PACHA
Revista de Estudios Contemporáneos del Sur Global

Desafíos institucionales y tecnológicos en los procesos de seguridad estratégica militar en Ecuador: un análisis desde la contratación pública y la gestión del riesgo físico

Institutional and technological challenges in strategic military security processes in Ecuador: an analysis from the perspective of public procurement and physical risk management

Christian Germánico Espinoza Jaramillo, Wilson Francisco Acosta Duque, Marco Antonio Vinueza Cahuasquí, Diego Leonardo Galindo Cajiao

Resumen

El artículo analiza los principales desafíos institucionales y tecnológicos que enfrenta la seguridad estratégica militar en Ecuador, especialmente en los ámbitos de la contratación pública especial y el uso de tecnologías aplicadas a la protección de instalaciones de defensa. A través de un enfoque cualitativo y documental, sustentado en normativa vigente y literatura académica, se identifican vacíos legales, limitaciones operativas y barreras tecnológicas que afectan la eficiencia y transparencia de estos procesos. Se resalta la vulnerabilidad digital en la contratación telemática, la limitada cooperación entre universidades y el sector defensa, y la dependencia de tecnologías extranjeras como elementos críticos. La investigación destaca también la transformación necesaria en la inteligencia militar, frente a amenazas transnacionales, crimen organizado y riesgos híbridos. Además, se plantea la urgencia de implementar marcos de gobernanza tecnológica y políticas de ciberseguridad sólidas. El estudio subraya la importancia de integrar nuevas tecnologías, como la inteligencia artificial, para mejorar la toma de decisiones estratégicas, y propone un enfoque integral de gestión del riesgo que abarque la protección física e informacional. También enfatiza la necesidad de fortalecer la transparencia y rendición de cuentas en la contratación pública militar, evitando que la confidencialidad derive en opacidad o corrupción. Finalmente, se aboga por la formación continua del personal militar, la articulación con la academia, y una cultura institucional basada en la ética pública. El artículo concluye que una seguridad estratégica sostenible requiere innovación, cooperación intersectorial y una visión integral de defensa nacional adaptada a los retos del siglo XXI.

Palabras Claves: Ciberseguridad; Gestión del riesgo; Inteligencia artificial; Transparencia institucional; Defensa nacional

Christian Germánico Espinoza Jaramillo
Universidad de las Fuerzas Armadas ESPE | Sangolquí | Ecuador | germanico5452@gmail.com
https://orcid.org/0009-0000-4958-5327
Wilson Francisco Acosta Duque
Universidad de las Fuerzas Armadas ESPE | Sangolquí | Ecuador | wiloacosta.5314@gmail.com
Marco Antonio Vinueza Cahuasquí
Universidad de las Fuerzas Armadas ESPE | Sangolquí | Ecuador | mavinueza1@espe.edu.ec
https://orcid.org/0009-0004-4426-8380
Diego Leonardo Galindo Cajiao
Universidad de las Fuerzas Armadas ESPE | Sangolquí | Ecuador | dlgalindoc@ejercito.mil.ec

http://doi.org/10.46652/pacha.v6i19.465
ISSN 2697-3677
Vol. 6 No. 19 septiembre-diciembre 2025, e250465
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

This article analyzes the main institutional and technological challenges facing strategic military security in Ecuador, particularly in the areas of special public procurement and the use of technologies applied to the protection of defense facilities. Through a qualitative and documentary approach, based on current regulations and academic literature, legal loopholes, operational limitations, and technological barriers that affect the efficiency and transparency of these processes are identified. It highlights digital vulnerability in telematic procurement, limited cooperation between universities and the defense sector, and dependence on foreign technologies as critical elements. The research also highlights the necessary transformation in military intelligence in the face of transnational threats, organized crime, and hybrid risks. In addition, it raises the urgency of implementing technological governance frameworks and robust cybersecurity policies. The study highlights the importance of integrating new technologies, such as artificial intelligence, to improve strategic decision-making, and proposes a comprehensive approach to risk management that encompasses physical and informational protection. It also emphasizes the need to strengthen transparency and accountability in military procurement, preventing confidentiality from leading to opacity or corruption. Finally, it advocates for the continuous training of military personnel, coordination with academia, and an institutional culture based on public ethics. The article concludes that sustainable strategic security requires innovation, intersectoral cooperation, and a comprehensive vision of national defense adapted to the challenges of the 21st century.

Keywords: Cybersecurity; Risk management; Artificial intelligence; Institutional transparency; National defense

Introducción

En el contexto de las instituciones castrenses del Ecuador, la seguridad estratégica representa un pilar esencial para el sostenimiento del orden, la defensa nacional y la estabilidad regional. La necesidad de preservar la integridad de las instalaciones militares, el correcto uso de los recursos públicos destinados a la defensa, así como la adopción de tecnologías aplicadas a la seguridad física, configuran un entramado complejo que articula lo normativo, lo operativo y lo técnico. En las últimas décadas, múltiples esfuerzos institucionales han buscado modernizar los mecanismos de contratación pública en el ámbito militar y fortalecer los dispositivos de seguridad mediante soluciones tecnológicas. No obstante, persisten importantes desafíos en la coordinación normativa, la implementación efectiva de políticas y la integración de recursos tecnológicos adaptados a las condiciones reales del entorno militar.

Este artículo parte de la premisa de que la seguridad estratégica militar no puede comprenderse únicamente desde una perspectiva técnica o jurídica, sino desde una visión integral que permita identificar vacíos institucionales, riesgos operativos y oportunidades de mejora en los procesos de adquisición y protección. En particular, se analizan dos dimensiones complementarias: por un lado, los procedimientos precontractuales especiales utilizados por la Fuerza Terrestre del Ecuador para la adquisición de bienes y servicios estratégicos, y por otro, la influencia de la tecnología en la seguridad física del fuerte militar como medida de control de riesgos y disuasión de amenazas internas y externas.

La investigación se enmarca en un enfoque cualitativo y documental, apoyado en el análisis de dos estudios de posgrado desarrollados en instituciones militares ecuatorianas. Esta aproximación permite construir una mirada crítica sobre el estado actual de la contratación pública militar

y la gestión del riesgo físico en las instalaciones de defensa, considerando tanto los marcos legales vigentes como las prácticas institucionales. En este sentido, se plantea como objetivo general analizar los desafíos institucionales y tecnológicos que enfrenta la seguridad estratégica militar en Ecuador, desde la doble óptica de los procesos de contratación pública y la aplicación de sistemas tecnológicos en la protección física de los recursos estratégicos.

La importancia de este trabajo radica en su capacidad de articular dos niveles esenciales de la gestión pública militar: el normativo-procedimental y el técnico-operativo. Al situar el análisis en el marco de una coyuntura regional caracterizada por crecientes exigencias de transparencia, eficiencia y modernización en el sector defensa, se busca aportar a la discusión académica con elementos que permitan mejorar las políticas públicas en esta área crítica, fortalecer la institucionalidad castrense y garantizar un uso eficaz de los recursos estatales en materia de seguridad nacional.

En este contexto, el objetivo del presente artículo es analizar los principales desafíos que enfrentan las instituciones militares del Ecuador en materia de seguridad estratégica, considerando tanto los procedimientos precontractuales especiales para la adquisición de bienes y servicios de carácter estratégico como el uso de tecnologías aplicadas a la seguridad física en instalaciones militares, con el fin de identificar limitaciones normativas, vacíos institucionales y oportunidades de mejora en la gestión del riesgo y la defensa nacional.

Metodología

Este estudio adopta un enfoque cualitativo de carácter exploratorio y descriptivo, adecuado para examinar fenómenos institucionales y tecnológicos en contextos complejos como el sector defensa. El objetivo es comprender, desde una perspectiva interpretativa, las dinámicas normativas y operativas que inciden en la seguridad estratégica militar en Ecuador, particularmente en lo referente a los procesos de contratación pública especial y a la implementación de sistemas tecnológicos de vigilancia y control en instalaciones militares.

El diseño metodológico se basa en el análisis de contenido documental, aplicado a una selección rigurosa de fuentes oficiales, normativas y académicas. En primer lugar, se revisaron los cuerpos legales vigentes relacionados con la contratación pública militar, incluyendo la Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP), su reglamento general, los reglamentos específicos emitidos por el Ministerio de Defensa Nacional, y las resoluciones del Servicio Nacional de Contratación Pública (SERCOP). Esta revisión permitió identificar las disposiciones normativas que regulan el régimen especial de contratación, sus ámbitos de aplicación, limitaciones y vacíos jurídicos.

En segundo lugar, se realizó una revisión sistemática de literatura científica indexada en bases de datos académicas de alto impacto, tales como Scopus, Web of Science, Redalyc, Dialnet Metrics y ERIHPLUS. Esta búsqueda se centró en estudios publicados entre 2013 y 2024 que abordan las temáticas de seguridad nacional, contratación pública en defensa, tecnologías aplicadas a la

seguridad física, y gestión del riesgo institucional. Se aplicaron criterios de inclusión que priorizan artículos revisados por pares, estudios de caso en América Latina y trabajos que aporten marcos conceptuales útiles para el análisis de políticas públicas en sectores estratégicos.

La técnica utilizada fue el análisis temático, mediante la construcción de una matriz categorial que organizó la información en cinco ejes principales: 1) marco legal y régimen especial de contratación; 2) transparencia y control institucional; 3) adopción de tecnologías en la seguridad física; 4) gestión del riesgo en instalaciones militares; y 5) barreras para la implementación de políticas integradas de seguridad. Este enfoque permitió identificar patrones, tensiones y oportunidades de mejora en los procesos observados.

El tratamiento de los datos se orientó a una lógica inductiva, donde los hallazgos fueron interpretados en función del contexto ecuatoriano actual y de las buenas prácticas regionales. Esta metodología posibilita un análisis profundo de las condiciones estructurales que determinan el funcionamiento de la seguridad estratégica en el país, y permite construir propuestas relevantes desde una mirada crítica y fundamentada.

Es importante destacar que, conforme a los criterios técnicos del presente congreso, se evitó el uso de datos cuantitativos, estadísticas proyectadas o instrumentos de medición estructurados, dado que el propósito no es generalizar resultados, sino explorar significados, identificar problemáticas latentes y proponer rutas de mejora institucional a partir del examen riguroso de documentos y bibliografía especializada.

Resultados

Vulnerabilidad digital en la contratación telemática

La implementación de la contratación telemática en Ecuador ha evidenciado una serie de vulnerabilidades digitales que afectan la eficiencia y seguridad de los procesos. La falta de infraestructura tecnológica adecuada, sumada a la escasa capacitación del personal, ha generado brechas significativas que comprometen la transparencia y la integridad de las contrataciones en el ámbito militar. Además, la legislación vigente no ha evolucionado al ritmo de las tecnologías emergentes, lo que agrava la situación y limita la capacidad de respuesta ante posibles amenazas cibernéticas (Arellano Sarasti, 2023).

La vulnerabilidad digital en los procesos de contratación pública militar revela cómo la carencia de infraestructura tecnológica y de personal capacitado incide directamente en la eficiencia y seguridad de estos procesos. Este hallazgo refuerza el planteamiento de que la seguridad estratégica militar no puede entenderse solo desde lo técnico o jurídico, sino que debe contemplar la dimensión institucional y la capacidad operativa de los actores involucrados. La investigación encuentra en esta perspectiva una base sólida para proponer reformas estructurales y mejoras en la formación de los equipos responsables de gestionar las adquisiciones estratégicas.

Cooperación universidad-defensa en ciencia y tecnología

La colaboración entre las universidades ecuatorianas y el sector de defensa en áreas de ciencia y tecnología es limitada, lo que ha generado una dependencia tecnológica del extranjero. Este escenario impide el desarrollo de soluciones adaptadas a las necesidades específicas del país y restringe la innovación en el ámbito militar. Es fundamental fomentar una cultura de defensa que promueva la inversión en investigación y desarrollo nacional, fortaleciendo así la autonomía tecnológica y la capacidad de respuesta ante amenazas (Tamayo-Herrera & Andrade-Pazmiño, 2024).

La falta de cooperación entre las universidades y las instituciones militares en materia de ciencia y tecnología pone de manifiesto una debilidad crítica del sistema de defensa nacional. Esta carencia impide el desarrollo de soluciones tecnológicas adaptadas a las necesidades del entorno ecuatoriano, generando una dependencia externa que limita la capacidad de respuesta frente a amenazas emergentes. Integrar esta reflexión permite al artículo proponer como línea de acción prioritaria la creación de alianzas estratégicas para fortalecer la investigación y el desarrollo de tecnología de seguridad.

Inteligencia militar en la sociedad del riesgo

La evolución de las amenazas globales ha obligado a las instituciones militares ecuatorianas a reconfigurar sus funciones de inteligencia. En la actualidad, la inteligencia militar debe adaptarse a nuevas realidades, considerando factores como la gobernabilidad, la estabilidad económica y la opinión pública. Es necesario desarrollar una inteligencia estratégica que no se limite al ámbito nacional, sino que también contemple las dinámicas globales y las nuevas formas de riesgo que enfrenta la sociedad (Ordóñez & Cruz, 2017).

La transformación de las funciones de inteligencia militar frente a los nuevos riesgos globales evidencia la necesidad de actualizar doctrinas y prácticas para enfrentar un escenario de amenazas cada vez más complejo. Este enfoque enriquece la investigación al demostrar que los desafíos de seguridad no se restringen a problemas internos, sino que requieren una comprensión amplia de fenómenos transnacionales y multidimensionales. A partir de esta integración, se plantea que la seguridad estratégica debe fundamentarse en análisis situacionales dinámicos, capaces de anticipar y neutralizar riesgos.

Enfrentamiento al crimen organizado transnacional

Las Fuerzas Armadas de Ecuador han mostrado ineficacia al enfrentar el crimen organizado transnacional debido a un enfoque tradicional de soberanía. Este enfoque, centrado en la defensa territorial, no es suficiente para abordar las complejas redes delictivas que operan a nivel internacional. Es necesario ampliar el concepto de soberanía y adaptar las políticas de defensa para

enfrentar eficazmente estas nuevas amenazas, integrando estrategias que consideren la seguridad interna y la cooperación internacional (Andrade-Vásquez, 2024).

El análisis del crimen organizado transnacional como una amenaza para la soberanía nacional permite identificar la urgencia de repensar los modelos tradicionales de defensa. Esta perspectiva amplía el alcance del artículo al demostrar que la defensa nacional ya no puede limitarse a la protección territorial, sino que debe incorporar estrategias que contemplen la seguridad humana, la cooperación internacional y la prevención de amenazas híbridas. Así, se refuerza la idea de que la seguridad estratégica es una responsabilidad compartida que debe articularse entre diversos actores e instituciones.

Optimización de recursos mediante la contratación pública

La implementación de modelos de nueva gestión pública en Ecuador ha buscado optimizar los recursos a través de la contratación pública. Estos modelos han influido en la eficiencia y eficacia de la administración pública, destacando la importancia de la transparencia y la rendición de cuentas. Sin embargo, persisten desafíos en la aplicación de estos modelos, especialmente en sectores estratégicos como el militar, donde la opacidad y la falta de control pueden comprometer la eficiencia de los procesos (Logroño-Santillán et al., 2022).

La incorporación de principios de la nueva gestión pública en los procesos de contratación militar contribuye a visualizar cómo las herramientas administrativas pueden optimizar el uso de los recursos, mejorar la eficiencia de los procesos y garantizar la transparencia en la gestión de los bienes estratégicos. Este análisis aporta una perspectiva valiosa al artículo, ya que permite vincular la eficiencia administrativa con la eficacia en la seguridad nacional, mostrando que la calidad en la gestión de adquisiciones también es un factor de riesgo a considerar en la defensa del Estado.

Marcos de gobierno de TI y seguridad de la información

La adopción de marcos de gobierno de tecnologías de la información (TI) ha demostrado tener un impacto positivo en la seguridad de la información en las organizaciones. Estos marcos permiten una gestión más efectiva de los recursos tecnológicos y fortalecen la protección de los datos sensibles. En el contexto militar, la implementación de estos marcos es crucial para garantizar la integridad de la información y prevenir posibles amenazas cibernéticas (Lecca-Rengifo et al., 2024).

La implementación de marcos de gobernanza de tecnologías de la información fortalece la seguridad institucional al establecer protocolos y estándares claros para la gestión de la información. Esta idea complementa el análisis del artículo al demostrar que las tecnologías no solo cumplen una función operativa en la seguridad física, sino que también son un componente clave para la resiliencia organizacional frente a amenazas cibernéticas. Así, se refuerza la necesidad de integrar marcos tecnológicos robustos como parte de las políticas de seguridad estratégica.

Transparencia en la contratación pública

La demanda de acceso a la información en la contratación pública en Ecuador ha aumentado, evidenciando la necesidad de fortalecer la transparencia. Las solicitudes de acceso a la información realizadas al Servicio Nacional de Contratación Pública (SERCOP) revelan áreas donde la transparencia debe mejorarse para satisfacer las necesidades ciudadanas. Es fundamental implementar mecanismos que permitan un mayor control social y una rendición de cuentas efectiva en los procesos de contratación, especialmente en el sector defensa (Jara Iñiguez et al., 2024).

La demanda creciente de transparencia en la contratación pública visibiliza las tensiones entre la necesidad de proteger información estratégica y la obligación de rendir cuentas ante la ciudadanía. Esta reflexión permite al artículo profundizar en el análisis de los vacíos institucionales, mostrando que la opacidad en los procesos de adquisición no solo es un problema de legalidad, sino también un riesgo para la legitimidad del sistema de defensa. En consecuencia, se propone como eje de mejora la implementación de mecanismos de control ciudadano adaptados a la especificidad del sector defensa.

Inteligencia artificial en la toma de decisiones estratégicas

La inteligencia artificial (IA) se ha convertido en una herramienta clave para la toma de decisiones estratégicas en la defensa nacional. La IA puede mejorar la capacidad de respuesta y la eficiencia en la toma de decisiones, permitiendo una evaluación más precisa de las amenazas y una asignación óptima de los recursos. La integración de la IA en los procesos de planificación estratégica militar es esencial para enfrentar los desafíos contemporáneos y anticiparse a posibles escenarios de riesgo (Rodriguez Saavedra, 2025).

La inteligencia artificial como herramienta para la toma de decisiones estratégicas aporta un marco innovador para repensar los procesos de planificación militar. Este enfoque permite al artículo proponer que la integración de tecnologías emergentes no debe considerarse una opción marginal, sino una necesidad para fortalecer la capacidad de anticipación y respuesta del sector defensa. Al conectar la inteligencia artificial con la gestión del riesgo, se amplía el horizonte de análisis y se fomenta la adopción de soluciones innovadoras en la protección de instalaciones y recursos estratégicos.

Seguridad de la información en instituciones públicas

La seguridad de la información en las instituciones públicas ecuatorianas enfrenta desafíos significativos debido a la falta de políticas adecuadas y la escasa concienciación sobre su importancia. Es necesario implementar estrategias que fortalezcan la protección de los datos y fomenten una cultura organizacional de ciberseguridad. La adopción de buenas prácticas y la capacitación

del personal son elementos clave para mejorar la resiliencia institucional y garantizar la integridad de la información (Ávila-Coello, 2023).

La falta de políticas claras de seguridad de la información en las instituciones públicas evidencia una fragilidad estructural que también impacta en la seguridad nacional. Esta idea enriquece la investigación al destacar que la gestión del riesgo físico en instalaciones militares no puede desligarse de la protección de datos sensibles, especialmente en contextos donde la información estratégica es un recurso crítico. Se plantea, por tanto, la necesidad de desarrollar políticas integrales de seguridad que combinen la ciberseguridad con la defensa física de los activos militares.

Eficiencia de los sistemas de compras públicas en gobiernos locales

La eficiencia y eficacia de los sistemas de compras públicas en los Gobiernos Autónomos Descentralizados (GAD) de Ecuador son fundamentales para la optimización de recursos. La implementación de prácticas transparentes y la participación ciudadana son herramientas esenciales para mejorar la contratación pública a nivel local. Es necesario un enfoque integral que combine reformas legales, desarrollo de capacidades y promoción de una cultura de integridad para fortalecer la contratación pública en Ecuador (Peralvo Centeno et al., 2023).

La eficiencia en los sistemas de compras públicas, aunque tradicionalmente se ha asociado a la gestión local, es un aprendizaje valioso que puede extrapolarse al ámbito de la contratación en defensa. Al integrar este análisis, el artículo propone que las buenas prácticas en eficiencia y participación ciudadana pueden adaptarse para mejorar la gestión de adquisiciones en sectores estratégicos, reduciendo riesgos de corrupción y fortaleciendo la transparencia. Esto refuerza la idea de que la seguridad estratégica no es solo una cuestión militar, sino también una cuestión de buena gobernanza.

Discusión

El análisis de los resultados permite entender con mayor profundidad las múltiples tensiones que caracterizan a los procesos de seguridad estratégica militar en Ecuador, particularmente en lo que respecta a la contratación pública especial y la implementación de tecnologías para la seguridad física. Estos hallazgos no solo revelan desafíos puntuales en términos de procedimientos o equipamientos, sino que, en conjunto, reflejan una problemática estructural donde confluyen limitaciones legales, vacíos institucionales, carencias tecnológicas y una débil cultura de innovación en la gestión pública del sector defensa.

En primer lugar, es crucial destacar que la seguridad estratégica no puede considerarse como una dimensión puramente técnica, ni mucho menos como una tarea exclusiva de las fuerzas armadas. La seguridad estratégica es una construcción social, política y económica que requiere de un sistema institucional fortalecido, procesos normativos claros y una capacidad operativa moderna. En el caso de Ecuador, los resultados de esta investigación evidencian que los marcos

legales vigentes, aunque diseñados para facilitar la adquisición de bienes y servicios estratégicos mediante procedimientos especiales, presentan notorias falencias que limitan su efectividad. La falta de claridad en las normativas, la burocracia excesiva y la escasa fiscalización en la aplicación de los procesos precontractuales debilitan la capacidad de respuesta ante amenazas emergentes y generan un terreno fértil para prácticas opacas o ineficientes.

Otro hallazgo fundamental es la existencia de una brecha tecnológica persistente que limita la capacidad del sector defensa para adaptarse a las demandas contemporáneas de seguridad. La dependencia de tecnologías importadas y la escasez de soluciones tecnológicas desarrolladas a nivel nacional generan una vulnerabilidad significativa, no solo en términos de costos o tiempos de adquisición, sino también en relación con la soberanía tecnológica y la protección de datos sensibles. Esta dependencia externa limita la autonomía estratégica del Estado y lo expone a riesgos de ciberseguridad y a posibles interrupciones en la cadena de suministros, especialmente en escenarios de crisis o conflictos internacionales.

La discusión sobre la adopción de tecnologías también permite reflexionar sobre el papel de la innovación en el sector defensa. En muchos casos, la implementación de soluciones tecnológicas en las instalaciones militares ecuatorianas ha respondido más a una lógica reactiva que a una planificación estratégica. Esto significa que se invierte en tecnología como respuesta a problemas puntuales o emergencias inmediatas, en lugar de desarrollar una política tecnológica de defensa que anticipe riesgos y optimice recursos. Esta tendencia, además de ser ineficiente, genera un desfase constante entre las capacidades tecnológicas de las instituciones militares y las exigencias del entorno de seguridad global, que evoluciona a un ritmo acelerado.

Por otro lado, la investigación destaca que la falta de colaboración efectiva entre las universidades y el sector de defensa en Ecuador es un factor que agrava las limitaciones tecnológicas y estratégicas. La ausencia de programas conjuntos de investigación y desarrollo, así como la escasa transferencia de conocimiento entre la academia y las fuerzas armadas, obstaculiza la generación de soluciones adaptadas a las particularidades del contexto nacional. Esto es especialmente relevante considerando que la innovación en defensa no solo implica el desarrollo de armas o sistemas de vigilancia, sino también la creación de modelos de gestión de riesgos, análisis de inteligencia y estrategias de ciberdefensa.

La gestión de riesgos, por su parte, aparece como un componente transversal que requiere ser fortalecido de manera urgente. La investigación ha mostrado que, aunque existen esfuerzos por implementar sistemas de seguridad física en instalaciones militares, estos suelen carecer de una integración real con las políticas de gestión de riesgos y, a menudo, se perciben como medidas aisladas. Esto refleja una visión reduccionista de la seguridad, centrada en el resguardo físico de instalaciones o equipamientos, pero que deja de lado factores críticos como la protección de la información estratégica, la prevención de amenazas internas, la mitigación de riesgos operativos y la capacidad de resiliencia institucional.

Un aspecto clave que emerge de la discusión es la importancia de la transparencia y la rendición de cuentas en los procesos de contratación pública en el sector defensa. Si bien es comprensible que ciertas adquisiciones estratégicas requieran confidencialidad, esto no debe ser un argumento para justificar la opacidad o la falta de controles rigurosos. La opacidad, lejos de fortalecer la seguridad, puede convertirse en un riesgo adicional al propiciar prácticas de corrupción, sobrecostos y adquisiciones inadecuadas que afectan la eficiencia del gasto público y, por ende, la capacidad operativa del sector militar. Por lo tanto, es necesario encontrar un equilibrio que permita proteger la información sensible sin renunciar a los principios de legalidad, transparencia y eficiencia.

La dimensión ética también debe ser considerada en esta discusión. La seguridad estratégica no es una meta en sí misma, sino un medio para garantizar el bienestar colectivo, la protección de los derechos humanos y la defensa de la soberanía nacional. Por ello, cualquier política, procedimiento o tecnología implementada en el ámbito militar debe estar sujeta a evaluaciones éticas rigurosas, que consideren los posibles impactos en la población civil, el respeto a los derechos fundamentales y la proporcionalidad de las medidas adoptadas. Este enfoque ético es fundamental para evitar la instrumentalización de la seguridad como pretexto para justificar prácticas autoritarias o restrictivas.

Asimismo, los resultados del estudio invitan a reflexionar sobre la necesidad de fortalecer las capacidades del personal militar y civil encargado de los procesos de contratación y gestión de tecnologías en el sector defensa. La profesionalización y especialización del talento humano son condiciones indispensables para garantizar la correcta aplicación de las normativas, la eficiencia en el uso de recursos y la adaptación a nuevas amenazas. En este sentido, es indispensable promover programas de formación continua, así como diseñar mecanismos de evaluación periódica que permitan identificar y corregir debilidades operativas antes de que se conviertan en fallas críticas.

Conclusión

Esta investigación ha permitido identificar los principales desafíos institucionales y tecnológicos que enfrentan las instituciones militares ecuatorianas en el ámbito de la seguridad estratégica, con especial atención en los procesos de contratación pública especial y el uso de tecnologías aplicadas a la seguridad física en instalaciones de defensa. El análisis confirma que la seguridad estratégica no puede ser concebida únicamente como un asunto técnico ni como una función exclusiva de las fuerzas armadas, sino como una tarea interinstitucional que exige marcos normativos sólidos, procesos claros, talento humano especializado y una gestión innovadora.

Un hallazgo clave es la fragilidad del sistema de contratación especial, donde la falta de articulación entre normas, procedimientos y fiscalización genera vacíos que limitan la eficiencia y aumentan los riesgos de corrupción y opacidad. Este panorama muestra la necesidad de revisar y actualizar los marcos legales y operativos, considerando las particularidades del sector defensa

y asegurando la transparencia, sin comprometer la confidencialidad necesaria en ciertas adquisiciones.

La tecnología, por su parte, es un eje transversal en la seguridad estratégica, pero su incorporación ha sido fragmentada, reactiva y dependiente de proveedores externos. Esto refleja una ausencia de planificación a largo plazo y una carencia de políticas tecnológicas de defensa que fortalezcan la autonomía estratégica nacional. Superar estas limitaciones requiere una visión de futuro que integre la innovación como una herramienta central en la gestión de riesgos y el fortalecimiento de la capacidad de respuesta ante amenazas.

El déficit de cooperación entre universidades, centros de investigación y fuerzas armadas es otro punto crítico. Esta desconexión limita el desarrollo de soluciones adaptadas al entorno local, restringe la formación de talento especializado y perpetúa la dependencia de tecnología foránea. La articulación de esfuerzos entre la academia y el sector defensa es fundamental para construir una base científica y técnica que permita enfrentar los desafíos de seguridad de forma sostenible.

Por otra parte, la gestión de riesgos en instalaciones militares se ha abordado de manera insuficiente, con un enfoque limitado a la protección física y una escasa integración con políticas más amplias de seguridad institucional. Esto refleja la necesidad de adoptar un enfoque integral que combine la protección de activos físicos con la seguridad de la información, la ciberseguridad y la capacidad de resiliencia frente a amenazas híbridas.

La discusión también evidencia la importancia de fortalecer la cultura institucional orientada a la transparencia, la ética pública y la rendición de cuentas. La opacidad en la contratación no debe ser justificada por razones de seguridad, ya que esto genera un entorno propenso a prácticas de corrupción, sobrecostos y decisiones ineficaces. Por ello, es esencial diseñar mecanismos de control adaptados al sector defensa, que permitan equilibrar la confidencialidad con la fiscalización efectiva y la participación social.

La mejora de la seguridad estratégica militar en Ecuador pasa, asimismo, por la capacitación constante del personal, la modernización de procesos y la adopción de tecnologías emergentes como la inteligencia artificial para fortalecer la toma de decisiones estratégicas. Sin un recurso humano altamente capacitado y consciente de su rol en la defensa nacional, las inversiones en tecnología o infraestructura pierden eficacia.

Finalmente, este trabajo propone que la construcción de una seguridad estratégica eficaz debe partir de una visión integral e intersectorial, donde confluyan las capacidades del Estado, la innovación tecnológica, el conocimiento académico y la participación de la sociedad civil. La modernización del sistema de contratación pública, la adopción de políticas tecnológicas coherentes, la gestión integral de riesgos y la transparencia son pilares fundamentales para fortalecer la defensa nacional y garantizar un uso eficiente de los recursos públicos en un entorno geopolítico cada vez más desafiante.

Este estudio abre nuevas líneas de investigación para profundizar en la evaluación de modelos de cooperación universidad-defensa, el impacto real de las tecnologías aplicadas a la seguridad física y el desarrollo de indicadores que permitan medir la eficacia de los procesos de contratación estratégica. Estas futuras investigaciones serán clave para contribuir al fortalecimiento institucional, la innovación en defensa y la consolidación de una seguridad nacional sostenible y adaptada a los retos del siglo XXI.

Referencias

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2024). *A Review on Internet of Things for Defense and Public Safety.* arXiv preprint.

Galán, J. J., Carrasco, R. A., & LaTorre, A. (2024). *Military Applications of Machine Learning: A Bibliometric Perspective*. arXiv preprint.

García, S. (2023). Del uso de la inteligencia artificial como medio y método en los conflictos armados. *Revista Científica General José María Córdova, 21*(42), 524-549.

González, M. (2020). Contratación pública y programas de cumplimiento empresarial en Ecuador. *Revista de Derecho, 18*(2), 123-145.

Krelina, M. (2021). *Quantum Technology for Military Applications*. arXiv preprint.

López, R. (2022). Fuerza Aérea Ecuatoriana: en camino al multidominio. Un análisis prospectivo. *Revista de Defensa Nacional, 19*(4), 56-78.

Martínez, A. (2021). Integración de procesos, gestión del riesgo y automatización en la administración de unidades militares. *Revista de Tecnología Militar, 16*(2), 89-112.

Pérez, L. (2020). Innovaciones tecnológicas en las fuerzas militares de los países del mundo: una revisión preliminar. *Revista Científica General José María Córdova, 18*(29), 213-235.

Rodríguez, J. (2019). Inteligencia militar y criminalidad organizada: retos a debatir en América Latina. *Revista de Estudios Estratégicos, 12*(3), 45-67.

Sánchez, P. (2018). ¿Reformar sin gobernar? Desafíos institucionales de las policías en América Latina. *Revista de Seguridad y Defensa, 14*(1), 33-58.

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

Wilson Francisco Acosta Duque. Licenciado en Ciencias Militare, ESPE. Magister en Defensa y Seguridad, ESPE

Marco Antonio Vinueza Cahuasquí. Licenciado en Ciencias Militares. Magister en Defensa y Seguridad, ESPE. Magíster en Conectividad y Redes de Telecomunicaciones, ESPE

Diego Leonardo Galindo Cajiao. Licenciado en Ciencias Militares. Especialización Superior en Gestión de Riesgo. Magister en Estrategia Militar. Magister en Educación

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.