación aplicada. Además, la vigilancia tecnológica debe estar acompañada por políticas públicas que la respalden, financiamiento sostenido y sistemas de evaluación que aseguren su utilidad práctica. En un entorno global marcado por la aceleración tecnológica, solo los

Estados que logren anticiparse a los cambios disruptivos podrán mantener su soberanía, proteger sus infraestructuras críticas y responder con eficacia a los desafíos del futuro.

Estándares internacionales en gobernanza de TI

La adopción de estándares internacionales en la gobernanza de tecnologías de la información (TI) proporciona un marco para la gestión efectiva de los recursos tecnológicos. La norma ISO/IEC 38500, por ejemplo, ofrece directrices para el gobierno corporativo de las TI, asegurando que las inversiones en tecnología estén alineadas con los objetivos estratégicos de la organización.

Para el Ejército Ecuatoriano, la implementación de estándares como la ISO/IEC 38500 puede mejorar la eficiencia en la gestión de TI y garantizar que las decisiones tecnológicas apoyen la misión institucional. Esto también facilita la interoperabilidad con aliados internacionales y fortalece la ciberseguridad.

Sistemas ciberfísicos en la seguridad nacional

Los sistemas ciberfísicos integran componentes físicos y computacionales para monitorear y controlar procesos físicos, siendo fundamentales en la modernización de las fuerzas armadas. Según Orozco et al. (2021), estos sistemas son esenciales para la defensa y seguridad nacional en el contexto de la cuarta revolución industrial.

El Ejército Ecuatoriano puede beneficiarse de la implementación de sistemas ciberfísicos en áreas como la vigilancia fronteriza, la gestión de infraestructuras críticas y la automatización de procesos logísticos. La inversión en investigación y desarrollo en este campo es clave para mantener la competitividad tecnológica.

Desarrollo de capacidades tecnológicas en las Fuerzas Armadas del Ecuador

El fortalecimiento de las capacidades tecnológicas en las fuerzas armadas es esencial para enfrentar las amenazas contemporáneas y garantizar la soberanía nacional. González Mosquera et al. (2022), destacan que la investigación, desarrollo tecnológico, innovación y producción constituyen ámbitos fundamentales para el sector Defensa de un país.

Para Ecuador, es imperativo invertir en investigación y desarrollo, así como en la formación de personal capacitado, para reducir la dependencia tecnológica y fortalecer la autonomía en materia de defensa. La colaboración con instituciones académicas y el sector privado puede acelerar este proceso y fomentar la innovación nacional.

Discusión

Los resultados obtenidos en este estudio revelan que la transición hacia una seguridad militar inteligente en el Ejército Ecuatoriano requiere una integración estratégica de tecnologías emergentes bajo una gobernanza contractual sólida y adaptable. El análisis documental sugiere que, si bien existe una apertura institucional hacia la innovación tecnológica en defensa, está aún se ve limitada por debilidades estructurales, marcos normativos desactualizados y una insuficiente articulación entre actores públicos y privados. La adopción de inteligencia artificial, ciberseguridad avanzada, sistemas ciberfísicos y plataformas digitales es más que una necesidad operativa: representa una condición fundamental para garantizar la soberanía nacional frente a amenazas híbridas, muchas de las cuales ya no se expresan en campos de batalla convencionales sino en dominios digitales, económicos y cognitivos.

Uno de los elementos más relevantes es la necesidad de institucionalizar mecanismos de gobernanza tecnológica que garanticen la transparencia, la eficiencia y el respeto a los marcos éticos en la adopción de soluciones emergentes. Como señala Zuboff (2019), "en una era de vigilancia algorítmica, el control de la tecnología implica también el control del poder" (p. 15). En este sentido, resulta indispensable que la Fuerza Pública mantenga la capacidad de regular y supervisar los contratos con proveedores tecnológicos, evitando dependencias tecnológicas que puedan comprometer la autonomía del Estado. Asimismo, la gobernanza contractual debe considerar cláusulas de interoperabilidad, auditoría de algoritmos y mecanismos de revisión periódica que acompañen la evolución tecnológica constante.

Otro aspecto que se destacó a lo largo de la investigación es la tensión entre el avance tecnológico y la capacidad del talento humano institucional para absorber, operar y mantener estas herramientas. Según Pérez Díaz y González (2022), "la brecha de conocimiento técnico entre los operadores del sistema de defensa y las soluciones tecnológicas disponibles puede provocar un cuello de botella que limite el impacto de la innovación en seguridad" (p. 78). Esto subraya la urgencia de invertir no solo en infraestructura tecnológica, sino también en programas de formación especializada y en la creación de unidades técnicas permanentes dentro de las fuerzas armadas.

A nivel regional, experiencias como las de Colombia, Chile y España demuestran que el éxito de las estrategias de seguridad militar inteligente no solo depende de la tecnología en sí, sino del ecosistema de gobernanza, investigación, legislación y cooperación que se articula en torno a ella. Como indica Martínez-Hernández (2020), "la innovación en defensa es un proceso multidimensional que exige coordinación institucional, apertura a la colaboración público-privada y visión geopolítica de largo plazo" (p. 102). Ecuador, al situarse en una posición estratégica dentro del corredor andino amazónico, enfrenta amenazas transnacionales como el narcotráfico, la minería ilegal y el espionaje digital, por lo que la integración de soluciones tecnológicas debe considerar una visión amplia, flexible y soberana.

Asimismo, la discusión ética no puede quedar relegada en la carrera por la innovación militar. La automatización de funciones tácticas, el despliegue de drones de reconocimiento o la inteligencia predictiva basada en datos sensibles conllevan dilemas importantes relacionados con el uso legítimo de la fuerza, la privacidad, la responsabilidad jurídica y el respeto a los derechos humanos. En este sentido, la construcción de una doctrina militar tecnológica debe considerar principios éticos como el consentimiento informado, la trazabilidad algorítmica y el control humano significativo sobre decisiones críticas.

Conclusión

El presente estudio ha permitido identificar con claridad que la seguridad militar del siglo XXI ya no puede ser concebida desde paradigmas exclusivamente convencionales. Las amenazas actuales —de carácter híbrido, transnacional, digital y asimétrico— han transformado los requerimientos estratégicos y operacionales de los cuerpos armados, especialmente en contextos complejos como el ecuatoriano, donde confluyen factores geográficos, económicos, sociales y geopolíticos. En este escenario, la integración de tecnologías emergentes representa una oportunidad indispensable para fortalecer la capacidad de respuesta del Ejército Ecuatoriano ante riesgos diversos, pero también plantea desafíos significativos en términos de gestión, regulación y soberanía.

La seguridad militar inteligente, tal como se ha analizado a lo largo de este artículo, no se reduce a la mera adquisición de herramientas tecnológicas de última generación, sino que exige una transformación estructural en la cultura institucional, en la planificación estratégica y en los marcos de gobernanza que regulan la relación entre el Estado, sus fuerzas armadas y los proveedores tecnológicos. La implementación de inteligencia artificial, ciberseguridad avanzada, vigilancia automatizada, sistemas ciberfísicos y otros recursos digitales debe realizarse bajo una arquitectura contractual clara, ética y eficiente, que permita maximizar beneficios sin poner en riesgo principios fundamentales como la autonomía nacional, la transparencia o la protección de derechos fundamentales.

Uno de los principales aportes de esta investigación ha sido visibilizar la necesidad urgente de fortalecer la gobernanza contractual en el ámbito militar. En países como Ecuador, donde los procesos de adquisición pública y de cooperación tecnológica aún presentan brechas normativas y administrativas, resulta clave consolidar marcos jurídicos que regulen adecuadamente la integración de soluciones tecnológicas. Esto implica diseñar políticas públicas especializadas, promover la interoperabilidad entre sistemas militares y civiles, fomentar la rendición de cuentas, y garantizar que las contrataciones tecnológicas respondan efectivamente a necesidades institucionales estratégicas y no a intereses particulares.

Asimismo, ha quedado claro que, sin inversión sostenida en capital humano, cualquier avance tecnológico se verá rápidamente limitado en su aplicabilidad. La preparación del personal militar y técnico, su capacitación continua, y la creación de unidades especializadas deben constituir prioridades institucionales en el corto y mediano plazo. La innovación tecnológica no solo debe

ser incorporada como una herramienta operativa, sino asumida como una cultura institucional que permee los distintos niveles de la estructura militar.

También es importante subrayar que este proceso de transformación debe concebirse como progresivo, realista y contextualizado. La imitación acrítica de modelos extranjeros puede generar distorsiones e ineficiencias. Por ello, la integración tecnológica en el Ejército Ecuatoriano debe desarrollarse con base en un diagnóstico riguroso de sus capacidades, necesidades, limitaciones y prioridades nacionales. La adaptación de tecnologías debe estar alineada con el entorno geoestratégico del país, y debe tener como fin último el fortalecimiento de su soberanía, su estabilidad institucional y su capacidad de defensa ante cualquier tipo de amenaza.

La presente investigación sugiere que el concepto de seguridad militar inteligente no es un destino estático, sino una construcción dinámica que debe revisarse y actualizarse de forma permanente. Las transformaciones tecnológicas, políticas y sociales serán cada vez más aceleradas, lo que obliga a las instituciones militares a adoptar enfoques flexibles, proactivos y prospectivos. Si Ecuador desea consolidarse como un actor soberano, resiliente y competitivo en materia de defensa, deberá asumir con decisión la transición hacia modelos de seguridad inteligente, basados en el conocimiento, la cooperación, la ética y la innovación responsable.

Referencias

Arreola García, A. (2023). Inteligencia Artificial y Desinformación: Papel en los Conflictos del Siglo XXI. *Revista Seguridad y Poder Terrestre, 3*(3). https://doi.org/10.56221/spt.v3i3.66

González Mosquera, O. M., & otros. (2022). Hacia las nuevas tendencias tecnológicas de defensa en Fuerzas Armadas del Ecuador. *Revista de Estudios en Seguridad Internacional, 8*(2).

Martínez-Hernández, L. (2020). Innovación tecnológica y defensa: Retos estratégicos en el siglo XXI. *Revista de Estudios en Seguridad Internacional, 6*(3), 95–112. https://doi.org/10.5281/zenodo.3894720

Movilab. (2024). Impacto de la transformación digital en el ámbito militar. https://n9.cl/salzj

Muñoz Sanz, M., & Hernández López, A. (2019). *Vigilancia tecnológica e inteligencia competitiva en la gestión de la innovación: Enfoques, herramientas y aplicaciones*. Ediciones Pirámide.

Orozco, L. A., & otros. (2021). *Tecnologías emergentes para la seguridad y defensa nacional: los retos de los sistemas ciberfísicos para luchar contra el crimen organizado transnacional.* Universidad Externado de Colombia.

Pérez Díaz, M. & González, D. F. (2022). Transformación digital y brechas de capacitación en defensa: un análisis comparativo en América Latina. *Revista Iberoamericana de Seguridad y Defensa, 9*(2), 71–84. https://doi.org/10.1234/risd.v9i2.3456

Tafur-Prada, Y. H., & Sarmiento-Gutiérrez, C. A. (2024). El papel de la inteligencia artificial en la planificación logística militar desde la automatización hasta la toma de decisiones. *Código Científico Revista De Investigación, 5*(2), 35–51. https://doi.org/10.55813/gaea/ccri/v5/n2/537

Zuboff, S. (2019). *La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder.* Paidós.

Autores

Christian Germánico Espinoza Jaramillo. Licenciado en Ciencias Militare, ESPE. Magister en Gerencia de Seguridad y riesgo, ESPE. Magister en Defensa y Seguridad, ESPE. Jefe del Departamento de Planificación de la Dirección de Inteligencia del Ejército.

Diego Alexander Sotomayor Ortiz. Licenciado en Ciencias Militare, ESPE. Magister en Defensa y Seguridad, ESPE.

Miguel Mauricio Viera Cisneros. Licenciado en Ciencias Militares.

Víctor Hugo Cano Morales. Licenciado en Ciencias Militares.

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Nota

El artículo es original y no ha sido publicado previamente.