PERSPECTIVAS EN INTELIGENCIA

Vol. 18 N. 27
Enero - junio / 2026
Bogotá, D.C., Colombia
ISSN 2145-194X (Impreso)
ISSN 2745-1690 (En línea)

2026

Revista Científica Interdisciplinaria, con un enfoque en **Ciencias Sociales**

Interdiciplinary scientific journal, with focus on Social Sciences.

ESICI
ESCUELA DE INTELIGENCIA Y CONTRAINTELIGENCIA
"BRIGADIER GENERAL RICARDO CHARRY SOLANO"
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Esta página queda intencionalmente en blanco

Revista Científica

PERSPECTIVAS EN INTELIGENCIA 2026

Escuela de Inteligencia y Contrainteligencia
"BG. Ricardo Charry Solano"
Institución Universitaria
https://esici.edu.co

Revista científica interdisciplinaria, con un enfoque en Ciencias Sociales
Interdisciplinary scientific journal, with a focus on Social Sciences.

Vol. 18 Núm. 27
Enero - Junio / 2026
Bogotá D.C., Colombia
ISSN: 2145-194X (impreso)
ISSN: 2745-1690 (en línea)
https://revistaseditorialejc.org/index.php/pei

Esta página queda intencionalmente en blanco

Revista Científica

PERSPECTIVAS EN INTELIGENCIA 2026

(Revista científica en Ciencias Sociales e interdisciplinaria)
ISSN 2145-194X (impreso) - ISSN 2745-1690 (en línea)

Volumen 18, Número 27, Enero-Junio 2026

DIRECTIVOS

Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano"

Teniente Coronel Felipe Eduardo Rodríguez Álvarez
Director

Mayor Julián Enrique Pineda Umaña
Subdirector

Mayor Eric Nicolás Villamil Sepulveda
Vicerrector Académico

Teniente Valentina Cortés Rodríguez
Jefe del Departamento de Ciencia, Tecnología, Investigación y Doctrina

EQUIPO EDITORIAL

Editor en Jefe
Hugo Armando Jurado Vásquez, Mgtr
Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Colombia

Editora Asociada
Alicia Camelo-Guarín, PhD
Universidad del Norte, Colombia

Asistente de edición
Javier Ramírez Narváez, PhD(s)
Universidad Cuauhtémoc de Aguascalientes, México

Asistente de edición técnico
John Fredy González Casagua, Ing(s)
Universidad abierta y a distancia (UNAD), Colombia

Diagramación
Valentina Rodríguez Rincón, M. AV
Politécnico Grancolombiano, Colombia

Corrección de Estilo
Omar Alfredo Pinilla Vargas, Comun. Soc
Universidad Jorge Tadeo Lozano, Colombia

Indexada en

Latindex (Catálogo 2.0 y Directorio), AmeliCA, Ideas, Google Scholar, MIAR, RePEc, AURA, FLACSO (LatinREV), Econpapers, Dimensions, OpenAlex, LivRe, Lens, ROAD, Crossref, SIS, Dialnet y DOAJ

Esta página queda intencionalmente en blanco

Revista Científica
PERSPECTIVAS EN INTELIGENCIA
2026

(Revista científica en Ciencias Sociales e interdisciplinaria)
ISSN 2145-194X (impreso) - ISSN 2745-1690 (en línea)
Volumen 18, Número 27, Enero-Junio 2026

La revista Perspectivas en Inteligencia de la Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Revista científica en Ciencias Sociales e interdisciplinaria) es una publicación científico-académica, de acceso abierto, revisada por pares y editada semestralmente por la ESICI.

Comité Científico / Editorial

Comité Editorial

Antonio Ariza-Montes, PhD
Universidad Loyola, España
Daniel Sansó-Rubert Pascual, PhD
Universidad Europea de Madrid, España
Alberto Fernández Rojas, PhD(s)
Universidad Autónoma de Madrid, España
Natalia Escobar Escobar, PhD
Universidad de Cundinamarca, Colombia
Catalina González-Cabrera, PhD
Universidad del Azuay, Ecuador
Sergio Gabriel Eissa, PhD
Universidad de Buenos Aires, Argentina
Jerónimo Ríos Sierra, PhD(s)
Universidad Complutense de Madrid, España
Manfred Grautoff Laverde, PhD(s)
Universidad Militar Nueva Granada, Colombia
Álvaro Cremades Guisado, PhD(c)
Universidad Antonio de Nebrija, España
Andrés Ultreras Rodríguez, PhD(c)
Universidad Autónoma de Sinaloa, México
Jean Carlo Mejía Azuero, PhD
Universidad Militar Nueva Granada, Colombia
Tania Gabriela Rodríguez Morales, PhD
Sofia University "St. Kliment Ohridski", Bulgaria

Comité Científico

Elói Martins Senhoras, PhD
Universidad Federal de Roraima, Brasil
Julia Pulido Gragera, PhD
Universidad Complutense de Madrid, España
Adrián Nicolás Marchal González, PhD
Universidad Antonio de Nebrija, España
Fernando Velasco Fernández, PhD
Universidad Rey Juan Carlos, España
Erick Leobardo Álvarez Aros, PhD
Universidad Popular Autónoma del Estado de Puebla, México
Nicolás Alejandro Liendo, PhD
Universidad Sergio Arboleda, Colombia
Rafael Martínez Martínez, PhD
Universidad de Barcelona, España
Cecilia Esperanza Ugalde-Sánchez, PhD
Universidad del Azuay, Ecuador
Mauricio Jaramillo Jassir, PhD
Universidad del Rosario, Colombia
Félix Ballesteros Leiva, PhD
Université Laval, Canadá
Ana Polack, PhD
Universidad Militar Nueva Granada, Colombia
German Darío Corzo Ussa, PhD
Universidad Popular Autónoma del Estado de Puebla, México

Pares Evaluadores

Eliot Gerardo Benavides González, Mgtr
Laura Janneth Delgado Nieto, Mgtr
Hernán Aljandro Olano García, PhD
Maria Camila Martínez Conde, Mgtr
Javier Ramírez Narváez, PhD(s)
Mauricio Pardo Rojas, Esp
German Ignacio Pinzón Zamora, Mgtr
Daniel Felipe Estupiñán Cuesta, Mgtr
Nelly Liliam Hernández Olaya, Mgstr
Leonardo Garzón Rayo, Mgtr
Jirley Vanessa Rojas Gómez, Mgtr
Vladimir Osorio-Isaza, PhD(s)
Jhonny Enrique Saavedra Medina, Mgtr
Reisner de Jesús Ravelo Méndez, PhD

Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (ESICI)
Carrera 8 A No. 101 – 33; Bogotá D.C., Colombia;
Teléfono: +57(1) 6017515
Código postal: 110111
Web oficial: *https://revistaseditorialejc.org/index.php/pei*
Contacto: *revistaperspectivas@esici.edu.co*

Los contenidos publicados por la revista Perspectivas en Inteligencia son de acceso abierto bajo una licencia Creative Commons: ***Reconocimiento-NoComercial-SinObrasDerivadas.*** *https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es_ES*

Las opiniones expresadas en este medio de comunicación son responsabilidad de sus autores y no corresponden a una posición institucional de la Escuela de Inteligencia y Contrainteligencia ESICI

Esta página queda intencionalmente en blanco

Revista Científica
Perspectivas en Inteligencia
Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (ESICI)
(Revista científica en Ciencias Sociales e interdisciplinaria)

Enfoque y Alcance

La revista Perspectivas en Inteligencia es una publicación semestral del Centro de Investigaciones de la ESICI, que tiene como finalidad difundir la producción académica e investigativa de los docentes y estudiantes de la ESICI, así como de las diferentes instituciones universitarias a nivel nacional e internacional. Por consiguiente, la revista se posiciona como un elemento de fuerte estímulo a la divulgación de temas del conocimiento en las áreas económica, social, administrativa y contable, o afines de actualidad nacional o internacional, que presenten el resultado de las investigaciones, del desarrollo de la creatividad y de la producción intelectual de los profesionales; el contenido de la revista está dirigido a especialistas, investigadores, estudiantes de pregrado y posgrado.

Misión y Visión

Ser un referente internacional en el debate y divulgación del nuevo conocimiento producido en las áreas temáticas que son de interés para la inteligencia estratégica y militar, por medio de la publicación de resultados originales de proyectos de investigación.

Ser el principal medio de difusión de los debates académicos, científicos y tecnológicos de la inteligencia estratégica y militar en Colombia con proyección en el ámbito internacional.

Orientación Temática

La revista Perspectivas en Inteligencia tiene como temática las líneas investigación, semilleros de investigación y eventos científicos, todos estos creados y liderados por la ESICI, del mismo modo con las realizadas por la comunidad académica que la conforma. Además de aportar nuevos conocimientos en el ámbito de la ciencia, lo que resulta muy significativo en nuestra función como institución de educación superior. De ello resultan temas de gran importancia para la seguridad nacional, en temas de inteligencia y contrainteligencia que responden a las necesidades de nuestro personal militar y académico respectivamente.

Está enmarcada en los siguientes ejes temáticos y disciplinas correspondientes: 1) Inteligencia y Contrainteligencia; 2) Economía; 3) Historia y filosofía; 4) Administración y finanzas; y 5) Tecnología y desarrollo, entre otros.

Responsabilidad de Contenidos

La responsabilidad por el contenido de los artículos publicados por la revista Perspectivas en Inteligencia corresponde exclusivamente a los autores. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional del Comando de Educación y Doctrina, el Ejército Nacional de Colombia o el Ministerio de Defensa Nacional.

Envío de Propuestas

La revista Perspectivas en Inteligencia fomenta la presentación de propuestas originales correspondientes a los ejes temáticos y disciplinas descritas anteriormente. Todos los envíos deben seguir las instrucciones para autores disponibles en: https://revistaseditorialejc.org/index.php/pei/information/authors, y deben enviarse electrónicamente a: https://revistaseditorialejc.org/index.php/pei/login

Esta página queda intencionalmente en blanco

Tabla de Contenido

Table of Contents

Editorial

Artículos

Esta página queda intencionalmente en blanco

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Integración de la inteligencia artificial generativa en la investigación científica: equilibrio entre innovación y rigor metodológico

Autor

Hugo Armando Jurado-Vásquez
https://orcid.org/0000-0001-8830-1139
✉ hugo.jurado@esici.edu.co
Escuela de Inteligencia y Contrainteligencia
"BG. Ricardo Charry Solano", Colombia

Citación APA: Jurado-Vásquez, H. A. (2026). Integración de la inteligencia artificial generativa en la investigación científica: equilibrio entre innovación y rigor metodológico. *Perspectivas en Inteligencia,18*(27), 15-23. http://doi.org/10.47961/2145194X.335

Publicado en línea: 2026

Los artículos publicados por la Revista Científica Perspectivas en Inteligencia son de acceso abierto bajo una licencia **Creative Commons: Atribución - No Comercial – Sin Derivados.**

Para enviar un artículo:
https://revistaseditorialejc.org/index.php/pei/about/submissions

Esta página queda intencionalmente en blanco

PERSPECTIVAS EN INTELIGENCIA 2026

Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 18, N° 27, enero - junio 2026, pp. 15-23
http://doi.org/10.47961/2145194X.335

Integración de la inteligencia artificial generativa en la investigación científica: equilibrio entre innovación y rigor metodológico

Integrating generative artificial intelligence into scientific research: balancing innovation and methodological rigor

Hugo Armando Jurado-Vásquez[1]

(1) Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Bogotá, D. C., Colombia.
✉ *hugo.jurado@esici.edu.co*

Resumen

La inteligencia artificial generativa (IAGen) se consolida como una tecnología clave en la transformación de la investigación científica, al facilitar la generación de contenido original y optimizar los procesos de redacción académica y producción del conocimiento. Su incorporación impulsa la eficiencia, calidad y creatividad en la comunicación científica, aunque exige un uso ético, responsable y transparente por parte de los autores, revisores y editores. Por ello, las políticas editoriales actuales subrayan la necesidad de declarar de forma explícita su utilización, detallando herramientas, propósitos y alcance, para preservar la integridad académica y garantizar la trazabilidad del conocimiento generado.

Asimismo, la IAGen es reconocida como una herramienta de apoyo en tareas como redacción, revisión bibliográfica, análisis de datos y generación de ideas, sin sustituir el proceso cognitivo, el juicio crítico y la responsabilidad intelectual de los investigadores. No obstante, se establecen límites claros frente a usos inadecuados, como la generación de resultados, la interpretación de datos o la creación de contenido sin supervisión humana significativa, prácticas contrarias a la ética científica. En consecuencia, resulta fundamental desarrollar marcos regulatorios que equilibren la innovación tecnológica con el rigor metodológico, asegurando la transparencia, la protección de datos y la credibilidad del sistema científico.

Clasificación JEL: C88, D78.

Palabras clave: inteligencia artificial generativa; ética científica; transparencia; producción del conocimiento; redacción académica.

Fecha de recepción: 11/04/2026 | Fecha de aprobación: 14/07/2026

Abstract

Generative artificial intelligence (GenAI) is establishing itself as a key technology in the transformation of scientific research by facilitating the generation of original content and optimizing academic writing and knowledge production processes. Its incorporation enhances efficiency, quality, and creativity in scientific communication, although it requires ethical, responsible, and transparent use by authors, reviewers, and editors. For this reason, current editorial policies emphasize the need to explicitly disclose its use—specifying the tools, purposes, and scope—to preserve academic integrity and ensure the traceability of the knowledge generated.

Furthermore, GenAI is recognized as a tool to support tasks such as writing, literature reviews, data analysis, and idea generation, without replacing researchers' cognitive processes, critical judgment, and intellectual responsibility. However, clear limits are established against inappropriate uses, such as generating results, interpreting data, or creating content without meaningful human oversight—practices that violate scientific ethics. Consequently, it is essential to develop regulatory frameworks that balance technological innovation with methodological rigor, ensuring transparency, data protection, and the credibility of the scientific system.

Keywords: generative artificial intelligence; scientific ethics; transparency; knowledge production; academic writing.

Introducción

La Inteligencia Artificial Generativa (IAGen) constituye una subdisciplina de la inteligencia artificial (IA) orientada a la producción de contenido original que, en muchos casos, resulta indistinguible del generado o creado por seres humanos. A diferencia de los enfoques tradicionales de la IA, que se han centrado principalmente en tareas de análisis, clasificación o predicción a partir de datos, la IAGen se caracteriza por su capacidad para generar nuevas representaciones y efectos (Cantos-Lucas et al., 2026; Diaz-Vera et al., 2024).

Este tipo de sistemas no solo procesa información existente, sino que también produce contenido novedoso en múltiples formatos, tales como texto, imágenes, audio y música; capacidades que se fundamentan en modelos avanzados de aprendizaje automático, los cuales han sido entrenados con grandes volúmenes de datos, que permiten identificar patrones complejos y reproducción de estructuras características de la creatividad humana (Salazar-Sisalima et al., 2024).

En este contexto, una de las principales implicaciones derivadas de la Inteligencia Artificial Generativa (IAGen), y que constituye el eje central del presente editorial, radica en su capacidad para transformar los procesos de producción, redacción y comunicación de la investigación científica a escala global. Dicha transformación no solo incide en la eficiencia de estos procesos, sino que también plantea la necesidad de fortalecer los principios de transparencia y uso responsable (Arredondo-Trapero et al., 2014). En consonancia con lo anterior, las revistas científicas de publicación digital han comenzado a implementar políticas o directrices que exigen a los autores declarar explícitamente el empleo de herramientas

de IAGen en cualquier etapa del proceso investigativo (Alcolea- López y Martínez-Carpio, 2026).

Al revisar la literatura sobre inteligencia artificial (IA) en los últimos años, se observa que los países miembros del Grupo de los Veinte, Ministerial Statement on Trade and Digital Economy (G20, 2019), ya promovían la apertura hacia el desarrollo y la adopción a la IA, como se evidencia a continuación:

> Para seguir impulsando la innovación en la economía digital, apoyamos el intercambio de buenas prácticas sobre políticas y marcos regulatorios eficaces, innovadores, ágiles, flexibles y adaptados a la era digital, incluso mediante el uso de entornos de prueba regulatorios. El desarrollo y uso responsable de la Inteligencia Artificial (IA) puede ser un motor para el avance de los Objetivos de Desarrollo Sostenible (ODS) y la consecución de una sociedad sostenible e inclusiva. (párr. 12)

A lo anterior, se suma lo descrito en uno de los textos más relevantes para contextualizar la IAGen en la investigación científica, en el cual Barradas-Gudiño (2023), sostiene que "es importante destacar que la aplicación de estas nuevas técnicas no debe reemplazar las formas tradicionales de investigación, sino complementarlas, interactuando para el procesamiento, análisis y la presentación de los datos relacionados con sus estudios" (p. 117).

En esta línea, Huang et al. (2022) argumentan que la dimensión ética asociada a la incorporación de la IAGen en la sociedad será objeto de múltiples interpretaciones, dado que se ha consolidado como un factor relevante en la investigación científica, así como una fuente de preocupación compartida por individuos, organizaciones, Estados y la sociedad en general.

Adicionalmente, autores como Khalifa y Albadawy (2024) señalan que, en el proceso de redacción académica, resulta fundamental que los investigadores mantengan un equilibrio entre el rigor informativo y la capacidad de captar el interés del lector, incorporando criterios de originalidad, ética y creatividad que favorezcan la coherencia y fluidez de las ideas. Bajo este escenario, la IAGen se posiciona como una herramienta de apoyo relevante que puede potenciar la productividad y mejorar la calidad de la escritura científica, siempre que su uso se enmarque en principios de transparencia y responsabilidad.

Autores como Švab et al. (2023) especifican que "las herramientas basadas en IA están facilitando la redacción científica y reduciendo el tiempo que requiere, lo que probablemente aumentará aún más el número de publicaciones científicas y, potencialmente, dará lugar a artículos de mayor calidad" (p. 109). En relación con lo anterior, la IAGen se consolida como un recurso de apoyo estratégico en la elaboración de textos académicos, ya que, cuando se emplea de manera adecuada y responsable, puede contribuir a optimizar los procesos de escritura y favorecer la producción de artículos con mayor rigor y calidad científica.

Así las cosas, es importante señalar que ninguna política editorial respalda la incorporación acrítica de contenido generado por IA. No obstante, las revistas científicas adoptan enfoques diversos: algunas permiten su uso bajo la supervisión y responsabilidad del autor,

mientras que otras lo restringen o prohíben para autores, editores y revisores. Estas posturas evidencian la necesidad de equilibrar el aprovechamiento de la IAGen con el cumplimiento de los principios de ética e integridad científica (Machin-Mastromatteo, 2025).

Por su parte, la revista Perspectivas en Inteligencia reconoce que la IAGen es un punto de inflexión, ya integrado en la vida cotidiana (Rodríguez-Álvarez y Osorio-Isaza,2025). Está transformando la investigación científica y su comunicación, por lo que exige a los autores declarar su uso en cualquier etapa de su investigación o redacción. A los efectos de esta política, se entiende por "herramientas de IAGen" aquellas tecnologías que crean contenido nuevo (texto, imágenes, código, datos) a partir de datos de entrenamiento, tales como ChatGPT, Gemini, Claude, Copilot, DALL-E, Midjourney y similares. Se distinguen de las herramientas asistenciales convencionales (correctores ortográficos integrados, gestores de referencias como Zotero o Mendeley), las cuales no requieren declaración.

El diseño de una política específica para el uso adecuado de herramientas de IAGen, dirigida a autores, evaluadores y editores en todas las fases del flujo editorial de una revista científica especializada, resulta fundamental para garantizar el cumplimiento de las buenas prácticas éticas en la publicación científica. Bajo este enfoque, se presentarán las principales características que deben considerarse para el diseño adecuado de una política institucional sobre IAGen en el ámbito de las revista científicas.

Declaración obligatoria de los(as) autores(as) por el uso de IAGen

La revista reconoce que el uso responsable de herramientas de IAGen puede mejorar la eficiencia en la investigación, facilitar el acceso a información relevante y contribuir a la calidad de los resultados, sin sustituir la responsabilidad intelectual de los autores.

En la actualidad, las herramientas de IAGen desempeñan un papel creciente en el apoyo a la investigación, al facilitar la recopilación, organización y síntesis de literatura especializada, entre otras funciones. Asimismo, proporcionan asistencia en la estructuración de contenidos y la optimización del lenguaje, lo que contribuye a mejorar la claridad, coherencia y legibilidad de los textos académicos. A este respecto, la revista Perspectivas en Inteligencia permite su uso como herramienta de apoyo en estas tareas, siempre bajo la responsabilidad del autor y sin reemplazar el pensamiento crítico, la experiencia ni el juicio evaluativo humano (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO], 2024).

Al enviar un manuscrito, los(as) autores(as) deben declarar explícitamente el uso de cualquier herramienta de IAGen en su manuscrito. Esta declaración debe incluirse en una sección titulada "Declaración de uso de IAGen" ubicada inmediatamente antes de la sección de "Referencias/Bibliografía". Esta declaración debe especificar:

- El nombre y la versión de la herramienta de IAGen utilizada.
- El propósito específico para el cual fue empleada.
- Las secciones del manuscrito en las que se utilizó.

- El alcance de su uso.
- La confirmación de que el autor revisó y verificó todo el contenido generado o asistido por IAGen.

Los/las autores/as deben citar adecuadamente la herramienta de IAGen utilizada en la sección de "Referencias", siguiendo el formato de citación APA séptima edición.

Si no se utilizó IAGen, los autores deberán incluir la siguiente declaración:

- "Los autores declaran que no se utilizaron herramientas de inteligencia artificial generativa en la preparación de este manuscrito."

Uso permitido de IAGen

La revista Perspectivas en Inteligencia promueve el uso responsable de herramientas de IAGen, siempre que estas cumplan con altos estándares de seguridad de la información, confidencialidad y protección de la propiedad intelectual. En este marco, se autoriza su utilización como recurso de apoyo en diversas fases del proceso investigativo y de producción académica, entre las que se destacan:

1. Asistencia en redacción y edición. La IAGen se puede utilizar para mejorar la claridad del lenguaje, coherencia, corrección gramatical y la fluidez del texto, pero los(as) autores(as) son responsables del contenido final y deben verificar su exactitud.
2. Revisión y gestión bibliográfica. Los(as) autores(as) pueden utilizar la IAGen como soporte en el proceso de búsqueda interactiva en línea con motores de búsqueda mejorados por modelo de lenguaje de gran tamaño (LLM), revisar la bibliografía y elaborar resúmenes de artículos, asegurando siempre que la información generada sea precisa y avalada por fuentes verificables.
3. Análisis de datos y modelaje. Se permite la integración de la IAGen para hacer análisis de datos y modelarlos, siempre y cuando los métodos sean transparentes, reproducibles y se garantice la fiabilidad de los datos resultantes.
4. Generación y desarrollo de ideas. Brainstorming (lluvia de ideas), exploración conceptual o enfoques metodológicos, siempre sujeta a validación critica por parte del autor y que este desarrolle las ideas.
5. Revisión de plagio y referencias. Los(as) autores(as) pueden utilizar herramientas de IAGen para verificar la originalidad de sus trabajos y mejorar la precisión de las citas y referencias mediante software especializado como (Zotero, Mendeley, EndNote).
6. Elaboración de recursos visuales. Incluyendo gráficos, diagramas o modelos explicativos, siempre basados en contenido previamente desarrollado en el manuscrito.

En todos los casos, el uso de IAGen debe entenderse como un apoyo complementario que no reemplaza el juicio crítico, la creatividad ni la responsabilidad ética de los autores, quienes deben garantizar la integridad, veracidad y originalidad del contenido presentado (Penabad-Camacho et al., 2024).

Usos no aceptados de la IAGen

Los(as) autores(as) no deben enviar manuscritos en los que hayan utilizado herramientas de IAGen de manera que sustituyan las responsabilidades fundamentales del investigador/a y del autor/a. En particular, se consideran prácticas inadecuadas aquellas en las que estas herramientas reemplazan el juicio crítico, la interpretación académica o la responsabilidad intelectual inherente al proceso científico, tales como las siguientes:

1. Interpretar datos o formular conclusiones científicas. La interpretación de resultados y la formulación de hallazgos son responsabilidades intelectuales exclusivas de los autores humanos.
2. Generar artículos completos o sustancialmente elaborados por IAGen sin supervisión humana significativa.
3. Fabricar datos, resultados o referencias bibliográficas.
4. Producir contenido que introduzca sesgo, información falsa o interpretaciones erróneas en la investigación.
5. Generación de texto o código sin revisión rigurosa.
6. Generación de datos sintéticos para sustituir datos faltantes sin una metodología sólida.
7. Creación y manipulación de Tablas y Figuras, ni de datos de investigación originales para su uso en los manuscritos. El término «Tablas y Figuras» incluye fotografías, gráficos, tablas de datos, modelos, imágenes médicas, fragmentos de imágenes, código informático y fórmulas. El término «manipulación» incluye aumentar, ocultar, mover, eliminar o introducir una característica específica dentro de una imagen o figura.

Este tipo de casos pueden ser objeto de investigación editorial. La omisión de divulgación, el no revelar el uso de la IAGen en los manuscritos se considera una falta de ética académica y puede implicar el rechazo de la propuesta o la retirada del artículo ya publicado.

Uso de IAGen en el proceso de revisión

El uso de manuscritos en sistemas de IAGen puede implicar riesgos significativos, particularmente en lo relacionado a la confidencialidad, la protección de datos y la posible vulneración de los derechos de propiedad intelectual. A este respecto, la incorporación de documentos inéditos en dichas plataformas podría derivar en la exposición no autorizada de información sensible o protegida (Resnik y Hosseini, 2025).

Por consiguiente, los editores deben abstenerse de cargar manuscritos no publicados inéditos, incluyendo archivos, imágenes o cualquier material asociado en herramientas de IAGen que no garanticen estándares adecuados de seguridad y privacidad. El incumplimiento de esta directriz no solo vulnera los principios éticos de la publicación científica, sino que también puede constituir una infracción de los derechos de propiedad intelectual de sus autores o titulares.

Los revisores, en su calidad de especialistas en sus respectivos campos disciplina-

res, deben abstenerse de emplear herramientas de IAGen para el análisis o la síntesis de manuscritos, ya sean completos o fragmentos de estos durante la elaboración de sus evaluaciones. Esta restricción responde a la necesidad de preservar la autonomía crítica, el rigor metodológico y la responsabilidad intelectual inherentes al proceso de revisión por pares (Miyahira, 2025).

En consecuencia, los revisores no deben cargar manuscritos no publicados inéditos, propuestas de investigación ni ningún material asociado, incluidos archivos, imágenes o datos en plataformas de IAGen, debido a los riesgos potenciales relacionados con la confidencialidad, la protección de datos y los derechos de propiedad intelectual. No obstante, tanto revisores como editores pueden utilizar herramientas de IAGen como apoyo complementario en el proceso de revisión, siempre que su uso se limite a funciones auxiliares y no sustitutivas de juicio académico. En consonancia con lo anterior, deberán:

1. Mantener la confidencialidad de los manuscritos.
2. No cargar manuscritos completos en plataformas de IAGen que no garanticen la privacidad de los datos.
3. Declarar el uso de IAGen en sus evaluaciones si es relevante.
4. Utilizar la IAGen para ayudar a mejorar el lenguaje de las revisiones, pero los revisores pares seguirán siendo en todo momento responsables de garantizar la exactitud e integridad de sus revisiones.

El equipo editorial evaluará el uso declarado de IAGen en relación con su impacto en la contribución teórica, empírica y metodológica de los manuscritos postulados para publicación en la revista Perspectivas en Inteligencia. En este sentido, se reserva el derecho de solicitar información adicional sobre el alcance y las condiciones de utilización de dichas herramientas.

Conclusiones

La inteligencia artificial generativa (IAGen) se configura como un factor estructural de transformación en la producción y comunicación del conocimiento científico, cuyo aprovechamiento debe orientarse al fortalecimiento de la calidad editorial, preservando la responsabilidad intelectual de los autores. En este marco de las publicaciones científicas, la incorporación de la IAGen demanda la consolidación de políticas editoriales claras que garanticen la trasparencia en su uso, mediante la declaración obligatoria y verificable en los manuscritos sometidos a evaluación.

El uso de herramientas de IAGen debe limitarse a funciones auxiliares dentro del proceso investigativo y de redacción, excluyendo su aplicación en la formulación de resultados, interpretación de hallazgos o generación sustantiva de contenido científico. La adopción de criterios regulatorios frente al uso de IAGen contribuye a salvaguardar principios fundamentales de la publicación científica, tales como la integridad académica, la protección de datos y la propiedad intelectual en el sistema editorial.

En consecuencia, la integración responsable de la IAGen en revistas científicas es-

pecializadas en Colombia debe orientarse hacia un equilibrio entre innovación tecnológica y rigor metodológico, asegurando la preservación de la credibilidad y legitimidad del conocimiento científico producido.

Declaración obligatoria de uso de IAGen

El autor declara que no se utilizaron herramientas de inteligencia artificial generativa en la preparación de este manuscrito.

Referencias

Alcolea-López, J. M. y Martínez-Carpio, P. A. (2026). El uso de la inteligencia artificial generativa en publicaciones científicas requiere declaración obligatoria. *Medicina Estética*, *(87)*, 7-11. https://doi.org/10.48158/MedicinaEstetica.087.E

Arredondo-Trapero, F. G., De la Garza-García, J. y Vázquez-Parra, J. C. (2014). Transparencia en las organizaciones, una aproximación desde la perspectiva de los colaboradores. *Estudios Gerenciales*, *30*(133), 408-418. https://doi.org/10.1016/j.estger.2014.06.007

Barradas-Gudiño, J. (2023). Inteligencia artificial como elemento transformador de la investigación científica. *Entrelíneas, 2*(1), 113-122. https://doi.org/10.56368/Entrelineas213

Cantos-Lucas, P. A., Mite-Albán, M. T., Herrera-Rivas, L. y Guerrero-Carrasco, M. J. (2025). Inteligencia artificial generativa: oportunidades para la comunidad universitaria y la importancia de las soft skills. *Revista Científica Profundidad Construyendo Futuro*, *24*(24), 130-146. https://doi.org/10.22463/24221783.5261

Diaz-Vera, J. P., Molina-Izurieta, R., Bayas-Jaramillo, C. M. y Ruiz-Ramírez, A. K. (2024). Asistencia de la inteligencia artificial generativa como herramienta pedagógica en la educación superior. *Revista de Investigación en Tecnologías de la Información, 12*(26), 61-76. https://doi.org/10.36825/RITI.12.26.006

Huang, C., Zhang, Z., Mao, B. y Yao, X. (2022). An Overview of Artificial Intelligence Ethics. *IEEE Transactions on Artificial Intelligence, 4*(4), 799-819. https://doi.org/10.1109/TAI.2022.3194503

Khalifa, M. y Albadawy, M. (2024). Using artificial intelligence in academic writing and research: An essential productivity tool. *Computer Methods and Programs in Biomedicine Update, 5*. https://doi.org/10.1016/j.cmpbup.2024.100145

Machin-Mastromatteo, J. D. (2025). Recomendaciones para elaborar políticas editoriales sobre el uso de inteligencia artificial generativa en la publicación científica. *Revista Estudios de la Información, 3*(2), 101-116. https://doi.org/10.54167/rei.v3i2.2193

Ministerial Statement on Trade and Digital Economy. (29 de junio de 2019). *G20 Osaka Leaders' Declaration.* G7/G20 Documents database. https://g7g20-documents.org/database/document/2019-g20-japan-leaders-leaders-language-g20-osaka-leaders-declaration

Miyahira , J. (2025). Uso de inteligencia artificial en el proceso de revisión por pares. *Revista Médica Herediana*, *36*(4), 291-293. https://doi.org/10.20453/rmh.v36i4.7482

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2024). *Guía para el uso de IA generativa en educación e investigación.* https://unesdoc.unesco.org/ark:/48223/pf0000389227

Penabad-Camacho, L., Morera-Castro, M. y Penabad-Camacho, M. A. (2024). Guía para el uso y Reporte de Inteligencia Artificial en Revistas Científico-Académicas. *Revista Electrónica Educare, 28*(S), 1-41. https://doi.org/10.15359/ree.28-S.19830

Resnik, D. B. y Hosseini, M. (2025). The ethics of using artificial intelligence in scientific research: new guidance needed for a new tool. *AI and Ethics, 5*, 1499-1521. https://doi.org/10.1007/s43681-024-00493-8 PMid:40337745 PMCid:PMC12057767

Rodríguez-Álvarez, F. E., & Osorio-Isaza, V. (2025). Inteligencia Artificial Generativa: del hito tecnológico al punto de inflexión complejo. *Perspectivas en Inteligencia, 17*(26), 17-32. https://doi.org/10.47961/2145194X.855

Salazar-Sisalima, M. C., Lapo-Fernández , J. M., Romero Sobenis, F. F. y La Rosa Navarro, Y. (2024). La inteligencia artificial generativa como herramienta de apoyo en la personalización del aprendizaje: Implicaciones y desafíos éticos en el aula para estudiantes de EGB. *Reincisol, 3*(6), 6983-7007. https://doi.org/10.59282/reincisol.V3(6)6983-7007

Švab, I., Klemenc-Ketiš, Z. y Zupanič, S. (2023). New Challenges in Scientific Publications: Referencing, Artificial Intelligence and ChatGPT. *Slovenian Journal of Public Health, 62*(3), 109-112. https://doi.org/10.2478/sjph-2023-0015 PMid:37327133 PMCid:PMC10263368

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Integración de la inteligencia artificial generativa en la investigación científica: equilibrio entre innovación y rigor metodológico

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Hugo Armando Jurado-Vásquez es Magister en Inteligencia Estratégica de la Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Colombia), es Ingeniero Electrónico de la Universidad ECCI (Colombia), es Tecnólogo en Soporte de Telecomunicaciones de la Universidad ECCI (Colombia), Tecnólogo en Instrumentación Industrial del Politécnico colombiano "Jaime Isaza Cadavid" (Colombia).

https://orcid.org/0000-0001-8830-1139 - Contacto: hugo.jurado@esici.edu.co

Esta página queda intencionalmente en blanco

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa

Autor

Carlos Galán-Cordero
https://orcid.org/0009-0006-3858-1666
✉ cgalan@nebrija.es
Universidad Nebrija, España

Citación APA: Galán-Cordero, C. (2026). Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa. *Perspectivas en Inteligencia, 18*(27), 27-47. http://doi.org/10.47961/2145194X.856

Publicado en línea: 2026

Los artículos publicados por la Revista Científica Perspectivas en Inteligencia son de acceso abierto bajo una licencia **Creative Commons: Atribución - No Comercial – Sin Derivados.**

Para enviar un artículo:
https://revistaseditorialejc.org/index.php/pei/about/submissions

Esta página queda intencionalmente en blanco

PERSPECTIVAS EN INTELIGENCIA 2026
Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 18, N° 27, enero - junio 2026, pp. 27-47
http://doi.org/10.47961/2145194X.856

Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa

Higher education and democratic resilience: a proposal for training in hybrid threat intelligence and information manipulation

Carlos Galán-Cordero[1]

(1) Universidad Nebrija, Madrid, España,
✉ cgalan@nebrija.es

Resumen

Objetivo: diseñar y fundamentar una propuesta de formación universitaria de posgrado que permita responder al déficit de capacitación interdisciplinar existente en materia de amenazas híbridas, desinformación, injerencia extranjera y manipulación informativa en el ciberespacio, mediante el desarrollo de competencias analíticas, jurídicas, tecnológicas e institucionales orientadas al fortalecimiento de la resiliencia democrática. **Metodología:** se adopta un enfoque cualitativo, documental y propositivo, basado en el diseño curricular orientado a competencias y en los principios del aprendizaje activo. El estudio analiza e integra aportaciones procedentes de los estudios estratégicos, el derecho, la ciberseguridad, la comunicación, la psicología social y el análisis de inteligencia. A partir de esta revisión interdisciplinar se estructura un programa semestral de posgrado, de entre seis y ocho créditos ECTS (European Credit Transfer and Accumulation System), dirigido a profesionales de los ámbitos jurídico, periodístico, diplomático, militar, policial, académico y de la Administración pública. **Resultados:** se obtiene un modelo pedagógico organizado en cinco bloques progresivos: fundamentos de las amenazas híbridas; ciberespacio como dominio estratégico; psicología y sociología de la desinformación; marco jurídico e institucional; y prevención y resiliencia institucional. El modelo combina contenidos conceptuales con análisis de casos, verificación digital, inteligencia de fuentes abiertas, simulaciones de crisis y comunicación estratégica. **Conclusiones:** una formación interdisciplinar, aplicada y orientada a competencias puede reducir la fragmentación académica existente y mejorar la capacidad profesional para identificar, analizar y responder de manera jurídicamente legítima y operativamente eficaz a las operaciones de manipulación informativa, contribuyendo al fortalecimiento futuro de la resiliencia institucional y democrática.

Clasificación JEL: D83, I23

Palabras clave: amenazas híbridas; desinformación; ciberespacio; educación superior; resiliencia democrática.

Fecha de recepción: 23/04/2026 | Fecha de aprobación: 22/07/2026

Abstract

Objective: to design and substantiate a postgraduate higher education programme aimed at addressing the existing deficit in interdisciplinary training on hybrid threats, disinformation, foreign interference and information manipulation in cyberspace, through the development of analytical, legal, technological and institutional competencies intended to strengthen democratic resilience. **Methodology:** the study adopts a qualitative, documentary and proposal-oriented approach based on competency-based curriculum design and active learning principles. It analyses and integrates contributions from strategic studies, law, cybersecurity, communication, social psychology and intelligence analysis. On the basis of this interdisciplinary review, a semester-long postgraduate programme of six to eight (European Credit Transfer and Accumulation System) ECTS credits is structured for professionals working in legal, journalistic, diplomatic, military, law-enforcement, academic and public-administration settings. **Results:** the study produces a progressive pedagogical model organised into five modules: foundations of hybrid threats; cyberspace as a strategic domain; psychology and sociology of disinformation; legal and institutional framework; and prevention and institutional resilience. The model combines conceptual content with case analysis, digital verification, open-source intelligence, hybrid-crisis simulations and strategic communication. **Conclusions:** interdisciplinary, applied and competency-based education can reduce the current fragmentation of academic training and enhance professionals' ability to identify, analyse and respond to information-manipulation operations in a legally legitimate and operationally effective manner, thereby contributing to the future strengthening of institutional and democratic resilience.

Keywords: hybrid threats; disinformation; cyberspace; higher education; democratic resilience.

Introducción

El entorno estratégico internacional contemporáneo se caracteriza por una creciente complejidad derivada de la digitalización global, la interdependencia tecnológica y la intensificación de la competencia geopolítica entre Estados. En este contexto han adquirido una relevancia creciente las denominadas **amenazas híbridas**, entendidas como la combinación coordinada de instrumentos políticos, informativos, económicos, tecnológicos y, en ocasiones, militares con el objetivo de explotar vulnerabilidades estructurales de los Estados y de las sociedades abiertas (Humprecht et al., 2020; Sanz-Caballero, 2023).

Uno de los componentes centrales de estas estrategias es el uso sistemático de **operaciones de manipulación informativa,** en las que se incluyen las campañas de desinformación, las interferencias en procesos políticos y las operaciones de influencia desarrolladas a través del ciberespacio. Estas actividades persiguen influir en la percepción pública de determinados acontecimientos, erosionar la confianza en las instituciones democráticas, polarizar a la opinión pública o alterar procesos electorales (Freelon y Wells, 2020; Tuñón-Navarro et al., 2019).

La expansión de las plataformas digitales y de las redes sociales ha facilitado el

desarrollo de nuevas técnicas de manipulación informativa basadas en el uso de automatización, análisis masivo de datos y microsegmentación de audiencias. Estas dinámicas han transformado profundamente el ecosistema informativo contemporáneo, generando nuevos desafíos para la gobernanza democrática y para la seguridad de los Estados (Arrese, 2024; Kozyreva et al., 2020; Salaverría et al., 2020).

A pesar de la creciente relevancia estratégica del fenómeno, la formación universitaria especializada en inteligencia para las amenazas híbridas y desinformación continúa siendo limitada y fragmentaria. Los programas académicos suelen abordar estas cuestiones desde perspectivas disciplinares aisladas -por ejemplo, desde la comunicación política, la seguridad internacional o la ciberseguridad- sin ofrecer una aproximación integrada que permita comprender la complejidad multidimensional del fenómeno (Huang et al., 2024; Wuyckens et al., 2022).

Esta carencia resulta especialmente significativa en la formación de profesionales que desempeñan funciones clave en la gestión de la información, la seguridad institucional y la protección de los procesos democráticos, como juristas, periodistas, diplomáticos, miembros de las fuerzas armadas o responsables de las administraciones públicas.

En este contexto, el presente trabajo propone una **metodología docente para un curso de posgrado semestral** orientado a la formación interdisciplinar en materia de inteligencia para las amenazas híbridas, campañas de desinformación e injerencia extranjera en el ciberespacio. El objetivo de la propuesta es contribuir al desarrollo de programas formativos que permitan mejorar la comprensión de estos fenómenos y fortalecer las capacidades analíticas y estratégicas de los profesionales que deben enfrentarse a ellos.

Metodología

Diseño pedagógico de la propuesta formativa

La propuesta formativa presentada en este trabajo se basa en un proceso de **diseño curricular orientado a competencias**, inspirado en los principios del aprendizaje activo y en enfoques pedagógicos utilizados en programas de seguridad, inteligencia y estudios estratégicos (Wuyckens et al., 2022; Yang et al., 2021).

La propuesta se elaboró mediante una revisión narrativa e interdisciplinar de literatura científica reciente sobre amenazas híbridas, desinformación, alfabetización mediática, resiliencia democrática y metodologías activas de aprendizaje. La selección priorizó artículos publicados desde 2020 en revistas académicas indexadas, complementados con normas y documentos institucionales de la Unión Europea indispensables para el análisis jurídico y de gobernanza.

El diseño del programa se articula en torno a tres principios metodológicos fundamentales: **interdisciplinariedad, aprendizaje aplicado y enfoque institucional.**

Enfoque interdisciplinar

Las amenazas híbridas constituyen un fenómeno complejo que combina dimensiones políticas, tecnológicas, jurídicas, comunicativas y psicológicas. En consecuencia, el programa docente integra conocimientos procedentes de diversos campos del saber, entre ellos (Freelon y Wells, 2020; Sanz-Caballero, 2023):

- Relaciones internacionales y estudios estratégicos.
- Derecho internacional, constitucional y europeo.
- Ciberseguridad y gobernanza del ciberespacio.
- Comunicación política y periodismo.
- Psicología social y sociología de la información.
- Análisis de inteligencia.

Este enfoque interdisciplinar permite ofrecer una comprensión más completa de las dinámicas que caracterizan las operaciones híbridas y las campañas de manipulación informativa.

Aprendizaje aplicado y metodologías activas

El segundo eje metodológico del programa es la incorporación de **metodologías docentes** activas, orientadas al desarrollo de competencias analíticas y operativas (Guess et al., 2020; Huang et al., 2024; Moore y Hancock, 2022).

Entre las principales actividades formativas se incluyen:

- Análisis de casos reales de campañas de desinformación.
- Talleres de verificación digital y fact-checking.
- Ejercicios de inteligencia de fuentes abiertas (OSINT).
- Simulaciones de crisis híbridas.

Estas metodologías permiten que el alumnado desarrolle habilidades analíticas directamente aplicables a contextos profesionales reales (Basol et al., 2020; Yang et al., 2021; Zhang et al., 2022).

Enfoque institucional

La propuesta docente está diseñada para un alumnado compuesto por profesionales procedentes de distintos ámbitos institucionales. En consecuencia, el programa se orienta no solo a la comprensión teórica del fenómeno, sino también a la identificación de **estrategias institucionales de prevención, resiliencia y respuesta** frente a las amenazas híbridas.

Modelo pedagógico del curso

El modelo pedagógico propuesto se basa en una estructura progresiva que conecta **conocimiento conceptual, análisis aplicado y desarrollo de capacidades estratégicas.**

Tabla 1. Modelo pedagógico del programa formativo

Modelo pedagógico del programa formativo	
Módulo 1: Comprensión conceptual	• Fundamentos de las amenazas híbridas. • Geopolítica de la información. • Funcionamiento del ecosistema digital.
Módulo 2: Análisis del fenómeno	• Campañas de desinformación. • Herramientas de manipulación digital. • Factores psicológicos y sociales.
Módulo 3: Marco institucional	• Derecho internacional y europeo. • Gobernanza del ciberespacio. • Políticas públicas frente a la desinformación.
Módulo 4: Capacidades operativas	• Análisis de inteligencia. • Verificación digital. • Diseño de respuestas institucionales.
Resultado final: Profesionales capaces de **identificar, analizar y responder a amenazas híbridas y campañas de manipulación informativa.**	

Nota: El modelo integra y sistematiza la literatura interdisciplinar citada en el apartado metodológico.

Fuente: Elaboración propia

Resultados

Estructura del programa formativo

Los resultados del proceso de diseño curricular se concretan en la estructura, secuencia y contenidos del programa formativo que se exponen a continuación.

El curso se concibe como un **programa de posgrado de un semestre**, con una carga docente aproximada de entre seis y ocho créditos ECTS.

La estructura curricular se organiza en los siguientes cinco módulos o bloques temáticos.

Fundamentos de las amenazas híbridas

Este primer bloque resulta indispensable porque proporciona el **marco conceptual y estratégico básico** sin el cual no sería posible comprender adecuadamente el resto de los contenidos del programa. La noción de amenaza híbrida no se refiere simplemente a una suma de riesgos dispersos, sino a la articulación coordinada de instrumentos heterogéneos -políticos, económicos, informativos, tecnológicos, cibernéticos y, en ocasiones, militares- orientados a explotar vulnerabilidades institucionales y sociales de un Estado o de una sociedad abier-

ta. En consecuencia, antes de abordar manifestaciones concretas, como la desinformación, la manipulación algorítmica o la injerencia extranjera, resulta necesario dotar al alumnado de una comprensión rigurosa de la lógica estratégica que integra y da sentido a dichos fenómenos (Humprecht et al., 2020; Sanz-Caballero, 2023).

La inclusión de este bloque se justifica, además, porque una parte sustancial de la dificultad analítica que plantean las amenazas híbridas deriva precisamente de su **ambigüedad estructural**. No suelen manifestarse como ataques abiertos, formalmente declarados o jurídicamente fáciles de calificar, sino como actuaciones graduales, acumulativas y frecuentemente situadas en la denominada **zona gris**, esto es, en el espacio intermedio entre la paz y el conflicto armado tradicional. Esta característica exige formar al alumnado en categorías analíticas que permitan identificar dinámicas de hostigamiento, erosión o desestabilización que, consideradas aisladamente, podrían parecer hechos inconexos o carentes de relevancia estratégica (Sanz-Caballero, 2023).

Asimismo, el estudio de este bloque permite superar visiones reduccionistas que tienden a identificar la guerra híbrida exclusivamente con la dimensión militar o, en sentido inverso, a tratar la desinformación como un problema meramente comunicativo. Una de las aportaciones centrales de este módulo es mostrar que las campañas de influencia, la presión económica, las operaciones cibernéticas, la instrumentalización del derecho, la explotación de fracturas sociales o la manipulación del debate público pueden formar parte de una misma arquitectura de acción estratégica. De este modo, el alumnado comprende que las amenazas híbridas no deben analizarse como incidentes aislados, sino como **procesos sistémicos de competencia y coerción.**

Desde una perspectiva docente, este bloque también cumple una función de **homogeneización conceptual**, especialmente relevante, dado el perfil heterogéneo del alumnado al que va dirigido el curso. Juristas, periodistas, diplomáticos, miembros de fuerzas armadas, responsables públicos o profesionales de la seguridad parten de lenguajes técnicos y tradiciones disciplinares diferentes. Por ello, el curso necesita un módulo inicial que establezca una base común sobre conceptos como *guerra híbrida, operaciones de influencia, competencia estratégica, vulnerabilidad social, resiliencia democrática o confrontación en la zona gris.* Sin esa base compartida, la posterior aproximación interdisciplinar correría el riesgo de fragmentarse en discursos paralelos sin verdadera integración metodológica.

En coherencia con esta finalidad, los contenidos del bloque -evolución del concepto de guerra híbrida, competencia estratégica en la zona gris e instrumentos de influencia política y comunicativa- no deben entenderse como una mera introducción teórica, sino como el **andamiaje intelectual del programa entero**. Su estudio permite al alumnado identificar la racionalidad estratégica que conecta el empleo del ciberespacio, la instrumentalización de narrativas, la presión sobre procesos democráticos y la explotación de debilidades institucionales. En consecuencia, este módulo no solo introduce el objeto de estudio, sino que configura la matriz interpretativa necesaria para comprender todos los demás.

Síntesis del Módulo

• Las amenazas híbridas combinan instrumentos políticos, informativos, tecnológicos, económicos y, en ocasiones, militares para explotar vulnerabilidades institucionales y sociales.

• Su análisis exige comprender la lógica estratégica que integra fenómenos aparentemente diversos como desinformación, presión económica, ciberoperaciones o manipulación política.

• Estas dinámicas suelen desarrollarse en la denominada **"zona gris"**, situada entre la paz y el conflicto armado tradicional.

• El estudio del concepto permite superar visiones reduccionistas que separan artificialmente la dimensión militar, comunicativa o tecnológica del conflicto contemporáneo.

• Este bloque proporciona el **marco conceptual común** necesario para un alumnado procedente de disciplinas y ámbitos profesionales diversos.

• Constituye el **andamiaje interpretativo del programa**, al ofrecer las categorías analíticas que permiten comprender el resto de los contenidos del curso.

El ciberespacio como dominio estratégico

La inclusión de un bloque específicamente dedicado al ciberespacio se justifica por el hecho de que, en el contexto contemporáneo, este constituye el **entorno operativo privilegiado** para el desarrollo, amplificación y sincronización de múltiples formas de amenaza híbrida. El ciberespacio no es únicamente una infraestructura técnica o un canal de comunicación, sino un espacio de interacción política, social y económica en el que convergen actores públicos y privados, plataformas digitales, sistemas automatizados, comunidades de usuarios y flujos masivos de información. Por ello, cualquier programa formativo sobre amenazas híbridas que no incorpore un análisis específico de este dominio quedaría sustancialmente incompleto (Arrese, 2024; Kozyreva et al., 2020).

La relevancia de este bloque radica, en primer lugar, en que el ciberespacio facilita la **baja visibilidad, la alta velocidad y el reducido coste de las operaciones de influencia y manipulación.** Las campañas de desinformación, las operaciones coordinadas de amplificación, el uso de cuentas automatizadas, la difusión de contenidos sintéticos o la segmentación estratégica de audiencias encuentran en el entorno digital un medio especialmente eficaz para multiplicar su alcance y dificultar su atribución. A diferencia de los mecanismos tradicionales de propaganda, las plataformas digitales permiten modular mensajes para públicos específicos, explotar dinámicas virales y operar de forma transnacional, todo ello con un grado de escalabilidad sin precedentes (Hwang et al., 2021; Salaverría et al., 2020).

En segundo lugar, este bloque resulta esencial porque las plataformas digitales no

son meros intermediarios neutrales, sino **estructuras sociotécnicas que condicionan la visibilidad, circulación y jerarquización de la información**. El funcionamiento de los algoritmos de recomendación, los sistemas de publicidad dirigida, los mecanismos de priorización de contenidos o las lógicas de monetización basadas en la atención afectan directamente a la forma en que los mensajes se propagan y adquieren relevancia pública. Comprender esta arquitectura es imprescindible para analizar cómo determinadas narrativas manipulativas logran amplificación, persistencia e impacto político (Ecker et al., 2022; Pennycook y Rand, 2021).

Además, el estudio del ciberespacio como dominio estratégico permite al alumnado advertir que muchas amenazas híbridas no dependen exclusivamente de la falsedad del contenido difundido, sino de la **explotación de vulnerabilidades estructurales del ecosistema digital**, tales como: opacidad algorítmica, fragmentación de audiencias, asimetrías informativas, desintermediación del debate público, facilidad de anonimización, automatización del comportamiento en red y escasa trazabilidad de determinados procesos de difusión. Desde esta perspectiva, la enseñanza sobre plataformas, algoritmos y arquitectura digital no cumple una función meramente técnica, sino que permite comprender por qué el entorno digital favorece determinadas formas de coerción e injerencia.

Este bloque es también imprescindible para formar profesionales que, desde ámbitos distintos, deberán interactuar con realidades tecnológicas que condicionan sus respectivas funciones. Un jurista necesita entender las lógicas técnicas mínimas que subyacen a la regulación de plataformas; un periodista debe conocer los mecanismos de amplificación y coordinación digital que afectan a la circulación de contenidos; un diplomático o un analista de seguridad debe ser capaz de interpretar la dimensión geopolítica de la infraestructura digital y su utilización estratégica por actores estatales y no estatales. En todos estos casos, el conocimiento del ciberespacio actúa como una **competencia transversal de alfabetización estratégica.**

Por ello, los contenidos del bloque -arquitectura técnica del ciberespacio, funcionamiento de plataformas digitales, algoritmos y amplificación de contenidos- están plenamente justificados dentro del programa. No se trata de añadir un componente tecnológico accesorio, sino de situar al alumnado ante el dominio en el que hoy se despliegan gran parte de las dinámicas híbridas. El módulo permite comprender no solo dónde ocurren muchas de estas operaciones, sino también por qué el ciberespacio altera profundamente sus formas, ritmos, escalas y efectos.

Síntesis del Módulo

• El ciberespacio se ha convertido en el principal entorno operativo para la ejecución y amplificación de amenazas híbridas y operaciones de influencia.

• Las plataformas digitales permiten desarrollar campañas de manipulación informativa con bajo coste, alta velocidad y gran alcance transnacional.

• Los algoritmos de recomendación, la publicidad dirigida y la arquitectura de las plataformas influyen decisivamente en la visibilidad y difusión de con-

tenidos.

• Muchas campañas de desinformación explotan **vulnerabilidades estructurales del ecosistema digital**, como la opacidad algorítmica o la fragmentación de audiencias.

• Comprender el funcionamiento técnico y sociopolítico de las plataformas es una competencia transversal para profesionales de distintos ámbitos institucionales.

• El estudio del ciberespacio permite explicar cómo la digitalización transforma las formas, ritmos y escalas de las operaciones de influencia.

Psicología y sociología de la desinformación

Este bloque se justifica porque las amenazas híbridas no persiguen únicamente alterar sistemas técnicos o interferir en procesos institucionales, sino influir sobre la **percepción, las emociones, las creencias y los comportamientos colectivos**. En consecuencia, el estudio de la desinformación no puede agotarse en el análisis del mensaje o del canal tecnológico; requiere también comprender los mecanismos psicológicos y sociológicos que explican por qué determinados contenidos manipulan con eficacia, se difunden con rapidez y producen efectos políticos o sociales relevantes (Ecker et al., 2022; Pennycook y Rand, 2021).

La inclusión de este módulo responde, en primer lugar, a la necesidad de superar una visión excesivamente instrumental o tecnocéntrica de la desinformación. Las campañas de manipulación informativa triunfan no solo por el uso de bots, plataformas o algoritmos, sino porque logran activar disposiciones cognitivas y emocionales preexistentes en los públicos destinatarios. Sesgos como el de confirmación, la heurística de disponibilidad, la percepción selectiva o la tendencia a aceptar información congruente con las propias creencias desempeñan un papel determinante en la recepción y circulación de mensajes manipulativos. Sin el estudio de estas dimensiones, el alumnado difícilmente podrá comprender por qué la mera rectificación factual suele resultar insuficiente frente a determinados procesos de polarización o radicalización narrativa (Kim et al., 2020; Sultan et al., 2024).

En segundo lugar, este bloque permite analizar la dimensión **colectiva y estructural** de la desinformación. Los contenidos manipulativos no operan en el vacío, sino en entornos sociales caracterizados por fragmentación del espacio público, crisis de confianza institucional, polarización afectiva, debilitamiento de autoridades epistémicas y transformación de las pautas de consumo informativo. Desde esta perspectiva, la sociología de la información y de la comunicación ofrece herramientas indispensables para comprender cómo se conforman comunidades interpretativas cerradas, cómo se consolidan las cámaras de eco o cómo determinadas narrativas se insertan en identidades políticas y culturales preexistentes (Arrese, 2024; Humprecht et al., 2020).

La justificación de este bloque se refuerza además por el hecho de que muchas amenazas híbridas explotan deliberadamente **fracturas sociales latentes**: tensiones territoriales, escisiones ideológicas, desconfianza hacia las élites, inseguridades culturales o agravios

percibidos. Las operaciones de influencia no necesitan inventar desde cero esas divisiones; les basta con intensificarlas, reencuadrarlas o utilizarlas para erosionar la cohesión democrática. Por ello, la formación en psicología y sociología de la desinformación resulta esencial para que el alumnado comprenda que la resiliencia frente a estas amenazas depende también de variables sociales profundas y no solo de mecanismos tecnológicos o regulatorios.

Desde el punto de vista profesional, este bloque tiene un valor añadido evidente para todos los perfiles destinatarios del curso. Para periodistas, permite entender mejor la dinámica de circulación y recepción de narrativas falsas o manipuladas. Para juristas y responsables públicos, ayuda a calibrar los límites y potencialidades de la regulación cuando el problema afecta a procesos sociales complejos y no solo a contenidos individualizables. Para fuerzas de seguridad, diplomáticos o analistas, facilita la comprensión del componente cognitivo de las operaciones híbridas. Para psicólogos y politólogos, ofrece un marco directamente conectado con sus respectivas áreas de especialización.

Los contenidos del bloque -sesgos cognitivos, polarización política y viralidad emocional de los contenidos digitales- se justifican porque permiten comprender la **dimensión antropológica y social de la amenaza híbrida**. Su función en el programa no es complementaria, sino central: explicar por qué ciertas narrativas encuentran terreno fértil, cómo se transforman en vectores de división y de influencia, y por qué la defensa frente a la desinformación exige actuar también sobre los factores de vulnerabilidad cognitiva y social que la hacen efectiva (Huang et al., 2024; Lewandowsky y Van der-Linden, 2021).

Síntesis del Módulo

• Las amenazas híbridas buscan influir sobre percepciones, creencias y emociones colectivas, por lo que requieren un análisis psicológico y sociológico.

• Los sesgos cognitivos y las heurísticas influyen decisivamente en la recepción y difusión de contenidos desinformativos.

• La polarización política y la fragmentación del espacio público favorecen la formación de **cámaras de eco y comunidades interpretativas cerradas.**

• Las campañas de manipulación informativa suelen explotar divisiones sociales preexistentes para intensificar tensiones políticas o identitarias.

• La comprensión de estos factores permite explicar por qué la refutación factual resulta a menudo insuficiente frente a determinadas narrativas manipulativas.

• Este bloque aporta una perspectiva interdisciplinar esencial para comprender la **dimensión cognitiva y social de las amenazas híbridas.**

Marco jurídico e institucional

La inclusión de un bloque dedicado al marco jurídico e institucional es imprescindible

porque las amenazas híbridas y las campañas de desinformación plantean problemas que no son solo estratégicos o tecnológicos, sino también profundamente **normativos, competenciales y de gobernanza democrática.** Cualquier programa formativo dirigido a juristas, responsables públicos, periodistas, diplomáticos o profesionales de la seguridad debe abordar necesariamente las preguntas relativas a qué instrumentos jurídicos son aplicables, qué competencias corresponden a cada nivel institucional, cuáles son los límites impuestos por los derechos fundamentales y cómo puede articularse una respuesta pública legítima y eficaz (Sanz-Caballero, 2023).

La necesidad de este bloque deriva, en primer lugar, de la propia naturaleza ambigua de las amenazas híbridas puesto que muchas de sus manifestaciones no encajan con facilidad en las categorías jurídicas tradicionales del uso de la fuerza, la agresión armada o incluso la injerencia clásica. Las operaciones de desinformación, las campañas de influencia, la manipulación de procesos electorales o ciertas ciberoperaciones de carácter no destructivo se sitúan frecuentemente en zonas de indeterminación normativa, lo que genera problemas de calificación, atribución de responsabilidad y activación de respuestas institucionales. Por ello, el alumnado debe familiarizarse con los debates contemporáneos sobre soberanía digital, responsabilidad internacional, atribución en el ciberespacio y protección de la integridad democrática.

En segundo lugar, este bloque resulta esencial porque la respuesta a la desinformación y a la manipulación informativa se encuentra atravesada por una tensión estructural entre, de un lado, la defensa de la seguridad, la integridad electoral y el orden democrático y, de otro, la garantía de la **libertad de expresión, el pluralismo informativo y otros derechos fundamentales**. Esta tensión convierte el análisis jurídico en una pieza central del programa: no basta con identificar riesgos, sino que es preciso determinar qué respuestas son compatibles con un Estado democrático de Derecho. En este sentido, la formación debe capacitar al alumnado para evitar tanto la infrarregulación ingenua como la sobrerreacción normativa incompatible con los principios constitucionales y europeos (Parlamento Europeo y Consejo de la Unión Europea, 2022; Sanz-Caballero, 2023).

Además, la dimensión institucional del bloque se justifica porque la gobernanza de estas amenazas es necesariamente **multinivel y multisectorial.** La regulación y la respuesta frente a la desinformación involucran a instituciones nacionales, a la Unión Europea, a plataformas digitales, a autoridades reguladoras, a organismos de supervisión electoral, a estructuras de ciberseguridad y a actores de la sociedad civil. Comprender esta arquitectura institucional resulta decisivo para formar profesionales capaces de moverse en entornos complejos de cooperación, coordinación y reparto competencial. De lo contrario, el análisis quedaría reducido a una abstracción académica desconectada de los marcos reales de toma de decisiones.

En el contexto europeo, además, la evolución normativa reciente ha convertido este bloque en particularmente necesario. La regulación de servicios digitales, la transparencia de la publicidad política, las políticas europeas frente a la manipulación informativa, las obligaciones de plataformas y las disposiciones relativas a contenidos sintéticos generados por inteligencia artificial son ya parte del entorno regulatorio en el que operan instituciones y profesionales. No incorporar estas materias supondría ofrecer una formación incompleta y poco adaptada a la realidad jurídica contemporánea (Comisión Europea, 2022; Parlamento

Europeo y Consejo de la Unión Europea, 2022, 2024a, 2024b).

Por ello, los contenidos del bloque -regulación internacional de las ciberoperaciones, políticas europeas frente a la desinformación y protección de los procesos democráticos- están plenamente justificados. Su función es dotar al alumnado de una **capacidad de encuadramiento jurídico e institucional** sin la cual no sería posible traducir el diagnóstico de las amenazas en propuestas de respuesta compatibles con el ordenamiento jurídico y con las exigencias de legitimidad propias de una democracia constitucional.

Síntesis del Módulo

• Las amenazas híbridas plantean desafíos jurídicos complejos relacionados con la atribución de responsabilidades y la calificación normativa de determinadas acciones.

• Muchas de estas actividades se sitúan en zonas de ambigüedad jurídica que dificultan la activación de mecanismos tradicionales de respuesta.

• La regulación frente a la desinformación debe equilibrar la protección de la seguridad democrática con el respeto a derechos fundamentales, como la libertad de expresión.

• La gobernanza de estas amenazas implica una arquitectura institucional multinivel y multisectorial, que incluye Estados, Unión Europea, plataformas digitales y sociedad civil.

• Las recientes iniciativas regulatorias europeas han reforzado la importancia del marco jurídico en la gestión de la manipulación informativa digital.

• Este bloque proporciona al alumnado herramientas para comprender las posibilidades y límites de la respuesta normativa frente a las amenazas híbridas.

Prevención y resiliencia institucional

Este bloque final se justifica porque un programa docente sobre amenazas híbridas no puede limitarse a la descripción del problema; debe orientarse también a la **acción preventiva, la preparación institucional y la construcción de resiliencia.** Las amenazas híbridas se caracterizan precisamente por explotar debilidades previas de los sistemas políticos y sociales. Por ello, una formación verdaderamente útil para profesionales debe capacitar no solo para identificar campañas de influencia o manipulación, sino para diseñar respuestas proporcionales, coordinadas y sostenibles (Lewandowsky y Van der-Linden, 2021; Roozenbeek et al., 2022).

La necesidad de este bloque deriva, en primer lugar, de que la mera detección de una campaña de desinformación o de una operación de injerencia no garantiza por sí sola una respuesta eficaz. Las instituciones necesitan capacidades de anticipación, mecanismos de alerta temprana, procedimientos de análisis, coordinación interinstitucional y estrategias

de comunicación pública capaces de reducir la vulnerabilidad del sistema. En este sentido, la prevención y la resiliencia no son complementos opcionales, sino el núcleo práctico de cualquier política seria frente a amenazas híbridas (Amazeen et al., 2022; Bertolotti y Catellani, 2023).

En segundo lugar, este bloque permite trasladar al plano operativo todo lo aprendido en los módulos anteriores. Si el alumnado ha adquirido un marco conceptual sobre amenazas híbridas, ha comprendido la centralidad del ciberespacio, ha analizado los factores psicológicos y sociales de la desinformación y conoce ya el marco jurídico e institucional aplicable, el siguiente paso lógico consiste en desarrollar capacidades para **transformar ese conocimiento en procedimientos de respuesta.** De ahí la importancia de incluir contenidos como análisis de inteligencia, OSINT y comunicación estratégica, que actúan como puentes entre la comprensión académica del fenómeno y su gestión práctica (Guess et al., 2020; Moore y Hancock, 2022).

La inclusión del **análisis de inteligencia** se justifica porque las amenazas híbridas suelen manifestarse a través de señales fragmentarias, ambiguas o aparentemente inconexas. Su detección exige metodologías sistemáticas de recogida, evaluación e interpretación de información. A su vez, la formación en OSINT resulta particularmente pertinente en el entorno digital actual, en el que una parte significativa de los indicios relevantes se encuentra en fuentes abiertas, redes sociales, bases de datos públicas, repositorios digitales o trazas accesibles en línea. Capacitar al alumnado en estas herramientas incrementa su autonomía analítica y su capacidad para contrastar, contextualizar y evaluar evidencias.

Por otra parte, el énfasis en la comunicación estratégica está plenamente justificado porque muchas respuestas institucionales fracasan no por ausencia de información, sino por incapacidad para **comunicar de forma creíble, oportuna y coherente**. En contextos de manipulación informativa, el silencio institucional, la reacción improvisada o la contradicción entre actores públicos pueden agravar el impacto de la campaña hostil. En consecuencia, este bloque debe enseñar que la resiliencia no depende únicamente de la capacidad de refutar falsedades, sino también de la construcción de confianza, la coherencia narrativa, la transparencia y la preparación comunicativa de las organizaciones (DiResta, 2024; Van der-Linden, 2023).

Finalmente, este módulo resulta esencial porque orienta el programa hacia su objetivo último: la formación de profesionales capaces de contribuir al fortalecimiento de la **resiliencia democrática e institucional**. La resiliencia, en este contexto, no debe entenderse como mera resistencia pasiva, sino como la capacidad de anticipar, absorber, adaptarse y responder a presiones híbridas sin comprometer los principios constitucionales ni la funcionalidad de las instituciones. Por ello, los contenidos del bloque no solo tienen una dimensión técnica, sino también una clara proyección cívica e institucional.

En suma, la presencia de este apartado en el programa se justifica porque convierte la propuesta formativa en una herramienta orientada a capacidades reales de prevención y respuesta. Los contenidos incluidos -análisis de inteligencia, OSINT y diseño de estrategias de comunicación estratégica- permiten cerrar coherentemente el itinerario formativo, integrando conocimiento conceptual, análisis crítico y aplicación profesional.

Síntesis del Módulo

• La respuesta eficaz a las amenazas híbridas requiere no solo capacidad de detección, sino también estrategias de prevención y fortalecimiento institucional.

• Las políticas de resiliencia buscan reducir vulnerabilidades estructurales y mejorar la capacidad de anticipación frente a campañas de influencia.

• El análisis de inteligencia permite interpretar señales fragmentarias y detectar patrones asociados a operaciones híbridas.

• Las herramientas de **OSINT** resultan especialmente relevantes en el entorno digital para el análisis de información procedente de fuentes abiertas.

• La comunicación estratégica es un elemento clave para contrarrestar narrativas manipulativas y preservar la confianza pública.

• Este bloque orienta el programa hacia su objetivo final: formar profesionales capaces de contribuir al fortalecimiento de la **resiliencia democrática e institucional.**

En conjunto, los cinco bloques temáticos responden a una lógica de progresión pedagógica que va desde la comprensión conceptual del fenómeno hasta la adquisición de capacidades aplicadas de análisis y respuesta. Esta secuencia permite evitar aproximaciones fragmentarias y dota al programa de una coherencia interna especialmente adecuada para un alumnado profesional y multidisciplinar, que necesita integrar marcos teóricos, comprensión normativa y herramientas operativas en un único itinerario formativo.

Con el fin de sintetizar la lógica pedagógica del programa y la relación entre los distintos bloques formativos, la tabla siguiente presenta la estructura del curso, su justificación y las competencias que se pretenden desarrollar en cada uno de los módulos.

Tabla 2. Estructura del curso, justificación, competencias y contenidos

Bloque formativo	Justificación pedagógica	Competencias que desarrolla	Contenidos principales
1. Fundamentos de las amenazas híbridas	Proporciona el marco conceptual necesario para comprender la lógica estratégica que integra fenómenos como la desinformación, las operaciones de influencia o las ciberacciones dentro de dinámicas de confrontación en la "zona gris". Permite además establecer una base conceptual común para un alumnado interdisciplinar.	Comprensión estratégica del fenómeno; capacidad de identificar dinámicas de amenaza híbrida; análisis de vulnerabilidades institucionales.	Evolución del concepto de guerra híbrida; competencia estratégica en la zona gris; instrumentos de influencia política, informativa y económica.

Bloque formativo	Justificación pedagógica	Competencias que desarrolla	Contenidos principales
2. El ciberespacio como dominio estratégico	Analiza el papel central del entorno digital como espacio operativo para la amplificación y coordinación de campañas de desinformación y manipulación informativa. Permite comprender cómo la arquitectura tecnológica condiciona la difusión de contenidos y las dinámicas de influencia.	Alfabetización estratégica en el entorno digital; análisis del funcionamiento de plataformas; comprensión de dinámicas de amplificación algorítmica.	Arquitectura técnica del ciberespacio; funcionamiento de plataformas digitales; algoritmos y sistemas de recomendación; difusión y viralización de contenidos.
3. Psicología y sociología de la desinformación	Permite comprender los mecanismos cognitivos y sociales que facilitan la eficacia de las campañas de manipulación informativa. Analiza cómo sesgos cognitivos, polarización política y fragmentación del espacio público influyen en la circulación de narrativas manipulativas.	Análisis crítico del impacto social de la desinformación; comprensión de procesos de polarización y viralidad emocional; interpretación de dinámicas sociopolíticas del ecosistema informativo.	Sesgos cognitivos; formación de cámaras de eco; polarización política; factores emocionales en la viralización de contenidos digitales.
4. Marco jurídico e institucional	Aborda los desafíos normativos y de gobernanza asociados a las amenazas híbridas y a la manipulación informativa. Permite analizar las posibilidades y límites de la respuesta jurídica en contextos en los que confluyen seguridad democrática y derechos fundamentales.	Interpretación del marco normativo aplicable; comprensión de la gobernanza multinivel; análisis jurídico de políticas públicas frente a la desinformación.	Regulación internacional de ciberoperaciones; políticas europeas frente a la desinformación; protección de procesos democráticos; responsabilidades de plataformas digitales.
5. Prevención y resiliencia institucional	Orienta el programa hacia la dimensión aplicada del problema, proporcionando herramientas para la detección temprana y la respuesta institucional frente a campañas de manipulación informativa y operaciones híbridas.	Análisis estratégico; uso de herramientas OSINT; diseño de estrategias de comunicación institucional; elaboración de informes de riesgo.	Metodologías de análisis de inteligencia; OSINT; sistemas de alerta temprana; comunicación estratégica y gestión institucional de crisis informativas.

Fuente: Elaboración propia

Discusión

Beneficios esperados de la implementación del programa

La implementación de un programa formativo como el propuesto puede generar diversos beneficios en el ámbito académico, institucional y social.

En primer lugar, contribuye a **reducir el déficit formativo existente en relación con las amenazas híbridas y la desinformación,** proporcionando a los profesionales herramientas analíticas para comprender fenómenos complejos que afectan al funcionamiento de los sistemas democráticos (Apuke et al., 2023; Huang et al., 2024).

En segundo lugar, el carácter interdisciplinar del programa favorece el desarrollo de **espacios de aprendizaje compartido entre profesionales de distintos sectores**, lo que resulta especialmente relevante en el ámbito de la seguridad y de la gobernanza democrática.

En tercer lugar, la utilización de metodologías activas, como las simulaciones de crisis híbridas o el análisis de campañas reales, facilita la **transferencia de conocimientos entre el ámbito académico y el profesional**, reforzando la utilidad práctica de la formación (Yang et al., 2021; Zhang et al., 2022).

Finalmente, este tipo de programas puede contribuir a fortalecer la **resiliencia institucional frente a operaciones de manipulación informativa**, al promover una comprensión crítica del ecosistema informativo digital y de los mecanismos utilizados para influir en la opinión pública (Basol et al., 2021; Hwang et al., 2021).

Conclusiones

La naturaleza multidimensional de las amenazas exige una formación interdisciplinar. Las amenazas híbridas, las campañas de desinformación, las operaciones de influencia y las distintas formas de manipulación informativa constituyen fenómenos complejos, transnacionales y tecnológicamente mediados que pueden afectar a la estabilidad institucional, la cohesión social y el funcionamiento de los sistemas democráticos. Su análisis no puede realizarse adecuadamente desde una única disciplina, puesto que en estas dinámicas confluyen factores estratégicos, tecnológicos, jurídicos, comunicativos, psicológicos, sociales y políticos. En consecuencia, su tratamiento formativo requiere integrar conocimientos y métodos procedentes de diferentes áreas académicas y profesionales.

La formación universitaria existente presenta una fragmentación que dificulta la comprensión integral del fenómeno. Las amenazas híbridas y la desinformación suelen abordarse separadamente desde ámbitos como la seguridad internacional, la comunicación política, la ciberseguridad, el derecho o la psicología social. Esta compartimentación puede impedir que el alumnado comprenda que las campañas de manipulación informativa forman parte, en determinados casos, de estrategias más amplias en las que se combinan instrumentos políticos, informativos, tecnológicos, económicos y psicológicos. Resulta necesario, por tanto, avanzar hacia modelos docentes capaces de relacionar estas dimensiones dentro de un marco analítico común.

El modelo propuesto responde a esa necesidad mediante la combinación de interdisciplinariedad, aprendizaje aplicado y orientación institucional. La interdisciplinariedad permite integrar aportaciones de los estudios estratégicos, el derecho, la ciberseguridad, la comunicación, la psicología social y el análisis de inteligencia. El aprendizaje aplicado

facilita la transferencia de los conocimientos teóricos a contextos profesionales mediante estudios de caso, actividades de verificación digital, ejercicios de inteligencia de fuentes abiertas, simulaciones de crisis y prácticas de comunicación estratégica. La orientación institucional vincula la formación con las capacidades de prevención, detección, coordinación y respuesta que requieren las organizaciones públicas y privadas.

La principal aportación del trabajo es la formulación de un itinerario pedagógico progresivo y coherente. Los cinco bloques propuestos -fundamentos de las amenazas híbridas; ciberespacio como dominio estratégico; psicología y sociología de la desinformación; marco jurídico e institucional; y prevención y resiliencia institucional- articulan una secuencia que parte de la comprensión conceptual del fenómeno y culmina con el desarrollo de capacidades aplicadas. Esta organización permite relacionar el conocimiento estratégico con el análisis tecnológico, social y jurídico, evitando una acumulación de contenidos desconectados entre sí.

El programa resulta especialmente adecuado para un alumnado profesional y multidisciplinar. Juristas, periodistas, diplomáticos, miembros de las fuerzas armadas y de seguridad, analistas, responsables públicos, politólogos, psicólogos o especialistas en comunicación parten de lenguajes técnicos y tradiciones metodológicas diferentes. La creación de una base conceptual común y la realización de actividades compartidas pueden favorecer una cultura de cooperación interdisciplinar e interinstitucional, necesaria para hacer frente a amenazas que atraviesan sectores, competencias y niveles territoriales distintos.

La formación debe incorporar los límites jurídicos y democráticos de la respuesta frente a la desinformación. La protección de la integridad institucional y de los procesos democráticos no puede justificar medidas indiscriminadas que restrinjan desproporcionadamente la libertad de expresión, el pluralismo informativo u otros derechos fundamentales. La formación especializada debe capacitar para distinguir entre información falsa o engañosa, propaganda, opinión legítima, error, discurso protegido y operaciones coordinadas de manipulación. Asimismo, debe proporcionar criterios para valorar la legalidad, necesidad y proporcionalidad de las actuaciones de los poderes públicos, las plataformas digitales y los demás actores implicados.

La prevención y la resiliencia institucional deben ocupar una posición central en el proceso formativo. La respuesta frente a la manipulación informativa no puede limitarse a la refutación posterior de contenidos falsos. Las organizaciones necesitan desarrollar sistemas de alerta temprana, metodologías de análisis de inteligencia, capacidades de verificación, protocolos de coordinación y estrategias de comunicación previamente definidas. La formación puede contribuir a sustituir una actuación exclusivamente reactiva por una política de preparación institucional orientada a anticipar riesgos, reducir vulnerabilidades y preservar la confianza pública.

La propuesta puede contribuir al fortalecimiento de la resiliencia democrática, aunque no permite todavía acreditar empíricamente dicho efecto. El programa está diseñado para mejorar la capacidad de los profesionales para identificar señales relevantes, contextualizar campañas informativas, analizar actores, objetivos y técnicas, valorar las implicaciones jurídicas y formular respuestas institucionales proporcionadas. Sin embargo, la

relación entre formación especializada y aumento efectivo de la resiliencia democrática deberá verificarse mediante la implementación y evaluación del programa en contextos académicos y profesionales concretos.

El carácter conceptual y propositivo del estudio constituye su principal limitación metodológica. El modelo curricular no ha sido todavía aplicado de forma completa a una cohorte determinada ni se han medido empíricamente los resultados de aprendizaje obtenidos. Por esta razón, el trabajo no pretende establecer relaciones causales entre la participación en el programa y la mejora de las capacidades institucionales. Su aportación se sitúa en el diseño fundamentado de una propuesta formativa susceptible de implantación, evaluación y revisión posterior.

Las futuras investigaciones deberán centrarse en la validación empírica y en la adaptación del modelo. Resultaría conveniente desarrollar experiencias piloto, definir indicadores de aprendizaje y comparar las competencias del alumnado antes y después de la formación. También sería pertinente evaluar la eficacia relativa de metodologías como las simulaciones, los estudios de caso, los laboratorios de verificación o los ejercicios de inteligencia de fuentes abiertas. El modelo podría, además, adaptarse a perfiles profesionales específicos, diferentes contextos nacionales y modalidades de formación continua.

La educación superior debe considerarse una capacidad estratégica frente a la manipulación informativa. Su función no consiste únicamente en transmitir conocimientos sobre amenazas emergentes, sino en formar profesionales capaces de integrar información fragmentaria, evaluar críticamente narrativas y evidencias, aplicar el marco jurídico correspondiente y diseñar respuestas institucionales legítimas y eficaces. La incorporación de programas especializados de esta naturaleza puede contribuir al fortalecimiento de la autonomía analítica, la anticipación, la cooperación interinstitucional y la resiliencia democrática frente a las formas contemporáneas de injerencia y competencia estratégica en el entorno digital.

Declaración obligatoria de uso de IAGen

El autor declara que no se utilizaron herramientas de inteligencia artificial generativa en la elaboración de este manuscrito.

Referencias

Amazeen, M. A., Krishna, A. y Eschmann, R. (2022). Cutting the bunk: Comparing the solo and aggregate effects of prebunking and debunking COVID-19 vaccine misinformation. *Science Communication, 44*(4), 387-417. https://doi.org/10.1177/10755470221111558

Apuke, O. D., Omar, B. y Tunca, E. A. (2023). Literacy concepts as an intervention strategy for improving fake news knowledge, detection skills, and curtailing the tendency to share fake news in Nigeria. *Child & Youth Services, 44*(1), 88-103. https://doi.org/10.1080/0145935X.2021.2024758

Arrese, Á. (2024). Cultural dimensions of fake news exposure: A cross-national analysis among European Union countries. *Mass Communication and Society, 27*(5), 827-850. https://doi.org/10.1080/15205436.2022.2123278

Basol, M., Roozenbeek, J., Berriche, M., Uenal, F., McClanahan, W. P. y Van der-Linden, S. (2021). Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation. *Big Data & Society, 8*(1), 1-18. https://doi.org/10.1177/20539517211013868

Basol, M., Roozenbeek, J. y Van der-Linden, S. (2020). Good news about bad news: Gamified inoculation boosts confidence and cognitive immunity against fake news. *Journal of Cognition, 3*(1), 1-9. https://doi.org/10.5334/joc.91 PMid:31934684 PMCid:PMC6952868

Bertolotti, M. y Catellani, P. (2023). Counterfactual thinking as a prebunking strategy to contrast misinformation on COVID-19. *Journal of Experimental Social Psychology, 104*. https://doi.org/10.1016/j.jesp.2022.104404

Comisión Europea. (16 de junio de 2022). *The strengthened code of practice on disinformation.* digital-strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

DiResta, R. (2024). *Invisible rulers: The people who turn lies into reality*. PublicAffairs.

Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., Kendeou, P., Vraga, E. K. y Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology, 1,* 13-29. https://doi.org/10.1038/s44159-021-00006-y PMCid:PMC9049321

Freelon, D. y Wells, C. (2020). Disinformation as political communication. *Political Communication, 37*(2), 145-156. https://doi.org/10.1080/10584609.2020.1723755

Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J. y Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences, 117*(27), 15536-15545. https://doi.org/10.1073/pnas.1920498117 PMid:32571950 PMCid:PMC7355018

Huang, G., Jia, W. y Yu, W. (2024). Media literacy interventions improve resilience to misinformation: A meta-analytic investigation of overall effect and moderating factors. *Communication Research.* https://doi.org/10.1177/00936502241288103

Humprecht, E., Esser, F. y Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. *The International Journal of Press/Politics, 25*(3), 493-516. https://doi.org/10.1177/1940161219900126

Hwang, Y., Ryu, J. Y. y Jeong, S.-H. (2021). Effects of disinformation using deepfake:

The protective effect of media literacy education. *Cyberpsychology, Behavior, and Social Networking, 24*(3), 188-193. https://doi.org/10.1089/cyber.2020.0174 PMid:33646021

Kim, H. K., Ahn, J., Atkinson, L. y Kahlor, L. A. (2020). Effects of COVID-19 misinformation on information seeking, avoidance, and processing: *A multi-country comparative study. Science Communication, 42*(5), 586-615. https://doi.org/10.1177/1075547020959670 PMid:38603002 PMCid:PMC7492825

Kozyreva, A., Lewandowsky, S. y Hertwig, R. (2020). Citizens versus the Internet: Confronting digital challenges with cognitive tools. *Psychological Science in the Public Interest, 21*(3), 103-156. https://doi.org/10.1177/1529100620946707 PMid:33325331 PMCid:PMC7745618

Lewandowsky, S. y Van der-Linden, S. (2021). Countering misinformation and fake news through inoculation and prebunking. *European Review of Social Psychology, 32*(2), 348-384. https://doi.org/10.1080/10463283.2021.1876983

Moore, R. C. y Hancock, J. T. (2022). A digital media literacy intervention for older adults improves resilience to fake news. *Scientific Reports, 12.* https://doi.org/10.1038/s41598-022-08437-0 PMid:35397631 PMCid:PMC8994776

Parlamento Europeo y Consejo de la Unión Europea. (19 de octubre de 2022). *Reglamento (UE) 2022/2065, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).* Diario Oficial de la Unión Europea, L 277, 1-102. eur-lex.europa.eu. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Parlamento Europeo y Consejo de la Unión Europea. (13 de marzo de 2024a). *Reglamento (UE) 2024/900, sobre transparencia y segmentación en la publicidad política.* Diario Oficial de la Unión Europea. eur-lex.europa.eu. https://eur-lex.europa.eu/eli/reg/2024/900/oj

Parlamento Europeo y Consejo de la Unión Europea. (13 de junio de 2024b). *Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828.* Diario Oficial de la Unión Europea. eur-lex.europa.eu. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Pennycook, G. y Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences, 25*(5), 388-402. https://doi.org/10.1016/j.tics.2021.02.007 PMid:33736957 PMCid:PMC11135712

Roozenbeek, J., Van der-Linden, S., Goldberg, B., Rathje, S. y Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on

social media. *Science Advances, 8*(34), eabo6254. https://doi.org/10.1126/sciadv.abo6254 PMid:36001675 PMCid:PMC9401631

Salaverría, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I. y Erviti, M. C. (2020). Desinformación en tiempos de pandemia: tipología de los bulos sobre la COVID-19. *El profesional de la información, 29*(3), e290315. https://doi.org/10.3145/epi.2020.may.15

Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications, 10*. https://doi.org/10.1057/s41599-023-01864-y

Sultan, M., Tump, A. N., Ehmann, N., Lorenz-Spreen, P., Hertwig, R., Gollwitzer, A. y Kurvers R. H. J. M. (2024). Susceptibility to online misinformation: A systematic meta-analysis of demographic and psychological factors. *Proceedings of the National Academy of Sciences, 121*(47), e2409329121. https://doi.org/10.1073/pnas.2409329121 PMid:39531500 PMCid:PMC11588074

Tuñón-Navarro, J., Oleart, A. y Bouza-García, L. (2019). Actores europeos y desinformación la disputa entre el factchecking, las agendas alternativas y la geopolítica. *Revista de comunicación, 18*(2), 245-260. https://dialnet.unirioja.es/servlet/articulo?codigo=7039215 https://doi.org/10.26441/RC18.2-2019-A12

Van der-Linden, S. (2023). *Foolproof: Why misinformation infects our minds and how to build immunity.* W. W. Norton & Company.

Wuyckens, G., Landry, N. y Fastrez, P. (2022). Untangling media literacy, information literacy, and digital literacy: A systematic meta-review of core concepts in media education. *Journal of Media Literacy Education, 14*(1), 168-182. https://doi.org/10.23860/JMLE-2022-14-1-12

Yang, S., Lee, J. W., Kim, H.-J., Kang, M., Chong, E. y Kim, E.-M. (2021). Can an online educational game contribute to developing information literate citizens? *Computers & Education, 161*, 104057. https://doi.org/10.1016/j.compedu.2020.104057

Zhang, L., Iyendo, T. O., Apuke, O. D. y Gever, V. C. (2022). Experimenting the effect of using visual multimedia intervention to inculcate social media literacy skills to tackle fake news. *Journal of Information Science. 51*(1), 135-145. https://doi.org/10.1177/01655515221131797

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web:https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Carlos Galán-Cordero es Doctor en Derecho de la Universidad Carlos III de Madrid (España), Magíster en Relaciones Internacionales y Comunicación de la Universidad Camilo Jose Cela (España), Licenciado en Derecho de la Universidad Autónoma de Madrid (España), es profesor de la Universidad Carlos III de Madrid, de la Universidad Oberta de Catalunya y de la Universidad Internacional de la Rioja (España), es experto en Ciberamenazas y Ciberinteligencia por la Universidad Pablo de Olavide de Sevilla (España), es Director de la Maestría en Análisis de Inteligencia y Ciberinteligencia de la Universidad Nebrija (España), es Director del Área de Amenazas Híbridas de la Agencia de Tecnología Legal y miembro del Grupo de Trabajo sobre Desinformación del Departamento de Seguridad Nacional de la Presidencia del Gobierno de España.

https://orcid.org/0009-0006-3858-1666 - Contacto: cgalan@nebrija.es

Esta página queda intencionalmente en blanco

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Las reformas de la Ley de inteligencia y contrainteligencia en Colombia: vacíos e importancia

Autor

Lina María Barrera-Quiroga
https://orcid.org/0009-0002-8901-0928
✉ lina.mbq01@gmail.com
Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Colombia

Citación APA: Barrera-Quiroga, L. M. (2026). Las reformas de la Ley de inteligencia y contrainteligencia en Colombia: vacíos e importancia. *Perspectivas en Inteligencia, 18*(27), 51-71. http://doi.org/10.47961/2145194X.858

Publicado en línea: 2026

Los artículos publicados por la Revista Científica Perspectivas en Inteligencia son de acceso abierto bajo una licencia **Creative Commons: Atribución - No Comercial – Sin Derivados.**

Para enviar un artículo:
https://revistaseditorialejc.org/index.php/pei/about/submissions

Esta página queda intencionalmente en blanco

PERSPECTIVAS EN INTELIGENCIA 2026

Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 18, N° 27, enero - junio 2026, pp. 51-71
http://doi.org/10.47961/2145194X.858

Las reformas de la Ley de inteligencia y contrainteligencia en Colombia: vacíos e importancia

Reforms to Colombia's intelligence and counterintelligence Law: gaps and significance

Lina María Barrera-Quiroga[1]

(1) Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Bogotá, D. C., Colombia.
✉ lina.mbq01@gmail.com

Resumen

La inteligencia y la contrainteligencia constituyen funciones estratégicas del Estado orientadas a la protección de la seguridad nacional, la defensa del orden constitucional y la prevención de amenazas. En Colombia, la Ley Estatutaria 1621 de 2013 estableció el marco jurídico que regula estas actividades bajo principios de legalidad, necesidad, proporcionalidad y control democrático. Sin embargo, recientes iniciativas de reforma han planteado modificaciones dirigidas a fortalecer la protección de los derechos fundamentales y los mecanismos de supervisión, sin un análisis integral de sus efectos sobre la gobernanza y la eficacia del sistema de inteligencia.

Este artículo realiza un análisis crítico de las reformas propuestas a la Ley Estatutaria 1621 de 2013, con el propósito de identificar los vacíos normativos que estas generan o profundizan y sus implicaciones para el control democrático y la operatividad de la inteligencia estatal. La investigación adopta un enfoque cualitativo basado en el análisis documental de marcos normativos, fuentes académicas y disposiciones legales vigentes. Los hallazgos evidencian que algunas reformas introducen ambigüedades normativas, debilitan el principio de reserva y afectan la seguridad jurídica de los agentes. Se concluye que, aunque las iniciativas buscan fortalecer las garantías democráticas, su diseño puede afectar la efectividad operativa del sistema y generar tensiones entre la protección de derechos y las necesidades de seguridad del Estado.

Clasificación JEL: G38, H56.

Palabras clave: inteligencia estratégica; contrainteligencia; Ley 1621 de 2013; reformas normativas; control democrático; gobernanza.

Fecha de recepción: 17/04/2026 | Fecha de aprobación: 29/07/2026

Abstract

Intelligence and counterintelligence are strategic functions of the State aimed at protecting national security and the constitutional order. In Colombia, Statutory Law 1621 of 2013 established the legal framework for these activities under the principles of legality, proportionality, and democratic control. However, in recent years, several reform initiatives have been introduced, ostensibly aimed at strengthening the protection of fundamental rights and oversight mechanisms, without a comprehensive analysis of their effects on the governance and effectiveness of the intelligence system.

This article provides a critical analysis of the proposed reforms to Statutory Law 1621 of 2013, with the aim of identifying the regulatory gaps that these reforms create or exacerbate, as well as their implications for democratic oversight and the operational effectiveness of state intelligence. The research adopts a qualitative approach based on a documentary analysis of regulatory frameworks, academic sources, and current legal provisions. The findings show that some reforms introduce regulatory ambiguities, undermine the principle of reserve, and affect the legal certainty of the parties involved. It is concluded that, although these initiatives seek to strengthen democratic safeguards, their design may affect the system's operational effectiveness and create tensions between the protection of rights and the state's security needs.

Keywords: strategic intelligence; counterintelligence; Law 1621 of 2013; legal reforms; democratic oversight; governance.

Introducción

La inteligencia y la contrainteligencia instauran pilares estratégicos de la seguridad nacional, específicamente en un contexto como el colombiano, representados por la persistencia de amenazas complejas y multidimensionales, entre ellos el crimen organizado transnacional, el terrorismo, las economías ilícitas, los ciberataques y las disputas territoriales internas. En este caso, la producción de inteligencia estratégica resulta esencial no solo para el adelantamiento de riesgos y la neutralización de amenazas, sino también para la enunciación de políticas públicas de seguridad, la toma de decisiones estratégicas y la protección del orden constitucional (Hernández-Estupiñán, 2020). Por ende, los sistemas de inteligencia no se limitan a una función operativa, sino que se fortalecen como instrumentos centrales de la gobernanza estatal en contextos de alta incertidumbre y riesgo, tal como lo señalan Gill y Phythian (2018) en su análisis sobre el papel de la inteligencia en los Estados contemporáneos.

La difusión de la Ley Estatutaria 1621 de 2013 representó un hito en la regulación de estas actividades en Colombia, al instaurar un marco jurídico orientado a nivelar la eficacia operativa de los organismos de inteligencia con el respeto por los derechos esenciales, el principio de legalidad y el fortalecimiento del control democrático. Esta Ley inquirió superar vacíos normativos históricos mediante la definición de principios rectores, límites funcionales, mecanismos de control institucional y garantías para el amparo de la información y los datos personales. La Ley Estatutaria 1621 de 2013 significó un progreso importante en la institucionalización de la actividad de inteligencia dentro del Estado Social de Derecho.

Sin embargo, a más de una década de su entrada en vigor, su ejecución ha probado limitaciones estructurales en materia de gobernanza, supervisión efectiva y aplicación tecnológica. En particular se han identificado debilidades en los mecanismos de supervisión parlamentaria, derivadas de irregularidades técnicas e informacionales entre los organismos de inteligencia y las instancias de control político, lo que ha limitado la capacidad de ejercer un control valioso sobre estas actividades. También, la limitada transparencia en los métodos de rendición de cuentas, la escasa regulación sobre el tratamiento y depuración de datos personales, y la ausencia de lineamientos normativos claros frente al uso de conocimientos emergentes, como la inteligencia artificial, el análisis masivo de datos y la ciberinteligencia, han forjado nuevos desafíos jurídicos y operativos.

Desde el punto de vista institucional y jurisprudencial, la Corte Constitucional ha repetido que las actividades de inteligencia se han desarrollado bajo estrictos principios de legalidad, necesidad, proporcionalidad y finalidad legítima, exponiendo simultáneamente la importancia de resguardar la reserva estratégica como condición para la validez operativa del Estado. Dicha tensión estructural entre la protección de los derechos fundamentales y la eficacia estratégica de la inteligencia establece uno de los principales desafíos en la configuración de su marco normativo. En esta línea, Casal-Oubiña et al. (2025) destacan que el equilibrio entre control democrático y eficacia operativa es un elemento esencial en los sistemas de inteligencia de Estados democráticos. Adicionalmente, los antecedentes institucionales y los debates legislativos recientes han justificado la necesidad de mejorar los mecanismos de control, supervisión técnica y seguridad jurídica, a fin de avalar que estas actividades se desarrollen dentro de los límites constitucionales sin complicar su capacidad anticipativa.

Como réplica a estas falencias, se han originado diversas iniciativas legislativas ubicadas a reformar el régimen jurídico vigente, destacándose entre ellas el Proyecto de Ley Estatutaria No. 225 de 2024 Senado, que formula modificaciones importantes en materia de control judicial, protección de datos, uso de tecnologías emergentes, optimización de mecanismos de supervisión y restructuración conceptual de los fines de la inteligencia (López-Obregón, 2024). Estas modificaciones se alinean con tendencias internacionales que buscan modernizar los métodos de inteligencia bajo principios de control democrático y rendición de cuentas, como lo señalan Sansó-Rubert Pascual y Pulido-Gragera (2022) en relación con la supervisión efectiva de los servicios de inteligencia en Estados democráticos.

No obstante, el actual artículo sustenta que varias de las reformas planteadas, si bien parten de un análisis legítimo sobre la necesidad de mejorar los dispositivos de control y supervisión, no solucionan de manera efectiva los problemas estructurales identificados y, en unos casos, pueden implantar nuevas imprecisiones normativas, las cuales pueden generar dilemas jurídicos afectando la gobernanza y operatividad del sistema de inteligencia. Especialmente, el incremento de los mecanismos de control sin el oportuno fortalecimiento de las capacidades técnicas de supervisión, la implementación de regulaciones normativas expresadas en términos generales y la reformulación de conceptos importantes sin criterios operativos claros pueden inquietar la seguridad jurídica de los agentes, disminuir la eficacia anticipativa del sistema y generar tensiones entre los principios de legalidad, eficacia y proporción. Los autores (Kniep et al., 2024), advierten que los sistemas de inteligencia en

democracias contemporáneas enfrentan una tensión estructural permanente entre el control institucional y la necesidad de mantener capacidades operativas efectivas.

El problema central no radica en la insuficiencia de reformar el marco normativo vigente, sino en la capacidad, coherencia y viabilidad de las reformas propuestas frente a los principios de gobernanza democrática, seguridad jurídica y eficacia estratégica que deben presidir las actividades de inteligencia en un Estado constitucional. La reforma normativa de este sector requiere una orientación que no solo defienda las garantías institucionales, sino que también salvaguarde la capacidad funcional del Estado para predecir, prevenir y neutralizar amenazas complejas en entornos importantes y dinámicos, en relación con los planteamientos de Gill y Phythian (2018) sobre el rol estructural de la inteligencia en la seguridad estatal contemporánea.

Con el propósito de respaldar esta tesis, el trabajo se organiza en cuatro partes principales. Para comenzar, se despliega el marco teórico y conceptual sobre inteligencia estratégica, gobernanza y control democrático, con la intención de instaurar los criterios analíticos que ubica el estudio. En segundo lugar, se observa el desarrollo normativo de la Ley Estatutaria 1621 de 2013 y la eficacia de las reformas planteadas en el Proyecto de Ley Estatutaria 225 de 2024. En tercer lugar, se inspeccionan los vacíos normativos persistentes y las contradicciones jurídicas, institucionales y estratégicas de las reformas, concretamente en relación con la defensa de los derechos fundamentales, la reserva legal, la seguridad jurídica de los agentes y la eficacia operativa del sistema.

De manera final, se ostentan las conclusiones y se manifiestan lineamientos orientados a robustecer la gobernanza, el control democrático y la seguridad jurídica, sin implicar la capacidad estratégica del Estado en materia de inteligencia y contrainteligencia, siguiendo una lógica de análisis estructurado coherente con diseños de investigación cualitativa (Creswell, 2014; Herrera-Rodríguez et al., 2015).

Las actividades de inteligencia y contrainteligencia cumplen una función estratégica dentro del Estado, puesta a la protección de la seguridad nacional, la soberanía y el orden constitucional. En Colombia, la Ley Estatutaria 1621 de 2013 significó un avance importante al establecer principios rectores, límites legales y mecanismos de control democrático, en respuesta a la crisis de legitimidad generada por los abusos cometidos por organismos de inteligencia en etapas anteriores. Sin embargo, a pesar de este desarrollo normativo, diversas reformas e iniciativas posteriores han intentado ajustar su alcance y funcionamiento legislativos presentadas en los últimos años y han sido justificadas bajo el argumento de fortalecer la protección de los derechos humanos y la transparencia, sin que exista un análisis riguroso de sus efectos reales sobre la eficacia, la reserva y la operatividad de la inteligencia estatal. Como advierte González-Cussac (2016), una norma excesivamente restrictiva o ambigua puede disminuir la capacidad preventiva del Estado y perturbar la función estratégica de la inteligencia.

Bajo esta perspectiva, el afianzamiento del marco normativo no puede deducirse únicamente como el incremento de controles formales, sino como la edificación de un sistema ligado a la gobernanza que combine legalidad, eficacia y legitimidad democrática. En la literatura sobre el tema se ha señalado que algunas reformas propuestas a la Ley Estatutaria

1621 de 2013 no solo buscan ajustar su funcionamiento, sino que también podrían profundizar ciertos vacíos normativos ya existentes, especialmente en aspectos como el control parlamentario, el acceso a información clasificada y la regulación de tecnologías emergentes, lo que eventualmente puede generar tensiones de inseguridad jurídica y discrecionalidad institucional (Ramírez, et al., 2017).

A su vez, la existencia de lagunas normativas -entendidas como la falta de reglas claras para situaciones concretas- delimita la capacidad del ordenamiento jurídico para alinear la toma de decisiones y debilita la gobernanza del sistema de inteligencia (Pérez-García, 2022). Dichas dificultades hacen necesario un análisis crítico que permita valorar si las reformas realmente fortalecen el sistema o si, por el contrario, introducen nuevas fragmentaciones.

A modo de cierre, las reformas propuestas adquieren especial notabilidad en concordancia con la protección jurídica e institucional de los agentes de inteligencia y contrainteligencia. En este punto, la imprecisión de la normativa y el debilitamiento del principio de reserva logran dar lugar a contextos de exposición indebida, judicialización de actuaciones legítimas y afectación de la moral y operatividad de los organismos de inteligencia. La Comisión Asesora para la Depuración de Datos y Archivos de Inteligencia y Contrainteligencia (2016) ya había avisado que una regulación incompleta en el manejo de la información y de los archivos puede complicar tanto los derechos fundamentales como la seguridad de los funcionarios y de las fuentes.

En este contexto, el presente trabajo se justifica en la medida en que evalúa críticamente las reformas a la Ley Estatutaria 1621 de 2013, identificando vacíos normativos y comprobando sus posibles implicaciones en la protección institucional y jurídica del sistema de inteligencia; lejos de fortalecer la inteligencia estatal, pueden debilitar su gobernanza, su control democrático efectivo y su capacidad estratégica en un contexto de crecientes amenazas complejas.

Marco teórico

La Ley Estatutaria 1621 de 2013 en Colombia, conocida como la Ley de Inteligencia y Contrainteligencia, representó un avance significativo en la medida de las actividades de inteligencia del Estado. Su expedición surgió de la necesidad de lograr un equilibrio entre la efectividad de los organismos de seguridad y la garantía de los derechos fundamentales. Esta normativa se enmarcó en un contexto de cuestionamientos sobre prácticas irregulares, especialmente seguimientos indebidos a periodistas, magistrados y figuras de oposición, lo que había debilitado la confianza en dichas instituciones. En concordancia, su aprobación respondió tanto a demandas internas de transparencia como a presiones de organismos nacionales e internacionales que exigían mayores controles y garantías en el ejercicio de la inteligencia estatal. Además, se estableció un marco legal que define límites claros para proteger la intimidad, la libertad de prensa, la oposición política y la participación democrática, en un contexto en el que el presunto abuso de poder había generado tensiones sociales.

La creación de un órgano de articulación entre diferentes instituciones (Fuerzas Militares, Policía, Presidencia, entre otros) favoreció la interoperabilidad frente a amenazas

complejas y, al regular la inteligencia bajo los principios de legalidad, necesidad y proporcionalidad, buscó que estas actividades se mantuvieran dentro del orden constitucional y no se convirtieran en instrumentos de persecución política.

Conceptualización de inteligencia y contrainteligencia

La inteligencia se entiende como el proceso de recolección, análisis y producción de información estratégica para apoyar la toma de decisiones de seguridad nacional (Gill, 2016). La contrainteligencia, por su parte, busca detectar y neutralizar amenazas contra el Estado y sus instituciones. Estos procesos deben desarrollarse dentro de un marco legal que respete los derechos fundamentales y garantice la legitimidad democrática (Born et al., 2012).

Los vacíos normativos, o también conocidos como lagunas jurídicas, según Pérez-García (2022) y Varsi-Rospigliosi y Colombo (2025), se relacionan con la plenitud basándolo en el hecho de que el sistema no cuenta con normas que prohíban o permitan determinados comportamientos y, si lo anteriormente expuesto puede ser comprobado, se puede decir que el sistema está incompleto y que el ordenamiento jurídico tiene alguna laguna en específico dando a entender que no existe justificación para la toma de decisiones jurídicas.

La gobernanza es considerada como sinónimo de gobierno (Hufty, 2009; Puentes-Sánchez, 2022; Zurbriggen, 2011), de esta forma, se puede conceptualizar como una herramienta política para la transformación de las sociedades. Como buena práctica se hace necesario el conocimiento de normas y la transparencia de los procedimientos.

De acuerdo con Fontaine y Gurza-Lavalle (2019) y Ríos-Ramírez y Fuentes-Vélez (2018) el control democrático es un concepto adoptado sin traducción del inglés, pero básicamente es un término razonable el cual se considera como la rendición de cuentas basándose en la responsabilidad y el control, más que todo en el ámbito político, esto debido al compromiso de informar acciones y decisiones tomadas en diferentes ámbitos.

En el artículo 4 de la Ley Estatutaria 1621 de 2013 de Inteligencia y Contrainteligencia se establecen los fines para la realización de sus actividades protegiendo las instituciones democráticas, respetando los derechos de las personas que residen en el país y aquellos colombianos que se encuentran en todo tiempo y lugar enfrentando las diferentes amenazas que se presenten; también la protección de los recursos naturales e intereses económicos de la Nación.

El marco jurídico de la inteligencia en Colombia

La Ley estatutaria 1621 de 2013 es la norma principal que regula las actividades de inteligencia y contrainteligencia en Colombia. Fue sancionada el 17 de abril de 2013 con el objeto de "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal, y se dictan otras disposiciones" (párr. 1).

La sentencia C-540/12 (Corte Constitucional Republica de Colombia, 2012) es clave

porque se pronunció sobre la constitucionalidad del proyecto de Ley que luego se convirtió en la Ley Estatutaria 1621 de 2013. La Corte Constitucional declaró exequible el proyecto de ley No. 263 de 2011 y el proyecto de ley No. 195 de 2011, ratificando que las actividades de inteligencia y contrainteligencia tienen soporte constitucional (artículos 2, 217, 218, etc.) y reconociendo que su ejercicio requiere reserva legal por la naturaleza de la información que manejan esos servicios.

En los últimos años han sido presentadas varias iniciativas legislativas para reformar la Ley Estatutaria 1621 de 2013 con el fin de fortalecer la protección de los derechos humanos, mejorar los mecanismos de control, supervisión y transparencia, así como regular aspectos como la depuración de datos y archivos de inteligencia (López-Obregón, 2024).

La jurisprudencia constitucional ha establecido límites y principios que deben respetarse en las actividades de inteligencia. Entre ellos: la legalidad, necesidad, proporcionalidad, reserva y protección de derechos fundamentales como la intimidad y el debido proceso. Por ejemplo, la Sentencia C-540 (Corte Constitucional Republica de Colombia, 2012) reafirma que la inteligencia debe tener un respaldo constitucional y que la reserva de la información es necesaria, pero también debe existir equilibrio para evitar abusos.

Gobernanza y control democrático de la inteligencia

La gobernanza de la inteligencia implica mecanismos de supervisión y rendición de cuentas que aseguren que las agencias actúen de manera proporcional, legal y transparente. Organization for Security and Co-operation in Europe (OSCE, 2017) y el Parlamento Europeo han establecido principios de control democrático que incluyen la supervisión parlamentaria independiente, revisión judicial de operaciones intrusivas, reportes públicos, periódicos y comités de auditoría técnica (European union agency for fundamental rights 2015).

La Ley Estatutaria 1621 de 2013 en el contexto colombiano

En Colombia, la Ley Estatutaria 1621 de 2013 creó la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia, pero su capacidad de control ha sido cuestionada por su limitada autonomía y acceso a información clasificada (Ramírez et al., 2017).

La Ley Estatutaria 1621 de 2013 constituye la base normativa para las actividades de inteligencia y contrainteligencia en Colombia, definiéndolas como funciones exclusivas del Estado orientadas a proteger la soberanía, la integridad territorial y los derechos de los ciudadanos. Sin embargo, un documento escrito por González-Cussac (2016) y el informe donde se plasman las recomendaciones sobre permanencia, retiro y destino de los datos y archivos de inteligencia y contrainteligencia que presenta la Comisión asesora para la depuración de datos y archivos de inteligencia y contrainteligencia (2016), han señalado debilidades en la implementación, más específicamente en lo relacionado con el control parlamentario y la protección de datos.

Desafíos en materia de derechos fundamentales y control

El artículo 15 de la Constitución protege la intimidad y los datos personales, pero el régi-

men de reserva legal de la Ley Estatutaria 1621 de 2013 dificulta el acceso a información para la sociedad civil y organismos como integrantes del Consejo de la República de Colombia en la presentación de proyectos de reforma a la Ley de inteligencia. López-Obregón (2024) plantea que el principio de reserva en materia de inteligencia debería revisarse, a fin de permitir mecanismos de auditoría externa que no comprometan la seguridad de las operaciones. En esta línea, algunas experiencias internacionales, como las de Canadá y el Reino Unido, evidencian que es viable articular seguridad y transparencia mediante protocolos definidos para el acceso, control y eventual destrucción de la información sensible (Born y Leigh, 2005).

Por otro lado, el desarrollo de tecnologías como el big data, la inteligencia artificial y la ciberinteligencia ha ampliado de manera significativa las capacidades de vigilancia y análisis en los sistemas de inteligencia contemporáneos. La Ley Estatutaria 1621 de 2013 no incorpora regulaciones específicas sobre el uso de estas herramientas, lo que abre vacíos normativos que podrían dar lugar a interpretaciones discrecionales (Zegart, 2022). Diversas propuestas de reforma sugieren la necesidad de establecer lineamientos claros para su utilización, incluyendo estándares de auditoría, trazabilidad y protección de datos sensibles.

Los marcos regulatorios de la Unión Europea, junto con las recomendaciones de la Geneva Centre for Security Sector Governance (DCAF, 2017), acopian buenas prácticas que pueden servir como referencia, tales como la creación de comités de supervisión con autonomía funcional y presupuestal, el establecimiento de controles judiciales previos y la implementación de informes públicos periódicos sobre las actividades de inteligencia. Estas experiencias resultan especialmente pertinentes para el caso colombiano, en el que persisten niveles de desconfianza ciudadana frente al uso de la inteligencia estatal y preocupaciones asociadas al posible abuso de poder. En esta línea, autores como Born y Wills (2012) y Wright (2016) destacan que la supervisión independiente y los mecanismos de rendición de cuentas son elementos esenciales para equilibrar seguridad nacional y respeto por los derechos fundamentales en sistemas democráticos.

Por otra parte, la revisión de la literatura y del marco normativo evidencia que, aunque la Ley Estatutaria 1621 de 2013 y sus posteriores ajustes representan un avance significativo, aún existen vacíos en materia de control democrático, transparencia institucional y regulación de tecnologías emergentes aplicadas a la inteligencia. Esto refuerza la necesidad de un análisis crítico que permita identificar dichas limitaciones y proponer ajustes normativos orientados a garantizar una actividad de inteligencia no solo eficaz, sino también legítima y sujeta a control democrático.

Metodología

Esta investigación adopta un enfoque cualitativo, en tanto que busca entender e interpretar los significados, dinámicas y tensiones que surgen en torno a la diligencia y control de la Ley Estatutaria 1621 de 2013, desde el análisis documental. Este tipo de aproximación es pertinente para el presente estudio, pues el tema de la inteligencia y la contrainteligencia en Colombia incluye dimensiones éticas, legales y políticas que requieren interpretación crítica, más que verificación empírica cuantitativa. El análisis documental se ubica a examinar cómo los marcos normativos, institucionales y de supervisión inciden en la legalidad

democrática del régimen de inteligencia colombiano. De acuerdo con Hernández-Sampieri et al. (2014) y Zerpa-De Kirby (2016), el camino cualitativo accede a estudiar fenómenos sociales y políticos en su contexto natural, reflexionando tanto en las perspectivas de los actores como las estructuras institucionales y los discursos que se establecen en la realidad analizada.

Complementariamente, autores como Creswell (2014) y Viramontes-Anaya (2024) señalan que la investigación cualitativa es sustancialmente útil cuando se intenta explorar procesos complejos y contextuales, en los que las interpretaciones y significados juegan un papel central. Bowen (2009) y Marín et al. (2016) mencionan que el análisis documental establece una estrategia válida de recolección y análisis de datos en estudios cualitativos y permite examinar metódicamente documentos oficiales, normativos e institucionales para identificar patrones, relaciones y significados relevantes.

El estudio se contextualiza en un diseño descriptivo de tipo documental, destinado a analizar las causas, relaciones y efectos derivados de la implementación de la Ley Estatutaria 1621 de 2013 en el ámbito de la seguridad, la transparencia y la protección de los derechos humanos. El diseño explicativo busca identificar las razones por las cuales ciertos fenómenos ocurren y cómo las variables contextuales se relacionan entre sí (Barco y Carrasco, 2018; Hernández-Sampieri et al., 2014). En este caso, el diseño se justifica porque se pretende explicar cómo los mecanismos de control establecidos por la Ley Estatutaria 1621 de 2013 han incidido en la gobernanza democrática de la inteligencia en Colombia, y por qué persisten vacíos normativos y operativos a más de una década de su promulgación. Se trata, por tanto, de un estudio que no solo describe, sino que interpreta y analiza las relaciones entre los componentes jurídicos, institucionales y políticos del sistema de inteligencia nacional.

Para la recolección de información se utilizó como instrumento una tabla de análisis documental, la cual se elaboró con el fin de organizar y clasificar los contenidos encontrados en las diferentes fuentes académicas vinculadas con los vacíos normativos, la gobernabilidad y los desafíos en la Ley de inteligencia. Este mecanismo permitió reconocer de forma estructurada los vacíos normativos, las limitaciones operativas y las propuestas de fortalecimiento institucional diseñadas por organismos de control, entidades legislativas y centros de investigación especializados. La tabla fue esbozada con categorías analíticas determinadas que agrupan aspectos como la importancia del control democrático, la autonomía de los órganos de supervisión, la transparencia y reserva legal de la información, así como la incorporación de tecnologías emergentes en los procesos de inteligencia.

Este tipo de sistematización es coherente con lo planteado por Giesecke (2020), Hernández-De la Torre y González-Miguel (2020) y Miles et al. (2014), quienes destacan el valor de organizar y reducir datos cualitativos mediante matrices que faciliten el análisis comparativo. Asimismo, el instrumento permitió contrastar fuentes que identificaron patrones, divergencias y buenas prácticas que contribuyen a comprender cómo los mecanismos de supervisión y gobernanza pueden mejorar la legalidad de los sistemas de inteligencia. Yin (2018) señala que el uso de estrategias de análisis documental comparado facilita la identificación de relaciones entre marcos normativos y su atención práctica en contextos institucionales complejos.

Como resultado, la tabla posibilitó evaluar la conexión entre los principios legales de la Ley Estatutaria 1621 de 2013 y su ejecución real, justificando los desafíos pendientes para consolidar una inteligencia estatal sujeta a controles civiles y judiciales efectivos. Complementariamente, Bowen (2009) y Corona (2025) resaltan que el análisis documental permite examinar de manera sistemática documentos oficiales para identificar significados, patrones y vacíos relevantes en la investigación social.

La población documental estuvo constituida o conformada por un total de 45 documentos académicos, legislativos y oficiales disponibles en repositorios institucionales y bases de datos nacionales e internacionales relacionados con las actividades de inteligencia y contrainteligencia en Colombia. La búsqueda se centró en fuentes provenientes del Congreso de la República de Colombia, la Procuraduría General de la Nación, la Defensoría del Pueblo, el Ministerio de Defensa Nacional y centros de investigación como De Justicia y la Fundación Ideas para la Paz (FIP). A su vez, se consultaron bases de datos académicas como Scopus, Google Scholar y ScienceDirect, con el fin de incluir literatura científica y jurídica relevante publicada entre los años 2013 y 2025, periodo que abarca la promulgación de la Ley Estatutaria 1621 de 2013 y sus principales reformas o debates legislativos.

Para la búsqueda inicial se emplearon términos como “Ley 1621 de 2013”, “inteligencia y contrainteligencia en Colombia”, “control democrático”, “gobernanza de la inteligencia”, “reserva legal”, “reformas normativas” y “protección de datos personales”. Esta estrategia de búsqueda permitió establecer como muestra para este estudio un total de 37 documentos, entre artículos científicos, informes institucionales, proyectos de ley, sentencias y tesis de posgrado. Dicho corpus documental constituyó la base de análisis cualitativo para examinar los vacíos normativos, las debilidades en la supervisión parlamentaria y las propuestas de reforma orientadas al fortalecimiento de la gobernanza y la transparencia en las agencias de inteligencia colombianas.

Se establecieron los siguientes criterios de inclusión:

- Documentos normativos, académicos o institucionales que abordaran explícitamente el análisis de la Ley Estatutaria 1621 de 2013 y sus reformas, así como la legislación complementaria en materia de inteligencia y contrainteligencia en Colombia.
- Fuentes que examinaran la gobernanza, el control democrático, la transparencia o la protección de derechos fundamentales dentro de las actividades de inteligencia estatal.
- Publicaciones relevantes para el contexto colombiano o que ofrecieran enfoques comparativos con experiencias internacionales en materia de control civil y supervisión parlamentaria de la inteligencia.
- Estudios y documentos con validez académica o institucional, revisados por pares o emitidos por entidades de investigación, organismos de control o centros de pensamiento especializados en seguridad y defensa.

Los criterios de exclusión consideraron:

• Documentos centrados exclusivamente en aspectos técnicos, tecnológicos u operativos de la inteligencia sin abordar dimensiones jurídicas, éticas o de control democrático.
• Publicaciones no verificadas o sin respaldo institucional, como notas de prensa, blogs o contenidos de opinión sin base investigativa.
• Fuentes anteriores a 2013 o que no hicieran referencia a la Ley Estatutaria 1621 de 2013 o sus proyectos de reforma posteriores.
• Textos escritos en idiomas distintos al español o inglés, que dificultaran la verificación y comparación de la información.

Para el procesamiento de la información se aplicó un análisis de contenido temático, el cual permitió identificar patrones discursivos, categorías conceptuales y relaciones entre los distintos enfoques normativos y doctrinales presentes en los documentos revisados. Este tipo de análisis se fundamenta en la organización sistemática de la información cualitativa, facilitando su interpretación estructurada (Braun y Clarke, 2006; Rueda-Sánchez et al., 2023). El procedimiento se desarrolló en tres etapas complementarias. En la primera fase se realizó una lectura exploratoria y selectiva de los documentos, con el propósito de reconocer ideas centrales y contextos relevantes para el estudio.

En la segunda fase se llevó a cabo la codificación y categorización del material, agrupando la información de acuerdo con los ejes analíticos definidos: control democrático, gobernanza institucional, reserva legal, derechos fundamentales y reformas normativas. Dicho proceso es consistente con los planteamientos de Saldaña (2016) y Vives-Varela y Hamui-Sutton (2021), quienes destacan la codificación como una herramienta clave para la organización de datos cualitativos.

En la tercera fase se realizó la interpretación y síntesis de los resultados, constituyendo los hallazgos con el marco teórico, a fin de construir un conocimiento acoplado al fenómeno jurídico y político incorporado a las reformas de la Ley Estatutaria 1621 de 2013. Esta etapa permitió establecer relaciones entre categorías, identificar patrones emergentes y consolidar una lectura analítica sustentada en la evidencia documental revisada.

Discusión

Importancia y contenido de las modificaciones propuestas a la Ley Estatutaria 1621 de 2013

La inteligencia en Colombia ha estado manejada por la Ley Estatutaria 1621 de 2013, pensada para fortalecer el marco jurídico de los organismos encomendados de estas actividades, accediendo a cumplir su misión constitucional dentro de la legalidad. Su implementación ha sido objeto de críticas, debido a la imprecisión en la aclaración de sus fines, lo que ha favorecido la persistencia de interpretaciones que pueden derivar en estigmatización de ciertos sectores de la sociedad civil.

Las decisiones legislativas más recientes, realizadas en proyectos como el de la Ley Estatutaria 225 de 2024 del Senado y su homólogo Proyecto de Ley Estatutaria 233 de

2025 en la Cámara de Representantes, proponen reformas sustanciales al sistema nacional de inteligencia (López-Obregón, 2024; Racero-Mayorca, 2025). El eje central de estas propuestas se orienta hacia la construcción de un sistema más estricto de depuración de datos y archivos, en respuesta a demandas históricas asociadas al conflicto armado y a la necesidad de garantías de no repetición (Ramírez et al., 2017). Este tipo de enfoques concuerda con lo planteado por Born y Wills (2012), quienes manifiestan que los sistemas de inteligencia en contenidos democráticos deben contar con mecanismos robustos de control y eliminación de información sensible para evitar abusos institucionales.

En procesos de contenido, las modificaciones plantean que la definición de amenazas a la seguridad nacional se establezca a hechos verificables y concretos, sujetando el uso de criterios amplios o probables (Racero-Mayorca, 2025). Igualmente, incorporan mecanismos basados en el derecho a la autodeterminación informativa que permiten a los ciudadanos interponer acciones de tutela y verificar si son objeto de actividades de inteligencia (López-Obregón, 2024). Este enfoque se alinea con los estándares internacionales de protección de datos y derechos digitales, como los expresados por Barreno-Salinas (2025), Niño-García (2022) y Zuboff (2019), quienes opinan sobre los riesgos del uso extensivo de datos personales en contextos de vigilancia.

Adicionalmente, se promueve la eliminación de archivos asociados a prácticas de estigmatización o perfilamiento por razones políticas, sindicales o de género, siguiendo lineamientos previamente establecidos por comisiones asesoras (Comisión Asesora para la Depuración de Datos y Archivos de Inteligencia y Contrainteligencia, 2016). En esta línea, las reformas también impulsan la transición hacia un modelo de seguridad humana, desplazando el enfoque tradicional centrado exclusivamente en la seguridad del Estado. Entre los cambios más relevantes se encuentra el fortalecimiento de capacidades técnicas bajo estrictos mecanismos de supervisión humana, prohibiendo que algoritmos o sistemas automatizados sustituyan la responsabilidad del agente estatal, en concordancia con los debates contemporáneos sobre gobernanza algorítmica y control democrático de la inteligencia (Zuboff, 2019).

Asimismo, se formula una reducción del periodo de reserva legal de la información, pasando de los 30 años constituidos originalmente a un máximo de 15 años, con el fin de concordar la normativa interna con la Ley de Transparencia y del Derecho de Acceso a la Información Pública (Ley 1712 de 2014) y con los estándares interamericanos en materia de derechos humanos establecidos por la Corte Interamericana de Derechos Humanos. Este tipo de ajustes se enmarca en los principios de gobierno abierto y rendición de cuentas desarrollados por la Organización de Estados Americanos et al. (2012), los cuales suscitan mayores niveles de claridad en la gestión pública sin afectar la seguridad nacional.

El Proyecto de Ley Estatutaria (PLE) No. 225 de 2024 expone cambios importantes:

> • ***Redeterminación conceptual:*** Se busca destacar el déficit de precisión normativa, concediendo contenido específico a requisitos como “inteligencia”, “amenaza” y “terrorismo”. A partir de ello, se implanta el enfoque de seguridad humana, que repercute en la protección exclusiva de las instituciones para centrarse en la dignidad y las libertades fundamentales de las personas. Esta orientación ha sido ampliamente

desarrollada por el Programa de las Naciones Unidas para el Desarrollo (PNUD, 1994), el cual esboza que la seguridad debe concebirse desde la protección integral del individuo y no únicamente desde la seguridad del Estado.

• ***Fortalecimiento tecnológico:*** La reforma registra que la Ley Estatutaria 1621 de 2013 ha quedado retardada frente al avance acelerado de las tecnologías de recolección y análisis de información. En este contexto, autores como Zuboff (2019) sugieren que la ampliación de los sistemas digitales de vigilancia exige marcos normativos más precisos que eviten abusos en el uso de datos y avalen controles democráticos positivos sobre la inteligencia estatal. Se regulan explícitamente el uso de inteligencia artificial y procesos automatizados, bajo el principio de no sustitución de la racionalidad humana, exigiendo supervisión humana suficiente en cada operación.

• ***Ajuste de la reserva legal:*** Uno de los cambios más drásticos es la reducción del término de reserva de 30 a 15 años. Esta medida busca armonizar la norma con la Ley de Transparencia (Ley 1712 de 2014) y cumplir con la sentencia de la Corte Interamericana de Derechos Humanos (Corte IDH) en el caso Colectivo de Abogados "José Alvear Restrepo" (CAJAR), permitiendo prórrogas excepcionales solo bajo autorización previa de la Comisión Legal de Seguimiento (Ministerio de Justicia y del Derecho de Colombia, 2024).

• ***Reforma Institucional:*** Propone elevar a un rango legal el Centro de Fusión de Inteligencia y crear el Consejo Nacional de Inspectores Generales para unificar criterios de supervisión y control.

Vacíos normativos e inconsistencias jurídicas: Análisis comparado e impacto en la gobernanza

A pesar de su retórica garantista, un análisis documental y comparado evidencia que estas reformas no logran subsanar las inconsistencias jurídicas preexistentes y, por el contrario, generan nuevos vacíos que afectan la gobernanza del sistema. Desde la perspectiva del derecho comparado, la normatividad colombiana presenta una configuración atípica del principio de reserva legal; por ejemplo, impone el deber de secreto a la ciudadanía en general de manera difusa, mientras otorga prerrogativas absolutas de exención a sectores como el periodístico, lo cual dista de los estándares internacionales de proporcionalidad (González-Cussac, 2016). Las reformas actuales ignoran esta asimetría y no proponen soluciones frente a la declaratoria de inexequibilidad que en el pasado sufrieron los regímenes penales y disciplinarios diseñados para castigar la filtración de información reservada (González-Cussac, 2016).

Existen además antinomias jurídicas significativas entre la Ley Estatutaria 1621 de 2013 y otras leyes estatutarias. Ramírez et al. (2017) señalan que la comunidad de inteligencia ha adoptado una interpretación de "reserva genérica, absoluta e inconstitucional", basada en una lectura aislada del artículo 33 de la Ley Estatutaria 1621 de 2013, ignorando los principios de proporcionalidad y razonabilidad exigidos por la Ley de Transparencia. Esta inconsistencia ha generado una cultura del secreto que obstaculiza la rendición de cuentas

y el acceso a la verdad en contextos de justicia transicional. En contraste con estándares internacionales, como los propuestos por Born y Leigh (2005), el sistema colombiano aún presenta debilidades en la autonomía de sus órganos de supervisión parlamentaria y en la capacidad técnica para auditar operaciones complejas.

Por otro lado, existe una profunda desconexión entre las reformas planteadas y la realidad operativa contemporánea. La literatura evidencia que los mayores desafíos para el control democrático y la protección a la privacidad en la última década provienen del uso de herramientas tecnológicas de interceptación y recolección masiva de datos en entornos digitales (Cortés-Castillo, 2014). Sorprendentemente, los proyectos de ley en trámite omiten regular de manera exhaustiva el ciberespacio, dejando un vacío normativo crítico frente a la inteligencia de señales (SIGINT) y la explotación de fuentes abiertas (OSINT).

De acuerdo con la OSCE (2017), frente a modelos como el de Reino Unido o Chile, la normativa colombiana presenta una supervisión interna mayoritariamente administrativa. Las reformas proponen transitar hacia un control judicial previo y posterior asignado a la jurisdicción de lo Contencioso Administrativo, buscando que los jueces evalúen la necesidad y proporcionalidad de las medidas intrusivas un estándar más cercano a las recomendaciones de la OSCE. De esta manera se evidencian los vacíos frente a actualización por parte de la Ley Estatutaria 1621 de 2013.

Implicaciones en la protección jurídica e institucional de los agentes

La ambigüedad en la redacción de las reformas impacta severamente la seguridad jurídica del personal operativo y analítico. Al flexibilizar la reserva legal y permitir que mediante decisiones judiciales de tutela se obligue a los organismos a revelar si una persona es blanco de inteligencia, se expone la identidad de los agentes, los métodos de recolección y las fuentes humanas (López-Obregón, 2024).

La literatura académica resalta que la inteligencia civil y militar en Colombia requiere de una doctrina clara que otorgue certeza sobre los límites de la actuación legítima (Ardila-Castro y Jiménez-Reina, 2020; Beltrán-Espinosa, 2023; Medina-Camacho, 2020; Moya-Sáenz, 2024). Sin embargo, al instituir contravenciones genéricas sobre lo que establece una "injerencia arbitraria" sin una restricción técnica concreta, los agentes estatales quedan expuestos a un riesgo indeleble de judicialización y control disciplinario. Esta situación puede generar un efecto inhibidor o *chilling effect* en las agencias de inteligencia, donde los especialistas optan por cuidarse de actuar frente a posibles amenazas emergentes por prevención a consecuencias legales, lo que termina aquejando la eficacia operativa del sistema (Urías, 2023).

Este fenómeno ha sido ampliamente analizado en la literatura sobre seguridad y derechos fundamentales. Balkin (2008) alude que los regímenes de vigilancia desmesuradamente restrictivos pueden ocasionar efectos de autocensura institucional que disminuyen la capacidad del Estado. De manera adicional, Casal-Oubiña et al. (2025) y Heymann (2003) proponen que la falta de claridad normativa en los sistemas de inteligencia genera tensiones estructurales entre el control democrático y la eficacia operativa, afectando el equilibrio entre seguridad y legalidad.

En este contexto, las reformas introducen una tensión ineludible entre la reserva de la información y los mecanismos de denuncia y control. Se establece que el principio de obediencia debida no aplica cuando se trate de órdenes relacionadas con violaciones de derechos humanos o crímenes internacionales. El agente cuenta ahora con protección legal para denunciar la recolección ilegal de información, asegurando que la reserva no le sea oponible para reportar tales hechos ante autoridades administrativas o penales. Esta "judicialización de la operación" mediante el control judicial previo para técnicas intrusivas brinda un piso de legalidad que protege al funcionario frente a futuras investigaciones por arbitrariedad, aunque plantea desafíos operativos en términos de rapidez y flexibilidad.

Desde el análisis estratégico, la Ley Estatutaria 1621 de 2013 requiere ajustes, pero no bajo la óptica reactiva y restrictiva de las reformas en curso. Un aparato de inteligencia funcional debe tener la capacidad de anticiparse a escenarios de riesgo complejo (terrorismo transnacional, ciberataques, economías ilícitas) sin que la normativa opere como un obstáculo insalvable. Estratégicamente, imponer cargas procesales desproporcionadas a los organismos de inteligencia y debilitar la confidencialidad de sus archivos destruye la ventaja asimétrica del Estado frente a las amenazas híbridas. La normatividad debe equilibrar la transparencia democrática con la eficacia institucional, cerrando las brechas sancionatorias para quienes vulneren la reserva, pero garantizando el anonimato y la protección integral de quienes ejecutan la labor de inteligencia en el marco de la Constitución Política.

Conclusiones

El análisis de los vacíos normativos y los desafíos institucionales en torno a la Ley Estatutaria 1621 de 2013 permite extraer reflexiones concluyentes sobre el rumbo que debe tomar la legislación en Colombia:

Inconveniencia de la reforma actual: Se sugiere no permitir que prosperen estas iniciativas tal como están planteadas (como el PLE 225 de 2024), ya que tienen un "sesgo retrospectivo" que busca corregir errores del pasado mediante una sobrerregulación punitiva que termina paralizando la función preventiva del Estado. Al debilitar el principio de reserva y exponer a los agentes a una judicialización constante mediante herramientas de autodeterminación informativa mal adaptadas al contexto de la seguridad nacional, se compromete gravemente la integridad del sistema de inteligencia y la soberanía del país.

Necesidad de una actualización liderada por las agencias: La reforma de la Ley Estatutaria 1621 de 2013 debe ser endógena, es decir, originada por la comunidad de inteligencia y son las agencias quienes poseen el conocimiento técnico-operativo para proponer cambios que equilibren el control democrático con las realidades del trabajo de campo y el análisis estratégico.

Integración de avances tecnológicos y nueva doctrina: Esta actualización endógena debe estar fundamentada en la actualización de la doctrina de inteligencia, orientándose hacia el futuro. Resulta apremiante cubrir las nuevas actividades de inteligencia derivadas de la era digital, estableciendo marcos jurídicos claros para el ciberespionaje, la inteligencia

artificial aplicada al análisis de grandes volúmenes de datos (*Big Data*), la recolección en fuentes abiertas digitales y la protección de infraestructuras críticas. Solo una ley adaptada a los avances tecnológicos contemporáneos garantizará un Estado verdaderamente resiliente y capaz de anticipar las amenazas del siglo XXI.

Declaración obligatoria de uso de IAGen

El autor declara que no se utilizaron herramientas de inteligencia artificial generativa en la elaboración de este manuscrito.

Referencias

Ardila-Castro, C. A. y Jiménez-Reina, J. (Eds.). (2020). *Aportes teóricos a la construcción del concepto de inteligencia estratégica.* Sello Editorial ESDEG. https://doi.org/10.25062/9789584288974 PMid:32904213 PMCid:PMC7452685

Balkin, J. M. (2008). The constitution in the national surveillance State. *Minnesota Law Review, 93*(1), Paper No. 168. https://doi.org/10.24926/265535.1421

Barco, B. y Carrasco, A. (2018). Explicaciones causales en la investigación cualitativa: elección escolar en Chile. Magis, *Revista Internacional de Investigación en Educación, 11*(22), 113-124. https://doi.org/10.11144/Javeriana.m11-22.ecic

Barreno-Salinas, M. M. (2025). El derecho a la privacidad en la era digital: desafíos y salvaguardias contra la vigilancia masiva desde una perspectiva de derechos humanos. VISUAL REVIEW. *Revista internacional de cultura visual, 17*(1), 235-245. https://doi.org/10.62161/revvisual.v17.5769

Beltrán-Espinosa, O. I. (2023). *Inteligencia civil para la seguridad y la defensa nacionales de Colombia: aportes a la teorización del concepto de inteligencia civil* [Tesis de Maestría, Escuela Superior de Guerra "General Rafael Reyes Prieto"]. Repositorio Institucional ESDEG. https://hdl.handle.net/20.500.14205/11166

Born, H. y Leigh, I. (2005). *Making intelligence accountable: legal standards and best practices for oversight of intelligence agencies*. Publishing House of the Parliament of Norway, Oslo. https://www.semanticscholar.org/paper/Making-intelligence-accountable-%3A-legal-standards-Born-Leigh/5d558c8475a8214ff43524267083d5e5e5b766b5

Born, H. y Wills, A. (2012). *Overseeing intelligence services: A toolkit.* The Geneva Centre for the Democratic Control of Armed Forces (DCAF). https://www.dcaf.ch/overseeing-intelligence-services-toolkit

Born, H., Leigh, I. y Wills, A. (2012). *International Intelligence Cooperation and Accountability.* Routledge. https://doi.org/10.4324/9780203831731

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Braun, V. y Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Casal-Oubiña, D., Gutiérrez-Villalta, J. y Viladrich-Sandín, B. (2025). Control político y democrático de los servicios de inteligencia. Estados Unidos, Reino Unido y Australia como estudios de caso. *TSN Transatlantic Studies Network,* (18), 189-204. https://doi.org/10.24310/tsn.18.2025.19025

Comisión Asesora para la Depuración de Datos y Archivos de Inteligencia y Contrainteligencia (2016). *Informe de recomendaciones sobre permanencia, retiro y destino de los datos y archivos de inteligencia y contrainteligencia.* Jurisdicción especial para la paz (JEP) - jep.gov.co. https://www.jep.gov.co/biblioteca/das/das6.pdf

Corona, P. (2025). Análisis documental: fundamento metodológico en la investigación científica. *Archivos de medicina, 21*(2). https://dialnet.unirioja.es/servlet/articulo?-codigo=10351408

Corte Constitucional República de Colombia (12 de julio de 2012). Sentencia C-540/12 (Jorge Iván Palacio Palacio, M. P.). https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

Cortés-Castillo, C. (2014). *Vigilancia de las comunicaciones en Colombia: El abismo entre la capacidad tecnológica y los controles legales.* Documentos Dejusticia 18. Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia. https://doi.org/10.2307/jj.16192262

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th Ed.). Sage Publications.

European union agency for fundamental rights (18 de noviembre de 2015). *Vigilancia por parte de los servicios de inteligencia - Volumen I: Marcos jurídicos de los Estados miembros.* fra.europa.eu. https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services-volume-i-member-states-legal-frameworks

Fontaine, G. y Gurza-Lavalle, A. (2019). Controles democráticos y cambio institucional en América Latina. Presentación del dossier. *Íconos. Revista de Ciencias Sociales,* (65), 7-28. https://doi.org/10.17141/iconos.65.2019.4041

Geneva Centre for Security Sector Governance (01 de septiembre de 2017). *Intelligence Oversight: Ensuring accountable intelligence within a framework of democratic governance.* DCAF - dcaf.ch. https://www.dcaf.ch/intelligence-oversight-ensuring-accountable-intelligence-within-framework-democratic-governance

Giesecke, M. P. (2020). Preparación y relevancia de la matriz de consistencia

cualitativa para la investigación en ciencias sociales. *Desde el Sur, 12*(2), 397-417. https://doi.org/10.21142/DES-1202-2020-0023

Gill, P. (2016). *Intelligence Governance and Democratisation: A comparative analysis of the limits of reform*. Routledge. https://doi.org/10.4324/9781315728063

Gill, P. y Phythian, M. (2018). *Intelligence in an insecure world* (3.ª ed.). Polity Press.

González-Cussac, J. L. (2016). La ley de inteligencia colombiana en perspectiva internacional. *Cuadernos de derecho penal,* (15), 11-32. https://doi.org/10.22518/20271743.576

Hernández-De la Torre, E. y González-Miguel, S. (2020). Análisis de datos cualitativos a través del sistema de tablas y matrices en investigación educativa. *Revista Electrónica Interuniversitaria de Formación del Profesorado, 23*(3). https://doi.org/10.6018/reifop.435021

Hernández-Estupiñán, P. A. (2020). Aportes al concepto de inteligencia estratégica. *Perspectivas en Inteligencia, 12*(21), 81-94. https://doi.org/10.47961/2145194X.233

Hernández-Sampieri, R., Fernández-Collado, C. y Baptista-Lucio, M. P. (2014). *Metodología de la investigación* (6. ª ed.). McGraw-Hill.

Herrera-Rodríguez, J. I., Guevara-Fernández, G.E. y Munster-De la Rosa, H. (2015). Los diseños y estrategias para los estudios cualitativos. Un acercamiento teórico-metodológico. *Gaceta Médica Espirituana, 17*(2). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1608-89212015000200013

Heymann, P. B. (2003). *Terrorism, freedom, and security: Winning without war.* MIT Press.

Hufty, M. (2009). Una propuesta para concretar el concepto de gobernanza: el marco analítico de la gobernanza en H. Mazurek (ed.), *Gobernabilidad y gobernanza en los territorios de América Latina.* (Primera edición, pp. 77-100). Tomo 25 de Actes & Mémoires de l'Institut Fran~s d'Études Andines

Kniep, R., Ewert, L., Leon-Reyes, B., Tréguer, F., Cluskey, E. M. y Aradau, C. (2024). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies, 50*(1), 209-229. https://doi.org/10.1017/S0260210523000013

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. 6 de marzo de 2014. D. O. No. 49084. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Ley Estatutaria 1621 de 2013. Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan

otras disposiciones. 17 de abril de 2013. D. O. No. 48764. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

López-Obregón, C. (2024). *Radicación Ponencia Positiva para primer debate del Proyecto de Ley Estatutaria No. 225 de 2024 Senado "Por la cual se reforma la Ley 1621 de 2013 para reforzar la protección a los derechos humanos y fortalecer el marco jurídico de los organismos que llevan a cabo actividades de inteligencia y contrainteligencia, se fortalece el Sistema de Depuración de Datos y Archivos de inteligencia y contrainteligencia y se dictan otras disposiciones"*. Congreso de la República de Colombia. https://www.comisionprimerasenado.com/documentos-pendientes-de-publicacion/ponencias-y-textos-aprobados/4148-ponencia-ple-225-de-2024-inteligencia-y-contrainteligencia/file

Marín, A., Hernández, E. y Flores, J. (2016). Metodología para el análisis de datos cualitativos en investigaciones orientadas al aprovechamiento de fuentes renovables de energía. *Revista Arbitrada Interdisciplinaria Koinonía, 1*(1), 60-75. https://www.fundacionkoinonia.com.ve/ojs/index.php/revistakoinonia/article/view/15

Medina-Camacho, J. E. (2020). Doctrina de Inteligencia Militar de Colombia frente a la doctrina política de los grupos terroristas, necesaria en el nuevo campo de batalla: «La internet». *Revista de Cultura de Paz, 4*, 257-270. Recuperado a partir de https://revistadeculturadepaz.com/index.php/culturapaz/article/view/90

Miles, M. B., Huberman, A. M. y Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd Ed.). Sage Publications.

Ministerio de Justicia y del Derecho de Colombia (6 de agosto de 2024). *Fallo de la Corte Interamericana contra Colombia por las graves violaciones de Derechos Humanos al colectivo de abogados José Alvear Restrepo.* minjusticia.gov.co. https://www.minjusticia.gov.co/Sala-de-prensa/Paginas/Caso-miembros-de-la-corporacion-colectivo-de-abogados-Jose-Alvear-Restrepo-vs-Colombia.aspx

Moya-Sáenz, L. G. (2024). La inteligencia estratégica en el orden multipolar del siglo XXI, *Revista Estrategia, Poder y Desarrollo, 3*(5), 7-24. https://doi.org/10.25062/2955-0289.4849

Niño-García, D. Y. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico. *Revista CES Derecho, 13*(1), 70-89. https://doi.org/10.21615/cesder.6386

Organización de los Estados Americanos, Secretaría de Asuntos Jurídicos y Departamento de Derecho Internacional (2012). *Ley Modelo Interamericana sobre Acceso a la Información Pública y su Guía de Implementación.* Canadian International Development Agency (CIDA) www.oas.org. https://www.oas.org/es/sla/ddi/docs/acceso_ley_modelo_libro_espanol.pdf

Organization for Security and Co-operation in Europe (3 de julio de 2017). *OSCE*

Guidebook Intelligence-Led Policing. (TNTD/SPMU Publication Series Vol. 13). OSCE - osce.org. https://www.osce.org/chairmanship/327476

Pérez-García, C. (2022). Lagunas jurídicas y voluntad de derecho. *Diálogos Jurídicos, 7*, 293-312. https://doi.org/10.17811/dj.7.2022.293-312

Programa de las Naciones Unidas para el Desarrollo (1994). Informe sobre desarrollo humano 1994: Nuevas dimensiones de la seguridad humana. Oxford University Press. https://hdr.undp.org/content/human-development-report-1994

Puentes-Sánchez, J. C. (2022). Del gobierno a la gobernanza: una aproximación normativa desde lo posmoderno. *Nuevo Derecho, 18*(31), 1-24. https://doi.org/10.25057/2500672X.1471

Racero-Mayorca, D. R. (2025). *Proyecto de Ley Estatutaria No. 233 de 2025 Cámara. Por la cual se reforma la Ley 1621 de 2013 para reforzar la protección a los derechos humanos y fortalecer el marco jurídico de los organismos que llevan a cabo actividades de inteligencia y contrainteligencia y se dictan otras disposiciones.* Congreso de la República de Colombia - Cámara de Representantes. https://www.camara.gov.co/ley-inteligencia-y-contrainteligencia-130/

Ramírez, A. M., Ángel, M. P., Albarracín, M., Uprimny-Yepes, R. y Newman-Pont, V. (2017). *Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo. Documentos 31 ideas para construir paz.* Djusticia. https://www.dejusticia.org/publication/acceso-a-los-archivos-de-inteligencia-y-contrainteligencia-en-el-marco-del-posacuerdo/

Ríos-Ramírez, A. y Fuentes-Vélez, L. (2018). Democracia, control político y rendición de cuentas. El antecedente griego. *Co-Herencia, 15*(28), 87-109. https://doi.org/10.17230/co-herencia.15.28.4

Rueda-Sánchez, M. P., Armas, W. J. y Sigala-Paparella, L. E. (2023). Análisis cualitativo por categorías a priori: reducción de datos para estudios gerenciales. *Ciencia y Sociedad, 48*(2), 83-96. https://doi.org/10.22206/cys.2023.v48i2.pp83-96

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Sage Publications.

Sansó-Rubert Pascual, D. y Pulido-Gragera, J. (2022). Cultura de inteligencia y sociedad. *URVIO: Revista Latinoamericana de Estudios de Seguridad*, (34), 8-19. https://dialnet.unirioja.es/servlet/articulo?codigo=8646425 https://doi.org/10.17141/urvio.34.2022.5738

Urías, J. (2023). El efecto disuasorio (chilling effect) sobre el ejercicio de los derechos en nuestra jurisprudencia constitucional. *Revista Española de Derecho Constitucional, (129)*, 305-336. https://doi.org/10.18042/cepc/redc.129.10

Varsi-Rospigliosi, E. y Colombo, M. (2025). Las lagunas de la ley: análisis de vacíos

normativos y su gestión en un sistema jurídico dinámico. *Revista da Faculdade de Direito UFMG, 86*, 41-63. https://revista.direito.ufmg.br/index.php/revista/es/article/view/2989 https://doi.org/10.12818/P.0304-2340.2025v86p41

Viramontes-Anaya, E. (2024). Análisis cualitativo en la investigación. *IE Revista De Investigación Educativa de la REDIECH, 15*. https://doi.org/10.33010/ie_rie_rediech.v15i0.2074

Vives-Varela, T. y Hamui-Sutton, L. (2021). La codificación y categorización en la teoría fundamentada, un método para el análisis de los datos cualitativos. *Investigación en Educación Médica, 10*(40), 97-104. https://doi.org/10.22201/fm.20075057e.2021.40.21367

Wright, S. (2016). Watching Them Watching Us. *Ethical Space: The International Journal of Communication Ethics, 12*(2/3). https://eprints.leedsbeckett.ac.uk/id/eprint/2096/

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th Ed.). Sage Publications.

Zegart, A. B. (2022). *Spies, lies, and algorithms: the history and future of American intelligence.* Princeton University Press. https://doi.org/10.1515/9780691223087 https://doi.org/10.2307/j.ctv1t8q8tp

Zerpa-De Kirby, Y. B. (2016). Lo cualitativo, sus métodos en las ciencias sociales. *Sapienza Organizacional, 3*(6), 207-230. http://erevistas.saber.ula.ve/index.php/sapienza/article/view/7832

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

Zurbriggen, C. (2011). Gobernanza: una mirada desde América Latina. *Perfiles latinoamericanos, 19*(38), 39-64. https://doi.org/10.18504/pl1938-039-2011

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web:https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Las reformas de la Ley de inteligencia y contrainteligencia en Colombia: vacíos e importancia

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Lina María Barrera-Quiroga es Magister en Inteligencia Estratégica de la Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Colombia), Abogada de la Escuela Militar de Cadetes General José María Córdova (Colombia), profesional en Ciencias Militares de la Escuela Militar de Cadetes General José María Córdova (Colombia).
https://orcid.org/0009-0002-8901-0928 - Contacto: lina.mbq01@gmail.com

Esta página queda intencionalmente en blanco

Revista Perspectivas en Inteligencia
(Scientific Journal of Social Sciences and Interdisciplinary Studies)
Volume 18, Number 27, January - June 2026
ISSN: 2145-194X (printed), 2745-1690 (online)
Website: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem

Authors:

Oscar Alberto Rojas-Martínez
https://orcid.org/0000-0002-3826-2706
✉ nacho_rojas07@hotmail.com
Escuela de Aviación del Ejército, Colombia

Heivar Yesid Rodríguez-Pinzón
https://orcid.org/0000-0002-9553-0455
✉ rodriguezphy@javeriana.edu.co
Pontificia Universidad Javeriana, Colombia

APA Citation: Rojas-Martínez, O. A. & Rodríguez-Pinzón, H. Y. (2026). Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem. *Perspectivas en Inteligencia, 18*(27), 75-97. http://doi.org/10.47961/2145194X.860

Published online: 2026

Articles published by the Revista Científica Perspectivas en Inteligencia are Open Access under a **Creative Commons license: Attribution - Noncommercial - No Derivatives.**

To submit an article:
https://revistaseditorialejc.org/index.php/pei/about/submissions

This page is intentionally left blank

PERSPECTIVAS EN INTELIGENCIA 2026

Revista Científica en Ciencias Sociales e Interdisciplinaria
Volume 18, Number 27, January - June 2026, pp. 75-97
ISSN 2145-194X (printed), 2745-1690 (online)
Bogotá, D. C., Colombia
http://doi.org/10.47961/2145194X.860

Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem

Sistemas Antidrones para la seguridad aérea en el ecosistema de la aviación civil colombiana

Oscar Alberto Rojas-Martínez[1] & Heivar Yesid Rodríguez-Pinzón[2]*

(1) Escuela de Aviación del Ejército, Bogotá, D. C., Colombia,
✉ nacho_rojas07@hotmail.com

(2) Pontificia Universidad Javeriana, Bogotá, D. C., Colombia,
✉ rodriguezphy@javeriana.edu.co

* Author to whom the correspondence is addressed

Abstract

In the era of the Fourth Industrial Revolution, the widespread adoption of emerging technologies across industries and society has fostered innovation in multiple processes. However, the misuse of certain technologies, particularly unmanned aerial vehicles (UAVs), has generated new risks and threats for different sectors due to limited governmental oversight and operational control. These risks may negatively affect society, industries, civil aviation, institutional stability, and ultimately the State itself. Within the Colombian aviation ecosystem, this study analyzes the impact of drones on comprehensive airport security, focusing on potential scenarios that threaten physical security and operational safety through the malicious use of advanced technologies, in some cases supported by artificial intelligence (AI). Using a preliminary interpretive approach, the research aims to examine the relevance of anti-drone technologies in Colombia from both aviation safety and security perspectives, contributing to the strengthening of these essential pillars for global air transport operations. Finally, by contextualizing the problem, this study contributes to the body of knowledge on anti-drone systems, their necessity, applications, and regulatory frameworks, drawing on national and international research experiences to assess operational contexts, determine their strategic importance, and highlight some of their advantages.

Classification JEL: H56, L93, O33.

Keywords: aviation safety; aviation security; surveillance systems; civil aviation; airport security; technological change.

Date received: 09/05/2026 | Date Accepted: 02/08/2026

Resumen

En la era de la cuarta revolución industrial, la adopción generalizada de tecnologías emergentes en las industrias y la sociedad ha impulsado la innovación en múltiples procesos. Sin embargo, el uso indebido de ciertas tecnologías, particularmente los vehículos aéreos no tripulados (UAV), ha generado nuevos riesgos y amenazas para diferentes sectores debido a la limitada supervisión gubernamental y al control operacional insuficiente. Estos riesgos pueden afectar negativamente a la sociedad, las industrias, la aviación civil, la estabilidad institucional y, en última instancia, al propio Estado. Dentro del ecosistema de la aviación colombiana, este estudio analiza el impacto de los drones en la seguridad aeroportuaria integral, enfocándose en escenarios potenciales que amenazan la seguridad física y la seguridad operacional mediante el uso malicioso de tecnologías avanzadas, en algunos casos apoyadas en inteligencia artificial (IA). Mediante un enfoque interpretativo preliminar, la investigación busca examinar la relevancia de las tecnologías antidrones en Colombia desde las perspectivas de seguridad operacional y seguridad física de la aviación, contribuyendo al fortalecimiento de estos pilares esenciales para las operaciones globales de transporte aéreo. Finalmente, al contextualizar el problema, este estudio contribuye al cuerpo de conocimiento sobre los sistemas antidrones, su necesidad, aplicaciones y marcos regulatorios, apoyándose en experiencias de investigación nacionales e internacionales para evaluar contextos operacionales, determinar su importancia estratégica y resaltar algunas de sus ventajas.

Palabras clave: seguridad operacional de la aviación; seguridad de la aviación; sistemas de vigilancia; aviación civil; seguridad aeroportuaria; cambio tecnológico.

Introduction

This article examines the need to implement anti-drone systems in Colombian civil and commercial aviation, with particular emphasis on the safe operation of airports in response to the increasing use of unmanned aerial vehicles (UAVs) that are not fully regulated by the national aviation authority. The implementation of such systems has become imperative to address an emerging and evolving threat, as well as to ensure the safety and continuity of civil air operations in Colombia. In this context, technological solutions capable of mitigating the risks associated with the misuse of drones in restricted and sensitive areas are analyzed.

Accordingly, it is essential to explore how anti-drone technologies can be effectively integrated into existing aviation security protocols in order to protect the civil aviation ecosystem and ensure comprehensive airport management across the country. In recent years, the rapid expansion of the unmanned aircraft market has been accompanied by the advancement of Artificial Intelligence (AI), which has enhanced the capabilities, autonomy, and range of applications of these aerial platforms. This convergence has generated new operational possibilities, while simultaneously introducing complex challenges for aviation safety and security.

Within this scenario, aviation authorities play a central role as the primary regulatory and supervisory bodies responsible for the use and integration of UAVs into national

airspace. As defined by Choi (2022), unmanned aircraft can be understood as "independent bodies" that represent a paradigm shift, exceeding traditional industry standards and evolving as a core technology interconnected with other emerging technologies (p. 1).

The growing use of drones has consequently posed significant challenges to aviation ecosystems. Although initially designed for recreational and commercial purposes, UAVs and their associated systems have increasingly been employed for malicious activities, posing potential threats to civil aviation operations. The uncontrolled commercial growth of drone sales may result in airspace interference, mid-air collisions, violations of privacy, and risks to critical infrastructure, among other safety and security concerns.

In this regard, it is necessary to examine whether the implementation of anti-drone systems in Colombian civil aviation can effectively mitigate risks and reduce threats associated with the misuse of UAVs, without adversely affecting aviation operations or technical systems (Jačionis, 2020). This research is therefore both relevant and necessary, as it responds to current protection demands in Colombian airports and seeks to contribute to the development of a safer operational environment. Furthermore, the deployment of such systems may strengthen the overall resilience of the aviation ecosystem against emerging security challenges.

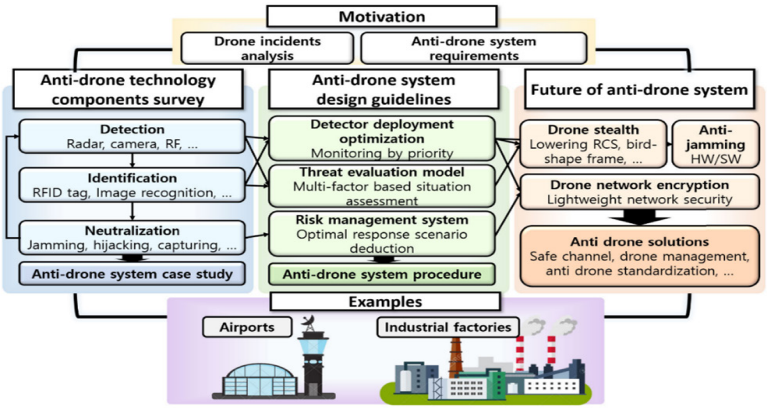
Based on a qualitative literature review on anti-drone systems and aviation security, this study aims to contribute to a deeper understanding of the current state and relevance of drones as a research phenomenon within civil aviation. Data collection and analysis are conducted within an interpretative paradigm, allowing for the assessment of the impact of unmanned aircraft on air security and the evaluation of potential countermeasures for their unregulated operation. This methodological approach supports the organization of the study into epistemological, theoretical, methodological, and results-oriented components.

Finally, the review of existing academic literature highlights the contribution of the Colombian National Army Aviation School (ESAVE), as a higher education institution within the aviation sector, through its presentation entitled Anti-Drone Systems: A Necessity for the Comprehensive Security of the Colombian Civil Aviation Ecosystem. This contribution provides a broad perspective on the phenomenon affecting air security and serves as a key motivation for the present manuscript, recognizing anti-drone systems as a pertinent, timely, and highly relevant topic currently demanded by the aviation industry.

Background and security context of unmanned aircraft systems

The increasing security challenges affecting aeronautical, industrial, and social ecosystems as a result of the rapid expansion of unmanned aircraft have led to the identification of a structured roadmap, as illustrated in Figure 1.

Figure 1. Roadmap for anti-drone system design and development



Source: Park et al. (2021)

This roadmap, developed across three main domains, reflects the general spectrum proposed by Park et al. (2021) and facilitates an understanding of the comprehensive landscape surrounding the relevance of anti-drone systems. It ranges from the motivations behind contemporary drone attacks to the prospective evolution of these aircraft and their implications for security and protection, highlighting the growing need for technological solutions capable of countering malicious drone activities (Chávez & Swed, 2021).

As shown in Figure 1, the use of unmanned aircraft influences a wide range of industries, particularly within non-military contexts where technological development is often more dynamic. From a civil aviation perspective, this evolving ecosystem presents complex operational and security challenges that must be addressed to ensure the protection of air transport systems.

Drones, also referred to as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UAS), are robotic platforms capable of operating autonomously or through various control mechanisms, including remote controllers, mobile devices, and advanced human–machine interfaces. Until the early 2000s, these systems were predominantly military assets and largely inaccessible to civilians. However, advances in hardware and software technologies have enabled the development of smaller, more affordable, and easier-to-operate platforms (Tezza & Andujar, 2019), leading to their widespread civilian adoption.

From a security perspective, the rapid proliferation of drones has introduced significant concerns. As noted by Balladares et al. (2024) and Kang et al. (2021), the increasing presence of drones requires a deeper understanding of their operational implications, as technological progress is now primarily constrained by human creativity and ethical considerations rather than technical limitations. Consequently, drones have become ubiquitous elements within modern societies.

Within the context of the Fourth Industrial Revolution, drones may generate adverse

effects on public safety. Hwang & Kim (2020) describe them as "an attractive tool for criminal and terrorist groups because they can be equipped with weapons at low cost, conceal their operators, and evade surveillance equipment" (p. 248). Table 1 summarizes several documented incidents involving the malicious use of drones across different industries and critical infrastructure sectors, underscoring the seriousness of this emerging threat.

Table 1 provides a brief compilation of selected global cases of drone misuse. In the aviation sector, such threats are associated with airspace interference, near-miss events, and collision risks, many of which remain underreported due to regulatory gaps, limited data availability, and the relatively recent integration of drones into civil airspace. As Shin et al. (2021) emphasize, the growth in unauthorized drone operations increases the likelihood of accidents, property damage, and intentional harm. Consequently, when illegal drone activity is detected in the vicinity of airports, immediate action is required to ensure aviation safety (Hwang & Kim, 2020).

Table 1. Selected global cases of drone-related incidents affecting critical infrastructure and aviation

Date	Country	Event Details
January, 2015	USA	In Washington D.C., a civilian UAV flew over the White House fence and crash-landed on the lawn.
April, 2015	JAPAN	Phantom 2 drone carrying traces of radiation was found on the roof of the Japanese Prime Minister's Official Residence.
October, 2016	Iraq	ISIS may have used a commercial drone rigged with explosives to kill two Kurdish Peshmerga soldiers and wound two French soldiers in Iraq.
August, 2016	South Africa	A small UAV crashed into a nuclear powerplant in Koeberg.
August, 2018	Venezuela	Two drone bombs used in an attempt to assassinate President Nicolas Maduro.
December, 2018	United Kingdom	Two drones found at Gatwick airport. The airport's closure led to more than 100,000 people being stranded or delayed.
September, 2019	Saudi Arabia	Two major Saudi oil installations hit by drone strike. Production of 5.7 million barrels a day was suspended.

Source: Reproduced from Hwang & Kim (2020)

In light of this context, the implementation of anti-drone systems has become a critical requirement for the Colombian civil aviation ecosystem. Such systems must be integrated into existing operational and industrial frameworks in a manner that safeguards both aviation safety and civil aviation security, while accommodating the continuous technological evolution of unmanned aircraft.

Airports and Drones

Within the context of Industry 4.0, technological advancements have significantly lowered the barriers to accessing and operating unmanned aerial vehicles (UAVs), enabling individuals and organizations to acquire drone-related skills for recreational, commercial, and mission-specific purposes. This accessibility has transformed the long-standing human aspiration of flight into a widely attainable capability through unmanned aviation. While these developments have fostered innovation across multiple scientific and industrial fields, they have also introduced new operational and security challenges, particularly within airport environments (Sichko, 2019).

The current era has been described as the "Drone Age", a concept articulated by Boyle (2020) to capture the rapid evolution and widespread availability of drone technologies for both state and non-state actors. Drones have progressed from simple reconnaissance platforms to highly capable systems able to conduct complex missions with minimal human intervention. This evolution raises ethical, legal, and regulatory concerns related to accountability, privacy, and oversight, as the diversity of drone applications increasingly intersects with fundamental human and societal values (Završnik, 2016).

From an aviation security perspective, the proliferation of UAVs has exposed airports to a range of emerging vulnerabilities, including cyber-related threats and operational disruptions. As highlighted by Costin et al. (2023) and Hurtado-Cubillos (2022), the growing dependence on unmanned systems across multiple sectors expands the attack surface of critical infrastructure, necessitating more robust and integrated security management approaches. Despite this reality, academic research has historically focused more on the technical development and operational capabilities of drones than on the identification of effective countermeasures or airport-specific mitigation strategies.

Only in the second decade of the 21st century has scholarly attention increasingly shifted toward regulatory and operational challenges associated with unmanned aviation. As noted by Merkert & Bushell (2020), contemporary aviation issues have expanded beyond traditional regulatory concerns to encompass novel risks that had not previously been encountered. In airport contexts, the misuse of drones represents a particularly disruptive threat, facilitated by their remote operation, low cost, and ease of access. Consequently, proactive airport security management requires systematic threat identification and scenario-based risk assessment, as emphasized by Cole (2014).

Airports operate under the assumption of persistent exposure to evolving threats, requiring continuous adaptation of mitigation strategies and security systems. While past approaches often focused on the detection of prohibited objects, there has been a gradual shift toward identifying malicious actors and intent. This transition reflects a broader movement toward intelligence-led and risk-based security management models that enhance decision-making and operational resilience.

The integration of drones into airport operations has further complicated this landscape. In recent years, controlled drone operations within airport environments have been introduced under strict regulatory conditions, including predefined corridors and restricted

zones to enable coexistence with commercial aviation (Shvetsova & Shvetsov, 2021). Nevertheless, collision risks remain, particularly during critical flight phases such as takeoff, approach, and taxiing, where manned aircraft operate at low altitudes. As La Cour-Harbo & Schiøler (2019) note, even when drones operate below 500 feet, residual risks persist within controlled aerodromes.

In Colombia, civil aviation oversight is exercised by the Special Administrative Unit of Civil Aeronautics, which is responsible for developing, interpreting, and enforcing civil aviation regulations. As a contracting State of the Convention on International Civil Aviation (Chicago Convention, December 7, 1944.), Colombia is a member of the International Civil Aviation Organization and is committed to implementing its standards and recommended practices, including those related to pilotless aircraft as addressed in Article 8 of the Convention (Law No. 12 of 1947).

In response to the growing relevance of unmanned aviation, Colombia has advanced strategic initiatives through its aviation authority, including the Action plan of the Unmanned Aviation Strategic Plan 2023-2026. This framework aims to support the safe and orderly integration of unmanned aircraft into national airspace, as illustrated in Figure 2, which outlines the corresponding action plan.

Figure 2 . Action plan of the Unmanned Aviation Strategic Plan 2023-2026

Source: (Unidad Administrativa Especial de Aeronáutica Civil de Colombia, 2023)

These measures are complemented by national regulations, such as RAC 100, which governs the operation of unmanned aircraft systems (UAS) within the Colombian aviation system.

Despite these efforts, regulatory and institutional frameworks alone are insufficient to fully address the risks associated with malicious drone activities. As emphasized by Hwang & Kim (2020), while legal mechanisms are necessary to enable legitimate drone operations, it is equally critical to protect national critical infrastructure from hostile or unlawful uses. The continuous evolution of drone technologies requires that regulatory systems remain dynamic and adaptive, supported by the development and implementation of anti-drone systems capable of detecting and neutralizing unauthorized UAVs across diverse operational scenarios.

Integrated Aviation Safety and Security

The integration of aviation safety and security presents a persistent challenge for airport management, particularly in the context of rapid technological evolution and increasing system complexity. The interaction between theory and practice requires adaptive strategies capable of addressing both accidental hazards and intentional threats within the aviation ecosystem. Although safety and security share common objectives, they differ in their technical focus, methodological approaches, and operational implications, as highlighted by Pettersen-Gould & Bieder (2020). As these authors argue, maintaining the effectiveness of safety-related defenses is essential for protecting hazardous technologies, given their reliance on past incidents and the dynamic, yet fragile, organizational structures that support them.

From a security perspective, the primary challenge lies in identifying and managing risks associated with hostile intent, manifested through internal or external acts of sabotage. As noted by Schulman (2020), a fundamental distinction between safety and security management lies in the primacy of malicious intent in security-related threats. This distinction is increasingly relevant in aviation, where societal trends and technological adoption often outpace regulatory and organizational responses, creating vulnerabilities within critical infrastructure such as airports.

These vulnerabilities are further exacerbated by the growing exposure of aviation systems to cyber threats. Cyberattacks targeting data integrity, communication networks, and operational platforms represent a significant concern for both safety and security management. As Schulman (2020) observes, the progressive incorporation of digital components into complex systems introduces additional layers of vulnerability, complicating the processes of risk forecasting and system comprehension. In aviation, where connectivity across multiple dimensions is essential, this cyber–physical interdependence amplifies the potential impact of malicious actions.

Within airport environments, the management of unmanned aircraft systems illustrates the limitations of traditional approaches to safety and security. As noted by Merkert & Bushell (2020), some airports have implemented measures to manage drone activity within their airspace; however, many of these approaches remain reactive or defensive in nature. Literature increasingly emphasizes the need for proactive and preventive management stra-

tegies that integrate safety and security considerations into a unified operational framework.

Academic definitions of safety and security commonly distinguish between the two based on intentionality and systemic orientation. Safety primarily addresses unintentional hazards and accidental risks, focusing on the system's capacity to avoid causing harm to its environment. In contrast, security is concerned with intentional threats and malicious actions, emphasizing the system's ability to withstand harm originating from its environment (Pettersen-Gould & Bieder, 2020). These distinctions underscore the necessity of coordinated management approaches capable of addressing both dimensions simultaneously.

From the perspective of airport user protection and operational resilience, Bongiovanni (2020) synthesizes these approaches by highlighting the legal and managerial dimensions of risk management through both differential and collaborative models. This synthesis, presented in Table 2, illustrates how safety and security measures can be aligned within airport management systems to enhance decision-making and organizational coordination.

Table 2. Approaches to safety and security in airports: a synthesis

Airport safety and security	Legal approach	Managerial approach	Design approach
Focus	Law	Resources/goals	Users
Mission	Zero unintentional accidents (safety); zero intentional incidents (security)	Efficiently mitigate risks	Delight users
Driver for innovation	Changes in societal practices cause regulations to change	Changes in regulations, business goals, and budget cause managerial practices to change	Changes in users' needs and jobs to be done change experience design
Lead-innovator	Legislator	Enlightened manager	User experience designer
Innovation source	Top-down	Top-down/bottom-up	Bottom-up
Should safety and security be separated or combined?	Separation: two different regimes	Separation/combination: depending on resources and goals	Combination: both are components of users' experience
Overarching question	"We need to meet specific standards in terms of safety and security events happening in the airport"	"We need to be compliant to regulations together with employing the most efficient mix of resources and achieving our business goals"	"We need to make safety and security a memorable experience for our users"

Source: Reproduced from (Bongiovanni, 2020, p. 60)

Despite the development of robust safety cultures, security risks often remain beyond the full control of organizations. External threats, such as terrorism or coordinated cyber-physical attacks, may materialize regardless of internal preparedness and are not necessarily linked to economic performance or production systems (Jore, 2020). Consequently, even well-managed organizations may experience severe disruptions resulting from security breaches.

Finally, the protection of critical air transport infrastructure against combined physical and cyber threats requires integrated management cycles that bridge safety and security functions. As emphasized by Mantzana et al. (2020), enhancing interoperability among existing systems and aligning physical and digital protection mechanisms are essential steps toward developing more resilient and adaptive aviation security solutions.

Methodology

Building on the research question, "How can anti-drone technologies be effectively integrated into existing security protocols to protect the civil aviation ecosystem and ensure comprehensive management in Colombian airports?", this study adopts a qualitative research approach based on systematic observation and documentary analysis. The research design is descriptive in nature and focuses on the identification, classification, and interpretation of academic and technical sources related to unmanned aircraft systems, aviation security, and counter-drone technologies.

The documentary analysis was conducted using specialized academic databases, including Scopus, EBSCOhost, and Google Scholar. The primary selection criteria prioritized peer-reviewed publications released between 2019 and the first semester of 2024, with limited exceptions made for earlier works considered highly relevant to the analytical framework. The reviewed literature is largely drawn from indexed journals specializing in aviation, aerospace systems, and security studies, as reflected in the reference list.

The methodological process followed three structured phases planning, execution, and completion adapted from the framework proposed by Niño-Rojas (2011). During the planning phase, the phenomenon under study was defined and the literature was systematically organized into three analytical categories: Airports and Drones, Integrated Aviation Security (safety–security), and Anti-Drone Systems as a Management Tool for Aeronautical Security.

The execution phase involved data processing, qualitative analysis, and interpretative synthesis of the selected sources, allowing for the identification of patterns, challenges, and emerging trends in the integration of counter-drone systems within airport security environments. Finally, the completion phase consisted of consolidating the analytical findings into a structured academic manuscript.

This methodological approach is grounded in an interpretive paradigm, drawing upon the researcher's empirical, academic, and ethical expertise. The interpretive perspective is considered appropriate for analyzing the evolving technological and regulatory lands-

cape of unmanned aircraft systems and anti-drone solutions, recognizing the dynamic and still-developing nature of knowledge in this domain.

Anti-drone systems for aviation safety management

Current drone detection systems used in aviation environments present operational limitations, making it necessary to assess the probability of threat detection under varying operational and environmental conditions. As noted by Łukasiewicz & Kobaszyńska-Twardowska (2022), these systems, "composed of devices operating on diverse principles, should be constructed based on the probability of detecting a drone under established conditions" (p. 96). Consequently, both the operational characteristics of unmanned aircraft and the contextual conditions of their deployment directly influence the effectiveness of preventive and neutralization measures.

From an operational perspective, it is essential to consider systems capable of identifying risks posed by both individual drones and coordinated drone swarms. This requires an analytical approach supported by probabilistic and experimental models that address the increasing autonomy and adaptability of unmanned aircraft. As highlighted by Öz & Sert (2019), emerging generations of drones pose significant challenges, particularly in relation to "complete situational awareness of airspace and the automatic execution of all types of missions" (p. 706). In this context, organizations face the fundamental question of how to protect critical aviation infrastructure against such agile and heterogeneous threats.

Importantly, the risks associated with malicious drone operations are not limited to physical intrusion. Cyber-related threats, including electronic interference and signal manipulation, have emerged as critical vulnerabilities affecting airports and other elements of national critical infrastructure. In response, the formal management of aviation security has become a standard requirement within international civil aviation. The implementation of Security Management Systems (SeMS), supported by Safety Management Systems (SMS), is currently regarded as best practice for addressing both physical and cyber-related threats, as emphasized by Stastny & Stoica (2022). In this context, Table 3 presents proposed measures aimed at enhancing the effectiveness of ATM-related SMS in the management of cybersecurity risks.

Table 3. Proposed measures to enhance ATM Safety Management System (SMS) effectiveness in addressing cybersecurity threats

SMS Elements	*Potential Organisational Vulnerability/Need*	Proposed Counter-Measures for SMS Enhancement
Safety Policy	Organisation insufficiently aware of need for defence against cybersecurity threats.	Incorporate the need to reinforce the SMS and support the SeMS within the organisation's safety policy.
Organisational Safety Responsibilities	Key personnel are unaware of their roles and responsibilities in respect of cybersecurity threats.	Define roles and responsibilities for key safety personnel in respect of cybersecurity threats, and the need to liaise with and support organisational security management personnel.

SMS Elements	*Potential Organisational Vulnerability/Need*	Proposed Counter-Measures for SMS Enhancement
Coordination of Emergency Response Plan (ERP)	Emergency Response Plan unprepared to cope with cyber-attacks.	Include cyber-attacks as a source of actual or potential disruption to be managed within the scope of the ERP.
Risk Management Process	Need to consider cybersecurity threats to safety alongside all other risks.	Include cybersecurity threats within the safety risk assessment and mitigation process, including a means of risk categorisation. Co-assurance methodologies (ref. para 6 above) may be used if consistent with the means of documenting safety arguments (e.g. use of safety cases).
Safety Interfaces	Need to ensure that SMS actions taken in respect of countering cybersecurity effects on safety are fully coordinated within the organisation.	Implement procedures to ensure full coordination between SMS responses to cybersecurity threats and wider organisational functions, including security management.
Safety Performance Monitoring	All threats to ATM safety need to be monitored to establish the scale and nature of the threats, as well as longer term trends.	Update performance monitoring procedures to include the effects of cybersecurity threats on ATM safety performance.
Continual SMS Improvement	SMS must be kept current in terms of known or anticipated threats to safety.	Updated assessments of cybersecurity threats to be taken into account as part of regular SMS effectiveness reviews.
Safety Reporting	Need to achieve full visibility of cybersecurity occurrences and their effect on safety performance.	Introduce further categorisation within the safety reporting system to take account of cybersecurity events, including a means of severity classification (in terms of safety impact).
SMS Audits	To ensure that cybersecurity counter-measures are in place and functioning effectively.	To include SMS measures to counter cybersecurity threats in regular SMS audits.
Safety Communication	Cybersecurity issues and events need to form part of normal organisational communications (internal and external) on safety matters.	To improve organisational awareness by including cybersecurity information within normal communications methods on safety matters.
Training and Education	A key need is awareness of cybersecurity threats and defences at all levels of the organisation.	To formalise awareness of cybersecurity matters through their inclusion in organisational training programmes.

Source: Reproduced from (Stastny & Stoica, 2022, p. 8)

With regard to technological solutions, currently available anti-drone systems despite their limitations commonly rely on radar-based detection, acoustic interception, infrared sensors, and electro-optical devices (Popescu, 2021; Semenyuk et al., 2025). Detection remains the primary enabling function, as it supports subsequent processes of recognition, identification, and localization, forming the foundational architecture of any counter-drone system. Within airport environments, the effective management of these technologies requires an integrated assessment of the electromagnetic spectrum, the physical layout of operational and administrative facilities, and the characteristics of controlled airspace, as noted by Mackie & Lawrence (2019) and Pérez-Herrera (2013). This holistic approach is essential not only for system implementation, but also for fostering an organizational security culture oriented toward the integrity and resilience of aviation protection systems.

Findings

The analysis indicates that the rapid expansion of unmanned aerial vehicles (UAVs) in the 21st century has significantly outpaced the capacity of the aviation sector to anticipate and regulate their operational implications. The widespread commercial availability and diversification of drone applications have accelerated their integration into air operations, while simultaneously increasing regulatory complexity and enforcement challenges.

A key finding of this study is that anti-drone systems are increasingly understood not merely as technological countermeasures, but as integral components of aviation safety and security management systems. The reviewed literature highlights that the effectiveness of such systems depends on their integration within structured management frameworks rather than on standalone technological solutions.

The findings also reveal that risks associated with drone operations extend beyond physical intrusion, encompassing cyber-related threats, privacy violations, and disruptions to airport operations. These risks are amplified in operational environments where detection, identification, and response capabilities are limited or insufficiently coordinated.

Furthermore, the analysis shows that regulatory instruments and technical standards alone are insufficient to ensure comprehensive protection against malicious or unregulated drone activities, particularly in complex airport environments. Instead, effective mitigation requires coordinated detection and response mechanisms adapted to the operational characteristics of each airport.

In the specific context of Colombian airports, the findings indicate that no single anti-drone technology is capable of effectively mitigating all potential threats. Rather, the integration of multiple complementary systems aligned with local technological infrastructure, airspace characteristics, personnel capabilities, and organizational context emerges as a necessary condition for managing drone-related risks and safeguarding the civil aviation ecosystem.

Discussion

The integration of unmanned aircraft into the aviation ecosystem has fundamentally reshaped not only operational practices, but also regulatory and security paradigms. The findings of this study highlight the growing gap between rapid technological innovation and the capacity of regulatory and management frameworks to respond effectively to emerging risks. In this context, anti-drone systems emerge not solely as technological solutions, but as critical enablers of aviation safety and security governance.

The discussion reveals that the accelerated adoption of drone technologies has challenged traditional regulatory approaches, which have struggled to adapt at the same pace as technological development. This imbalance has contributed to regulatory fragmentation and uneven enforcement, particularly in complex environments such as airports. From this perspective, the application of analytical frameworks such as game theory helps to illustrate the strategic interaction between drone operators, regulatory authorities, and security stakeholders, underscoring the adaptive and dynamic nature of contemporary airspace threats.

These findings suggest that regulatory agencies must move beyond reactive rulemaking toward anticipatory and adaptive regulatory models. Proactive frameworks that account for future technological developments would facilitate the safe integration of drones into controlled airspace while reducing vulnerabilities associated with malicious or unauthorized operations. Within this regulatory landscape, anti-drone systems play a complementary role by reinforcing compliance and supporting enforcement mechanisms rather than replacing regulatory oversight.

At the operational level, the deployment of anti-drone technologies raises important considerations related to privacy, proportionality, and civil liberties. Effective security strategies must balance the need to protect critical infrastructure -such as airports- with the obligation to respect individual rights. Achieving this balance requires coordinated collaboration among regulatory authorities, airport operators, technology providers, and the broader civil community.

The discussion further emphasizes that the diversity and cultural specificity of operational contexts limit the effectiveness of singular or standardized security solutions. Airport environments vary significantly in terms of infrastructure, traffic density, and surrounding land use, requiring adaptive and context-sensitive approaches to counter-drone management. In densely populated areas, for example, the selection of detection and neutralization technologies must minimize collateral risks while maintaining operational effectiveness.

Finally, the successful integration of anti-drone systems depends not only on technological capabilities, but also on organizational preparedness. Personnel training, system interoperability, and the integration of human factors with technological systems are essential to ensuring effective aviation safety management. A holistic approach combining detection technologies, data analysis tools, and structured management systems supports a resilient and adaptive security posture tailored to the specific needs of each aerodrome.

In the specific context of Colombia, the discussion of anti-drone systems acqui-

res particular urgency given the country's unique security landscape. Unlike most nations where drone threats to civil aviation are primarily associated with reckless recreational use, Colombia faces the compounded challenge of organized armed groups systematically deploying unmanned aerial vehicles for surveillance, armed attacks, and logistics support to illicit activities.

The proliferation of low-cost commercial drones among violent non-state actors has been extensively documented in the academic literature: Chávez & Swed (2023) demonstrate that the tactical adoption of commercial UAV platforms by insurgent groups represents a structural shift in asymmetric warfare, reducing the technical and financial barriers that previously limited airpower to state actors. This dynamic is particularly salient in Colombia, where dissident factions of the Fuerzas Armadas Revolucionarias de Colombia (FARC) and the Ejército de Liberación Nacional (ELN) have progressively integrated drone capabilities into their operational arsenals.

According to the Presidencia de la República de Colombia (2025), a total of 115 drone-related incidents were recorded in 2024 alone, primarily perpetrated by illegal armed organizations and terrorist groups, targeting both security forces and critical infrastructure. Matiz-Rojas & Fernández-Camargo (2023) situate this phenomenon within the broader transformation of armed conflict in Colombia, highlighting the role of artificial intelligence and autonomous systems in reconfiguring the tactical environment for non-state actors. This figure represents a dramatic escalation compared to previous years and underscores the structural nature of the threat, consistent with global trends identified by Schwartz et al. (2022) in their cross-national analysis of armed drone proliferation and its implications for security governance. President Gustavo Petro publicly acknowledged in late 2025 that the conflict had evolved into a "war of drones and anti-drones," signaling the extent to which unmanned systems have reshaped the operational environment for national defense and aviation security alike (El Universo, 2026).

In response to this escalating threat, the Colombian government launched the Proyecto Escudo Nacional Antidrones (National Anti-Drone Shield Project), described by the Ministry of Defense as the most ambitious aerial defense strategy in the country's history (Segurilatam, 2026). With an initial budget of approximately USD 1.68 billion (COP 6.3 trillion), the project is structured around three foundational pillars: legislation and doctrine, training and operations, and technological deployment. Rather than constituting a simple procurement initiative, the Escudo Nacional represents a comprehensive framework that integrates detection networks based on radar and radio-frequency sensors, targeting the protection of critical infrastructure including energy facilities, governmental headquarters, and strategic military installations.

This multi-layered institutional approach aligns with recommendations in the counter-UAS literature, argue that effective anti-drone systems for facilities of national importance must be engineered around probabilistic detection models rather than single-technology deployments, a principle clearly reflected in the Colombian framework. The creation of a multidisciplinary drone and anti-drone unit comprising personnel from the armed forces and the National Police similarly resonates with findings by Okpaleke et al. (2023), who demonstrate in the context of West African counterinsurgency operations that cross-ins-

titutional drone coordination significantly improves both detection rates and operational response.

At the tactical level, Colombia has taken concrete steps toward deploying specific Counter-Unmanned Aircraft Systems (C-UAS) capabilities. The Ministry of Defense contracted the Dedrone Tracker AI C2 system developed by U.S.-based Dedrone Tactical at a cost of approximately USD 25.4 million, providing 360-degree spatial coverage with integrated electronic warfare capabilities for Army and Air Force installations across the country (Saumeth, 2025).

Simultaneously, regional authorities such as the Valle del Cauca and Cauca departmental governments have independently acquired ORION-10 MP and ORION-D MP systems from Singapore-based TRD Systems, incorporating both active inhibition and passive detection capabilities with a geolocation range of up to three kilometers (Webinfomil, 2024).

The decentralized nature of these acquisitions reflects the severity and geographic dispersion of drone-based threats across Colombian territory, a pattern consistent with what Mittal & Goetz (2025) describe as the "distributed threat" model characteristic of modern drone conflicts, in which adversaries exploit geographic breadth to overwhelm centralized defense architectures. Furthermore, the Fuerza Aeroespacial Colombiana (FAC) and the Corporación de Alta Tecnología para la Defensa (Codaltec) have jointly developed a domestic mobile anti-drone system capable of inhibiting GPS, GLONASS, and Wi-Fi signals. This development is significant not only operationally but also in terms of the emergence of national technological self-sufficiency in this domain, a capacity that Park et al. (2021) identify as a critical enabler of long-term counter-UAS governance for states facing persistent asymmetric drone threats.

On the regulatory front, Colombia has pursued parallel legislative efforts to accompany these technological investments. The Ministerio de Defensa, together with the Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) and the Ministerio de Transporte, introduced draft legislation before Congress to establish a comprehensive regulatory framework governing drone importation, registration, and operation, as well as the deployment of counter-drone systems. A key provision of this initiative designates MinTIC as the technical authority responsible for monitoring and blocking radio frequencies used by drones in illicit activities, including in airport zones and energy installations (Ministerio de Tecnologías de la Información y las Comunicaciones, 2025).

This approach to spectrum governance as a counter-drone instrument is consistent with the technical recommendations advanced by Popescu (2021) and later elaborated by Stastny & Stoica (2022), who identify radio-frequency management as a foundational layer of any national C-UAS framework for civil aviation. Additionally, Resolution 000242, enacted in January 2026, restricts UAV imports to designated entry points including El Dorado International Airport and the port of Cartagena, while prohibiting postal delivery as an import channel—a measure specifically designed to curtail smuggling of drones for criminal purposes (Dudenhoeffer, 2020; Dirección de Impuestos y Aduanas Nacionales, 2026). These regulatory developments demonstrate a growing recognition

that effective counter-drone governance requires the alignment of airspace regulation, spectrum management, and security policy within a unified national framework, a conclusion that resonates with Merkert & Bushell (2020) finding that regulatory fragmentation remains the primary structural barrier to effective UAS risk management across aviation systems.

Conclusions

The strategic management of unmanned aerial vehicles and anti-drone systems presents a growing challenge for civil aviation, particularly in the context of balancing technological innovation with regulatory control. This study highlights that the rapid expansion of drone operations both legal and illicit has exposed structural limitations within existing airspace management and security frameworks, especially in airport environments.

The findings support the conclusion that regulatory instruments alone are insufficient to address the risks associated with unregulated or malicious drone activities. Instead, an adaptive and proactive regulatory environment is required, supported by integrated management approaches that incorporate anti-drone systems within established aviation security protocols. Such integration should not rely on a single technological solution, but rather on a coordinated combination of detection, identification, and response systems tailored to the operational characteristics of each airport.

Furthermore, effective mitigation of drone-related threats depends on cross-sector collaboration involving governmental authorities, airport operators, industry stakeholders, and academic institutions. This collaborative approach is essential to anticipate emerging risks, address privacy and security concerns, and ensure the resilience of the civil aviation ecosystem.

Finally, the evolving nature of drone technologies and their potential misuse underscores the need for continued research and policy development. Future studies should further explore adaptive regulatory models, technological interoperability, and human factors within anti-drone and aviation safety management systems, contributing to a comprehensive and sustainable approach to safeguarding airport operations.

In the Colombian context, the conclusions of this study acquire additional dimensions that extend beyond the traditional scope of civil aviation security. The country presents a dual threat scenario in which drone misuse is simultaneously linked to airport operational disruptions and to active armed conflict involving illegal organizations. As documented by the Colombian Presidency (2025) and corroborated by regional security reports, the use of armed drones by dissident FARC factions and other non-state actors has inflicted significant human and material losses on the national armed forces, while also raising critical concerns regarding the security of civilian infrastructure including airports, energy facilities, and urban centers.

This phenomenon demonstrate that violent non-state groups increasingly exploit the affordability and versatility of commercial drone platforms to compensate for their conventional military inferiority, a trend that has accelerated sharply in Colombia since 2022. The

States facing higher levels of intrastate conflict and terrorism are significantly more likely to pursue and accelerate counter -drone programs- a pattern that Colombia's Proyecto Escudo Nacional clearly exemplifies. This dual threat profile demands that anti-drone strategies in Colombia be conceived not only within a civil aviation safety framework, but also as a component of national defense and public security policy, integrating civil-military coordination mechanisms.

The Proyecto Escudo Nacional Antidrones, launched in January 2026 with an initial investment of approximately USD 1.68 billion, represents the most significant institutional response to the drone threat in Colombian history and, according to available evidence, in the Latin American region as a whole. Structured around three pillars -legislation and doctrine, training and operations, and technological deployment- the initiative reflects the multi-dimensional approach advocated throughout this study and corroborated by comparative analyses of national counter-UAS programs.

The integration of electronic warfare capabilities with radar-based detection and AI-assisted command-and-control systems produces significantly higher threat neutralization rates than single-modal deployments—a finding with direct implications for the design of the Escudo Nacional. Its success will depend not only on the effective procurement and deployment of detection and neutralization systems, but on the simultaneous development of legal frameworks, institutional capacity, interoperability standards, and personnel training programs.

In this regard, regarding the organizational fragility of safety-security hybrid systems are particularly pertinent: the durability of the Escudo Nacional will require sustained investment in organizational learning and adaptive governance mechanisms beyond the initial technology procurement phase. The process of selecting technology providers through competitive evaluation involving more than 100 companies from 21 countries, with tests commencing in March 2026, is itself indicative of the complexity and strategic stakes involved.

From a civil aviation perspective, the conclusions of this study reinforce the urgency of extending anti-drone system integration to airport environments specifically. The Aeropuerto Internacional El Dorado, as the principal air hub of the country and a node for strategic infrastructure, has been the subject of prior technical studies proposing RF-based jamming systems capable of covering the full approach and landing area. These efforts, complemented by broader security technology upgrades including AI-assisted behavioral detection and high-definition monitoring systems implemented at El Dorado by the end of 2024, represent important advances but do not yet constitute a fully integrated counter-drone architecture.

This gap between incremental technological upgrades and systemic integration is precisely what identify as the central challenge for airports seeking to operationalize C-UAS capabilities: achieving functional coexistence between counter-drone systems and the electromagnetic environment of active airport operations remains technically demanding and institutionally complex. As this study concludes, such integration remains both a technical and institutional imperative for safeguarding the Colombian civil aviation ecosystem. Fu-

ture policy and research efforts should prioritize the harmonization of civil and defense anti-drone frameworks, ensuring that the protection of airport environments is explicitly addressed within the broader national aerial defense strategy an alignment that is achievable through the systematic expansion of Safety Management Systems to incorporate cybersecurity and counter-UAS dimensions as co-equal components of aviation security governance.

Mandatory Declaration on the Use of Generative AI

The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

References

Balladares, P., Bustos-Estrella, A., Albuja, G. & Alarcón, M. (2024). Advances in military drone technologies. *Athenea Engineering Sciences Journal, 5*(18), 7-18. https://doi.org/10.47460/athenea.v5i18.81

Bongiovanni, I. (2020). User safety and security experience: Innovation through design-inspired methods in airports in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 53-61). Springer. https://doi.org/10.1007/978-3-030-47229-0_6 PMid:32116208

Boyle, M. J. (2020). *The drone age: How drone technology will change war and peace.* Oxford Academic. https://doi.org/10.1093/oso/9780190635862.001.0001

Chávez, K. & Swed, O. (2021). The proliferation of drones to violent nonstate actors. *Defence Studies, 21*(1), 1-24. https://doi.org/10.1080/14702436.2020.1848426

Chávez, A. & Swed, O. (2023). Emulating underdogs: Tactical drones in the Russia-Ukraine war. *Contemporary Security Policy, 44*(4), 592-605. https://doi.org/10.1080/13523260.2023.2257964

Choi, Y. J. (2022). Security Threat Scenarios of Drones and Anti-Drone Technology. *Academy of Strategic Management Journal, 21*(1), 1-7. https://www.abacademies.org/abstract/security-threat-scenarios-of-drones-and-antidrone-technology-13612.html

Cole, M. (2014). Towards proactive airport security management: Supporting decision making through systematic threat scenario assessment. *Journal of Air Transport Management, 35*, 12-18. https://doi.org/10.1016/j.jairtraman.2013.11.002

Costin, A., Turtiainen, H., Khandker, S. & Hämäläinen, T. (2023). Towards a Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD) technologies and communications. *arXiv preprint arXiv:2302.08359.* https://doi.org/10.48550/arXiv.2302.08359 https://doi.org/10.14722/spacesec.2023.239280

Dirección de Impuestos y Aduanas Nacionales. (2 de febrero de 2026). *DIAN implementó nuevas medidas aduaneras para el control de la importación e ingreso de drones al país.* dian.gov.co. https://www.dian.gov.co/Prensa/Paginas/NG-DIAN-actualiza-disposiciones-y-fortalece-el-control-aduanero-para-el-ingreso-e-importacion-de-drones-al-pais.aspx

Dudenhoeffer, D. D. (2020). Day of the drone: Protecting critical infrastructure from terrorist use of unmanned aerial systems In A. Brill., K. Misheva. and M. Hadji-Janev (Eds.), *Toward effective cyber defense in accordance with the rules of law* (pp. 17-31). IOS Press. https://doi.org/10.3233/NHSDP200038

El Universo. (21 de enero de 2026). *El ambicioso escudo antidrones con el que Colombia quiere combatir las ofensivas aéreas de los grupos armados.* eluniverso.com. https://www.eluniverso.com/noticias/internacional/el-ambicioso-escudo-antidrones-con-el-que-colombia-quiere-combatir-las-ofensivas-aereas-de-los-grupos-armados-nota/

Hurtado-Cubillos, A. E. (2022). *Riesgos de las aeronaves remotamente tripuladas bajo el enfoque de ciberseguridad* [Tesis de especialización, Universidad Piloto de Colombia]. Repositorio institucional. http://repository.unipiloto.edu.co/handle/20.500.12277/12519

Hwang, S. P. & Kim, D. H. (2020). A study on the establishment of anti-drone system for the protection of national important facilities. *Journal of Digital Convergence, 18*(11), 247-257. https://doi.org/10.14400/JDC.2020.18.11.247

Jačionis, T. (2020). Modern methods for detection of unmanned aerial vehicles. *Mokslas Lietuvos ateitis / Science - Future of Lithuania, 12.* https://doi.org/10.3846/mla.2020.11435

Jore, S. H. (2020). Security and Safety Culture-Dual or Distinct Phenomena? in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 43-51). Springer. https://doi.org/10.1007/978-3-030-47229-0_5

Kang, D., Lee, G. & Choi, J. Y. (2021). Secure authentication protocol for drones in LTE networks [Conference paper]. *Advances in security, networks, and Internet of Things* (pp. 17-32). Springer, Cham. https://doi.org/10.1007/978-3-030-71017-0_2

La Cour-Harbo, A. & Schiøler, H. (2019). Probability of Low-Altitude Midair Collision Between General Aviation and Unmanned Aircraft. *Risk analysis: an official publication of the Society for Risk Analysis, 39*(11), 2499-2513. https://doi.org/10.1111/risa.13368 PMid:31291487 PMCid:PMC6899918

Law No. 12 of 1947. Whereby the Convention on International Civil Aviation, signed in Chicago on December 7, 1944, is hereby approved. November 7, 1947. D.O. No. 26537. https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/arbol/1422.htm

Łukasiewicz, J. & Kobaszyńska-Twardowska, A. (2022). Proposed method for building an anti-drone system for the protection of facilities important for state security. *Security and Defence Quarterly, 39*(3), 88-107. https://doi.org/10.35467/sdq/149268

Mackie, T. & Lawrence, A. (2019). Integrating unmanned aircraft systems into airport operations: From buy-in to public safety. *Journal of Airport Management, 13*(4), 380-390. https://doi.org/10.69554/JJJB3489

Mantzana, V., Georgiou, E., Chasiotis, I., Gkotsis, I., Stelkens-Kobsch, T. H., Kazoukas, V., Papagiannopoulos, N., Nikas, A. & Komninos, F. (2020). Airports' crisis management processes and stakeholders involved. *Annals of Disaster Risk Sciences, 3*(1). https://doi.org/10.51381/adrs.v3i1.47

Matiz-Rojas, A. H. & Fernández-Camargo, J. A. (2023). On the use of artificial intelli -gence as a means and methods in armed conflicts. *Revista Científica General José María Córdova, 21*(42), 525-549. https://doi.org/10.21830/19006586.1151

Merkert, R. & Bushell, J. (2020). Managing the drone revolution: A systematic literature review into the current use of airborne drones and future strategic directions for their effective control. *Journal of Air Transport Management, 89*, 101929. https://doi.org/10.1016/j.jairtraman.2020.101929 PMid:32952321 PMCid:PMC7489224

Ministerio de Tecnologías de la Información y las Comunicaciones. (30 de julio de 2025). *Ministerios TIC y de Defensa radican proyecto de Ley para regular el uso de drones en el país.* mintic.gov.co. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/404027:Ministerios-TIC-y-de-Defensa-radican-proyecto-de-Ley-para-regular-el-uso-de-drones-en-el-pais

Mittal, V. & Goetz, J. (2025). A quantitative analysis of the effects of drone and counter-drone systems on the Russia-Ukraine battlefield. *Defense & Security Analysis, 41*(3), 490-503. https://doi.org/10.1080/14751798.2025.2479973

Niño-Rojas, V. M. (2011). *Metodología de la investigación: Diseño y ejecución.* Ediciones de la U.

Okpaleke, F. N., Nwosu, B. U., Okoli, C. R. & Olumba, E. E. (2023). The case for drones in counter-insurgency operations in West African Sahel. *African Security Review, 32*(4), 351-367. https://doi.org/10.1080/10246029.2023.2217158

Öz, T. & Sert, S. (2019). The present role of anti-drone technologies in modern warfare and projected developments. *Güvenlik Stratejileri Dergisi, 15*(32), 691-711. https://doi.org/10.17752/guvenlikstrtj.668216

Park, S., Kim, H. T., Lee, S., Joo, H. & Kim, H. (2021). Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access, 9*, 42635-42659. https://doi.org/10.1109/ACCESS.2021.3065926

Pérez-Herrera, P. G. (2013). Estudio y simulación de un sistema de vigilancia aeronáutica para el control de aproximación de aeronaves a el aeropuerto El Dorado, basado en la tecnología MLAT (Multilateración). *Redes de Ingeniería, 4*(1), 85-94. https://doi.org/10.14483/2248762X.6426

Pettersen-Gould, K. & Bieder, C. (2020). Safety and security: The challenges of bringing them together in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 1-8). Springer. https://doi.org/10.1007/978-3-030-47229-0_1

Popescu, L. R. (2021). The existing technologies on anti-drone systems. [Paper presentation]. *International Conference on Knowledge-Based Organization,* Volume 27, Issue 3, 83-91. https://doi.org/10.2478/kbo-2021-0093

Presidencia de la República de Colombia. (8 de enero de 2025). *Colombia fortalece seguridad nacional con plan anti-drones para contrarrestar amenazas y proteger infraestructuras estratégicas.* Presidencia.gov.co. https://www.presidencia.gov.co/prensa/Paginas/Colombia-fortalece-seguridad-nacional-con-plan-anti-drones-para-contrarrest-250108.aspx#:~:text=Bogot%C3%A1%2C%208%20de%20enero%20de,de%20energ%C3%ADa%20y%20centros%20poblados

Saumeth, E. (3 de junio de 2025). *Colombia adquiere sistemas antidron por 25 millones de dólares.* Infodefensa.com. https://www.infodefensa.com/texto-diario/mostrar/5312190/074-colombia-colombia-adquiere-sistemas-anti-dron-25-millones-dolares

Schulman, P. R. (2020). Safety and security: Managerial tensions and synergies in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 87-95). Springer. https://doi.org/10.1007/978-3-030-47229-0_9

Schwartz, J. A., Fuhrmann, M. & Horowitz, M. C. (2022). Do Armed Drones Counter Terrorism, Or Are They Counterproductive? Evidence from Eighteen Countries. *International Studies Quarterly, 66(*3), sqac047, https://doi.org/10.1093/isq/sqac047

Segurilatam. (23 de enero de 2026). *¿En qué consiste el Proyecto Escudo Nacional Antidrones de Colombia?* Segurilatam.com. https://www.segurilatam.com/actualidad/proyecto-escudo-nacional-antidrones-de-colombia_20260123.html

Semenyuk, V., Kurmashev, I., Lupidi, A., Alyoshin, D., Kurmasheva, L. & Cantelli-Forti, A. (2025). Advances in UAV detection: integrating multi-sensor systems and AI for enhanced accuracy and efficiency. *International Journal of Critical Infrastructure Protection, 49*, 100744. https://doi.org/10.1016/j.ijcip.2025.100744

Shin, J. M., Kim, Y. S., Ban, T. W., Choi, S., Kang, K. M. & Ryu, J. Y. (2021). Position tracking techniques using multiple receivers for anti-drone systems. *Sensors, 21*(1),

35. https://doi.org/10.3390/s21010035 PMid:33374686 PMCid:PMC7793488

Shvetsova, S. V. & Shvetsov, A. V. (2021). Ensuring safety and security in employing drones at airports. *Journal of Transportation Security, 14,* 41-53. https://doi.org/10.1007/s12198-020-00225-z

Sichko, P. (2019). Integrating unmanned aerial system operations into the Dallas/Fort Worth airport environment. *Journal of Airport Management, 13*(3), 206-214. https://doi.org/10.69554/CMDK2637

Stastny, P. & Stoica, A. M. (2022). *Protecting aviation safety against cybersecurity threats* [Paper presentation]. IOP Conference Series: Materials Science and Engineering, Volume 1226(1), 012025, Salerno. https://doi.org/10.1088/1757-899X/1226/1/012025

Tezza, D. & Andujar, M. (2019). The state-of-the-art of human–drone interaction: A survey. *IEEE Access, 7*, 167438-167454. https://doi.org/10.1109/ACCESS.2019.2953900

Unidad Administrativa Especial de Aeronáutica Civil de Colombia. (2023). *Action plan of the Unmanned Aviation Strategic Plan 2023-2026*. https://www.aerocivil.gov.co/autoridad_aeronautica/publicaciones/3958/aviacion-no-tripulada-uasdrones/

Webinfomil. (13 de septiembre de 2024). *El Ejército de Colombia recibió sistemas antidrones ORION-10 MP y ORION-D MP.* Webinfomil.com. https://www.webinfomil.com/2024/09/el-ejercito-de-colombia-recibio.html

Završnik, A. (2016). Introduction: Situating Drones in Surveillance Societies in A. Završnik (Ed.), *Drones and unmanned aerial systems* (pp. 1-18). Springer. https://doi.org/10.1007/978-3-319-23760-2_1

Revista Perspectivas en Inteligencia
(Scientific Journal of Social Sciences and Interdisciplinary Studies)
Volume 18, Number 27, January - June 2026
ISSN: 2145-194X (printed), 2745-1690 (online)
Website: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem

Disclosure Statement

The authors declare that there are no potential conflicts of interest related to this article.

Funding

The authors do not report any source of funding for the preparation of this article.

About the author(s)

Oscar Alberto Rojas-Martínez Master's Degree in Education from the Nueva Granada Military University (Colombia), with a specialization in Aeronautical and Aerospace Administration from the Nueva Granada Military University (Colombia), a degree in Business Administration from the Nueva Granada Military University (Colombia), and a degree in Military Sciences from the Escuela Militar de Cadetes General José María Córdova (Colombia), he is a university professor and researcher in the areas of aviation operational safety, higher education, human factors, security, and defense.

https://orcid.org/0000-0002-3826-2706 - Contact: nacho_rojas07@hotmail.com

Heivar Yesid Rodríguez-Pinzón Ph.D. candidate in Management Administration at Benito Juárez University (Mexico), holds a Master's degree in Economic Sciences from Santo Tomás University (Colombia) and a degree in Statistics from the National University (Colombia), he is a university professor and scientific researcher specializing in time-series and econometric models.

https://orcid.org/0000-0002-9553-0455 - Contact: rodriguezphy@javeriana.edu.co

Esta página queda intencionalmente en blanco

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Control territorial en el marco de la explotación ilícita de yacimientos de oro en Antioquia (2015-2025)

Autor

Edison Mauricio Calderón-Lozano
https://orcid.org/0009-0001-1656-3719
✉ edison.calderon@esdeg.edu.co
Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia

Citación APA: Calderón-Lozano, E. M. (2026). Control territorial en el marco de la explotación ilícita de yacimientos de oro en Antioquia (2015-2025). *Perspectivas en Inteligencia, 18*(27), 101-127. http://doi.org/10.47961/2145194X.868

Publicado en línea: 2026

Los artículos publicados por la Revista Científica Perspectivas en Inteligencia son de acceso abierto bajo una licencia **Creative Commons: Atribución - No Comercial – Sin Derivados.**

Para enviar un artículo:
https://revistaseditorialejc.org/index.php/pei/about/submissions

Esta página queda intencionalmente en blanco

PERSPECTIVAS EN INTELIGENCIA 2026

Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 18, N° 27, enero - junio 2026, pp. 101-127
http://doi.org/10.47961/2145194X.868

Control territorial en el marco de la explotación ilícita de yacimientos de oro en Antioquia (2015-2025)

Territorial control in the context of the illicit exploitation of gold deposits in Antioquia (2015-2025)

Edison Mauricio Calderón-Lozano[1]

(1) Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá, D. C., Colombia,
✉ edison.calderon@esdeg.edu.co

Resumen

En Colombia la extracción ilegal de oro figura hoy entre las economías ilícitas de mayor peso, pues provee recursos a estructuras armadas ilegales, altera los órdenes territoriales y mina la capacidad de regulación del Estado. Este trabajo analiza la manera en que la gobernanza criminal ligada a esta actividad configuró el control del territorio en Antioquia durante el periodo 2015-2025 y sus implicaciones para la seguridad nacional. Con base en informes oficiales, producción académica y datos territoriales, los hallazgos indican que la explotación ilícita de oro rebasa lo extractivo y opera como un dispositivo de regulación social, económica y coactiva; mediante él, los grupos armados restringen desplazamientos, arbitran disputas e imponen reglas de conducta, sobre todo en el Bajo Cauca y el Nordeste antioqueño. El estudio sostiene que tales arreglos desgastan la soberanía estatal, agravan la debilidad institucional y los conflictos socioambientales, y plantean retos de control territorial, articulación interinstitucional y protección de comunidades y ecosistemas.

Clasificación JEL: Q34, Q53.

Palabras clave: explotación ilícita de oro; oro de aluvión; gobernanza criminal; control territorial; Antioquia.

Abstract

In Colombia illegal gold extraction is among the most significant criminal economies, as it bankrolls unlawful armed structures, reshapes territorial orders, and undermines the State's regulatory capacity. This paper analyzes how criminal governance tied to this activity shaped territorial control in Antioquia between 2015 and 2025, and discusses its implications for national security. Drawing on official reports, scholarship, and territorial data, the findings indicate that illegal gold exploitation moves past the extractive sphere and operates as a device of social, economic, and coercive regulation: through it, armed

Fecha de recepción: 15/05/2026 | Fecha de aprobación: 31/07/2026

groups restrict movement, arbitrate disputes, and dictate rules of conduct, with particular intensity in Bajo Cauca and Northeastern Antioquia. The study argues that such arrangements erode State sovereignty, aggravate institutional weakness and socio-environmental conflicts, and raise challenges regarding territorial control, inter-institutional coordination, and the protection of communities and ecosystems.

Keywords: illicit gold mining; alluvial gold exploitation; criminal governance; territorial control; Antioquia.

Introducción

En Colombia la extracción ilegal de oro se ha afianzado como una de las economías criminales con mayor aptitud para entrelazar el deterioro ambiental, la apropiación de rentas y la redefinición del dominio territorial. Dentro de ese panorama, Antioquia resulta un caso particularmente sensible, sus enclaves mineros perduran en subregiones como el Bajo Cauca y el Nordeste, sus corredores fluviales y logísticos cumplen un papel central, y en su territorio confluyen la explotación aurífera, los grupos armados ilegales y circuitos comerciales de escasa trazabilidad.

Según la línea base, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) construyó un estudio junto con el Gobierno de Colombia, en el que en 2014 se contabilizaron 78.939 hectáreas con indicios de explotación de oro de aluvión, situadas sobre todo en Antioquia (33 %) y Chocó (46 %); entre los municipios más golpeados figuraban Nechí, Zaragoza, Cáceres, El Bagre, Tarazá, Caucasia, Segovia, Remedios, Anorí y Amalfi (Ministerio de Minas y Energía de Colombia y Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2018, 2022).

Más allá de su dimensión extractiva, el oro presenta atributos que lo convierten en un recurso especialmente funcional para economías ilegales: alto valor, facilidad de transporte, posibilidad de almacenamiento y amplias oportunidades de mezcla con circuitos aparentemente legales. En Antioquia esta condición ha favorecido mecanismos de ocultamiento de la producción, estrategias de "legalización" del mineral y prácticas de lavado de activos difíciles de rastrear, configurando una economía sumergida orientada a la captura de rentas y al sostenimiento de redes ilegales (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC] et al., 2017).

En esa misma dirección, Global Financial Integrity et al. (2021) advierten que distinguir entre oro de origen lícito e ilícito resulta particularmente complejo y que la vulnerabilidad del metal se extiende a lo largo de toda la cadena, desde la extracción hasta la comercialización y exportación. Esta característica obliga a analizar la explotación ilícita no solo como un problema ambiental o minero, sino como un circuito económico y logístico con implicaciones directas para la seguridad.

La relevancia del problema también radica en que la explotación ilícita de oro se inserta en territorios en los que la autoridad estatal opera de manera fragmentada, selectiva o insuficiente. En estos escenarios, las rentas auríferas no solo financian actores

armados ilegales, sino que pueden convertirse en base material de arreglos de regulación coercitiva sobre comunidades, mercados y corredores estratégicos. Esta dinámica puede examinarse a partir del concepto de gobernanza criminal, entendido como la creación, imposición o administración de reglas por parte de actores criminales que, en determinadas circunstancias, coexisten, compiten o se superponen con estructuras estatales.

Por consiguiente, la literatura reciente ha mostrado que estos arreglos no emergen necesariamente en contextos de vacío absoluto de autoridad, sino en órdenes híbridos en los que actores estatales, políticos y criminales disputan o comparten capacidades de regulación (Feldmann y Luna, 2022; Uribe et al., 2026). Esta precisión es clave para el caso antioqueño, donde la existencia de operativos, oficinas públicas y marcos normativos no ha impedido que organizaciones armadas impongan reglas sobre la extracción, la movilidad y la comercialización del oro.

En Antioquia esta problemática resulta estratégica por al menos tres razones. En primer lugar, porque la explotación ilícita de oro fortalece economías criminales con capacidad de reproducir violencia, financiar estructuras armadas y sostener redes de intermediación política y económica. En segundo lugar, porque la actividad se concentra en espacios que conectan producción minera, control de corredores y proyección de otras economías ilícitas, lo que incrementa su valor territorial.

En tercer lugar, porque la respuesta estatal enfrenta un dilema persistente entre interdicción, formalización y legitimidad local, aunque la destrucción de maquinaria puede afectar capacidades extractivas cuando no se acompaña de rutas viables de regularización, coordinación institucional y alternativas económicas; también puede profundizar la conflictividad social y abrir espacio a nuevas formas de intermediación coercitiva (Cante-Maldonado y Trujillo-Paredes, 2014; Méndez et al., 2025).

Partiendo de esa problemática, el interrogante que guía el artículo se formula así: ¿Cómo ha configurado el control del territorio en el departamento de Antioquia, entre 2015 y 2025, la gobernanza criminal vinculada a la explotación ilícita de yacimientos de oro, y qué repercusiones estratégicas y retos genera para la seguridad nacional colombiana? En consonancia, el objetivo general es analizar la forma en que dicha gobernanza criminal estructuró el dominio territorial en Antioquia a lo largo de ese lapso, junto con las consecuencias estratégicas y los desafíos que el fenómeno implica para la seguridad nacional.

De ese objetivo general se derivan tres objetivos específicos: *i)* caracterizar las dinámicas territoriales de la explotación ilícita de oro en Antioquia y su articulación con los grupos armados ilegales que operan en el departamento; *ii)* identificar los mecanismos de gobernanza criminal mediante los cuales dichos actores regulan la cadena aurífera y consolidan el control territorial; y *iii)* evaluar los efectos estratégicos de estas dinámicas sobre la soberanía estatal, la estabilidad institucional y la capacidad de respuesta del Estado frente a amenazas de naturaleza compleja.

Con ese propósito, el artículo se organiza en tres apartados principales. El primero examina las dinámicas territoriales de la explotación ilícita de oro en Antioquia y su

evolución entre 2015 y 2025. El segundo analiza la cadena operativa del oro ilícito, sus vínculos con actores armados ilegales y los mecanismos de gobernanza criminal que sostienen el control territorial. El tercero evalúa los impactos estratégicos de estas dinámicas y los desafíos que plantean para la seguridad nacional colombiana.

Metodología

Categorías teóricas de análisis

El presente artículo se llevó a cabo mediante una revisión documental de naturaleza analítica, dirigida a estudiar el nexo entre la explotación ilícita de yacimientos de oro, la gobernanza criminal y el dominio territorial en Antioquia a lo largo del periodo 2015-2025. Con tal fin se consultaron y articularon producciones académicas, informes técnicos e institucionales, instrumentos normativos y análisis territoriales referidos a la minería aurífera, las economías criminales, los grupos armados ilegales y la seguridad nacional, siguiendo una lógica cercana a los abordajes cualitativos y documentales empleados en investigaciones recientes sobre la gobernanza del oro en Antioquia (Bonilla-Calle, 2022; Eslava y Preciado-Restrepo, 2019).

El acervo documental comprendió treinta y dos elementos, de un lado, trabajos académicos sobre gobernanza criminal, conflictividad minera, dominio territorial y economías ilícitas; de otro, informes oficiales y técnicos, en particular los reportes de Explotación de Oro de Aluvión (EVOA) y otras publicaciones producidas por organismos nacionales e internacionales; y, por último, normas y directrices de política pública atinentes a interdicción, formalización minera, empleo de mercurio y trazabilidad.

Como complemento, se sumaron análisis de coyuntura y prensa especializada para situar acontecimientos recientes o ilustrar mutaciones territoriales del fenómeno, sin que tales materiales fungieran como base principal del razonamiento. La pertinencia de esta selección radicó en el valor analítico de los datos técnicos y georreferenciados para describir la explotación aurífera ilegal y sus lazos con actividades criminales, en la línea de lo que exponen los informes EVOA (Ministerio de Minas y Energía de Colombia, 2022; Ministerio de Minas y Energía de Colombia y UNODC, 2018).

La delimitación temporal 2015-2025 permitió observar tanto la persistencia de nodos históricos de explotación ilícita de oro en Antioquia como la reconfiguración de actores armados y mecanismos de regulación criminal en el contexto posterior al Acuerdo de Paz. A partir de este recorte, la información se organizó en tres ejes de análisis: *i)* las dinámicas territoriales de la explotación ilícita de oro en Antioquia; *ii)* los mecanismos de gobernanza criminal mediante los cuales actores armados ilegales regularon la cadena aurífera y consolidaron control territorial; y *iii)* los impactos estratégicos y desafíos que estas dinámicas plantearon para la seguridad nacional colombiana.

En el terreno conceptual, el examen se sustentó en cuatro categorías de referencia. La inicial correspondió a la gobernanza criminal, comprendida como la aptitud de actores armados no estatales para crear, imponer o administrar reglas en territorios y mercados específicos, incluso en coexistencia conflictiva con instituciones formales (Feldmann y Luna,

2022; Uribe et al., 2026).

Asimismo, la segunda fue la de control territorial, asumida como la capacidad de regular la movilidad, el acceso a recursos, los flujos económicos y ciertas formas de orden local. La tercera correspondió a la cadena aurífera ilícita o economía criminal del oro, empleada para observar la articulación entre extracción, insumos, acopio, transporte, comercialización, documentación y lavado de activos (International Crisis Group, 2017; Laverde-Rodríguez et al., 2025; Ortiz-Riomalo y Rettberg, 2018). La cuarta categoría fue la de seguridad nacional, utilizada para interpretar los efectos de estas dinámicas sobre la soberanía estatal, la estabilidad institucional, la seguridad humana y la capacidad de respuesta del Estado.

Más que cuantificar exhaustivamente el fenómeno, esta revisión buscó identificar patrones, continuidades y transformaciones en la articulación entre economía aurífera ilegal, violencia organizada y debilitamiento de la autoridad estatal. En ese sentido, el estudio adoptó una perspectiva interpretativa y analítico-descriptiva, adecuada para integrar evidencia dispersa y producir una lectura comprensiva del caso antioqueño. Como límite, se reconoció que el artículo dependió de fuentes secundarias y, por tanto, no pretendió sustituir investigaciones de campo, sino ofrecer una síntesis crítica y argumentada de la evidencia disponible.

Sobre la base de este marco analítico, y con el propósito de proyectar sus categorías teóricas al plano del planeamiento operacional, se derivó un instrumento propio denominado Matriz de Evaluación de Gobernanza Criminal en un Área de Operaciones o Área de Responsabilidad (AO/AOR). La matriz operacionaliza las cuatro dimensiones de la gobernanza criminal -política, económica, social y ambiental- en dieciséis indicadores observables (Bloque A, diagnóstico) y las cruza con las cinco líneas de acción concurrentes propuestas en este trabajo (Bloque B, respuesta), permitiendo identificar brechas críticas y priorizar el esfuerzo institucional.

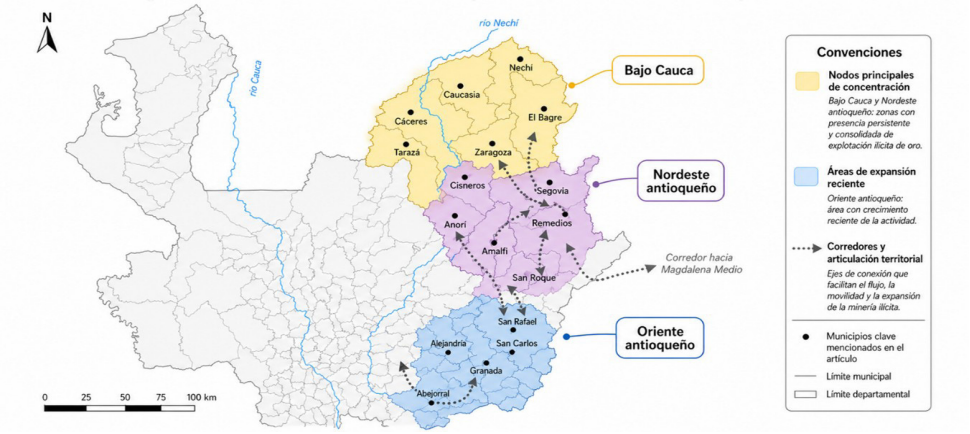
Su presentación formal se realiza en la sección final antes de las conclusiones (Tabla 4 y Tabla 5), y su desarrollo completo, con la escala de valoración cualitativa y la regla de priorización operacional, se recoge en la herramienta de doble propósito para el planeamiento de operaciones y análisis de los factores que afectan la seguridad y defensa en un AO/AOR, elaborado en formato Excel. Este instrumento articula los referentes teóricos de Feldmann y Luna (2022) con la realidad territorial estudiada, sirviendo de puente entre la evidencia empírica y las conclusiones estratégicas.

Dinámicas territoriales de la explotación ilícita de oro en Antioquia

A lo largo de la última década, la explotación ilícita de oro en Antioquia no se ha repartido de forma uniforme. Antes bien, se ha agrupado en enclaves territoriales claramente delimitados, donde convergen factores geográficos, logísticos y económicos que propician su continuidad. Los seguimientos basados en percepción remota evidencian que el fenómeno reaparece en corredores ribereños, llanuras aluviales y municipios de larga tradición minera, particularmente en el Bajo Cauca y el Nordeste antioqueño.

Antes que una dispersión aleatoria de puntos de extracción, lo que aparece es una red de nodos relativamente estables de explotación, circulación y comercialización del mineral, con capacidad para ajustarse a la presión estatal sin perder continuidad territorial (Ministerio de Minas y Energía de Colombia y UNODC, 2018, 2020).

Figura 1. Localización de los principales nodos territoriales de la explotación ilícita de oro en Antioquia (2015-2025)



Fuente: Elaboración propia, a partir de (Méndez et al., 2025; Ministerio de Minas y Energía de Colombia y UNODC, 2018, 2020, 2022)

La línea base nacional elaborada por la UNODC para 2014 ya advertía una concentración importante del fenómeno en Antioquia y Chocó, departamentos que reunían el 79 % del área detectada con evidencias de explotación de oro de aluvión, y señalaba a Nechí como el municipio con mayor afectación del país. Ese hallazgo anticipaba el lugar central de Antioquia dentro de la expansión de esta economía y dejaba ver, desde temprano, la existencia de territorios especialmente expuestos a la convergencia entre extracción aurífera, criminalidad organizada y degradación ambiental (Ministerio de Minas y Energía de Colombia y UNODC, 2018).

En este contexto, antes de examinar la evolución del fenómeno por periodos, resulta pertinente identificar los principales nodos territoriales en los que se articula la explotación ilícita de oro, así como sus modalidades predominantes, mecanismos de control criminal e impactos estratégicos, tal como se presenta en la Tabla 1.

Tabla 1. Nodos territoriales y patrones de control criminal asociados a la explotación ilícita de oro en Antioquia

Subregión / nodo	Municipios y espacios críticos	Modalidad predominante	Mecanismo de control territorial	Impacto estratégico
Bajo Cauca	Nechí, Zaragoza, Cáceres, El Bagre, Caucasia y Tarazá; ríos Cauca y Nechí.	Explotación aluvial mecanizada, dragas, dragones y motobombas.	Cobro por ingreso de maquinaria, control de insumos, gravámenes sobre producción y regulación coercitiva de operadores.	Concentración de rentas, conflictividad social, presión sobre corredores fluviales y debilitamiento de la autoridad estatal.

Subregión / nodo	Municipios y espacios críticos	Modalidad predominante	Mecanismo de control territorial	Impacto estratégico
Nordeste	Segovia, Remedios, Cisneros y San Roque; entables, socavones y nodos logísticos.	Minería de veta y enclaves de abastecimiento para explotación aluvial y subterránea.	Acopio de explosivos y químicos, custodia armada de entables y conexión con rutas de comercialización.	Expansión de la cadena criminal, articulación entre producción y logística y proyección hacia nuevas áreas del departamento.
Oriente antioqueño	Granada, San Carlos, Alejandría, San Rafael, Abejorral y cuencas de los ríos Calderas, Nare, Santo Domingo, Arma y La Miel.	Incursión reciente de dragas, retroexcavadoras y entables en zonas de alto valor ambiental.	Ocupación de cuencas, instalación de campamentos, protección armada y reapertura de minas o socavones.	Difusión territorial del fenómeno, afectación de áreas de reserva y conexión con el corredor hacia el Magdalena Medio.

Fuente: Elaboración propia, a partir de (Méndez et al., 2025; Ministerio de Minas y Energía de Colombia y UNODC, 2020, 2022)

Evolución temporal de la explotación ilícita de oro en Antioquia (2015-2025)

A. 2015-2017: consolidación territorial y captura inicial de rentas bajo coerción

Entre 2015 y 2017, Antioquia ofrecía condiciones particularmente favorables para la consolidación de la extracción aluvial mecanizada como economía ilícita: disponibilidad de cuencas estratégicas, alta liquidez del oro y debilidades institucionales en zonas periféricas. En ese contexto, la minería aurífera ilegal se convirtió en una fuente central de rentas para actores armados que obtenían beneficios mediante extorsiones a operadores y barequeros, cobros por autorización para dragar o batear, apropiación de parte de la producción e intermediación en la compra y venta del mineral (International Crisis Group, 2017; Maldonado-Sarmiento y Rozo-Gutiérrez, 2014).

Esta dinámica no debe entenderse únicamente como un problema extractivo, sino como la conformación de una cadena económica ilegal que, en muchos casos, fortalece y financia estructuras criminales organizadas (Ministerio de Minas y Energía de Colombia y UNODC, 2018). En consecuencia, el control territorial no solo servía para blindar los frentes extractivos frente a operativos estatales, sino también para asegurar obediencia social, protección armada e intermediación económica en torno a la renta aurífera (International Crisis Group, 2017).

Aunque los reportes de EVOA se consolidaron como fuente oficial a partir de 2016, sus antecedentes permiten reconstruir con mayor precisión esta primera fase. El ejercicio adelantado por el Sistema Integrado de Monitoreo de Cultivos Ilícitos (SIMCI) en 2015 marcó un punto de inflexión al proponer un sistema de detección de evidencias de explotación de oro de aluvión mediante percepción remota, integrado a plataformas de información geográfica y orientado a fortalecer el control, la gestión territorial y la focalización de intervenciones (Ministerio de Minas y Energía de Colombia y UNODC, 2018).

Ese esfuerzo, desarrollado en el marco del Convenio 589 de 2015, respondió a la ne-

cesidad de contar con evidencia técnica robusta para analizar la relación entre explotación aurífera, vulnerabilidad territorial y actividades ilegales (Ministerio de Minas y Energía de Colombia y UNODC, 2018). Mirado en perspectiva, este entramado metodológico permitió corroborar que la posterior persistencia del fenómeno en el Bajo Cauca y el Nordeste no respondía a hechos aislados, sino al asentamiento de corredores de explotación y recaudo de relativa duración.

B. 2018-2020: Expansión y estabilización en puntos clave y cambios en el control territorial

En el lapso 2018-2020, el comportamiento del fenómeno mezcló crecimiento puntual y afianzamiento en enclaves estratégicos. Según el informe EVOA 2019, Antioquia transitó de 36.447 hectáreas con evidencias de explotación de oro de aluvión en tierra en 2018 a 40.201 hectáreas en 2019, esto es, un aumento del 10 %. Resulta aún más revelador que Zaragoza, Nechí, Cáceres y El Bagre reunieran el 66 % del total departamental, dato que ratifica la presencia de núcleos territoriales en los que la actividad, lejos de extinguirse, se intensifica y se reacomoda con el paso del tiempo (Ministerio de Minas y Energía de Colombia y UNODC, 2020).

A ello se suma la expansión a lo largo de los ríos Cauca, Nechí, Porce, Bagre y Tigüí, así como de sus quebradas asociadas, lo que sugiere una lógica de ramificación espacial que permite desplazar operaciones hacia nuevas áreas cuando aumenta la presión estatal o se agotan ciertos puntos de extracción (Ministerio de Minas y Energía de Colombia y UNODC, 2020).

Este comportamiento espacial coincidió con la reconfiguración del conflicto armado posterior al Acuerdo de Paz. Como advirtió International Crisis Group (2017), el repliegue de las Fuerzas Armadas Revolucionarias de Colombia (FARC) abrió disputas por comunidades, territorios aislados y economías ilícitas, en escenarios en los que los grupos armados buscaron legitimarse ofreciendo protección y resolución autoritaria de conflictos a poblaciones que dependían de estos circuitos económicos.

En el Bajo Cauca, esta lógica se tradujo en una disputa persistente por la gobernanza territorial; análisis más recientes muestran que esa tendencia derivó en la consolidación de un orden armado en el que el Clan del Golfo, el Ejército de Liberación Nacional (ELN) y disidencias de las FARC compiten o coexisten alrededor del control de rentas, corredores y mercados locales vinculados al oro (Méndez et al., 2025). Así, los principales enclaves auríferos de Antioquia deben entenderse no solo como espacios de extracción, sino como territorios donde se articulan coerción, regulación económica y dominio local.

C. 2021-2025: Persistencia adaptativa, sofisticación de la cadena y gobernanza armada de la economía aurífera

Entre 2021 y 2025, la explotación ilícita de oro en Antioquia no solo persistió, sino que mostró una clara capacidad de readaptación territorial y económica. El informe EVOA 2021 señaló que, en el conjunto del país, el 65 % de la explotación de oro de aluvión con maquinaria en tierra tenía carácter ilícito, una cifra particularmente significativa para Antioquia,

donde esta actividad se entrelaza con disputas armadas y con el control de rutas, insumos y circuitos de comercialización (Ministerio de Minas y Energía de Colombia y Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2022).

En el Bajo Cauca, esa continuidad se tradujo en una expansión material del negocio. A lo largo del periodo 2019-2024, la maquinaria destinada a la explotación aurífera en el río Nechí aumentó de 105 a 335 unidades, lo que da cuenta de la capacidad de crecimiento de la actividad, incluso en un contexto de presión estatal sostenida. En esta subregión, actores armados como el Clan del Golfo, el ELN y disidencias de las FARC han disputado el control de municipios estratégicos como Zaragoza, El Bagre, Tarazá, Cáceres, Caucasia y Nechí (Méndez et al., 2025).

Más que involucrarse de forma directa en cada fase de la extracción, estos grupos han afianzado mecanismos de regulación coercitiva sobre la economía minera, mediante el control de insumos, el cobro de tributos y la administración de rentas. A esto se añade la participación de gatekeepers[1] profesionales que facilitan el ocultamiento del origen del mineral y su legalización fraudulenta, reforzando los vínculos entre economía criminal, control territorial y apariencia de legalidad (Global Financial Integrity [GFI], 2025).

La evidencia disponible sugiere, además, que no se está ante una actividad meramente persistente, sino ante un fenómeno con una importante estabilidad espacial. Aunque Antioquia mostró una leve reducción en el área detectada de EVOA entre 2020 y 2021, el comportamiento acumulado siguió evidenciando una fuerte permanencia en enclaves ya consolidados, especialmente en Nechí, Zaragoza, Cáceres y El Bagre (Ministerio de Minas y Energía de Colombia y UNODC, 2022). En conjunto, esta etapa muestra que la minería ilegal en Antioquia ha logrado sostenerse a partir de la combinación de coerción armada, redes logísticas, debilidades institucionales y mecanismos que permiten dar una apariencia de legalidad a una actividad esencialmente ilícita.

Dinámicas operativas: de la extracción a la renta (cadena, regulación y adaptación)

La explotación ilícita de oro en Antioquia puede entenderse como una cadena de valor criminal que articula extracción -aluvial o de veta-, control de maquinaria e insumos, acopio, transporte y comercialización. Su rentabilidad, sumada a la débil trazabilidad del mineral, facilita su circulación en mercados informales y su utilización como vehículo para ocultar recursos de origen ilícito. En este esquema, los grupos armados no capturan renta de una sola forma, sino mediante mecanismos combinados: cobros por autorización para barequear o dragar, apropiación de una porción de la producción e incluso inversión o intermediación en la compra y venta a través de terceros (International Crisis Group, 2017).

Esta lógica ayuda a explicar por qué la actividad persiste aun después de intervenciones estatales focalizadas. Lo decisivo no es solo el control del punto de extracción, sino el dominio de los eslabones que convierten el oro en flujo de renta. A nivel local, el circuito se sostiene por la convergencia entre coerción, capital y logística. En el Bajo Cauca, por

[1] Específicamente para notarios, contadores, abogados, cooperativas y, en algunos casos, autoridades locales.

ejemplo, los grupos armados pueden mantener el negocio sin operar directamente la maquinaria, siempre que conserven la capacidad de recaudo y regulación coercitiva sobre el circuito aurífero (Méndez et al., 2025).

A ello se añade la intervención de "inversionistas de alto riesgo" capaces de movilizar capital desde grandes ciudades, lo que muestra que la economía ilícita se apoya tanto en el control territorial como en flujos financieros externos (GFI, 2025). En este contexto, los principales mecanismos mediante los cuales los actores armados regulan la cadena aurífera ilegal y consolidan su control territorial se sintetizan en la Tabla 2.

Tabla 2. Cadena operativa del oro ilícito y puntos de captura criminal de renta

Eslabón	Manifestación operativa	Mecanismo de captura criminal	Resultado territorial
Extracción	Dragas, dragones, motobombas, retroexcavadoras y socavones en ríos o frentes de veta.	Cobro por permiso de operación, participación directa o indirecta y vigilancia armada del frente minero.	Instalación de enclaves productivos bajo reglas de facto.
Maquinaria e insumos	Ingreso de explosivos, combustible, mercurio, cianuro y repuestos.	Extorsión, control del abastecimiento y autorización del ingreso de equipos.	Dependencia económica de operadores frente a estructuras armadas.
Acopio y compraventa	Compra local, fundición inicial, mezcla con producción legal y uso de registros de comercialización.	Carga de oro ilegal a barequeros o compraventas y lavado de activos mediante intermediarios.	Normalización aparente del producto y opacidad en la trazabilidad.
Transporte y exportación	Movilización por rutas fluviales, terrestres y aéreas; correos humanos, joyas, lingotes y concentrados polimetálicos.	Protección de rutas, articulación con redes externas y aprovechamiento de vacíos de control.	Inserción del mineral en circuitos nacionales e internacionales y ampliación de la renta criminal.
Trazabilidad documental y refinación	Soportes de origen, declaraciones de peso y precio, refinerías y exportaciones con posibilidad de subfacturación, sobrefacturación o mezcla con oro legal.	Lavado de origen, uso de comercializadores, empresas de papel y gatekeepers profesionales, además de opacidad sobre contrapartes y destino final.	Internacionalización de rentas, blindaje financiero del negocio y mayor dificultad para separar minería tradicional de circuitos criminales.
Simulación de legalidad y gatekeepers	Uso de registros, contratos, concesiones, notarías, contabilidad, cooperativas y empresas de papel para dar apariencia de licitud al mineral y a los flujos financieros.	Ocultamiento del origen, triangulación documental, mezcla con oro legal y soporte profesional a la comercialización y al lavado.	Blindaje financiero del negocio, mayor opacidad y ampliación de la capacidad de reproducción criminal.

Fuente: Elaboración propia, a partir de (Blanquicet, 2025; El Colombiano, 2025; GFI et al., 2021; GFI, 2025; International Crisis Group, 2017; Organization of American States [OAS]. y Department against Transnational Organized Crime [DTOC], 2022)

La cadena, además, no termina en el frente extractivo. Reportes recientes indican que el oro ilegal colombiano se dirige a once países y circula mediante joyas, lingotes ocultos, correos humanos, rutas fluviales, pasos terrestres y exportaciones de concentrados polimetálicos. De acuerdo con la Policía, este mercado rondaría los 12 billones de pesos al año y sobrepasaría las 35 toneladas extraídas anualmente, lo que obliga a analizar la explotación ilícita en Antioquia como parte de una red multiescalar donde extracción, logística, lavado y exportación integran un mismo circuito criminal (Blanquicet, 2025).

La principal fragilidad de esta cadena no reside únicamente en el transporte físico del mineral, sino en su facilidad para incorporarse a circuitos aparentemente legales. La Organisation for Economic Co-operation and Development (OECD, 2016) advierte que el oro proveniente de territorios en conflicto o de alto riesgo demanda controles rigurosos de debida diligencia, comprobación de procedencia, conocimiento de las contrapartes y verificación documental al momento de exportar.

En el caso colombiano, GFI et al., (2021), OECD (2016) y Pardo-Herrera (2022) muestran que la portabilidad del metal, su capacidad de almacenar valor y la posibilidad de subfacturar o sobrefacturar envíos, alterar pesos o simular operaciones comerciales convierten la trazabilidad en un punto crítico para la seguridad económica. Por ello, la captura criminal de renta no se agota en la extracción sino que continúa en la documentación, la compraventa, la refinación y la exportación del oro.

Para 2019-2024, la evidencia de terreno y de prensa, sistematizada mediante análisis de coyuntura, muestra un aumento considerable en el número de equipos de explotación en el río Nechí (dragas, dragones y motobombas), lo que ilustra la capacidad de expansión material de la actividad y su resiliencia ante medidas de control (GFI, 2025). La combinación de alta rentabilidad, movilidad de la maquinaria y disponibilidad de capital favorece ciclos de rápida sustitución; cuando se destruye o se incauta equipo, este suele ser reemplazado si no se afectan los flujos de financiación y comercialización (GFI, 2025).

A esta cadena extractiva debe añadirse un eslabón de sofisticación financiera y documental. Estudios recientes muestran que el oro ilegal se infiltra en múltiples puntos de la producción y comercialización mediante subfacturación, sobrefacturación, mezcla con oro legal, uso de empresas de papel, manipulación de registros de proveedores y aprovechamiento de zonas francas o incluso de concesiones legales para blanquear el origen. La cadena también depende del abastecimiento ilícito de mercurio, explosivos y maquinaria -frecuentemente vía contrabando o financiamiento criminal-, lo que confirma que la gobernanza criminal no se limita al frente minero, sino que integra logística, documentación, comercio y lavado de activos como una sola arquitectura operativa (GFI, 2025; OAS y DTOC, 2022).

Vínculos con actores armados ilegales: control territorial, violencia y gobernanza criminal

Los informes oficiales de monitoreo evidencian el vínculo entre la explotación ilícita de oro y la presencia armada en Antioquia. En los municipios con mayor detección de EVOA (Zaragoza, Nechí, Cáceres, El Bagre, Remedios, Segovia, Tarazá, Anorí, Caucasia y Amalfi), se ha registrado la actividad de disidencias de las FARC-EP, del ELN, de las Autodefensas Gaitanistas de Colombia (AGC) y de organizaciones como Los Rastrojos. La violencia en estos territorios se asocia con el control de economías vinculadas a la extracción ilícita de oro (Ministerio de Minas y Energía de Colombia y UNODC, 2020).

El mismo análisis reporta fluctuaciones significativas en los homicidios, con picos en 2012 y 2015, así como tasas superiores al promedio nacional en varios de estos municipios. Estos datos sugieren una interacción entre la disputa armada, la captura de rentas y la

degradación de la seguridad local (Ministerio de Minas y Energía de Colombia y UNODC, 2020).

Para el periodo 2023-2025, los diagnósticos territoriales recientes refuerzan esta interpretación. En el Bajo Cauca se reporta la presencia del Clan del Golfo, del ELN y de disidencias de las FARC, en un contexto caracterizado por la disputa por la gobernanza territorial y el control local (Méndez et al., 2025). Este entorno competitivo se manifiesta tanto en la coerción, las amenazas y la extorsión como en el control de mercados, insumos y rutas.

El paro minero y la conflictividad social en la subregión ejemplifican cómo estas dinámicas generan tensiones abiertas entre las comunidades, el Estado y los actores armados. En el Bajo Cauca se observa un modelo productivo en el que coexisten la minería ancestral o artesanal, una empresa relevante en la explotación aluvial y diversos actores armados ilegales, con predominio del Clan del Golfo/AGC, que integran la minería criminal entre sus fuentes de financiación (Ministerio de Minas y Energía de Colombia y UNODC, 2020). Durante el paro analizado, se registró una movilización de treinta y tres días (del 2 de marzo al 5 de abril), con demandas centradas en protocolos de legalización y formalización, y tensiones alimentadas por déficits en la respuesta institucional y desacuerdos previos (Ministerio de Minas y Energía de Colombia y UNODC, 2020).

Al cierre del periodo analizado se identifica una mayor sofisticación del ecosistema criminal. Además del control armado directo, existen relaciones operativas con profesionales que actúan como "gatekeepers" (notarios, contadores, abogados, cooperativas y, en algunos casos, autoridades locales), quienes pueden facilitar la simulación contractual, el ocultamiento contable, la legalización fraudulenta u omisiones institucionales para mantener el circuito del oro ilegal (Bernal et al., 2020; GFI, 2025). En el Bajo Cauca, el Clan del Golfo se caracteriza como un actor controlador con capacidad para ejercer un control territorial sostenido, manifestado en patrullaje armado, "aplicación de la ley" local, extorsión sistemática y regulación violenta del acceso a la maquinaria y a las rutas de comercialización, así como en mecanismos de control poblacional, como amenazas o desplazamiento forzado (GFI, 2025; Hernández-Cetina et al., 2018).

En síntesis, las dinámicas descritas permiten concluir que, entre 2015 y 2025, la explotación ilícita de oro en Antioquia: *i)* se concentra en nodos territoriales persistentes, como Bajo Cauca y Nordeste; *ii)* opera como una cadena adaptable en la que la renta se captura mediante coerción, intermediación y control logístico-financiero; y *iii)* mantiene una estrecha vinculación con actores armados ilegales que disputan y regulan territorios, lo que afecta la seguridad y la gobernabilidad local.

Mecanismos de gobernanza criminal y consolidación del control territorial

En Antioquia, la gobernanza criminal vinculada al oro puede entenderse como una forma relativamente estable de ordenar la vida económica, social y política desde estructuras armadas no estatales. No se trata, estrictamente, de un vacío del Estado, sino de una coexistencia tensa y selectiva entre instituciones formales, élites locales y actores armados que compiten por las rentas, la seguridad y la regulación cotidiana del territorio (Bonilla-Calle,

2022; Duque-Daza, 2021). Desde esa lógica, la explotación ilícita de oro no solo financia a los grupos armados: también les da margen para arbitrar conflictos, definir reglas de acceso a recursos estratégicos y afianzar formas de control territorial que combinan coerción, mediación económica e intermediación institucional (Ortiz-Riomalo y Rettberg, 2018).

A. Regulación económica de la cadena aurífera

Uno de los pilares de esa gobernanza es el control económico de la cadena del oro. En el Bajo Cauca y en Buriticá se ha documentado que las estructuras armadas cobran por "seguridad", autorizan la explotación, fijan cuotas sobre las transacciones, vigilan el transporte (formal e informal) y median en disputas entre mineros, dueños de predios y trabajadores.

A esto se suman las vacunas y otros tributos sobre la actividad extractiva, lo que muestra que el control territorial no depende tanto de operar directamente la maquinaria como de sostener una administración constante sobre los flujos de dinero y mercancías que genera la minería (Bonilla-Calle, 2022; Montoya-Restrepo, 2024). En ese sentido, como plantean Ortiz-Riomalo y Rettberg (2018), el oro termina insertándose en una cadena de valor en la que actores armados y no armados capturan rentas en distintos puntos: desde la extracción hasta el acopio, el transporte y la comercialización.

B. Producción de orden social y justicia de facto

La gobernanza criminal se consolida cuando la organización armada deja de actuar de manera esporádica y empieza a imponer reglas más o menos previsibles sobre la vida diaria. En los territorios mineros analizados se registran restricciones a la movilidad, controles sobre personas foráneas, prohibiciones de portar armas y sanciones frente a hurtos, agresiones, violencia intrafamiliar u otras conductas consideradas disruptivas del orden local.

Del mismo modo, estas estructuras intervienen en conflictos vecinales, laborales y económicos, y aplican castigos que van desde multas, trabajos comunitarios y expulsión del territorio hasta violencia letal (Bonilla-Calle, 2022). La rapidez de estas respuestas, sumada a la baja capacidad, la distancia o la desconfianza frente a la justicia formal, hace que muchos actores locales terminen recurriendo a ellas por necesidad, cálculo práctico o miedo.

C. Cooptación institucional, élites locales y coexistencia selectiva con el Estado

El control territorial no se sostiene solo con armas. También se apoya en la captura selectiva de recursos institucionales y en la articulación con actores que operan dentro de la legalidad formal. Bonilla-Calle (2022) advierte que la gobernanza criminal en Antioquia se configura en escenarios de presencia estatal desigual, donde agencias formales e informales terminan coproduciendo órdenes regionales. En una línea similar, Duque-Daza (2021) muestra que los cogobiernos entre políticos y paramilitares combinan componentes legales e ilegales dentro de un mismo continuo, en el que autoridades electas, funcionarios, recursos públicos y organizaciones criminales pueden confluir en la gestión del territorio.

Desde esta perspectiva, la minería ilícita no solo provee recursos para la guerra, sino que también alimenta redes de protección política, corrupción administrativa y apropiación

de presupuestos, contratos y decisiones estratégicas. La permanencia de estructuras armadas posteriores a las AUC, volcadas al control de economías altamente rentables como el oro, confirma que esta articulación entre crimen e institucionalidad es también una adaptación histórica del conflicto colombiano (García-Pérez, 2020).

Conviene subrayar, además, que la cooptación institucional no puede reducirse a hechos aislados de corrupción. Bonilla-Calle (2022) muestra que en el Bajo Cauca y en Buriticá se producen órdenes regionales configuradas en la interacción entre Estado y actores criminales, mientras que la literatura comparada sugiere que la gobernanza criminal puede operar más como un control compartido de la coerción entre dos actores que como una sustitución completa del Estado (Uribe et al., 2026). En Antioquia, esto significa que la autoridad formal y la autoridad armada no siempre se excluyen; muchas veces se superponen, negocian y compiten, generando zonas grises en las que la población distingue claramente entre la mera presencia estatal y la capacidad real de proteger, resolver disputas o regular la economía.

La evidencia más reciente sugiere, además, que esa coexistencia selectiva adopta formas muy concretas. En el Bajo Cauca, varios análisis sobre ilegalidad aurífera señalan la posible intervención de notarios, contadores, abogados y autoridades locales como gatekeepers capaces de validar ventas entre testaferros, simular ingresos mineros, blindar contratos o permitir la omisión de controles sobre origen, licencias y movimientos financieros. Esto no significa que toda formalidad esté contaminada, pero sí muestra que la criminalidad aurífera ha desarrollado apoyos profesionales que disminuyen los costos de la ilegalidad, aumentan la capacidad de lavado y profundizan la captura institucional. En términos estratégicos, esa mediación técnica convierte la gobernanza criminal en un sistema híbrido, sostenido a la vez por coerción armada y por una apariencia de legalidad (GFI, 2025).

D. Del enclave minero al corredor estratégico

En Antioquia, la explotación ilícita de oro adquiere un valor estratégico porque no se limita a puntos aislados de extracción, sino que se despliega en nodos y corredores que conectan la producción aurífera con otras economías ilegales y con rutas de movilidad regional. El Bajo Cauca enlaza el interior del departamento con el Caribe; el Nordeste concentra distritos mineros históricos, como Segovia y Remedios; y en ambos casos la minería se cruza con narcotráfico, deforestación, extorsión y disputas por corredores. Así, el oro deja de ser solo un recurso extractivo y pasa a convertirse en una base de dominación territorial, proyección de violencia y articulación multiescalar de economías criminales (Bernal-Guzmán, 2018; Bonilla-Calle, 2022; Montoya-Restrepo, 2024).

El reciente avance hacia el Oriente antioqueño y la localización de nodos logísticos en el Nordeste respaldan esta interpretación. Durante 2024 se informó de entables instalados en los ríos Calderas, Nare, Verde, Santo Domingo, Arma y La Miel, así como del descubrimiento de campamentos, dragas, retroexcavadoras y plantas de energía en áreas de gran fragilidad ecológica. Ya en 2025, un operativo realizado en Cisneros logró incautar 215 barras de indugel, 50 kilos de Anfo, 500 kilos de cianuro y 8 kilos de mercurio. La inteligencia policial estableció que estos insumos surtían entables ilegales asociados a la subestructura Pacificadores del Samaná del Clan del Golfo, en coordinación con la subes-

tructura Edwin Román Velásquez Valle (El Colombiano, 2025). Tomados en conjunto, tales hallazgos apuntan a que la gobernanza criminal no descansa solo en el frente extractivo, sino en la posibilidad de garantizar suministro, protección armada y expansión territorial hacia nuevas subregiones del departamento (Alda-Mejías, 2023).

Impactos estratégicos y desafíos para la seguridad nacional colombiana

Una de las consecuencias estratégicas más visibles de esta dinámica es la fragmentación de la soberanía estatal en el nivel subnacional. Cuando actores armados regulan la circulación, imponen formas de seguridad, administran justicia de facto o condicionan el acceso a economías locales, el monopolio legítimo de la coerción se debilita y surgen formas de soberanía paralela o, al menos, compartida.

Díaz-Navarro et al. (2024) interpretan este fenómeno como un desmembramiento de la soberanía estatal, mientras que Bonilla-Calle (2022) muestra que, en Antioquia, no hay una ausencia total de Estado, sino una producción conflictiva del orden en la que interactúan instituciones formales y actores armados. En términos de seguridad nacional, esto se traduce en menor capacidad para gobernar periferias estratégicas, hacer cumplir la ley y evitar la captura criminal de decisiones públicas.

Además, la gobernanza criminal deteriora la estabilidad institucional y erosiona la calidad de la democracia local. Duque-Daza (2021) advierte que estas formas de gobernanza articulan componentes legales e ilegales y suelen orientarse a apropiarse de recursos públicos bajo fachadas de legalidad. En esa misma línea, Piedrahíta-Bustamante et al. (2025) identifican mecanismos como las alianzas entre élites, el poder político, el control de la tierra y las conexiones entre política y delito, todos ellos relevantes para explicar la persistencia de órdenes sociales ilegales en Colombia. En el caso antioqueño, esto implica que la renta aurífera ilícita no solo fortalece economías criminales, sino también redes de protección, corrupción y captura institucional que desbordan el ámbito minero y afectan la gobernabilidad municipal y departamental.

A ello se suma el impacto socioambiental, que incide directamente sobre la seguridad humana. En Segovia y Remedios, la convergencia entre minería de gran escala, pequeña minería y presencia de actores armados ha intensificado conflictos sociales, despojo, violaciones de derechos humanos y deterioro ecosistémico (Bernal-Guzmán, 2018). Para el Bajo Cauca, Montoya-Restrepo (2024) subraya que el extractivismo aurífero se ha entrelazado con debilidades de la política pública, destrucción ambiental, pobreza persistente y un tratamiento violento de los conflictos socioambientales.

Los desplazamientos asociados a la violencia y al daño ambiental muestran, además, que la minería ilegal no solo genera renta sino que también fractura el tejido social y aumenta la presión sobre la capacidad estatal de respuesta (Díaz-Navarro et al., 2024). En conjunto, estos efectos permiten identificar un patrón de impactos estratégicos que trasciende el ámbito extractivo y compromete dimensiones centrales de la seguridad nacional, tal como se resume en la Tabla 3.

Tabla 3. Impactos estratégicos de la gobernanza criminal aurífera sobre la seguridad nacional

Dimensión	Manifestación en Antioquia	Implicación para la seguridad nacional
Soberanía estatal	Sustitución parcial de funciones estatales en seguridad, regulación económica y resolución de conflictos en enclaves mineros.	Fragmentación de la autoridad pública y pérdida de capacidad de gobierno territorial.
Estabilidad institucional	Protestas recurrentes, cooptación selectiva, vacíos de coordinación y captura de rentas locales.	Debilitamiento de la gobernabilidad, menor legitimidad institucional y mayores costos de intervención.
Seguridad humana y ambiental	Contaminación con mercurio y cianuro, destrucción de cauces, desplazamiento, restricciones a la movilidad y deterioro de medios de vida.	Expansión de riesgos sanitarios, humanitarios y socioambientales con efectos de largo plazo.
Financiación armada	Cobro de tributos, control de maquinaria, acopio, comercialización y aprovechamiento de mercados internacionales.	Fortalecimiento financiero de estructuras armadas y prolongación de disputas territoriales.
Control de corredores	Articulación entre Bajo Cauca, Nordeste, Oriente y conexiones hacia Magdalena Medio y otras economías ilícitas.	Mayor movilidad criminal, convergencia entre narcotráfico, minería ilegal y extorsión, y mayor complejidad operativa para el Estado.
Formalización y trazabilidad	Cuellos de botella en trámites, baja capacidad territorial para resolver solicitudes, opacidad comercial y debida diligencia insuficiente en la cadena aurífera.	Persistencia de mercados grises, mayor capacidad de lavado de activos y dificultades para focalizar la acción estatal sin afectar a pequeños mineros.
Gobernanza regulatoria y mercurio	Brechas entre interdicción, formalización, trazabilidad comercial, control del mercurio y asistencia técnica territorial para pequeños productores.	Persistencia de mercados grises, continuidad del daño socioambiental acumulado y menor efectividad de la respuesta estatal.

Fuente: Elaboración propia, a partir de (Blanquicet, 2025; Bonilla-Calle, 2022; Duque-Daza, 2021; Hernández-Naranjo, 2026; Ley 1658 de 2013; Ley 1892 de 2018; Montoya-Restrepo, 2024; Procuraduría General de la Nación, 2024)

A. Desafíos para la seguridad nacional

Frente a este panorama, los desafíos para la seguridad nacional colombiana pueden sintetizarse en cuatro frentes. El primero consiste en dejar atrás enfoques centrados exclusivamente en la destrucción de maquinaria y avanzar hacia intervenciones integrales sobre toda la cadena de valor del oro, desde el acopio y el transporte hasta la comercialización, el lavado de activos y las redes de facilitación política y profesional (Ortiz-Riomalo y Rettberg, 2018). El segundo exige fortalecer una presencia estatal efectiva en los territorios mineros, no solo en clave coercitiva, sino también en justicia, infraestructura, formalización diferenciada, protección ambiental y alternativas económicas, de modo que comunidades y mineros reduzcan su dependencia frente a órdenes armados (Bonilla-Calle, 2022; Eslava y Preciado-Restrepo, 2019).

El tercero pasa por articular las políticas de seguridad, minería, ambiente y desarrollo territorial, corrigiendo las tensiones entre fomento extractivo, protección ecológica y respuesta militar que han marcado varios escenarios del Bajo Cauca (Montoya-Restrepo, 2024). El cuarto obliga a reconocer el carácter multiescalar de la amenaza, que combina violencia armada, captura institucional, degradación ecosistémica y economías ilícitas conectadas con corredores estratégicos. Desde esta perspectiva, el fenómeno aurífero ilegal no puede entenderse solo como delito económico, sino como un problema de gobernanza territorial y resiliencia estatal.

Por eso, la respuesta estatal no puede agotarse en la interdicción de maquinaria. El Decreto 2235 de 2012 ya advertía que la exploración y explotación ilícita con maquinaria pesada y uso de mercurio o cianuro podía constituir una amenaza grave para el ambiente y para la seguridad nacional, al favorecer desplazamiento, extorsión, lavado de activos y financiamiento de grupos armados. Sin embargo, la política pública reciente también deja claro que el problema exige capacidades administrativas sostenidas en el tiempo. El Plan Único de Legalización y Formalización Minera identifica cuellos de botella asociados a la confianza institucional, el financiamiento, las condiciones territoriales, la incertidumbre ambiental, la asistencia técnica y la débil articulación entre niveles de gobierno (Ministerio de Minas y Energía de Colombia, 2022).

Para Antioquia, además, prevé mesas técnico-jurídicas, matrices de seguimiento en tiempo real, planes trimestrales de priorización y acompañamiento directo a pequeños mineros. En otras palabras, la seguridad nacional depende tanto de la acción contra estructuras criminales como de la capacidad estatal para distinguir entre minería tradicional susceptible de formalización y economías armadas que capturan la cadena aurífera.

B. Formalización, trazabilidad y control del mercurio

Aunque Colombia ha construido un marco normativo importante para contener la ilegalidad y los daños socioambientales -Decreto 2235 de 2012 para la interdicción de maquinaria, Ley 1658 de 2013 para reducir y eliminar el uso de mercurio, Ley 1892 de 2018 de aprobación del Convenio de Minamata, y Ley 2250 de 2022, junto con el Plan Único de Legalización y Formalización Minera-, la persistencia del fenómeno evidencia una brecha profunda entre el diseño normativo y la capacidad real de implementación en los territorios. El propio Plan Único reconoce obstáculos estructurales relacionados con la confianza institucional, el acceso a financiación, la asistencia técnica, la falta de información actualizada y la incertidumbre sobre áreas libres y restricciones ambientales.

A su vez, la Procuraduría General de la Nación advirtió en 2024 que el Bajo Cauca y el Nordeste antioqueño se han convertido en epicentros de contaminación por mercurio en ríos como el Cauca, Nechí, Porce y Nare, mientras que las Mesas Territoriales 2023-2024 mostraron que cualquier respuesta integral debe articular dimensiones ambientales, mineras, de seguridad y de derechos humanos.

En ese sentido, uno de los desafíos estratégicos más complejos no es únicamente cerrar frentes de explotación o destruir maquinaria, sino intervenir la interfaz entre interdicción, formalización, trazabilidad comercial y sustitución tecnológica, para evitar que la simulación de legalidad siga operando como escudo del control criminal (Ley 1658 de 2013; Ley 1892 de 2018; Ministerio de Minas y Energía de Colombia, 2022; Procuraduría General de la Nación, 2024). Vista desde la seguridad nacional, la cuestión no se agota en reducir las superficies explotadas: el reto consiste en evitar que el oro siga operando como sostén financiero y político de órdenes armados regionales.

En 2026 se alertó sobre el hecho de que las economías regionales del país se expanden al amparo de la regulación informal, la apropiación de rentas y el control armado, en tanto las estructuras ilegales rebasan los 27.000 integrantes entre combatientes y redes cri-

minales (Hernández-Naranjo, 2026). Llevado al caso antioqueño, esto significa que la minería ilegal no puede tratarse como un asunto sectorial, porque alimenta mercados locales bajo reglas armadas, genera costos fiscales ocultos, consolida dependencias comunitarias y restringe la capacidad del Estado para recaudar, regular y garantizar derechos.

Por ello, una estrategia eficaz debe combinar interdicción selectiva sobre maquinaria, insumos y comercializadores; trazabilidad financiera y comercial; formalización diferenciada para la minería de subsistencia; y reconstrucción de presencia institucional con coordinación entre nación, departamento y municipios (Lopera-González, 2020).

Del diagnóstico a la acción: matriz de evaluación de la gobernanza criminal en un Área de Operaciones y un Área de Responsabilidad AO/AOR

La evidencia sistematizada en las secciones previas -dinámicas territoriales, cadena operativa del oro ilícito, impactos estratégicos, desafíos institucionales y debate sobre formalización y mercurio- exige un instrumento analítico que traduzca los hallazgos en categorías operables para el planeamiento estratégico. Con ese propósito se propone la Matriz de Evaluación de Gobernanza Criminal en un Área de Operaciones o Área de Responsabilidad (AO/AOR), un instrumento de doble bloque -diagnóstico y respuesta- que operacionaliza la tesis central del artículo y sirve de puente entre la evidencia acumulada y las conclusiones estratégicas.

El Bloque A opera como matriz de diagnóstico. Descompone la gobernanza criminal en las cuatro dimensiones que estructuran el análisis del artículo -política, económica, social y ambiental- y las traduce en dieciséis indicadores con su respectiva señal observable y su fundamento teórico. Cada indicador se valora mediante una escala cualitativa de tres niveles: alto (fuerte indicio de gobernanza criminal, exige acción prioritaria), medio (configuración parcial, requiere vigilancia y refuerzo) y bajo (indicio débil o contenido, sostener y monitorear).

Del promedio de los indicadores se obtiene, además, el nivel general del AO/AOR: incipiente (índice 1,00-1,66; el actor extrae, pero aún no gobierna), consolidada (1,67-2,33; regula la cadena aurífera y provee orden local en nodos definidos) o hegemónica (2,34-3,00; sustituye ampliamente la autoridad legítima y fragmenta la soberanía en el nivel subnacional). La Tabla 4 sintetiza el conjunto de indicadores del Bloque A.

Tabla 4. Matriz de diagnóstico de gobernanza criminal en un AO/AOR (Bloque A)

Dimensión	Indicador	Señal observable	Fundamento teórico
Política	Sustitución de funciones estatales.	El actor armado administra justicia, resuelve disputas o impone normas de conducta.	Feldmann y Luna (2022)
	Cooptación o captura institucional.	Debilitamiento de la gobernabilidad, menor legitimidad institucional y mayores costos de intervención.	Bonilla-Calle (2022)
	Regulación de la movilidad y el territorio.	Controla ingreso y salida, corredores y define quién opera en las zonas de extracción.	Uribe et al. (2026)
	Fragmentación de la soberanía.	La autoridad legítima no ejerce control efectivo; coexisten reglas paralelas.	Feldmann y Luna (2022)

Dimensión	Indicador	Señal observable	Fundamento teórico
Económica	Renta ilícita del oro.	Extracción, cobro por acceso, mercurio, maquinaria o comercialización como fuente de financiación del actor armado.	Duque-Daza (2021); Uribe et al. (2026)
	Regulación de la cadena aurífera.	El actor cobra, arbitra o impone reglas sobre extracción, maquinaria, insumos o comercialización.	Ortiz-Riomalo y Rettberg (2018)
	Control de insumos y logística.	Dominio sobre mercurio, combustible, maquinaria amarilla o rutas de comercialización.	International Crisis Group (2017)
	Lavado y financiación armada.	El oro como vector de lavado de activos y sostén financiero del actor armado.	Blanquicet (2025); Hernández-Naranjo (2026)
	Dependencia económica comunitaria.	La economía local depende de la actividad ilícita y de los intermediarios armados.	Bernal-Guzmán (2018)
Social	Provisión de orden y bienes por el actor.	Provee seguridad, empleo o mediación que el Estado no garantiza (legitimidad de facto).	Feldmann y Luna (2022)
	Coerción y control social.	Imposición de normas, castigos, desplazamiento o reclutamiento en la población.	Feldmann y Luna (2022)
	Erosión de la confianza institucional.	La comunidad percibe al actor -no al Estado- como la autoridad que resuelve.	Feldmann y Luna (2022)
	Afectación a líderes y tejido social.	Amenazas o violencia contra líderes sociales, ambientales o comunitarios.	Uribe et al. (2026)
Ambiental	Daño ambiental como instrumento de control.	La degradación (deforestación, sedimentación) acompaña y consolida el dominio.	International Crisis Group (2017)
	Uso de mercurio y contaminación hídrica.	Empleo de mercurio y afectación de fuentes hídricas por la extracción ilícita.	Ortiz-Riomalo y Rettberg (2018)
	Ocupación de áreas sensibles o protegidas.	Extracción en reservas, retiros de ríos o ecosistemas estratégicos.	EVOA y autoridades ambientales
	Costos socioambientales ocultos.	Externalidades no cuantificadas (salud, agua, suelo) que profundizan la vulnerabilidad.	Hernández-Naranjo (2026)

Nota: Los indicadores traducen las cuatro dimensiones del marco conceptual en señales observables para el planeamiento operacional.

Fuente: Elaboración propia

El Bloque B es una matriz de respuesta que evalúa la cobertura y la eficacia de las cinco líneas de acción concurrentes propuestas por este trabajo, cruzando cada línea con su efecto esperado sobre las cuatro dimensiones del fenómeno. A diferencia del Bloque A, la lectura del semáforo se invierte: una cobertura alta se representa como situación favorable y una cobertura baja como brecha crítica, pues aquí se mide la fortaleza de la acción estatal, no la del fenómeno criminal.

Este cruce permite visualizar por qué la aplicación fragmentada de las cinco líneas -persecución financiera sin control de insumos, o control de corredores sin fortalecimiento institucional local- ha resultado insuficiente: cada línea produce efectos parciales que solo se estabilizan cuando se despliegan de manera simultánea y coordinada. La Tabla 5 presenta la estructura del Bloque B y el objetivo estratégico asignado a cada línea de acción.

Tabla 5. Matriz de respuesta: cinco líneas de acción concurrentes frente a las cuatro dimensiones de la gobernanza criminal (Bloque B)

Línea de acción concurrente	Política	Económica	Social	Ambiental	Objetivo estratégico
1. Inteligencia financiera y trazabilidad	Alta	Alta	Alta	Alta	Perseguir la renta y no solo la extracción: atacar el lavado de activos y la comercialización.
2. Control de corredores, insumos y maquinaria	Baja	Alta	Baja	Alta	Asfixiar la logística criminal (mercurio, combustible, maquinaria, rutas de comercialización).
3. Fortalecimiento de la justicia y la institucionalidad local	Alta	Baja	Alta	Alta	Recuperar la capacidad reguladora del Estado y la provisión de justicia y bienes públicos.
4. Formalización diferenciada y viable	Alta	Alta	Alta	Alta	Reducir la dependencia comunitaria frente a los intermediarios armados (minería de subsistencia).
5. Protección de comunidades y ecosistemas	Alta	Media	Media	Alta	Fin último de la intervención: seguridad humana, líderes sociales, agua, suelo y biodiversidad.

Nota: La celda indica el efecto esperado -cobertura o eficacia potencial- de cada línea de acción sobre la dimensión correspondiente. En este bloque la lectura del semáforo se invierte: alta cobertura equivale a situación favorable y baja cobertura a brecha crítica.

Fuente: Elaboración propia

La articulación de ambos bloques habilita una regla de priorización operacional: el esfuerzo institucional debe concentrarse allí donde el Bloque A registre un nivel alto de gobernanza criminal en una dimensión determinada y, simultáneamente, el Bloque B evidencie baja cobertura o eficacia de las líneas de acción vinculadas a esa dimensión. Ese cruce -fenómeno intenso, respuesta débil- identifica la brecha crítica del AO/AOR y orienta la asignación diferencial de capacidades entre Fuerzas Militares, Policía Nacional, Fiscalía, unidades de inteligencia financiera, autoridades ambientales y gobiernos territoriales.

Bajo esta lógica, la matriz cumple tres funciones simultáneas: a) traduce la categoría analítica de gobernanza criminal en un instrumento de diagnóstico verificable; b) hace explícito el carácter sistémico de las cinco líneas de acción, mostrando sus efectos cruzados sobre las cuatro dimensiones; y c) provee una base común para la coordinación interinstitucional, evitando que la respuesta estatal se disperse en operaciones tácticas sin lectura estratégica compartida. Este instrumento sirve, por tanto, de puente entre los hallazgos del caso antioqueño y las conclusiones y recomendaciones estratégicas que se formulan a continuación.

Conclusiones

El análisis desarrollado a lo largo de este artículo permite sostener una tesis central de alcance estratégico para la seguridad y defensa nacional: entre 2015 y 2025, la explotación ilícita de yacimientos de oro en Antioquia dejó de ser una simple fuente complementaria de financiación de los actores armados ilegales para convertirse en una verdadera plataforma de gobernanza criminal. Esta constatación obliga al Estado colombiano a reconceptualizar el problema y a comprender que no enfrenta un delito ambiental o económico aislado, sino un sistema de poder territorial que compite con la autoridad legítima.

La evidencia revisada demuestra que el fenómeno se concentró en nodos territoriales persistentes -de manera destacada en el Bajo Cauca y el Nordeste antioqueño-, donde la minería ilegal articuló extracción, logística, comercialización y control de corredores bajo esquemas estables de coerción y captura de rentas. Por consiguiente, el primer aporte de este trabajo es evidenciar que la explotación ilícita de oro no se distribuye de forma aleatoria, sino que se organiza en enclaves estratégicos con continuidad territorial y notable capacidad de adaptación frente a la presión estatal, lo que exige que la planeación de seguridad abandone las respuestas reactivas y adopte un enfoque anticipatorio y sostenido en el tiempo.

En segundo lugar, el estudio concluye que los actores armados ilegales no se limitan a apropiarse de una renta extractiva, sino que instauran mecanismos de gobernanza criminal que regulan la cadena aurífera y producen formas propias de orden local. El control de insumos y maquinaria, el cobro de tributos, la regulación de la movilidad, la mediación de conflictos, la imposición de normas de conducta y la cooptación selectiva de funciones institucionales consolidan un dominio territorial que trasciende el punto de extracción.

De ello se desprende una recomendación de fondo para la doctrina de seguridad y defensa: el control territorial debe redefinirse operacionalmente, dejando de entenderse solo como ocupación armada del espacio para asumirse como la disputa por la capacidad de regular comportamientos, administrar flujos económicos y condicionar decisiones públicas. En términos propositivos, esto implica que la recuperación del territorio por parte del Estado no culmina con la presencia de la fuerza pública, sino que requiere restituir de manera integral y participativa la provisión de justicia, seguridad y bienes públicos que hoy administran las estructuras criminales, involucrando activamente a las autoridades locales y a las comunidades mineras en el diseño de la respuesta.

En tercer lugar, los resultados permiten concluir que estas dinámicas comprometen de manera directa la seguridad y defensa nacional de Colombia. La gobernanza criminal asociada al oro ilegal fragmenta la soberanía estatal en el nivel subnacional, erosiona la gobernabilidad local, amplía la capacidad financiera y la autonomía operacional de las estructuras armadas, profundiza los conflictos socioambientales y deteriora la seguridad humana de las comunidades mineras.

Por tal razón, este artículo plantea con carácter propositivo que la explotación ilícita de oro debe elevarse al nivel de amenaza estratégica dentro de la Política de Seguridad y Defensa Nacional, superando su tratamiento como asunto sectorial, ambiental o de policía. Ello supone articular a las Fuerzas Militares, la Policía Nacional, la Fiscalía, las unidades

de inteligencia financiera y las autoridades ambientales en torno a objetivos comunes, con mecanismos de coordinación interinstitucional medibles y con la corresponsabilidad de los gobiernos territoriales, de modo que la respuesta del Estado sea integral, sostenida y verificable.

Desde una perspectiva estratégica, el principal reto para Colombia consiste en desmontar la función política del oro ilegal dentro de las economías criminales, es decir, su capacidad de producir orden y autoridad al margen del Estado. Este artículo propone, en consecuencia, una estrategia de lucha estructurada en cinco líneas de acción concurrentes: *i)* inteligencia financiera y trazabilidad que persigan la renta y no solo la extracción, atacando el lavado de activos y la comercialización; *ii)* control de corredores, insumos y maquinaria para asfixiar la logística criminal; *iii)* fortalecimiento de la justicia y la institucionalidad local para recuperar la capacidad reguladora del Estado; *iv)* formalización diferenciada y viable de la minería tradicional que reduzca la dependencia de las comunidades frente a los intermediarios armados; y *v)* protección de las comunidades y los ecosistemas como fin último de la intervención estatal.

La aplicación combinada de estas cinco líneas se sintetiza en la Tabla 5, cuya lectura cruzada con la Tabla 4 permite identificar en cada AO/AOR las brechas críticas y priorizar el esfuerzo institucional. Estas líneas deben desplegarse de forma simultánea y coordinada, pues su aplicación fragmentada explica en buena medida la persistencia del fenómeno. Mientras el oro siga ofreciendo liquidez, facilidad de ocultamiento y capacidad de regulación territorial, seguirá constituyendo un vector crítico de inseguridad nacional en Antioquia y en otras periferias mineras del país; por ello, la eficacia de la respuesta dependerá de sostenerla en el tiempo, medir sus resultados y construirla con la participación de los actores territoriales.

Finalmente, como principal recomendación de política pública, este artículo propone adoptar formalmente el concepto de "gobernanza criminal" como categoría analítica y operativa, operacionalizada mediante la Matriz de Evaluación de Gobernanza Criminal en un AO/AOR (Tabla 4 y Tabla 5), en el diseño de las nuevas políticas públicas de seguridad y defensa para Colombia. Nombrar el fenómeno con precisión es el primer paso para enfrentarlo: hablar de gobernanza criminal, y no solo de minería ilegal o de economías ilícitas, permite visibilizar que el verdadero campo de disputa es la autoridad sobre el territorio y no únicamente el recurso aurífero.

Incorporar esta categoría en la doctrina, el planeamiento estratégico y los instrumentos de política pública orientaría la acción del Estado hacia la recuperación de su capacidad de regular la vida social en las zonas afectadas, facilitaría la construcción de indicadores que midan la presencia efectiva del Estado -no solo el número de operaciones- y promovería un diseño de políticas participativo, en el que las comunidades, las autoridades locales y la fuerza pública actúen de manera corresponsable. En síntesis, comprender la explotación ilícita de oro como una forma de gobernanza criminal no es un ejercicio meramente conceptual, sino una condición necesaria para formular respuestas estratégicas, sostenibles y legítimas que devuelvan al Estado colombiano el control de sus territorios y garanticen la seguridad de sus ciudadanos.

Declaración obligatoria de uso de IAGen

El autor declara que no se utilizaron herramientas de inteligencia artificial generativa en la elaboración de este manuscrito.

Referencias

Alda-Mejías, S. (2023). Neopatrimonialismo y gobernanza criminal en América Latina. *Revista Científica General José María Córdova, 21*(43), 667-684. https://doi.org/10.21830/19006586.1177

Bernal, J. V., Montoya, M. F. y Olarte-Rodríguez, F. (2020). Extracción ilícita de minerales en Colombia: realidad social, jurídica y económica. *Revista de Derecho Administrativo, (19)*, 85-107. https://revistas.pucp.edu.pe/index.php/derechoadministrativo/article/view/24304

Bernal-Guzmán, L. J. (2018). Gold Mining in Northeast Antioquia: A Territorial Dispute over Development. *Gestión y Ambiente, 21*(2Supl), 74-85. https://doi.org/10.15446/ga.v21n2supl.77865

Blanquicet, J. A. (18 de mayo de 2025). *Negocio del oro ilegal en varias regiones ya pesa más en rentas criminales que la coca: informe especial.* eltiempo.com. https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/oro-ilegal-en-varias-regiones-ya-pesa-mas-en-rentas-criminales-que-la-coca-3455013

Bonilla-Calle, D. (2022). Gobernanza criminal de la minería del oro en la región del Bajo Cauca y en el municipio de Buriticá, Antioquia. *Estudios Políticos*, (65), 241-270. https://doi.org/10.17533/udea.espo.n65a09

Cante-Maldonado, F. y Trujillo-Paredes, L. F. (2014). Posibilidades de gobernabilidad y gobernanza en distintos tipos de minería. *Opera, 14*(14), 27-45. https://revistas.uexternado.edu.co/index.php/opera/article/view/3839

Decreto 2235 de 2012 [con fuerza de ley]. Por el cual se reglamentan el artículo 6° de la Decisión número 774 del 30 de julio de 2012 de la Comunidad Andina de Naciones, y el artículo 106 de la Ley 1450 de 2011 en relación con el uso de maquinaria pesada y sus partes en actividades mineras sin las autorizaciones y exigencias previstas en la ley. 30 de octubre de 2012. D.O. No. 48599. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50153

Díaz-Navarro, D. E., Martínez-Londoño, C. P. y Velandia-Canosa, E. A. (2024). El desplazamiento ambiental forzado en Colombia: Un examen sociojurídico sobre las causas multifactoriales de los movimientos poblacionales en el siglo XXI. *Estudios de Derecho, 81*(178), 54-78. https://doi.org/10.17533/udea.esde.v81n178a3

Duque-Daza, J. (2021). Gobernanza criminal. Cogobiernos entre políticos y paramilitares en Colombia. *Revista Mexicana de Ciencias Políticas y Sociales, 66*(241), 347-380. https://doi.org/10.22201/fcpys.2448492xe.2020.241.75094

El Colombiano (12 de noviembre de 2025). *Golpe a la minería ilegal: Policía incautó 500 kilos de cianuro y más de 200 barras de explosivos del Clan del Golfo en Antioquia.* elcolombiano.com. https://www.elcolombiano.com/antioquia/operativo-contra-clan-del-golfo-mineria-cisneros-antioquia-AJ30823366

Eslava, A. y Preciado-Restrepo, A. F. (2019). Ideas sobre la minería en Antioquia. Desarrollo, gobernanza comunitaria y arreglos colectivos. *Sociedad y Economía,* (38), 6-20. https://doi.org/10.25100/sye.v0i38.6212

Feldmann, A. E. y Luna, J. P. (2022). Criminal governance and the crisis of contemporary Latin American States. *Annual Review of Sociology, 48*, 441-461. https://doi.org/10.1146/annurev-soc-030420-124931

García-Pérez, P. (2020). Organizaciones armadas post Autodefensas Unidas de Colombia: Del pasado contrainsurgente al presente de criminalidad transnacional. 2006-2016. *Izquierdas, 49,* 141-158. https://doi.org/10.4067/S0718-50492020000100209

Global Financial Integrity (2025). *Potential links between criminal groups and professional gatekeepers in the dynamics of illegal gold mining in Colombia*. gfintegrity.org. https://gfintegrity.org/wp-content/uploads/2025/10/Potential-links-between-criminal-groups-and-professional-gatekeepers-in-the-dynamics-of-illegal-gold-1.pdf

Global Financial Integrity, Alliance for Responsible Mining y Centro de Estudios del Trabajo (10 de febrero de 2021). *The gold standard: addressing illicit financial flows in the Colombian gold sector through greater transparency.* gfintegrity.org. https://gfintegrity.org/report/the-gold-standard-addressing-illicit-financial-flows-in-the-colombian-gold-sector-through-greater-transparency/

Hernández-Cetina, A. W. C., Ripoll, A., y García-Perilla, J. C. (2018). "El Clan del golfo": ¿el nuevo paramilitarismo o delincuencia organizada? *El Ágora USB, 18*(2), 512-526. https://doi.org/10.21500/16578031.3363

Hernández-Naranjo, D. (4 de febrero de 2026). *Economías regionales crecen bajo control de grupos armados mientras los combatientes superan los 27.000 en Colombia.* Portafolio.co. https://www.portafolio.co/economia/regiones/economias-regionales-crecen-bajo-control-de-grupos-armados-mientras-los-combatientes-superan-los-27-000-en-colombia-487670

International Crisis Group (19 de octubre de 2017). *Los grupos armados de Colombia y su disputa por el botín de la paz.* (Report # 63). crisisgroup.org. https://www.crisisgroup.org/es/rpt/latin-america-caribbean/colombia/063-los-grupos-armados-de-colombia-y-su-disputa-por-el-botin-de-la-paz

Laverde-Rodríguez, C. A., Laverde-Rojas, H. y Devia-Barbosa, M. E. (2025). La economía ilegal del oro en América Latina: evidencia empírica sobre gobernanza, criminalidad y control estatal (2016-2022). *Revista Científica General José María Córdova, 23*(52), 819-842. https://doi.org/10.21830/19006586.1529

Ley 1658 de 2013. Por medio de la cual se establecen disposiciones para la comercialización y el uso de mercurio en las diferentes actividades industriales del país, se fijan requisitos e incentivos para su reducción y eliminación y se dictan otras disposiciones. 15 de julio de 2013. D.O. No. 48852. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53781

Ley 1892 de 2018. Por medio de la cual se aprueba el "Convenio de Minamata sobre el Mercurio", hecho en Kumamoto (Japón) el 10 de octubre de 2013. 11 de mayo de 2018. D.O. No. 50590. http://www.secretariasenado.gov.co/senado/basedoc/ley_1892_2018.html

Ley 2250 de 2022. Por medio de la cual se establece un marco jurídico especial en materia de Legalización y Formalización Minera, así como para su financiamiento, comercialización y se establece una normatividad especial en materia ambiental. 11 de julio de 2022. D.O. No. 52092. http://www.secretariasenado.gov.co/senado/basedoc/ley_2250_2022.html

Lopera-González, M. A. (2020). La formalización minera en el Bajo Cauca antioqueño a través de las áreas de reserva especial. Una aproximación al diseño institucional desde el marco de análisis y desarrollo institucional. *Estudios Políticos,* (58), 141-166. https://doi.org/10.17533/udea.espo.n58a07

Maldonado-Sarmiento, I. E. y Rozo-Gutiérrez, L. M. (2014). Convergencia de los grupos armados organizados al margen de la ley en la minería aurífera aluvial en la subregión del Bajo Cauca antioqueño. *Revista Criminalidad, 56*(3), 119-138. https://doi.org/10.47741/17943108.183

Méndez, M. L., Medina, D., García, A. y Valderrama-Arriola, M. (2025). *La batalla que estamos perdiendo en el Bajo Cauca.* Instituto para las Transiciones Integrales (IFIT) y Fundación Ideas para la Paz (FIP). https://ideaspaz.org/publicaciones/investigaciones-analisis/2025-10/la-batalla-que-estamos-perdiendo-en-el-bajo-cauca

Ministerio de Minas y Energía de Colombia (14 de noviembre de 2022). *Plan único de legalización y formalización minera*. minenergia.gov.co. https://minenergia.gov.co/es/servicio-al-ciudadano/foros/plan-%C3%BAnico-de-legalizaci%C3%B3n-y-formalizaci%C3%B3n-minera/

Ministerio de Minas y Energía de Colombia y Oficina de las Naciones Unidas contra la Droga y el Delito (2018). *Explotación de oro de aluvión, evidencias a partir de percepción remota 2016.* repositoriobi.minenergia.gov.co. https://repositoriobi.minenergia.gov.co/handle/123456789/2681?show=full

Ministerio de Minas y Energía de Colombia y Oficina de las Naciones Unidas contra la Droga y el Delito (2020). *Explotación de oro de aluvión. Evidencias a partir de percepción remota 2019.* https://www.unodc.org/documents/colombia/2020/Octubre/Informe_EVOA_2019_ESP_B.pdf

Ministerio de Minas y Energía de Colombia y Oficina de las Naciones Unidas contra la Droga y el Delito (2022). *Explotación de oro de aluvión: Evidencias a partir de percepción remota 2021*. biesimci.org. https://www.biesimci.org/index.php?id=174

Montoya-Restrepo, L. P. (2024). Los conflictos socioambientales en el Bajo Cauca antioqueño (Colombia): sentidos y políticas públicas. *Estudios de Derecho, 81*(177), 119-142. https://doi.org/10.17533/udea.esde.v81n177a6

Oficina de las Naciones Unidas contra la Droga y el Delito, Sistema Integrado de Monitoreo de Cultivos Ilícitos y Ministerio de Minas y Energía de Colombia (2017). *Caracterización de los rasgos más sobresalientes en la dinámica de explotación ilícita de oro en el departamento de Antioquia.* biesimci.org. https://www.biesimci.org/index.php?id=114

Organisation for Economic Co-operation and Development (6 de abril de 2016). *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas.* Third Edition. oecd.org. https://doi.org/10.1787/9789264252479-en

Organization of American States y Department against Transnational Organized Crime (2022). *On the Trail of Illicit Gold Proceeds: Strengthening the Fight Against Illegal Mining Finances (Colombia).* oas.org. https://www.oas.org/ext/en/security/fight-illegal-mining-financing

Ortiz-Riomalo, J. F. y Rettberg, A. (2018). Minería de oro, conflicto y criminalidad en los albores del siglo XXI en Colombia: Perspectivas para el posconflicto colombiano. *Colombia Internacional,* (93), 17-63. https://doi.org/10.7440/colombiaint93.2018.02

Pardo-Herrera, C. (2022). *Illegal Trade in Gold from Peru and Colombia. Understanding the Dynamics, Routes, and U.S. Linkages.* Terrorism The Transnational Crime and Corruption Center. George Mason University. Arlington, Va. https://cina.gmu.edu/projects/illicit-gold-from-peru-and-colombia-understanding-the-trade-routes-and-u-s-linkages/

Piedrahíta-Bustamante, P., Casas-Ramírez, D., Duque-Díez, M. y Serrano-Corredor, C. (2025). Élites y criminalidad en Colombia: Análisis desde el informe de la Comisión de la Verdad. *Historia y Comunicación Social, 30*(2), 343-355. https://doi.org/10.5209/hics.105877

Procuraduría General de la Nación (2024). *Informe nacional: Minería ilegal y conta-*

minación por mercurio en Colombia. procuraduria.gov.co. https://www.procuraduria.gov.co/Pages/mineria-ilegal-afecta-29-departamentos-colombia-informe-procuraduria.aspx

Uribe, A., Lessing, B., Schouela, N. y Stecher, E. (2026). Criminal Governance in Latin America: Prevalence and Correlates. *Perspectives on Politics, 24*(1), 124-142. https://doi.org/10.1017/S1537592725101849

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web:https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Control territorial en el marco de la explotación ilícita de yacimientos de oro en Antioquia (2015-2025)

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Edison Mauricio Calderón-Lozano es estudiante de la Maestría de Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (Colombia), Especialista en Docencia Universitaria del Centro de Educación Militar (Colombia), Especialista en Administración de Recursos Militares para la Defensa Nacional del Centro de Educación Militar (Colombia), Especialista en Conducción y Administración de Unidades Militares del Centro de Educación Militar (Colombia), Administrador de Empresas del Politécnico Grancolombiano (Colombia), profesional en Ciencias Militares de la Escuela Militar de Cadetes General José María Córdova (Colombia).

https://orcid.org/0009-0001-1656-3719 - Contacto: edison.calderon@esdeg.edu.co

Esta página queda intencionalmente en blanco

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Exposición al combate en escenarios de amenaza por UAS y salud mental operacional en soldados del Ejército Nacional desplegados en el Cauca (2024)

Autor

Jorge Luis Forero-Herrera
https://orcid.org/0000-0003-0868-5000
✉ joforero8@poligran.edu.co
Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Colombia

Citación APA: Forero-Herrera, J. L. (2026). Exposición al combate en escenarios de amenaza por UAS y salud mental operacional en soldados del Ejército Nacional desplegados en el Cauca (2024). *Perspectivas en Inteligencia, 18*(27), 131-167. http://doi.org/10.47961/2145194X.871

Publicado en línea: 2026

Los artículos publicados por la Revista Científica Perspectivas en Inteligencia son de acceso abierto bajo una licencia **Creative Commons: Atribución - No Comercial – Sin Derivados.**

Para enviar un artículo:
https://revistaseditorialejc.org/index.php/pei/about/submissions

Esta página queda intencionalmente en blanco

PERSPECTIVAS EN INTELIGENCIA 2026

Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 18, N° 27, enero - junio 2026, pp. 131-167
http://doi.org/10.47961/2145194X.871

Exposición al combate en escenarios de amenaza por UAS y salud mental operacional en soldados del Ejército Nacional desplegados en el Cauca (2024)

Combat exposure in scenarios of UAS threat and operational mental health among National Army soldiers deployed in Cauca (2024)

Jorge Luis Forero-Herrera[1]

(1) Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Bogotá, D. C., Colombia
✉ joforero8@poligran.edu.co

Resumen

Esta investigación analiza el impacto del empleo recurrente de sistemas aéreos no tripulados (UAS) por grupos armados organizados en el Cauca, Colombia, sobre la salud mental operacional del personal del Ejército Nacional de Colombia, en un escenario que desplaza el centro de gravedad del combate desde la destrucción física hacia la degradación de la integridad psicológica del combatiente. Se empleó un enfoque cuantitativo, con diseño no experimental transversal y alcance descriptivo-correlacional, sobre una muestra no probabilística por conveniencia de 130 militares desplegados en el departamento del Cauca durante 2024. Se aplicaron la *Combat Exposure Scale*, adaptada a estresores propios de la amenaza aérea, y tres instrumentos de tamizaje de amplio uso internacional: la PCL-5, el GAD-7 y el PHQ-9. Los resultados evidencian asociaciones positivas y estadísticamente significativas entre la exposición operacional y la sintomatología postraumática ($\rho = 0,43$), ansiosa ($\rho = 0,40$) y depresiva ($\rho = 0,35$), así como una elevada comorbilidad entre las tres condiciones clínicas ($\rho = 0,70$ a $0,87$). Si bien las medias muestrales se sitúan en rangos subclínicos, el 18,5% de los participantes superó el punto de corte de la PCL-5 y el 13,3% el del PHQ-9, lo que revela una distribución heterogénea de la afectación y un subgrupo crítico que los estadísticos de tendencia central invisibilizan. La literatura sobre guerra con drones atribuye este patrón a la vigilancia aérea persistente y al estímulo acústico de los motores como activadores de miedo condicionado, hipótesis que el presente diseño no permite contrastar directamente. Se argumenta que el desgaste emocional derivado de la amenaza aérea persistente debe elevarse a la categoría de indicador de alerta temprana e integrarse al ciclo de inteligencia, y se identifica un vacío en instrumentos psicométricos validados para el contexto operacional colombiano.

Clasificación JEL: H56, I12

Palabras clave: guerra de drones; salud mental operacional; inteligencia estratégica; dominio cognitivo; riesgo psicosocial.

Fecha de recepción: 19/03/2026 | Fecha de aprobación: 14/08/2026

Abstract

This study examines the impact of the recurrent use of unmanned aerial systems (UAS) by organized armed groups in Cauca on the operational mental health of Colombian National Army personnel, in a scenario that shifts the center of gravity of combat from physical destruction toward the degradation of the combatant's psychological integrity. A quantitative approach was adopted, with a non-experimental, cross-sectional design and a descriptive-correlational scope, applied to a non-probabilistic convenience sample of 130 service members deployed in the department of Cauca during 2024. The instruments administered were the *Combat Exposure Scale*, adapted to stressors specific to the aerial threat, along with three widely used screening instruments: the PCL-5, the GAD-7, and the PHQ-9. The results reveal positive, statistically significant associations between operational exposure and posttraumatic ($\rho = 0.43$), anxiety ($\rho = 0.40$), and depressive ($\rho = 0.35$) symptomatology, as well as high comorbidity among the three clinical conditions ($\rho = 0.70$ to 0.87). Although the sample means fall within subclinical ranges, 18.5% of participants exceeded the PCL-5 cutoff score and 13.3% exceeded that of the PHQ-9, revealing a heterogeneous distribution of impairment and a critical subgroup that measures of central tendency render invisible. The literature on drone warfare attributes this pattern to persistent aerial surveillance and to the acoustic stimulus of the engines as triggers of conditioned fear-a hypothesis that the present design does not allow to be tested directly. The study argues that the emotional attrition stemming from a persistent aerial threat should be elevated to the status of an early-warning indicator and integrated into the intelligence cycle, and it identifies a gap in psychometric instruments validated for the Colombian operational context.

Keywords: drone warfare; operational mental health; strategic intelligence; cognitive domain; psychosocial risk.

Introducción

Osowski resume el impacto de los drones así:

"Es un poco como tener a Dios encima de tu cabeza. Y el rayo cae con forma de misil Hellfire"

(Como se citó en Sohr, 2025, párr. 17)

En el departamento del Cauca, los grupos armados organizados han incorporado sistemas aéreos no tripulados (UAV) de bajo costo como instrumento habitual de hostigamiento y control del ambiente operacional. Las cifras oficiales dimensionan el fenómeno: durante 2024 la Policía departamental registró cien ataques con drones en el Cauca, el mayor número del país, concentrados en cinco municipios de economía cocalera, y la tendencia se sostuvo en 2025 con cincuenta y nueve eventos solo hasta el mes de mayo (Mendoza et al., 2025). Los ataques provienen principalmente de las disidencias de las FARC y del ELN, y las operaciones militares en la región han permitido incautar equipos empleados tanto para acciones ofensivas contra la Fuerza Pública como para labores de vigilancia ilegal (Rodríguez, 2026).

Pese a la creciente frecuencia de estos ataques, persiste un vacío crítico en la comprensión de su impacto psicológico sobre el personal militar colombiano. Esta modalidad

-que en el presente estudio se denomina guerra irregular aérea- altera las condiciones básicas del combate para la tropa desplegada. El atacante opera sin exposición y sin necesidad de superioridad aérea, mientras el soldado enfrenta una amenaza que no puede localizar, anticipar ni neutralizar con los medios a su disposición, en una relación que suprime la bidireccionalidad tradicional del enfrentamiento (Chamayou, 2016). A ello se suma que los sensores térmicos y las cámaras de alta resolución integradas en estas plataformas anulan el valor protector del terreno (Laghari et al., 2023), los elementos que antes brindaban cobertura ahora facilitan la exposición. Se configura así una vulnerabilidad radical que fractura el ethos militar, en la medida en que el combatiente pierde el control sobre su propia seguridad sin haber sido derrotado en un enfrentamiento.

La justificación de este estudio radica en la necesidad de elevar el estado emocional del soldado a la categoría de indicador de alerta temprana dentro del ciclo de inteligencia (Lowenthal, 2008). La institución dispone hoy de mecanismos para registrar la afectación material de sus unidades -bajas, pérdida de equipo, control territorial-, pero carece de instrumentos que permitan detectar el desgaste psicológico antes de que se traduzca en fallas operacionales. Documentar esa afectación con evidencia empírica es condición previa para incorporarla a los procesos de decisión del mando.

El propósito general de esta investigación fue analizar la relación entre la exposición operacional al combate, en un escenario caracterizado por el empleo de sistemas aéreos no tripulados, y la sintomatología clínica de estrés postraumático, ansiedad y depresión en soldados del Ejército Nacional desplegados en el Cauca durante 2024. Para ello se implementó un enfoque cuantitativo con diseño no experimental, transversal y de alcance descriptivo-correlacional, sobre una muestra de 130 militares, empleando tres instrumentos clínicos estandarizados y una versión de la Combat Exposure Scale (CES) adaptada para incorporar los estresores propios de la amenaza aérea irregular.

En coherencia con este propósito, se plantearon tres objetivos específicos: caracterizar el nivel de exposición operacional y la magnitud de la sintomatología clínica en el personal evaluado; determinar la proporción de participantes que superan los puntos de corte clínicos de cada instrumento; y establecer la asociación entre la exposición operacional y la sintomatología de estrés postraumático, ansiedad y depresión.

De lo expuesto se deriva la hipótesis de trabajo que orienta el estudio: la exposición operacional se asocia positivamente con la sintomatología clínica, si bien dicha afectación no se distribuye de manera homogénea en la muestra, sino que se concentra en un subgrupo del personal evaluado cuya magnitud queda parcialmente encubierta por los estadísticos de tendencia central.

Marco teórico

Evolución del centro de gravedad: de la trinidad de Clausewitz a la cuarta revolución industrial

La evolución de la guerra en la Cuarta Revolución Industrial ha desplazado el centro

de gravedad del combate desde la destrucción física de activos hacia la degradación de la integridad psicológica del combatiente. Esta caracterización se presenta como marco interpretativo del fenómeno y no como resultado empírico del presente estudio, que no evalúa transformaciones históricas ni centros de gravedad militares.

Este desplazamiento se inscribe en la lógica de las amenazas híbridas, entendidas como la combinación de medios convencionales, irregulares y tecnológicos por parte de actores estatales y no estatales, categoría cuya pertinencia para los conflictos latinoamericanos ha sido documentada por Ortiz (Ortiz, 2015) , y en la que los sistemas aéreos no tripulados operan como vectores de una guerra informacional y cognitiva. La proliferación de plataformas comerciales de bajo costo ha permitido que organizaciones sin capacidad de proyección aérea accedan a funciones antes reservadas a fuerzas estatales -observación persistente, adquisición de blancos y ataque-, alterando la ecuación de costos del enfrentamiento asimétrico (Conde y Whiskeyman, 2026; Cox, 2025).

Dentro de esta categoría se inscribe una modalidad que el presente estudio propone denominar guerra irregular aérea: el empleo sistemático de medios aéreos no convencionales, particularmente sistemas no tripulados de bajo costo, por parte de actores no estatales o fuerzas irregulares, con el fin de producir efectos tácticos, psicológicos y estratégicos sostenidos sobre fuerzas regulares, sin requerir superioridad aérea ni capacidad de proyección convencional. A diferencia del empleo estatal de plataformas armadas -caracterizado por la asimetría tecnológica entre potencias- y del atentado aislado con medios improvisados, la guerra irregular aérea se define por su carácter continuo y por la desproporción entre el costo del medio empleado y el efecto psicológico que produce sobre la fuerza atacada.

Esta transición obliga a reinterpretar la trinidad formulada por Clausewitz (2021) , en la que el odio y la enemistad corresponden al pueblo, el juego del azar y la probabilidad al comandante, y la subordinación a la política al gobierno. Los tres componentes se ven alterados por una tecnología que suprime la fricción para el atacante y la multiplica para las tropas desplegadas en el área de operaciones: el azar deja de distribuirse entre las partes y se concentra en una sola, con lo que la incertidumbre -que Clausewitz consideraba condición compartida del combate- se convierte en carga unilateral del defensor.

Esta evolución implica, además, que el daño ya no persigue únicamente la conquista territorial, sino la penetración del imaginario colectivo y de la psique del combatiente. (Fenstermacher et al., 2023) sostienen que el primer escudo a penetrar es el cerebro del soldado, mediante el empleo del neuroaprendizaje y la inteligencia artificial para inducir la dislocación del adversario. En esta lógica, al anular la capacidad de refugio, el dron convierte el entorno operacional en un espacio de exposición total, donde la superioridad técnica del oponente se constituye en el núcleo del estrés de combate contemporáneo (Wirtz, 2016).

Guerra cognitiva y la alteración de la percepción de seguridad

La guerra cognitiva se define como un nuevo dominio operativo donde la mente humana es el blanco estratégico principal, lo que exige la recolección de COGINT o inteligencia

cognitiva para mapear, salvaguardar y explotar las arquitecturas de decisión (Conde y Whiskeyman, 2026). Desde el ámbito de la investigación en defensa se ha señalado que este dominio integra la manipulación de la percepción, la atención y la toma de decisiones como objetivos operacionales en sí mismos (Fenstermacher et al., 2023). Para el soldado desplegado en el Cauca, esto se traduce en una alteración de su percepción de seguridad, donde el objetivo del adversario es instaurar una incertidumbre social y militar recurrente mediante la manipulación de la información y el engaño (Jiménez-Almeira, 2022).

El cerebro del combatiente es bombardeado por señales de vulnerabilidad, como el zumbido constante de los motores, que actúa como un recordatorio persistente de una muerte inminente, factor que satura su capacidad atencional y lo conduce a un estado de fatiga decisional y distorsiones sistemáticas (Chamayou, 2016). Esta afectación no es únicamente subjetiva: evidencia longitudinal en personal militar desplegado a zonas de guerra documenta reducciones volumétricas en la corteza cingulada anterior, la corteza prefrontal ventromedial y el tálamo, regiones implicadas en el procesamiento contextual y la regulación emocional, alteraciones que persisten incluso meses después del repliegue (Kühn et al., 2021).

Esta saturación sensorial activa procesos de evaluación cognitiva donde el individuo evalúa la situación como una amenaza imbatible ante la cual su capacidad de afrontamiento es insuficiente, lo que desborda su respuesta motora y adaptativa frente al estrés (Ministerio del Trabajo y Pontificia Universidad Javeriana, 2016b). La "superioridad cognitiva" buscada por el atacante utiliza analítica conductual y mapeo neuronal para manipular la conciencia colectiva, explotando la relación cada vez más íntima entre la cognición humana y los sistemas digitales (Conde y Whiskeyman, 2026; Hartley III y Jobson, 2021). De este modo, la guerra en el departamento del Cauca deja de ser un simple enfrentamiento de fuerzas para convertirse en una operación de ingeniería social y psicológica sistemática orientada a desestabilizar a las fuerzas militares y a la población (Du Cluzel, 2020; Jiménez-Almeira, 2022).

En definitiva, el empleo de drones en misiones de hostigamiento aéreo utilizados por los GAO busca invalidar el estatus que tenían las fuerzas militares de Colombia en épocas anteriores, reduciéndolos a la categoría de blancos pasivos (Chamayou, 2016; Fernández-Osorio, 2025). Este fenómeno, descrito como una "cacería humana" tecnológica que transforma profundamente la experiencia bélica y la subjetividad del combatiente (Zulaika, 2022), altera radicalmente las formas de vida y las metodologías del medioambiente del área de operaciones, instaurando un estado de vulnerabilidad radical (Chamayou, 2016; Patiño Camargo, 2024). Al no poder identificar el origen de la amenaza ni entablar un duelo simétrico debido a la falta de reciprocidad efectiva, el soldado experimenta un quiebre en su lógica de protección (Chamayou, 2016; Vargas-Cano et al., 2025). Lo anterior debilita los cimientos de la disciplina militar y la operatividad técnica frente a un enemigo que domina el espectro de guerra irregular aérea a través de métodos asimétricos y la manipulación mediática.

Conviene indicar que la evidencia disponible sobre efectos psicológicos del empleo de drones procede de tres poblaciones que no son directamente equiparables: los operadores de sistemas no tripulados, cuyo desgaste se asocia a la exposición sostenida

a imágenes de combate y a dilemas morales derivados del acto de observar (Chappelle et al., 2014); las poblaciones civiles sometidas a vigilancia aérea persistente, en las que se documentan aislamiento social y alteración de las rutinas cotidianas (Edney-Browne, 2019); y las tropas terrestres expuestas a hostigamiento aéreo, objeto del presente estudio. La extrapolación entre estas poblaciones es analógica y no sustituye la evidencia específica sobre personal desplegado, precisamente la que resulta escasa en el contexto colombiano.

La sorpresa táctica y la suspensión del diálogo bélico

La inteligencia estratégica define el empleo de drones como una sorpresa táctica, una maniobra diseñada para que el método o el momento del ataque no sea descubierto por el defensor, incluso si este conoce las capacidades generales de su adversario (Lowenthal, 2008). El conflicto en Ucrania ha evidenciado cómo la incapacidad de anticipar el empleo adversario de sistemas no tripulados constituye una falla de inteligencia con consecuencias operacionales directas (Dylan y Grossfeld, 2025).

En las condiciones del terreno del departamento del Cauca, esta sorpresa técnica se ve potenciada por la dificultad de detección temprana, lo que anula la capacidad de respuesta inmediata de las unidades que realizan control territorial. La incapacidad de predecir el ataque genera una parálisis operativa análoga a la que Clausewitz (2021) describe como colapso de la voluntad ante la incertidumbre, entendida aquí, en términos operacionales, como la pérdida transitoria de la capacidad de decisión y de respuesta coordinada de la unidad ante un ataque cuyo origen no puede identificarse, un estado donde el colapso de las esperanzas de control situacional deja al combatiente a merced del azar y el destino, rompiendo su equilibrio psicológico (Clausewitz, 2021; Wirtz, 2016).

De estos planteamientos se deduce que la sorpresa logra desorganizar las estrategias defensivas al romper la lógica interactiva del combate (Wirtz, 2016). Al eliminar a un oponente activo del campo de batalla mediante la asimetría técnica, la guerra deja de ser una interacción estratégica para convertirse en una cuestión de "mera administración" y logística para el atacante (Wirtz, 2016). Fenomenológicamente, el soldado experimenta un ataque unilateral donde no hay oportunidad de defensa proporcional, lo que transforma su moral y genera una frustración profunda que erosiona la autoconfianza. Esta ruptura del diálogo bélico tradicional se inscribe en la lógica de la guerra irrestricta, entendida como la explotación de dominios no convencionales -tecnológico, doctrinal y normativo- para erosionar la eficacia del actor estatal.

Cabe precisar que la asimetría técnica aquí descrita no equivale al *lawfare*, que designa específicamente el uso estratégico del derecho como medio de confrontación: se trata de fenómenos concurrentes, pero conceptualmente distintos (Liang y Xiangsui, 2015), categoría en la literatura colombiana en seguridad y defensa que se ha analizado bajo el marco de las guerras irrestricta e híbrida (Fonseca-Ortiz y Sierra-Zamora, 2022).

Por último, la asimetría tecnológica y la sorpresa recurrente, condiciones que (Handel, 1984) analiza como determinantes de la falla de anticipación, alteran la función protectora del terreno. En zonas de conflicto Colombiano como Argelia, El Plateado y el

cañón del Micay, entre otros, las formaciones del terreno que antes brindaban cobertura ahora facilitan la exposición total ante instrumentos que integran sensores térmicos y cámaras de alta resolución (Laghari et al., 2023), provocando que el combatiente pierda el control sobre su propia seguridad (Chamayou, 2016). Esta indefensión técnica constituye el núcleo del estrés de combate moderno, donde la sorpresa no es un evento aislado sino un estado de vulnerabilidad permanente que degrada la resiliencia operacional y la estabilidad mental de los soldados en operación del departamento del Cauca (Cox, 2025; Drone Warfare Innovations, 2026).

El trastorno de estrés postraumático (TEPT) y el encarcelamiento psíquico

El TEPT en el ámbito militar moderno se conceptualiza como una alteración psicopatológica derivada de sucesos de alto impacto emocional, donde la severidad de la exposición al combate actúa como un moderador crítico (Wolf et al., 2014). Sin embargo, en el contexto de drones, el trauma no requiere siempre de combate físico -teniendo presente que estos pueden arrojar elementos improvisados como explosivos-; se deriva de la "hipervigilancia sostenida" y la exposición visual y psicológica del área de control territorial (Chappelle et al., 2014; Saini et al., 2021).

En el departamento del Cauca se describe esta condición como un encarcelamiento psíquico, en el que el soldado se percibe atrapado en un panóptico, observado perpetuamente por una vigilancia letal que puede atacar en cualquier momento (Chamayou, 2016; Matiz-Rojas y Fernández-Camargo, 2023). La evidencia empírica en poblaciones sometidas a vigilancia aérea persistente documenta efectos psicosociales que trascienden el síntoma individual, entre ellos el aislamiento social y la percepción de sí mismo como objeto observable antes que como agente (Edney-Browne, 2019).

La validación de la PCL-5 en Colombia ha demostrado que este trastorno afecta no solo al estar expuestos a combates terrestres, sino también como respuesta a la adversidad acumulada (Muñoz-Burbano y Toro-López, 2021). Adaptaciones equivalentes desarrolladas en otros países de la región respaldan la solidez del instrumento en población hispanohablante (Durón-Figueroa et al., 2019). Los síntomas de reexperimentación y evitación en tropas expuestas a drones son comparables a los de las unidades en contacto directo con fuego enemigo, subrayando la necesidad de herramientas de diagnóstico adaptadas culturalmente (Alejo y Cuartas-Arias, 2024). El estrés postraumático, por tanto, surge de la pérdida de control y la percepción de ser una presa constante en un entorno en el que no hay refugio posible, teniendo presente las condiciones del terreno del Cauca y los cultivos ilícitos de esta zona del territorio nacional.

Asimismo, la etiología del TEPT en el escenario Caucano es multicausal y acumulativa, involucrando micro-traumas diarios causados por el hostigamiento, campos minados, francotiradores, guerra irregular aérea, entre otros. Estos factores de riesgo, clasificados como intralaborales extremos por el Ministerio del Trabajo de Colombia y Pontificia Universidad Javeriana (2016a), agotan la capacidad adaptativa del soldado. El resultado es un "estrés crónico de supervivencia" que se manifiesta en procesos de despersonalización, donde el individuo se percibe como un observador externo de su propio deterioro físico y mental ante la amenaza (Ministerio del Trabajo de Colombia y Pontifi-

cia Universidad Javeriana, 2016b).

Ansiedad anticipatoria e hiperreactividad sensorial

La ansiedad en el entorno militar se identifica como una respuesta emocional y fisiológica ante agentes estresantes que implican una amenaza seria a la integridad física, manifestándose en signos como taquicardia, sudoración y una excesiva prevención. En contextos clínicos, se ha validado que el distrés emocional derivado de escenarios de combate presenta una correlación significativa con el desarrollo de síntomas de Trastorno de Estrés Postraumático (TEPT) (Carvalho et al., 2015; Williamson et al., 2021). Esta afectación no se limita a la esfera emocional: la exposición sostenida a contextos de violencia se asocia además con el deterioro de funciones cognitivas superiores, lo que amplifica su impacto sobre el desempeño operacional (Herrera-Merchán y Cañas-Betancur, 2020).

En poblaciones expuestas a la guerra moderna, la presencia persistente de drones genera una ansiedad anticipatoria severa; este fenómeno se debe a que la vigilancia constante y la imprevisibilidad de los ataques alteran la percepción de seguridad, creando una aprehensión permanente hacia conductas rutinarias (Cox, 2025; Naeem et al., 2025). En el personal de infantería, el zumbido único de los motores de las aeronaves funciona como un potente activador psicológico *(trigger)* de terror; testimonios de guerra describen que el ronroneo lejano del motor opera como un recordatorio constante de una muerte inminente (Cox, 2025; Drone Warfare Innovations, 2026).

Esta sintomatología, que puede ser evaluada mediante escalas de tamizaje de salud mental, se manifiesta a través de alteraciones del sueño como insomnio y pesadillas, irritabilidad y una respuesta de sobresalto exagerada ante estímulos menores (Ministerio del Trabajo de Colombia y Pontificia Universidad Javeriana, 2016b; Naeem et al., 2025). Los soldados que operan en áreas críticas del Cauca pueden desarrollar una hiperreactividad sensorial donde se pierde la capacidad de distinguir el riesgo real de la amenaza percibida, manteniendo un estado de alerta o "superalerta" incluso en periodos donde no hay drones visibles (Cox, 2025; Muñoz-Burbano y Toro-López, 2021). Estos estímulos auditivos, descritos por combatientes como recordatorios persistentes de peligro, degradan la salud mental y la capacidad de concentración, elementos clasificados en Colombia como efectos de factores de riesgo psicosocial intralaboral (Cox, 2025; Drone Warfare Innovations, 2026).

La incertidumbre y la anticipación ansiosa constituyen un núcleo de desgaste psicológico que debilita procesos cognitivos superiores como la toma de decisiones y la atención (Cox, 2025; The Lancet, 2025). Al sentirse blanco de un ataque que puede ocurrir en cualquier momento desde un ángulo invisible, dado que los drones pueden navegar alrededor de coberturas tradicionales del terreno como montañas o estructuras, se describe un estado de vulnerabilidad radical, denominado encarcelamiento psíquico (Cox, 2025; Drone Warfare Innovations, 2026). Esta ansiedad no es solo un síntoma individual, sino un factor de morbilidad que afecta la cohesión de las unidades y la efectividad operativa, requiriendo herramientas de evaluación validadas para el contexto nacional que identifiquen estos riesgos de manera temprana (Alejo y Cuartas-Arias, 2024).

Depresión y herida moral en el ethos militar

La depresión en el personal militar se conceptualiza como una alteración grave de la salud mental derivada de la exposición persistente a conflictos y estresores operacionales que agotan los recursos de afrontamiento del individuo (Fernández-Duarte et al., 2024). Diversas investigaciones evidencian que esta patología se manifiesta a través de un desgaste acumulativo que deteriora la operatividad técnica y se vincula estrechamente con un riesgo incrementado de ideación e intento suicida (Pineda-Julio y Bonilla-Córdoba, 2017). El riesgo de estas conductas autolesivas aumenta de manera significativa cuando los soldados enfrentan experiencias de combate que involucran eventos inesperados o que desafían sus normas morales y éticas (Bastidas-Goyes et al., 2021).

Este fenómeno se relaciona directamente con el concepto de herida moral, entendido como el impacto psicológico y espiritual que surge al ser testigo o partícipe de acciones que violan convicciones éticas profundas (Corzo, 2009; Jinkerson, 2016). En la guerra moderna, el uso de drones introduce una crisis en el ethos militar convencional, ya que altera la percepción tradicional del combate al eliminar la reciprocidad en la exposición al peligro (Chamayou, 2016; Rivera-López, 2017). Esta asimetría tecnológica transforma la confrontación en lo que teóricos describen como una "cacería humana" unilateral, donde el combatiente se siente en un estado de vulnerabilidad radical ante una fuerza invisible que no puede controlar (Chamayou, 2016; Baleta-López, 2018).

En este escenario, la salud mental del soldado se ve comprometida en contextos de vigilancia letal y constante, condición que se asocia con sentimientos de desesperanza e impotencia psicológica (The Lancet, 2025). Estímulos sensoriales específicos, como el zumbido persistente de las aeronaves, actúan como recordatorios de una muerte inminente y funcionan como activadores de terror incluso cuando la amenaza no es visible (Cox, 2025; Drone Warfare Innovations, 2026; Naeem et al., 2025). Para mitigar estas "lesiones invisibles", es fundamental implementar intervenciones que fortalezcan la resistencia psicológica (hardiness), la cual actúa como un escudo protector que disminuye significativamente los síntomas de depresión en el personal que regresa de áreas de conflicto (Bartone et al., 2008; Zueger et al., 2022).

Debe precisarse que los constructos de encarcelamiento psíquico, herida moral, fatiga decisional y robustez psicológica proceden de artículos precedentes y constituyen marcos interpretativos del fenómeno. Ninguno de ellos fue evaluado directamente mediante los instrumentos aplicados en el presente estudio, por lo que su mención debe entenderse como hipótesis explicativa pendiente de contrastación empírica.

Resiliencia estratégica y gestión del talento humano

La integración de estos conceptos revela una comorbilidad sistémica en la que los síntomas del Trastorno de Estrés Postraumático (TEPT), la ansiedad y la depresión convergen en las tropas expuestas a la guerra moderna con drones, generando un impacto clínico transdiagnóstico que afecta significativamente el bienestar general (Bonvie et al., 2025). Para mitigar este efecto, la resiliencia debe abordarse desde un modelo que considere la interacción entre el individuo y su entorno institucional, entendiéndola como la capacidad

de sobreponerse a la adversidad y salir fortalecido tras la exposición a eventos altamente estresantes (Forés y Grané, 2008). Cuando la organización provee medidas de protección, entrenamiento especializado y un liderazgo comprometido, el soldado fortalece su capacidad operativa y recupera la sensación de control ante las amenazas tecnológicas (Booth-Kewley et al., 2013; Cox, 2025).

La dureza psicológica (hardiness) actúa como un amortiguador crítico, facilitando el compromiso operativo y la tolerancia al estrés bajo condiciones extremas (Bartone et al., 2008). En escenarios de alta complejidad donde la salud mental del personal militar se ve comprometida por el riesgo de exposición traumática acumulada, el fortalecimiento de estas actitudes de resistencia permite reencuadrar el peligro del dron no como una fuerza imparable, sino como un desafío táctico enfrentable (Bartone y Homish, 2020; Muñoz-Burbano y Toro-López, 2021). Asimismo, la implementación de estrategias de afrontamiento activo permite que el soldado gestione sus respuestas emocionales sin que estas interfieran con su juicio táctico, preservando la operatividad en situaciones de presión extrema (Ministerio del Trabajo de Colombia y Pontificia Universidad Javeriana, 2016b).

La incorporación de la ciberpsicología resulta esencial para estudiar cómo el comportamiento humano es impactado por el entorno técnico y digital del conflicto contemporáneo (Ramos-Del Río y Martí-Noguera, 2022). Es fundamental la implementación de técnicas de desensibilización sistemática ante situaciones de ansiedad, las cuales permiten entrenar al personal en la respuesta a los estímulos visuales y auditivos provocados por la vigilancia adversaria (Ministerio del Trabajo de Colombia y Pontificia Universidad Javeriana, 2016b).

Mediante la aplicación de protocolos de acción para el manejo del estrés agudo y la reestructuración cognitiva, se logra una disminución de la reactividad sensorial y la normalización de la respuesta ante la tecnología adversaria (Ministerio del Trabajo de Colombia y Pontificia Universidad Javeriana, 2016b). La administración estratégica del capital humano debe fundamentarse en la comprensión de que estos cambios representan una evolución en la sintomatología militar ante la creciente intensidad de los conflictos actuales (Corzo, 2009; Moreno-Chaparro et al., 2022).

Marco legal

La base legal de este estudio se basó en un sistema jerárquico que surgió de la Constitución Política de Colombia (1991), que estableció a Colombia como un Estado Social de Derecho basado en el respeto de la dignidad humana (Artículo 1). Este artículo establece que el Estado adoptó un papel de garante en relación a la salud de los ciudadanos, derecho que obtuvo una categoría independiente e irrenunciable de acuerdo con lo establecido por la Ley Estatutaria de Salud (Ley Estatutaria 1751 de 2015).

En el contexto particular de la Fuerza Pública, esta protección no se restringió a la provisión de servicios sino que se transformó en un requisito esencial para la consecución de los objetivos fundamentales del Estado. La Constitución Política de Colombia

(1991) otorgó a las Fuerzas Militares la tarea principal de proteger la soberanía y el orden constitucional (Artículo 217), un papel que la jurisprudencia de la Corte Constitucional entendió como una relación especial de sujeción, que exige al Estado proporcionar las condiciones ideales para mantener la integridad psicofísica de aquellos que practicaban la profesión militar.

Desde el punto de vista del sistema nacional, el manejo de la salud mental en el ámbito de la defensa se ajustó a la Ley de Salud Mental (Ley 1616 de 2013), que destacó la atención integral y la prevención de trastornos mentales como pilares esenciales de la salud pública. Sin embargo, considerando la importancia crucial del ambiente de trabajo, el Consejo Superior de Salud de las Fuerzas Militares y de la Policía Nacional emitió el Acuerdo No. 090 de 2024. Esta reglamentación se estableció como el pilar técnico-jurídico al dictar las directrices de salud mental para el Sistema de Salud de las Fuerzas Militares y de la Policía Nacional (SSMP). El pacto no solo estipuló el acto médico, sino que también vinculaba la salud mental con la aptitud psicofísica para el trabajo, reconociendo que enfermedades como el estrés postraumático, la fatiga de combate y las dinámicas características del conflicto armado interno requerían una estrategia distinta que asegurara la rehabilitación completa del combatiente.

En el marco del Derecho Operacional (DO), la salud mental se erigió como un factor determinante para la legitimidad de las operaciones terrestres unificadas. Según lo dispuesto en el Manual Fundamental de Referencia del Ejército MFE 6-27 (Ejército Nacional de Colombia, 2017), el DO integró los preceptos legales con el planeamiento y la ejecución de las misiones militares. En este sentido, la estabilidad cognitiva del soldado fue considerada el presupuesto básico para dar cumplimiento a los principios de distinción, proporcionalidad y necesidad militar propios del Derecho Internacional Humanitario. Complementariamente, el Acuerdo No. 060 de 2015 y el Acuerdo No. 061 de 2015 delimitaron la Salud Operacional como el conjunto de estrategias orientadas a mantener la capacidad de respuesta del personal uniformado. Así, la gestión del riesgo en salud mental, articulada mediante el Modelo de Atención Integral en Salud (MATIS) y el Acuerdo No. 070 de 2019, trascendió la esfera clínica para convertirse en un activo estratégico que brindó seguridad jurídica al mando institucional.

Finalmente, la praxis investigativa y clínica en este estudio se sujetó a regulaciones estrictas en materia ética y de protección de datos. La Ley 1090 de 2006 estableció el Código Deontológico y Bioético para el ejercicio de la psicología, donde se consagró el secreto profesional como una garantía inalienable del evaluado. Asimismo, el tratamiento de datos sensibles derivados de diagnósticos de salud mental se adhirió a los estándares de la Ley Estatutaria 1581 de 2012 (Ley de Protección de Datos Personales), asegurando la privacidad en un contexto donde la confidencialidad fue crítica para mitigar procesos de estigmatización. En cuanto al rigor científico, se aplicó la Resolución 8430 de 1993 del Ministerio de Salud, la cual normó las pautas éticas para la investigación en seres humanos, garantizando que el estudio respetara la dignidad del personal militar participante y asegurara la validez de los hallazgos ante la comunidad científica internacional.

Métodos

La investigación se inscribe en el paradigma positivista y adopta un enfoque cuantitativo. Su alcance es descriptivo y correlacional, dado que se orientó, por una parte, a caracterizar la magnitud de la sintomatología clínica y, por otra, a establecer el grado de asociación estadística entre la exposición operacional al combate, en un escenario de amenaza por sistemas aéreos no tripulados, y la sintomatología identificada en el personal militar evaluado. En concordancia con lo anterior, se empleó un diseño no experimental de tipo transversal. La recolección de la información se realizó en un único momento temporal, lo que permitió obtener una caracterización del estado de salud mental del personal militar desplegado en el área de operaciones del departamento del Cauca durante el año 2024, sin manipulación deliberada de las variables de estudio.

La población estuvo conformada por personal militar -oficiales, suboficiales y soldados profesionales del Ejército Nacional de Colombia- desplegado en el departamento del Cauca durante 2024. La muestra estuvo constituida por 130 integrantes, seleccionados mediante muestreo no probabilístico por conveniencia, determinado por criterios de accesibilidad, disponibilidad operativa y condiciones de seguridad propias del contexto militar.

En cuanto a su composición, el núcleo principal estuvo integrado por unidades de la Fuerza de Despliegue Rápido N.º 4 (FUDRA 4) y miembros de fuerzas especiales destacados en la Tercera División del Ejército Nacional, ubicados en la ciudad de Popayán, quienes enfrentan de manera directa las exigencias y presiones inherentes al área de operaciones. Los criterios de inclusión fueron: *1*) haber estado expuesto directa o indirectamente a eventos operacionales que involucraran el uso de drones; *2*) contar con una permanencia mínima de cuatro meses en la zona de operaciones, con el fin de asegurar una carga alostática significativa; y *3*) haber otorgado de manera voluntaria el consentimiento informado.

En lo concerniente al procedimiento y al trabajo de campo en Popayán, la recolección de datos no se asumió como un proceso distante. Con el propósito de garantizar que los participantes se encontraran en un entorno de confianza, el equipo investigador se desplazó directamente a la Tercera División. Durante una estancia de cinco días se convivió y dialogó con el personal, circunstancia que favoreció que la evaluación se desarrollara de manera más cercana y contextualizada. Esta inmersión permitió, además, identificar estresores operacionales específicos de la amenaza aérea disponible que las investigaciones no recogen, y orientó la formulación de los reactivos incorporados a la escala de exposición.

Para la toma de datos se empleó una encuesta en formato virtual mediante *Microsoft Forms.* Dicha decisión obedeció a criterios de facilidad y accesibilidad para los soldados, permitiendo que cada uno respondiera de manera autónoma y privada, al tiempo que se optimizaron los tiempos en una zona donde la disponibilidad operativa constituye una prioridad permanente. El registro incluyó el correo institucional del participante como mecanismo de control de duplicidad de respuestas; dicho identificador fue disociado de la base de análisis previamente al procesamiento estadístico y custodiado de forma

independiente. Se garantizó la confidencialidad de la información y el carácter reservado de los resultados individuales, los cuales no fueron incorporados al historial militar ni tuvieron implicaciones sobre la carrera administrativa del personal evaluado.

Para la recolección de la información se empleó una batería de cuatro instrumentos psicométricos autoadministrados, validados internacionalmente: la Combat Exposure Scale (CES), la PTSD Checklist for DSM-5 (PCL-5), la Generalized Anxiety Disorder-7 (GAD-7) y el Patient Health Questionnaire-9 (PHQ-9).

La exposición a eventos operacionales se evaluó mediante la CES, desarrollada por Keane et al. (1989), instrumento compuesto por siete ítems con formato Likert de cinco puntos. Para el presente estudio se realizó una adaptación específica: se conservaron los siete reactivos originales y su formato de respuesta, incorporando en el enunciado de cada uno los estresores propios de la amenaza aérea irregular -ataque directo o indirecto mediante drones, observación y seguimiento persistente, y sobrevuelo hostil durante las operaciones-.

La puntuación total se obtuvo aplicando el esquema de conversión ponderada establecido por los autores originales, con un rango de 0 a 41 puntos, y se interpretó conforme a las cinco categorías de exposición definidas para el instrumento (ligera, ligera-moderada, moderada, moderada-intensa e intensa). Esta decisión metodológica se sustentó en la evidencia de que las escalas centradas exclusivamente en el combate directo omiten exposiciones relevantes para la salud mental del personal desplegado, especialmente en quienes no cumplen roles de combate convencional (Bovin et al., 2023). La formulación de los reactivos adaptados se apoyó en la observación directa del investigador en el área de operaciones y en el diálogo sostenido con el personal durante el trabajo de campo, procedimiento que permitió identificar los estresores efectivamente presentes en el escenario evaluado. El texto completo de los reactivos se presenta en el Anexo A.

La sintomatología postraumática se evaluó mediante la PTSD Checklist for DSM-5 (PCL-5), instrumento de 20 ítems que mide la severidad de los síntomas conforme a los criterios del DSM-5, con un rango de puntuación entre 0 y 80 y un punto de corte de 31 puntos para la identificación de casos probables. Este instrumento cuenta con adaptaciones al español validadas en población latinoamericana que respaldan sus propiedades psicométricas (Durón-Figueroa et al., 2019). La ansiedad se midió con la Generalized Anxiety Disorder-7 (GAD-7), escala de siete ítems empleada para tamizaje, en la que una puntuación igual o superior a 10 indica sintomatología clínica relevante. Finalmente, la sintomatología depresiva se evaluó con el Patient Health Questionnaire-9 (PHQ-9), instrumento de nueve ítems que establece como punto de corte una puntuación igual o superior a 10 para depresión mayor probable.

En la presente muestra, los coeficientes de consistencia interna fueron elevados en las cuatro escalas: CES adaptada $\alpha = 0{,}90$; PCL-5 $\alpha = 0{,}98$; GAD-7 $\alpha = 0{,}96$; PHQ-9 $\alpha = 0{,}97$. Estos valores deben interpretarse considerando la marcada concentración de respuestas en el extremo inferior de las escalas.

El estudio se desarrolló siguiendo las fases propias de la ruta cuantitativa. En una

fase preparatoria se gestionaron y obtuvieron los permisos institucionales correspondientes, así como la construcción de la adaptación de la *Combat Exposure Scale*. Posteriormente, en la fase de campo, los instrumentos fueron aplicados de manera controlada en las unidades militares participantes, garantizando condiciones de privacidad y confidencialidad. Finalmente, en la fase de procesamiento, los datos fueron codificados, depurados y organizados en una matriz digital para su posterior análisis estadístico.

En relación con el procesamiento de la información, los datos fueron analizados mediante el software estadístico *SPSS (versión 29)*. Se aplicaron técnicas de estadística descriptiva -medidas de tendencia central y de dispersión- con el fin de caracterizar la muestra y la severidad de la sintomatología clínica, y se calcularon las frecuencias y porcentajes de participantes situados por encima de los puntos de corte clínicos de cada instrumento (PCL-5 ≥ 31; GAD-7 ≥ 5, ≥ 10 y ≥ 15; PHQ-9 ≥ 5, ≥ 10 y ≥ 15). La consistencia interna de las escalas se estimó mediante el coeficiente alfa de Cronbach.

En el plano inferencial, dado que las distribuciones de las escalas presentaron una marcada asimetría positiva, con desviaciones estándar superiores a la media en varios instrumentos, se adoptó el coeficiente de correlación de *Spearman (ρ)* como análisis principal, por su robustez ante distribuciones no normales, y el de *Pearson (r)* como referente secundario. Adicionalmente, con el fin de identificar qué estresores operacionales presentan mayor asociación con la sintomatología clínica, se calcularon correlaciones de Spearman entre cada reactivo de la escala de exposición, considerado de forma independiente, y las puntuaciones totales de la PCL-5, el GAD-7 y el PHQ-9. Se aplicó la prueba H de Kruskal-Wallis para contrastar la sintomatología clínica entre categorías de grado militar, y la prueba U de Mann-Whitney para el contraste entre subgrupos.

Finalmente, la investigación se rigió por lo establecido en la Ley 1090 de 2006, correspondiente al Código Deontológico y Bioético del Psicólogo, por la Resolución 8430 de 1993 del Ministerio de Salud y por los principios éticos de la Declaración de Helsinki. Todos los participantes otorgaron consentimiento informado previo, en el que se explicitó el carácter voluntario de la participación, la posibilidad de retirarse en cualquier momento sin consecuencia alguna y la desvinculación absoluta de los resultados. El estudio no fue sometido a la evaluación de un comité de ética institucional formalmente constituido, circunstancia que se declara en el apartado de limitaciones.

Resultados

En términos generales, la investigación contó con la participación de 130 personas que diligenciaron el cuestionario. Dado que ninguno de los participantes se negó a responder los instrumentos de evaluación, fue posible realizar el análisis con la totalidad de la información recolectada.

Resultados sociodemográficos

Las características sociodemográficas de la población participante se analizaron considerando variables relacionadas con el sexo, la edad y el estado civil, con el fin de describir

el perfil general de los integrantes de la muestra.

En relación con el sexo, se observa una clara predominancia del personal masculino. Del total de participantes (N=130), 124 corresponden al sexo masculino (95,4%), mientras que 6 participantes son de sexo femenino (4,6%). Esta distribución refleja la composición tradicional de las unidades operacionales evaluadas, donde la presencia masculina es significativamente mayor.

Respecto a la edad, los resultados evidencian que la mayor proporción de los participantes se concentra en el rango de 30 a 45 años, con 85 individuos (65,4%). En segundo lugar, se encuentra el grupo entre 18 y 25 años, conformado por 23 participantes (17,7%), seguido del rango entre 25 y 30 años, con 22 participantes (16,9%). Estos resultados indican que la muestra está compuesta principalmente por personal con una edad adulta y con una trayectoria operativa consolidada.

En cuanto al estado civil, los resultados muestran una distribución relativamente equilibrada entre las categorías de soltero(a) y unión libre, cada una con 42 participantes (32,3%). Asimismo, 39 participantes (30,0%) reportaron encontrarse casados, mientras que 5 participantes (3,8%) indicaron estar separados y 2 participantes (1,5%) se identificaron como divorciados. Esta distribución sugiere que una proporción importante del personal mantiene vínculos de pareja o estructuras familiares estables.

En conjunto, estos resultados permiten caracterizar la muestra como una población predominantemente masculina, adulta y con una distribución diversa en su estado civil, lo cual constituye un contexto relevante para la interpretación posterior de los análisis relacionados con la exposición al combate y los indicadores de salud mental evaluados en el estudio.

En cuanto al nivel de escolaridad alcanzado, se identifica que la mayor parte de la muestra cuenta con formación de nivel bachiller, representando al 59,2% (N=77) de los participantes. Le sigue el personal con formación técnica o tecnológica con un 25,4% (N= 33). Por otro lado, el personal con estudios de pregrado (profesional) constituye el 10,8%, mientras que los niveles de posgrado (especialista y magíster) suman en conjunto un 4,6%. Esta configuración educativa sugiere una base operativa con formación técnica sólida, concentrando los niveles profesionales y de maestría en una minoría estratégica.

Respecto a la jerarquía institucional, los resultados por grado militar muestran que el 53,8% (n= 70) de los evaluados son soldados profesionales, seguidos por los suboficiales con un 33,8% (n= 44) y, finalmente, los oficiales con un 12,3% (n = 16). Esta distribución es coherente con la estructura piramidal de la Fuerza, donde la base operativa (soldados profesionales) constituye el grueso de la población expuesta a factores de riesgo psicosocial en el terreno.

Finalmente, al analizar la antigüedad en la institución, se observa una población con alta experiencia acumulada. El 36,2% de los participantes tiene entre 10 y 15 años de servicio, y un 35,4% cuenta con 15 años o más. Esto significa que más del 70% de la muestra posee una trayectoria extensa, lo que implica una exposición prolongada a las di-

námicas propias del servicio y, potencialmente, una mayor habituación o, por el contrario, un desgaste acumulativo frente a eventos críticos. El personal con menor antigüedad (1 a 10 años) representa el 28,5% restante.

Resultados en los instrumentos de medición
Combat exposure scale

La exposición a eventos críticos de combate fue evaluada mediante la Combat Exposure Scale (CES) en su versión adaptada, instrumento diseñado para cuantificar la intensidad y frecuencia de experiencias operativas potencialmente traumáticas en personal militar.

Los resultados descriptivos muestran una puntuación media de 11,03 puntos (DE = 10,37) y una mediana de 8,5 puntos, con valores que oscilaron entre un mínimo de 0 y un máximo de 41 puntos, sobre el rango completo del instrumento, para un total de 130 participantes evaluados.

La desviación estándar, prácticamente equivalente al valor de la media, evidencia una alta dispersión en las puntuaciones, lo cual sugiere heterogeneidad en la experiencia operativa de la muestra. En términos prácticos, ello indica que mientras una proporción significativa de los participantes reporta niveles bajos de exposición, existe un subgrupo que ha experimentado eventos operacionales de mayor intensidad, reflejado en los valores más altos registrados en la escala.

De acuerdo con las categorías de exposición establecidas por los autores de la escala, 65 participantes (50,0%) se ubicaron en el nivel de exposición ligera y 30 (23,1%) en el de ligera-moderada. Por encima de estos rangos, 19 participantes (14,6%) alcanzaron exposición moderada, 10 (7,7%) exposición moderada-intensa y 6 (4,6%) exposición intensa, de modo que el 26,9% de la muestra (n = 35) registró un nivel de exposición moderado o superior.

Estos resultados indican que, si bien la mayor parte del personal evaluado se concentra en niveles bajos o moderados de exposición, existe un segmento no despreciable con una acumulación considerable de experiencias operativas críticas. Desde la perspectiva de la gestión del talento humano y la prevención del riesgo psicosocial en contextos militares, este subgrupo demanda atención prioritaria, en la medida en que la acumulación de eventos operacionales constituye un factor asociado al desarrollo de sintomatología clínica, susceptible de gestión mediante estrategias de monitoreo y apoyo psicosocial focalizado.

Sintomatología asociada al trastorno por estrés postraumático (PCL-5)

La sintomatología asociada al Trastorno por Estrés Postraumático (TEPT) fue evaluada mediante la PTSD Checklist for DSM-5 (PCL-5). Los resultados descriptivos evidenciaron una puntuación media de 13,32 puntos (DE = 17,37) y una mediana de 6 puntos, con valores que oscilaron entre un mínimo de 0 y un máximo de 68 puntos sobre un rango posible de 0 a 80, en una muestra de 130 participantes.

La amplitud del rango y el hecho de que la desviación estándar supere ampliamente el valor de la media indican una elevada dispersión en las puntuaciones, lo que refleja una muestra marcadamente heterogénea en términos de sintomatología postraumática. La diferencia entre la media y la mediana confirma una distribución con asimetría positiva pronunciada: mientras la mitad de los participantes se ubica por debajo de los 6 puntos, un subgrupo presenta puntuaciones considerablemente elevadas, compatibles con manifestaciones clínicas de mayor severidad.

Aplicando el punto de corte de 31 puntos habitualmente empleado para la identificación de casos probables de TEPT, 24 participantes (18,5%) se situaron por encima de dicho umbral. Este resultado indica que, pese a que la media de la muestra se ubica en el rango subclínico, casi uno de cada cinco militares evaluados presenta sintomatología postraumática compatible con criterios clínicos, lo que respalda la necesidad de estrategias de detección temprana, seguimiento psicológico e intervención preventiva focalizadas.

Al relacionar estos resultados con la Escala de Exposición al Combate (CES), se observa una asociación positiva entre ambas variables. El análisis correlacional evidenció una correlación positiva y estadísticamente significativa entre la exposición al combate y la sintomatología postraumática ($\rho = 0{,}433$; $p < 0{,}001$; r de Pearson = 0,596), lo que indica que a mayor exposición a eventos críticos de combate, mayor intensidad de síntomas compatibles con TEPT. Este hallazgo es consistente con el comportamiento esperado en contextos militares de alta exigencia y sugiere que la experiencia acumulada de combate constituye un factor relevante en la aparición de reexperimentación, evitación, hiperactivación y alteraciones cognitivas y emocionales.

No obstante, el hecho de que el promedio general de la escala se mantenga por debajo del umbral clínico, pese a la existencia de casos con puntuaciones elevadas, indica que la respuesta psicológica del personal no es homogénea. Esto permite plantear que, junto a la exposición operacional, podrían estar interviniendo factores protectores individuales e institucionales, tales como entrenamiento, cohesión de unidad, experiencia previa, apoyo social y recursos de afrontamiento, los cuales podrían modular el impacto psicológico de los eventos traumáticos en una parte considerable de la muestra.

Análisis de la escala de ansiedad generalizada (GAD-7)

La sintomatología ansiosa de los participantes fue evaluada mediante la escala Generalized Anxiety Disorder-7 (GAD-7). Los resultados descriptivos evidenciaron una puntuación media de 3,97 puntos (DE = 5,80) y una mediana de 1 punto, con un rango de respuesta que osciló entre 0 y 21 puntos, correspondiente al valor máximo posible del instrumento, en una muestra de 129 participantes con datos válidos.

De acuerdo con los puntos de corte clínicos del GAD-7, el promedio observado se ubica en el nivel de ansiedad mínima, lo que sugiere que, en términos generales, la muestra no presenta una sintomatología ansiosa elevada. Sin embargo, la amplitud del rango y el hecho de que la desviación estándar supere ampliamente el valor de la media indican una marcada heterogeneidad en las respuestas.

El análisis por puntos de corte permite dimensionar esta heterogeneidad. Treinta y nueve participantes (30,2%) alcanzaron puntuaciones iguales o superiores a 5 puntos, umbral correspondiente a sintomatología ansiosa leve o superior; 21 (16,3%) superaron el corte de 10 puntos, indicativo de ansiedad moderada; y 12 (9,3%) se situaron en el rango de ansiedad severa, con puntuaciones iguales o superiores a 15 puntos.

Estos resultados indican que, si bien el comportamiento promedio de la muestra se concentra en niveles bajos de ansiedad, aproximadamente uno de cada seis participantes presenta sintomatología ansiosa de intensidad clínicamente relevante, lo que configura un subgrupo que requiere atención preventiva, monitoreo psicológico y estrategias focalizadas de intervención dentro del contexto institucional.

Desde una lectura integrada con los instrumentos previamente analizados, los resultados del GAD-7 muestran que la ansiedad se relaciona de manera significativa tanto con la exposición operacional como con la sintomatología postraumática. El análisis correlacional evidenció asociaciones positivas y estadísticamente significativas entre ansiedad y exposición al combate ($\rho = 0,396$; $p < 0,001$) y, de manera considerablemente más marcada, entre ansiedad y síntomas de TEPT medidos mediante la PCL-5 ($\rho = 0,750$; $p < 0,001$). Asimismo, la ansiedad mostró la asociación más elevada de todo el estudio con la sintomatología depresiva ($\rho = 0,868$; $p < 0,001$), lo que evidencia un patrón de comorbilidad psicológica en la muestra evaluada.

En conjunto, estos resultados indican que la ansiedad no constituye una manifestación aislada, sino parte de una respuesta psicológica más amplia frente a contextos operacionales caracterizados por amenaza persistente, incertidumbre táctica e hipervigilancia continua.

Sintomatología depresiva (PHQ-9)

La presencia de síntomas depresivos fue evaluada mediante el Patient Health Questionnaire-9 (PHQ-9). Los resultados descriptivos evidenciaron una puntuación media de 3,65 puntos (DE = 6,64) y una mediana de 0 puntos, con valores que oscilaron entre 0 y 27 puntos, en una muestra de 128 participantes con datos válidos.

De acuerdo con los puntos de corte clínicos del instrumento, el promedio obtenido se ubica dentro del rango de depresión mínima, lo que sugiere que la mayoría de los participantes no presenta sintomatología depresiva significativa. Sin embargo, la amplitud del rango observado y una desviación estándar que casi duplica el valor de la media indican una variabilidad considerable en las respuestas.

El análisis por puntos de corte permite precisar esta distribución. Veintisiete participantes (21,1%) alcanzaron puntuaciones iguales o superiores a 5 puntos, correspondientes a sintomatología depresiva leve o superior; 17 (13,3%) superaron el umbral de 10 puntos, indicativo de depresión mayor probable; y 14 (10,9%) se ubicaron en el rango moderado-severo, con puntuaciones iguales o superiores a 15 puntos.

Adicionalmente, el análisis del reactivo 9 del PHQ-9, referido a la presencia de

pensamientos de muerte o autolesión, evidenció respuesta afirmativa en 18 participantes (14,1% de los casos válidos). Aunque este reactivo no constituye por sí solo un indicador diagnóstico de riesgo, su frecuencia en la muestra evaluada respalda la pertinencia de incorporar protocolos de tamizaje y derivación sistemática en las unidades desplegadas.

Al integrar estos resultados con los hallazgos obtenidos en las escalas previamente analizadas, se observa que la sintomatología depresiva presenta relaciones estadísticamente significativas con los síntomas de ansiedad y de estrés postraumático. El análisis correlacional evidenció una asociación muy alta entre depresión y ansiedad ($\rho = 0,868$; $p < 0,001$), una asociación alta entre depresión y síntomas de TEPT ($\rho = 0,701$; $p < 0,001$) y una correlación moderada entre depresión y exposición al combate medida mediante la CES ($\rho = 0,351$; $p < 0,001$).

Análisis integrado de los instrumentos

Tabla 1. Estadísticos descriptivos de las escalas aplicadas

Escala	n	M	DE	Mdn	Min	Max
CES	130	11,03	10,37	8,5	0	41
PCL-5	130	13,32	17,37	6,0	0	68
GAD-7	129	3,97	5,80	1,0	0	21
PHQ-9	128	3,65	6,64	0,0	0	27

Fuente: Elaboración propia

Tabla 2. Distribución de la muestra según puntos de corte clínicos

Escala	Punto de corte	n	%
PCL-5 — TEPT probable	≥ 31	24	18,5
GAD-7 — ansiedad leve o superior	≥ 5	39	30,2
GAD-7 — ansiedad moderada o superior	≥ 10	21	16,3
GAD-7 — ansiedad severa	≥ 15	12	9,3
PHQ-9 — depresión leve o superior	≥ 5	27	21,1
PHQ-9 — depresión mayor probable	≥ 10	17	13,3
PHQ-9 — depresión moderada-severa	≥ 15	14	10,9

Fuente: Elaboración propia

Una vez descrito el comportamiento general de las escalas, se procedió al análisis de correlación entre exposición al combate, sintomatología postraumática, ansiedad y depresión, con el fin de identificar la magnitud y dirección de las asociaciones entre estas variables.

Análisis correlacional

Dada la marcada asimetría positiva de las distribuciones, el coeficiente de correlación de Spearman constituye el análisis principal del estudio. La Tabla 3 presenta la matriz de correlaciones entre las cuatro escalas aplicadas.

Tabla 3. Correlaciones entre exposición operacional y sintomatología clínica

Par de variables	ρ (Spearman)	r (Pearson)	Magnitud	Interpretación
CES – PCL-5	0,433	0,596	Moderada	A mayor exposición operacional, mayor sintomatología postraumática,5
CES – GAD-7	0,396	0,588	Moderada	La exposición acumulada se asocia con incremento de la ansiedad,0
CES – PHQ-9	0,351	0,578	Moderada baja	Asociación más débil del estudio entre exposición y sintomatología
PCL-5 – GAD-7	0,750	3,65	Alta	Comorbilidad marcada entre estrés postraumático y ansiedad
PCL-5 – PHQ-9	0,701	0,852	Alta	Los casos con mayor TEPT presentan también mayor sintomatología depresiva
GAD-7 – PHQ-9	0,868	0,880	Muy alta	Asociación más elevada del estudio: afectación emocional conjunta

Nota: N = 130 (GAD-7, n = 129; PHQ-9, n = 128; correlaciones calculadas por pares). Spearman constituye el análisis principal; Pearson se reporta como referente complementario. p < ,001.

Fuente: Elaboración propia

La Tabla 3 evidencia dos patrones diferenciados. La exposición operacional muestra asociaciones positivas y significativas con las tres condiciones clínicas, todas de magnitud moderada, siendo mayor con la sintomatología postraumática (ρ = 0,433) y menor con la depresiva (ρ = 0,351). Las tres escalas clínicas, en cambio, presentan entre sí asociaciones sustancialmente más elevadas, con un máximo entre ansiedad y depresión (ρ = 0,868). Este contraste indica que la sintomatología clínica constituye un cuadro fuertemente interrelacionado, cuya magnitud no se explica únicamente por el nivel de exposición registrado.

Los coeficientes de Pearson mantienen la dirección y la significación observadas, aunque con magnitudes sensiblemente mayores en las asociaciones que involucran la exposición al combate. Esta divergencia es consistente con la marcada asimetría positiva de las distribuciones e indica que los coeficientes paramétricos están influidos por un subgrupo reducido de casos con puntuaciones extremas. Lejos de constituir un artefacto, este comportamiento refuerza la interpretación central del estudio: la afectación no se distribuye de manera homogénea, sino que se concentra en un subgrupo crítico cuya señal queda diluida en los estadísticos de tendencia central.

Análisis diferencial por estresor operacional

Con el propósito de discriminar el peso relativo de cada estresor, se calcularon correlaciones de Spearman entre cada reactivo de la escala de exposición y las puntuaciones totales de los tres instrumentos clínicos.

Tabla 4. Correlaciones de Spearman entre reactivos de exposición y sintomatología clínica

Reactivo	PCL-5	GAD-7	PHQ-9
1. Patrullajes y tareas operacionales peligrosas	0,379	0,281	0,274
2. Bajo fuego enemigo o ataque, incluidos drones	0,350	0,332	0,277
3. Unidad rodeada, cercada o vigilada de forma persistente, incluida observación con drones	0,270	0,268	0,267
4. Porcentaje de bajas en la unidad	0,317	0,327	0,291
5. Participación en combate directo, incluida respuesta a amenazas aéreas	0,342	0,370	0,271
6. Presenciar a integrantes alcanzados por fuego o explosiones	0,448	0,444	0,398
7. Peligro de resultar herido o morir, incluido sobrevuelo hostil	Asociación más débil del estudio entre exposición y sintomatología	0,431	0,373

Nota: N = 130 (GAD-7, n = 129; PHQ-9, n = 128). *** p < 0,001; ** p < 0,01. Procesado en IBM SPSS Statistics (versión 29).

Fuente: Elaboración propia

Todos los reactivos presentaron asociaciones positivas y estadísticamente significativas con las tres escalas clínicas, con magnitudes comprendidas entre ρ = 0,27 y ρ = 0,45. Las asociaciones más elevadas correspondieron a presenciar la afectación de integrantes de la unidad (ρ = 0,448 con PCL-5) y a la percepción de peligro inminente de muerte durante las operaciones (ρ = 0,413), mientras que el reactivo referido al cerco y la vigilancia persistente registró la asociación más baja del instrumento (ρ = 0,270).

Sintomatología clínica según grado militar

El contraste mediante la prueba H de Kruskal-Wallis evidenció diferencias estadísticamente significativas en sintomatología depresiva según el grado militar (H = 6,15; p = 0,046), con puntuaciones superiores en el grupo de soldados profesionales. Las diferencias observadas en sintomatología postraumática y ansiosa siguieron la misma dirección sin alcanzar significación estadística (p = 0,200 y p = 0,338, respectivamente). No se identificaron diferencias significativas asociadas a la antigüedad en la institución.

Análisis correlacional general

En conjunto, los resultados muestran que la exposición operacional se relaciona de manera significativa con la sintomatología psicológica evaluada, con mayor intensidad en el caso del estrés postraumático. La interrelación entre ansiedad, depresión y sintomatología postraumática resultó sustancialmente más elevada que la observada entre cada una de ellas y la exposición, lo que evidencia un patrón de comorbilidad psicológica en la población analizada.

Discusión

La investigación evidenció una composición demográfica mayoritariamente masculina (95,4%), concentrada en un rango de edad entre los 30 y 45 años, lo que permite inferir una población con trayectoria operativa consolidada, aunque sometida de manera sostenida a exigencias acumulativas propias de una carga alostática prolongada (McEwen, 2007).

El hallazgo central del estudio reside en la magnitud de la afectación clínica identificada. El 18,5% de los participantes superó el punto de corte de la PCL-5 para casos probables de estrés postraumático, el 16,3% el umbral de ansiedad moderada del GAD-7 y el 13,3% el de depresión mayor probable del PHQ-9. Estas proporciones contrastan con unas puntuaciones medias que se ubican en rangos subclínicos en las tres escalas, y esa discrepancia constituye por sí misma un resultado: el impacto psicológico no se distribuye de manera homogénea en la fuerza, sino que se concentra en un segmento del personal cuya afectación queda invisibilizada por los estadísticos de tendencia central. Un enfoque de vigilancia epidemiológica basado en promedios institucionales concluiría que la tropa evaluada se encuentra en condiciones adecuadas de salud mental; el análisis por puntos de corte revela que casi uno de cada cinco militares presenta sintomatología postraumática compatible con criterios clínicos.

La convergencia entre las proporciones de exposición y de afectación refuerza esta lectura. Mientras el 26,9% de la muestra registró exposición operacional moderada o superior, el 18,5% superó el punto de corte de la PCL-5. La similitud entre ambas magnitudes, junto con la asociación positiva identificada entre las dos variables (ρ = 0,433), sugiere que el subgrupo con mayor acumulación de experiencias operacionales críticas coincide en buena medida con aquel que presenta sintomatología clínicamente relevante. No obstante, la magnitud moderada de la asociación indica que la relación no es unívoca: una parte de los casos con sintomatología significativa proviene de participantes con niveles de exposición ligeros o moderados, lo que apunta a la intervención de factores individuales de vulnerabilidad y protección no capturados por el instrumento.

En este sentido, junto a la exposición operacional podrían estar interviniendo factores protectores individuales e institucionales -entrenamiento, cohesión de unidad, experiencia previa, apoyo social y recursos de afrontamiento- que modularían el impacto psicológico de los eventos críticos en una parte considerable de la muestra. Sin embargo, esta interpretación compite con una explicación alternativa que los datos disponibles no

permiten descartar: el subregistro de sintomatología por temor al estigma y a consecuencias sobre la aptitud psicofísica, fenómeno consistentemente documentado en población militar (Hoge et al., 2004). Ambas hipótesis resultan compatibles con el patrón observado y su contrastación requiere diseños que incorporen medidas objetivas o de informante múltiple.

Análisis comparativo: asimetría y fase de transición

Al comparar estos resultados con la información previa se evidencian tanto continuidades como desplazamientos en la configuración del trauma operacional. El estudio desarrollado con soldados del Batallón de Infantería N.º 7 General José Hilario López, en Popayán, determinó que la sintomatología asociada al TEPT estaba vinculada principalmente a la vivencia directa de combates terrestres (Muñoz-Burbano y Toro-López, 2021). En el combate convencional allí examinado, el militar enfrentaba una amenaza de carácter bidireccional; la introducción sistemática de sistemas aéreos no tripulados fractura esa reciprocidad y configura una condición de vulnerabilidad radical, en la que el combatiente pierde el control sobre su propia seguridad sin haber sido derrotado en un enfrentamiento.

No obstante, el análisis por reactivo permite matizar el alcance de este desplazamiento. Los estresores que mostraron mayor asociación con la sintomatología postraumática fueron presenciar la afectación de integrantes de la unidad (ρ = 0,448) y la percepción de peligro inminente de muerte durante las operaciones (ρ = 0,413), mientras que el reactivo referido al cerco y la vigilancia persistente registró la asociación más baja del instrumento (ρ = 0,270). Este resultado sugiere que, en el escenario evaluado, el desplazamiento del centro de gravedad del trauma hacia el dominio de la vigilancia constituye un proceso incipiente y no consumado: los estresores propios del combate convencional conservan el mayor peso explicativo, en tanto la exposición a la observación persistente opera como un factor concurrente de menor magnitud. Esta lectura debe considerarse preliminar, dado que cada reactivo de la escala integra en un mismo enunciado estresores de combate convencional y de amenaza aérea, lo que impide atribuir las diferencias observadas de manera inequívoca a una u otra modalidad.

Desde la perspectiva de la inteligencia estratégica, este hallazgo resulta relevante en sí mismo. Sitúa a la fuerza en una fase de transición en la que la amenaza aérea irregular todavía no ha reconfigurado por completo el perfil de desgaste psicológico del combatiente, lo que abre una ventana de anticipación antes de que dicha reconfiguración se consolide. La experiencia de escenarios donde el empleo de sistemas no tripulados alcanzó densidades operacionales mayores indica que esa consolidación tiende a producirse conforme aumenta la frecuencia y la persistencia de la exposición (Cox, 2025); anticiparla exige instrumentos de vigilancia epidemiológica capaces de detectar el cambio de patrón antes de que se traduzca en afectación consumada.

Las expresiones de hipervigilancia y ansiedad anticipatoria identificadas resultan consistentes con la evidencia sobre poblaciones expuestas a operaciones con drones, en las que el daño psicosocial se manifiesta incluso en ausencia de contacto cinético directo (Edney-Browne, 2019). Desde la visión de la guerra cognitiva, ello indica que el dron no se limita a producir afectación física, sino que opera también como dispositivo orientado

al deterioro emocional de la unidad mediante una vigilancia que erosiona la percepción de seguridad. El patrón de correlaciones observado sugiere, sin embargo, que en el contexto colombiano este mecanismo aún se superpone al del combate convencional en lugar de sustituirlo.

Tabla 5. Contraste de los hallazgos con la literatura precedente

Tipo de evidencia	Estudio	Diseño y muestra	Hallazgo principal	Contraste con este estudio
Empírica - exposición a UAV	Chappelle et al. (2014)	Transversal; 1.084 operadores de sistemas pilotados a distancia (RPA) de la USAF	Fatiga y sintomatología asociadas a carga cognitiva y vigilancia sostenida	Converge en la fatiga por alerta persistente, pero desde la posición inversa: aquí el UAV es la amenaza, no el medio propio
Empírica - exposición a UAV	Edney-Browne (2019)	Cualitativo; población civil expuesta a ataques con drones	Daño psicosocial en ausencia de contacto cinético directo	Extiende el hallazgo a personal militar: el efecto no depende del impacto físico
Empírica - combate convencional	Hoge et al. (2004)	Transversal; 6.201 efectivos de infantería de EE. UU. (2.530 predespliegue y 3.671 posdespliegue), Irak y Afganistán	Prevalencia elevada de TEPT, ansiedad y depresión tras el despliegue	La prevalencia observada en el Cauca fue menor; la robustez psicológica se plantea como hipótesis explicativa, no como conclusión
Empírica - contexto local	Muñoz-Burbano y Toro-López (2021)	Trabajo de grado (enfoque cuantitativo); 100 soldados profesionales del Batallón de Infantería N.º 7, Popayán	Síntomas de TEPT asociados a combate terrestre	Línea base local de comparación. El diseño del presente estudio no permite aislar el efecto diferencial de la amenaza aérea
Teórica	Chamayou (2016)	Ensayo teórico-filosófico; sin muestra	Pérdida de reciprocidad del combate y trauma por indefensión estructural	Marco interpretativo de la "vulnerabilidad radical" descrita en la discusión
Empírica - inteligencia estratégica	Dylan y Grossfeld (2025)	Estudio de caso; fallos de inteligencia en el conflicto de Ucrania	La incapacidad de anticipar el empleo adversario de sistemas no tripulados constituye una falla de inteligencia con consecuencias operacionales	Marco para interpretar el fallo de anticipación ante amenazas no lineales; respalda la propuesta de integrar la salud mental en el ciclo de inteligencia
Normativa	Resolución 2764 de 2022 (Colombia)	Batería de instrumentos para riesgo psicosocial laboral; población trabajadora civil	Referente técnico obligatorio para la evaluación de factores de riesgo psicosocial	Se argumenta su insuficiencia para capturar los estresores propios del entorno operacional militar

Fuente: Elaboración propia

Un aspecto crítico que emerge de este análisis es la escasez de herramientas psicométricas específicas para el contexto colombiano. La presente investigación evidenció que los instrumentos actualmente disponibles no responden de manera suficiente a las

particularidades del trauma asociado a la guerra irregular aérea, especialmente en escenarios caracterizados por una marcada asimetría en el dominio aéreo. Esta limitación no es exclusiva del contexto nacional: la necesidad de desarrollar medidas breves de exposición bélica ajustadas a las condiciones de los despliegues contemporáneos ha sido documentada también en población veterana estadounidense (Bovin et al., 2023).

En razón de esta carencia fue necesario realizar una adaptación de la Combat Exposure Scale, incorporando en cada reactivo los estresores derivados del empleo de sistemas aéreos no tripulados. La versión resultante alcanzó una consistencia interna elevada en la muestra evaluada (α = 0,92) y produjo un patrón de asociaciones coherente con el esperado teóricamente, lo que constituye evidencia preliminar favorable a su comportamiento psicométrico. No obstante, la adaptación no fue sometida a validación de contenido por panel de jueces ni a análisis factorial confirmatorio, por lo que sus propiedades requieren verificación en estudios posteriores antes de su empleo en decisiones individuales de selección, seguimiento o aptitud.

La dependencia de instrumentos diseñados en realidades operacionales distintas configura una debilidad estructural del campo de la salud mental militar en Colombia. El desarrollo de escalas específicas y validadas para el contexto nacional, capaces de discriminar entre estresores de combate convencional y estresores derivados de la amenaza aérea persistente, constituye un vacío técnico que debe ser abordado de manera prioritaria. Esta distinción resulta particularmente relevante a la luz de los resultados obtenidos: la imposibilidad de separar ambos tipos de exposición en el instrumento empleado limitó el alcance del análisis diferencial y, en consecuencia, la precisión con que puede caracterizarse el impacto específico de la guerra irregular aérea.

Hallazgos críticos: el sesgo del promedio y la robustez

El contraste entre unas puntuaciones medias situadas en rangos subclínicos y la existencia de casos con severidad extrema -hasta 68 puntos en la PCL-5, frente a una media de 13,32- constituye el hallazgo de mayor relevancia estratégica del estudio. La divergencia entre los coeficientes de Pearson y de Spearman confirma estadísticamente este patrón: la reducción de las asociaciones al emplear el análisis no paramétrico indica que los coeficientes paramétricos están traccionados por un subgrupo reducido de casos extremos, cuya señal se diluye en los estadísticos de tendencia central.

Este comportamiento admite dos lecturas que los datos disponibles no permiten discriminar. La primera atribuye las medias bajas a la robustez psicológica del personal, que operaría como factor protector frente a la exposición acumulada. La segunda apunta al subregistro de sintomatología por temor al estigma y a consecuencias sobre la aptitud psicofísica, fenómeno ampliamente documentado en población militar (Hoge et al., 2004). Ambas explicaciones resultan compatibles con el patrón observado y su contrastación exige diseños que incorporen medidas objetivas o de informante múltiple.

Con independencia de cuál predomine, la implicación institucional es la misma: un enfoque de vigilancia epidemiológica basado exclusivamente en promedios concluiría que la tropa evaluada se encuentra en condiciones adecuadas de salud mental, cuando el

18,5% supera el punto de corte de casos probables de estrés postraumático y el 14,1% reporta pensamientos de muerte o autolesión. Esta discrepancia configura un riesgo estratégico silencioso: personal aparentemente funcional que opera bajo un estado de afectación no detectada por los indicadores institucionales convencionales.

Esta configuración corresponde a lo que la perspectiva sistémica de la seguridad denomina condiciones latentes: factores que permanecen inactivos en el sistema, comunes a toda organización, y que solo derivan en falla cuando concurren con desencadenantes activos en el contexto operacional. De ahí que su gestión exija una monitorización proactiva y no meramente reactiva (Marchitto, 2011).

Limitaciones e inteligencia estratégica
Limitaciones del estudio

Los hallazgos de esta investigación deben interpretarse a la luz de varias limitaciones. En primer lugar, el muestreo fue no probabilístico por conveniencia, determinado por criterios de accesibilidad y disponibilidad operativa; en consecuencia, las proporciones reportadas describen a la muestra evaluada y no constituyen estimaciones de prevalencia generalizables al conjunto del Ejército Nacional ni a otras áreas de operaciones.

En segundo lugar, el diseño transversal impide establecer relaciones de causalidad o precedencia temporal entre la exposición operacional y la sintomatología clínica. Las asociaciones identificadas indican covariación, no determinación causal, y no puede descartarse la influencia de variables no controladas, como la exposición traumática previa al ingreso a la institución, los factores de riesgo psicosocial extralaborales o el historial clínico individual.

En tercer lugar, la totalidad de los instrumentos aplicados son de autorreporte, administrados en un contexto institucional jerárquico. Aun cuando se garantizó la confidencialidad de la información y se informó expresamente que los resultados no tendrían efecto sobre la hoja de vida ni la carrera administrativa, las fuentes documentan de manera consistente que el personal militar tiende a subreportar sintomatología de salud mental por temor al estigma y a consecuencias sobre la aptitud psicofísica (Hoge et al., 2004). Este sesgo constituye una explicación alternativa plausible para las medias bajas observadas y compite con la interpretación basada en la robustez psicológica.

En cuarto lugar, el estudio no contó con un grupo de comparación conformado por personal no expuesto a la amenaza de sistemas aéreos no tripulados, lo que impide aislar el efecto diferencial de esta modalidad frente a la exposición al combate convencional. Esta limitación resulta particularmente relevante dado que cada reactivo del instrumento de exposición integra en un mismo enunciado estresores de combate terrestre y estresores derivados de la amenaza aérea, circunstancia que restringe el alcance del análisis diferencial por estresor y obliga a considerar sus resultados como preliminares. El personal evaluado se encuentra además expuesto de forma concurrente a minas antipersonal, francotiradores y combate convencional, factores cuyo peso relativo el presente diseño no permite desagregar.

En quinto lugar, la adaptación de la Combat Exposure Scale no fue sometida a validación de contenido por panel de jueces ni a análisis factorial confirmatorio. Su formulación se apoyó en la observación directa del investigador en el área de operaciones, procedimiento que garantiza pertinencia contextual, pero no equivale a evidencia formal de validez.

Asimismo, la recolección se realizó por unidades militares, sin que el análisis incorporara la estructura de agrupamiento resultante. La posible correlación intraclase entre miembros de una misma unidad no fue modelada, circunstancia que puede afectar la precisión de las estimaciones y que aconseja el empleo de modelos multinivel en estudios posteriores.

Finalmente, la recolección mediante formulario virtual autoadministrado no permitió controlar las condiciones ambientales de respuesta ni verificar la comprensión de los ítems, y el estudio no fue sometido a la evaluación de un comité de ética institucional formalmente constituido, aunque se aplicaron los estándares de la Ley 1090 de 2006, la Resolución 8430 de 1993 y la Declaración de Helsinki.

Proyección hacia la inteligencia estratégica

Los resultados de esta investigación permiten sostener que la transformación de los datos clínicos en insumos de inteligencia estratégica constituye una necesidad para comprender y anticipar la dinámica del entorno operacional actual. Si bien se dispone de instrumentos internacionales de alta precisión para la medición de síntomas, el estudio evidenció un vacío en la producción científica nacional enfocada específicamente en la guerra irregular aérea, brecha que subraya la necesidad de convertir cada hallazgo psicométrico en un activo estratégico.

Bajo esta perspectiva, la información derivada del estado emocional del soldado deja de ser un dato clínico aislado para constituirse en un indicador de alerta temprana. Al integrar estos resultados en el ciclo de inteligencia -entendido como la secuencia de requerimiento, recolección, procesamiento, análisis y difusión (Lowenthal, 2008)-, la Fuerza puede identificar vulnerabilidades antes de que se traduzcan en degradación de la capacidad combativa. La experiencia reciente en otros escenarios muestra que las fallas en la anticipación de amenazas emergentes suelen originarse en marcos de inteligencia que no incorporan variables ajenas a lo estrictamente cinético (Dylan y Stivang, 2025).

El patrón identificado en el análisis por estresor cobra aquí su pleno sentido operativo. La constatación de que el desplazamiento del trauma hacia el dominio de la vigilancia constituye un proceso incipiente sitúa a la institución en una fase de anticipación: existe margen para desarrollar instrumentos de monitoreo y protocolos de tamizaje antes de que la amenaza aérea irregular reconfigure por completo el perfil de desgaste psicológico del combatiente. Aprovechar esa ventana exige mediciones sistemáticas y repetidas en el tiempo, capaces de detectar el cambio de patrón cuando comience a producirse.

Hipótesis prospectiva: lesión moral y amenaza aérea persistente

A partir de la naturaleza asimétrica de la amenaza identificada en el departamento del Cauca, y del patrón de resultados obtenido en el presente estudio, se formula una línea de investigación prospectiva orientada a un constructo que los instrumentos aquí empleados no capturan.

La lesión moral (moral injury) designa el daño psicológico derivado de actos o situaciones que transgreden las convicciones morales profundas del individuo, y se distingue del estrés postraumático en que su núcleo no es el miedo sino la ruptura de expectativas normativas sobre lo que debía ocurrir (Litz et al., 2009). Esta distinción resulta pertinente para el escenario evaluado: la exposición a un adversario que observa y ataca sin exponerse no vulnera únicamente la seguridad física del combatiente, sino la reciprocidad que estructura el ethos militar.

Sobre esta base se propone la siguiente hipótesis: la exposición sostenida a la amenaza aérea irregular se asocia con niveles de lesión moral superiores a los observados en personal expuesto a combate convencional de intensidad equivalente, aun cuando la sintomatología postraumática resulte comparable entre ambos grupos. Su contrastación requiere un diseño con grupo de comparación, instrumentos específicos de lesión moral -como la Moral Injury Events Scale- y una medida de exposición que permita discriminar entre ambas modalidades de amenaza, condición que el instrumento empleado en esta investigación no satisface.

La relevancia de esta línea para la inteligencia estratégica reside en que la lesión moral erosiona la confianza institucional y la cohesión de unidad por una vía distinta a la del trauma clásico, lo que implica que su detección exigiría indicadores diferentes de los actualmente disponibles.

Conclusiones

La investigación sobre la exposición al combate en un escenario de amenaza por sistemas aéreos no tripulados y su impacto en la salud mental operacional de los soldados desplegados en el departamento del Cauca durante 2024 permite extraer conclusiones que trascienden el ámbito clínico para situarse en el terreno de la inteligencia estratégica. La incorporación de tecnologías disruptivas -UAV comerciales y sistemas con vista en primera persona- por parte de grupos armados organizados marca un punto de inflexión en la asimetría del conflicto colombiano, al desplazar el centro de gravedad desde la confrontación física hacia el dominio cognitivo y humano.

En primer término, se concluye que el conflicto en el Cauca evoluciona hacia una modalidad que este estudio propone denominar guerra irregular aérea: el empleo sistemático de medios aéreos no convencionales, particularmente sistemas no tripulados de bajo costo, por parte de actores no estatales, con el fin de producir efectos tácticos, psicológicos y estratégicos sostenidos sobre fuerzas regulares, sin requerir superioridad aérea ni capacidad de proyección convencional. Este cambio no es únicamente técnico. El dron deja de ser un instrumento de vigilancia para constituirse en vector de una vulnera-

bilidad radical: mientras el combate convencional supone bidireccionalidad y posibilidad de respuesta simétrica, la amenaza aérea irregular impone una unilateralidad que reduce al combatiente a la condición de blanco. Esta pérdida de reciprocidad fractura el ethos militar y anula el valor protector del terreno frente a sensores térmicos y cámaras de alta resolución.

En segundo término, el estudio identifica asociaciones positivas y estadísticamente significativas entre la exposición operacional al combate y la sintomatología de estrés postraumático (ρ = 0,433), ansiedad (ρ = 0,396) y depresión (ρ = 0,351), así como una comorbilidad marcada entre las tres condiciones clínicas, con un máximo entre ansiedad y depresión (ρ = 0,868). Las investigaciones sobre exposición a operaciones con drones atribuyen este patrón al estímulo acústico persistente y a la vigilancia continua como activadores de miedo condicionado y fatiga decisional; el diseño del presente estudio no permite contrastar directamente ese mecanismo, pero los resultados obtenidos resultan compatibles con él.

En tercer término, se documenta una brecha entre las puntuaciones medias de la muestra y los casos de severidad clínica. Aunque los promedios se sitúan en rangos subclínicos, el 18,5% de los participantes supera el punto de corte de casos probables de estrés postraumático, el 16,3% el de ansiedad moderada, el 13,3% el de depresión mayor probable y el 14,1% reporta pensamientos de muerte o autolesión. La divergencia entre los coeficientes paramétricos y no paramétricos confirma que esta afectación se concentra en un subgrupo cuya señal queda diluida. Se concluye que un enfoque de vigilancia basado exclusivamente en promedios institucionales oculta vulnerabilidades críticas, y que el diagnóstico del desgaste emocional debe elevarse a la categoría de inteligencia estratégica.

En cuarto término, el análisis por estresor permite precisar el alcance de la transformación descrita. Los reactivos asociados a presenciar la afectación de integrantes de la unidad y a la percepción de peligro inminente de muerte registraron las asociaciones más elevadas con la sintomatología clínica, mientras que el referido a la vigilancia persistente obtuvo la más baja. Se concluye que, en el escenario evaluado, el desplazamiento del trauma hacia el dominio de la vigilancia constituye un proceso incipiente y no consumado. Este resultado sitúa a la institución en una fase de anticipación, con margen para desarrollar instrumentos de monitoreo antes de que la reconfiguración se complete.

En quinto término, la investigación evidencia la ausencia de herramientas psicométricas específicas y validadas para el contexto colombiano capaces de discriminar entre estresores de combate convencional y estresores derivados de la amenaza aérea persistente. La dependencia de escalas construidas en realidades operacionales distintas deja vacíos técnicos que limitan la precisión del diagnóstico. Se concluye que el desarrollo de instrumentos propios, junto con protocolos de tamizaje y de fortalecimiento de la flexibilidad psicológica, constituye una necesidad prioritaria para la salud mental operacional de la Fuerza.

Finalmente, la niebla de la guerra descrita por Clausewitz (2021) persiste en el siglo XXI, manifestada ahora a través del empleo irregular de sistemas aéreos no tripu-

lados. Frente a un adversario que ha logrado disputar el dominio del espectro aéreo en el nivel táctico, la integración del estado emocional del personal al ciclo de inteligencia, como indicador de alerta temprana, constituye la vía para identificar vulnerabilidades antes de que se traduzcan en degradación de la capacidad combativa.

Declaración obligatoria de uso de IAGen

Durante la creación y preparación de este documento, el autor empleó diversas herramientas de inteligencia artificial y soporte digital:

Para la búsqueda y el análisis bibliográfico se utilizaron *Connected Papers*, que facilitaron la identificación de literatura relevante a través del análisis de citaciones, así como *Perplexity AI* y *ChatGPT (OpenAI)*, que ayudaron en la localización de fuentes y en la exploración temática inicial. Para la síntesis y la organización del material bibliográfico consultado, se utilizó *NotebookLM (Google)*. Por último, para la mejora de la redacción académica, la reestructuración de los apartados y la verificación de la coherencia interna entre los datos presentados en el texto y las tablas, se recurrió a *Claude (Anthropic)*.

El autor verificó personalmente la totalidad de las referencias bibliográficas citadas en sus fuentes originales. Los análisis estadísticos fueron llevados a cabo por el autor utilizando *IBM SPSS Statistics (versión 29)*. Ninguna de estas herramientas fue utilizada para la generación de datos, la obtención de resultados o la formulación de conclusiones. El autor llevó a cabo una revisión y edición exhaustiva de todo el contenido del manuscrito y asume la responsabilidad total por su originalidad, validez e integridad.

Referencias

Acuerdo No. 060 de 2015 [Consejo superior de salud de las Fuerzas Militares y de la Policía Nacional de Colombia]. Por el cual se establecen las políticas, estrategias y planes en salud como apoyo al cumplimiento de la misión constitucional de las Fuerzas Militares y se determinan los lineamientos para el desarrollo del Programa de Salud Operacional de las Fuerzas Militares. 25 de marzo de 2015. https://www.sanidadfuerzasmilitares.mil.co/transparencia-acceso-informacion-publica/2-normatividad/2-1-normativa-entidad-autoridad/2-1-3-normativa-aplicable-1/2-1-3-1-normatividad-ssfm/acuerdos/acuerdo-060-2015-se-establecen-las-politicas

Acuerdo No. 061 de 2015 [Consejo superior de salud de las Fuerzas Militares y de la Policía Nacional de Colombia]. Por el cual se promueven las políticas, estrategias, planes, programas de salud como apoyo del servicio policial y se determinan los lineamientos para el desarrollo del Programa de Salud Operacional de la Policía Nacional. 16 de julio de 2015. https://www.sanidadfuerzasmilitares.mil.co/transparencia-acceso-informacion-publica/2-normatividad/2-1-normativa-entidad-autoridad/2-1-3-normativa-aplicable-1/2-1-3-1-normatividad-ssfm/acuerdos/acuerdo-061-2015-se-promueven-las-politicas-1

Acuerdo No. 070 de 2019 [Consejo superior de salud de las Fuerzas Militares y de la

Policía Nacional de Colombia]. Por el cual se establece el Modelo de Atención Integral en Salud para el Sistema de Salud de las Fuerzas Militares y de la Policía Nacional. 2 de agosto de 2019. https://www.sanidadfuerzasmilitares.mil.co/transparencia-acceso-informacion-publica/2-normatividad/2-1-normativa-entidad-autoridad/2-1-3-normativa-aplicable-1/2-1-3-1-normatividad-ssfm/acuerdos/acuerdo-070-2019-se-establece-modelo

Acuerdo No. 090 de 2024 [Consejo superior de salud de las Fuerzas Militares y de la Policía Nacional de Colombia]. Por el cual se establece la Política y los lineamientos de salud mental para el Sistema de Salud de las Fuerzas Militares y de la Policía Nacional. 28 de octubre de 2024. https://www.sanidadfuerzasmilitares.mil.co/transparencia-acceso-informacion-publica/2-normatividad/2-1-normativa-entidad-autoridad/2-1-3-normativa-aplicable-1/2-1-3-1-normatividad-ssfm/acuerdos/acuerdo-n0-090-2024-se-establece-politica

Alejo, E. G. y Cuartas-Arias, J. M. (2024). Validación de la lista de chequeo del trastorno por estrés postraumático (PCL-5) en adolescentes colombianos víctimas de adversidad. *Diversitas, 20*(2), 39-62. https://doi.org/10.15332/22563067.10709

Baleta-López, E. (2018). Terrorismo, tecnología y guerra asimétrica. *Tabula Rasa*, (28), 371-384. https://doi.org/10.25058/20112742.n28.16

Bartone, P. T. y Homish, G. G. (2020). Influence of hardiness, avoidance coping, and combat exposure on depression in returning war veterans: A moderated-mediation study. *Journal of Affective Disorders, 265*, 511-518. https://doi.org/10.1016/j.jad.2020.01.127

Bartone, P. T., Roland, R. R., Picano, J. J. y Williams, T. J. (2008). Psychological hardiness predicts success in US Army special forces candidates. *International Journal of Selection and Assessment, 16*(1), 78-81. https://doi.org/10.1111/j.1468-2389.2008.00412.x

Bastidas-Goyes, A., Tuta-Quintero, E., Hincapié-Díaz, G., Rueda-Rodríguez, A., Piotrostanalsky, A. y Contreras-Candelo, S. (2021). Trastorno de estrés postraumático en una cohorte de militares con trauma de guerra. Revista Cubana de Medicina Militar, 50(4), e02101591. https://revmedmilitar.sld.cu/index.php/mil/article/view/1591

Bonvie, J. L., Matta, S. E., Andriichenko, S., Slobodian, I., Leiner, A., Brockdorf, Y. y Stern, T. A. (2025). Psychological sequelae of drone attacks. *The primary care companion for CNS disorders, 27*(6), 25f04056. https://doi.org/10.4088/PCC.25f04056

Booth-Kewley, S., Schmied, E. A., Highfill-McRoy, R. M., Larson, G. E., Garland, C. F. y Ziajko, L. A. (2013). Predictors of psychiatric disorders in combat veterans. *BMC Psychiatry, 13*, 130. https://doi.org/10.1186/1471-244X-13-130

Bovin, M. J., Schneiderman, A., Bernhard, P. A., Maguen, S., Hoffmire, C. A., Blosnich, J. R., Smith, B. N., Kulka, R. y Vogt, D. (2023). Development and validation of a brief warfare exposure measure among U.S. Iraq and Afghanistan war veterans: The deployment risk and resilience inventory-2 warfare exposure-short form (DRRI-2 WE-SF). *Psychological Trauma: Theory, Research, Practice, and Policy, 15*(8), 1248-1258. https://doi.org/10.1037/tra0001282 PMid:35653745 PMCid:PMC10364240

Carvalho, T., Cunha, M., Pinto-Gouveia, J. y Da Motta, C. (2015). Development of the combat distress scale of the Combat Experiences Questionnaire (CEQ). *Journal of Affective Disorders, 174*, 602-610. https://doi.org/10.1016/j.jad.2014.11.054 PMid:25569613

Chamayou, G. (2016). *Teoría Del Dron* (Trad. I. Herrera). Herder Editorial.

Chappelle, W., Goodman, T., Reardon, L. y Thompson, W. (2014). An analysis of post-traumatic stress symptoms in United States Air Force drone operators. *Journal Of Anxiety Disorders, 28*(5), 480-487. https://doi.org/10.1016/j.janxdis.2014.05.003 PMid:24907535

Clausewitz, C. V. (2021). *De la guerra*. Ediciones Obelisco. (Obra original publicada en 1832).

Conde, S. y Whiskeyman, A. (2026). The emergence of cognitive intelligence (COGINT) as a new military intelligence collection discipline. *International Journal of Intelligence and CounterIntelligence. 39*(3), 774-800. https://doi.org/10.1080/08850607.2025.2571497

Constitución Política de Colombia [Const]. Art. 1 y Art. 217. 6 de julio de 1991 (Colombia). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Corzo, P. A. (2009). Trastorno por estrés postraumático en psiquiatría militar. *Revista Med, 17*(1), 81-86. https://dialnet.unirioja.es/servlet/articulo?codigo=3660013

Cox, N. L. (2025). Psychological implications of drone warfare on the modern warfighter. *Military Psychology.* 1-7. https://doi.org/10.1080/08995605.2025.2594335

Drone Warfare Innovations. (2026). *Impacto psicológico y doctrinal de la guerra con drones.* Investigación sobre drone-warfare.com. https://drone-warfare.com/research/drone-warfare-psychological-impact/

Du Cluzel, F. (2020). *Cognitive warfare*. NATO Allied Command Transformation Innovation. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

Durón-Figueroa, R., Cárdenas-López, G., Castro-Calvo, J. y De la Rosa-Gómez, A. (2019). Adaptación de la lista checable de trastorno por estrés postraumático para

DSM-5 en población mexicana. *Acta de Investigación Psicológica, 9*(1), 26-36. https://doi.org/10.22201/fpsi.20074719e.2019.1.03

Dylan, H. y Grossfeld, E. (2025). Unveiling Russian intelligence failures in the Ukraine conflict: A strategic culture perspective. *Intelligence and National Security, 40*(5), 926-950. https://doi.org/10.1080/02684527.2025.2544460

Dylan, H. y Stivang, N. (2025). Emerging technologies and national security intelligence. Intelligence and National Security, 40(6), 988-1009. https://doi.org/10.1080/02684527.2025.2565948

Edney-Browne, A. (2019). The psychosocial effects of drone violence: Social isolation, self-objectification, and depoliticization. *Political Psychology, 40*(6), 1341-1356. https://doi.org/10.1111/pops.12629

Ejército Nacional de Colombia. (2017). *Manual Fundamental de Referencia del Ejército MFE 6-27: Derecho Operacional Terrestre.* Centro de Doctrina del Ejército. https://www.ejercito.mil.co/recurso_user/doc_contenido_pagina_web/800130633_4/458774/mfe_6_27_derecho_operacional_terrestre.pdf

Fenstermacher, L., Uzcha, D., Larson, K., Vitiello, C. y Shellman, S. (2023). New perspectives on cognitive warfare. *Signal Processing, Sensor/Information Fusion, and Target Recognition, 12547.* https://doi.org/10.1117/12.2666777

Fernández-Duarte, C. A., Flores-Pedroso, M. D., Gonzales-Calle, S., García-Carrillo, J. A. y Urazan-Chinchilla, J. C. (2024). Operaciones militares, despliegues de tropa y alteraciones en salud mental: una revisión de la literatura. *Brújula Semilleros de Investigación, 12*(23), 48-73. https://doi.org/10.21830/23460628.159

Fernández-Osorio, A. E. (2025). Drones y guerras de quinta generación: implicaciones humanitarias en el conflicto colombiano. *Revista Logos Ciencia & Tecnología, 17*(2), 32-49. https://doi.org/10.22335/rlct.v17i2.2127

Forés, A. y Grané, J. (2008). *La resiliencia: crecer desde la adversidad.* Plataforma Editorial.

Fonseca-Ortiz, T. L. y Sierra-Zamora, P. A. (Eds.). (2022). *Guerras irrestricta e híbrida en los desafíos a la seguridad y defensa nacionales.* Sello Editorial ESDEG. https://doi.org/10.25062/9789585377882 PMid:31880769

Handel, M. I. (1984). Intelligence and the problem of strategic surprise. *Journal of Strategic Studies, 7*(3), 229-281. https://doi.org/10.1080/01402398408437190

Hartley III, D. S. y Jobson, K. O. (2021). *Cognitive superiority: information to power.* Springer International Publishing. https://doi.org/10.1007/978-3-030-60184-3

Herrera-Merchán, E. J. y Cañas-Betancur, D. C. (2020). El estrés postraumático como precursor de daños en salud mental y cognición en víctimas de violencia.

Diversitas, 16(2), 311-323. https://doi.org/10.15332/22563067.6297

Hoge, C. W., Castro, C. A., Messer, S. C., McGurk, D., Cotting, D. I. y Koffman, R. L. (2004). Combat duty in Iraq and Afghanistan, mental health problems, and barriers to care. *New England Journal of Medicine, 351*(1), 13-22. https://doi.org/10.1056/NEJMoa040603

Jiménez-Almeira, G. A. (2022). Narrativas y operaciones de información: una mirada al contexto ciberespacial de la guerra híbrida en T. L. Fonseca-Ortiz y P. A. Sierra-Zamora (Eds.), *Guerras irrestricta e híbrida en los desafíos a la seguridad y defensa nacionales* (pp. 23-40). Sello Editorial ESDEG. https://doi.org/10.25062/9789585377882.02

Jinkerson, J. D. (2016). Defining and assessing moral injury: A syndrome perspective. *Traumatology, 22*(2), 122-130. https://doi.org/10.1037/trm0000069

Keane, T. M., Fairbank, J. A., Caddell, J. M., Zimering, R. T., Taylor, K. L. y Mora, C. A. (1989). Clinical evaluation of a measure to assess combat exposure. *Psychological Assessment, 1*(1), 53-55. https://doi.org/10.1037/1040-3590.1.1.53

Kühn, S., Butler, O., Willmund, G., Wesemann, U., Zimmermann, P. y Gallinat, J. (2021). The brain at war: Effects of stress on brain structure in soldiers deployed to a war zone. *Translational Psychiatry, 11*, 247. https://doi.org/10.1038/s41398-021-01356-0 PMid:33903597 PMCid:PMC8076198

Laghari, A. A., Jumani, A. K., Laghari, R. A. y Nawaz, H. (2023). Unmanned aerial vehicles: A review. *Cognitive Robotics, 3*, 8-22. https://doi.org/10.1016/j.cogr.2022.12.004

Ley 1090 de 2006. Por la cual se reglamenta el ejercicio de la profesión de Psicología, se dicta el Código Deontológico y Bioético y otras disposiciones. 6 de septiembre de 2006. D.O. No. 46383. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=66205

Ley 1616 de 2013. Por medio de la cual se expide la ley de Salud Mental y se dictan otras disposiciones. 21 de enero de 2013. D.O. No. 48680. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51292

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012. D.O. No. 48587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley Estatutaria 1751 de 2015. Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones. 16 de febrero de 2015. D.O. No. 49427. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60733

Liang, Q. y Xiangsui, W. (2015). *Unrestricted warfare: China's master plan to destroy America.* Echo Point Books & Media.

Litz, B. T., Stein, N., Delaney, E., Lebowitz, L., Nash, W. P., Silva, C. y Maguen, S. (2009). Moral injury and moral repair in war veterans: A preliminary model and intervention strategy. *Clinical Psychology Review, 29*(8), 695-706. https://doi.org/10.1016/j.cpr.2009.07.003

Lowenthal, M. M. (2008). *Intelligence: From secrets to policy* (4.ª ed.). CQ Press.

Marchitto, M. (2011). El error humano y la gestión de seguridad: la perspectiva sistémica en las obras de James Reason. *Laboreal, 7*(2), 56-64. https://doi.org/10.4000/laboreal.7750

Matiz-Rojas, A. H. y Fernández-Camargo, J. A. (2023). Sobre el uso de la inteligencia artificial como medio y método en los conflictos armados. *Revista Científica General José María Córdova, 21*(42), 525-549. https://doi.org/10.21830/19006586.1151

McEwen, B. S. (2007). Physiology and neurobiology of stress and adaptation: Central role of the brain. *Physiological Reviews, 87*(3), 873-904. https://doi.org/10.1152/physrev.00041.2006

Mendoza, C., Saumeth, E., Grautoff, M. y Padilla, R. (3 de julio de 2025). Drones: una nueva amenaza en el conflicto armado en Colombia. *France 24*. https://www.france24.com/es/programas/los-observadores/20250703-drones-una-nueva-amenaza-en-el-conflicto-armado-en-colombia

Ministerio del Trabajo de Colombia y Pontificia Universidad Javeriana. (2016a). *Reacción a estrés agudo: Protocolo de prevención y actuación en el entorno laboral.* perfilesycapacidades.javeriana.edu.co. https://perfilesycapacidades.javeriana.edu.co/es/publications/reacci%C3%B3n-a-estr%C3%A9s-agudo-protocolo-de-prevenci%C3%B3n-y-actuaci%C3%B3n-en-el/

Ministerio del Trabajo de Colombia y Pontificia Universidad Javeriana. (2016b). *Trastorno de estrés postraumático: Protocolo de actuación temprana y manejo de casos en el entorno laboral.* perfilesycapacidades.javeriana.edu.co. https://perfilesycapacidades.javeriana.edu.co/es/publications/trastorno-de-estr%C3%A9s-postraum%C3%A1tico-protocolo-de-actuaci%C3%B3n-temprana/

Moreno-Chaparro, J., Piñeros-Ortiz, S., Rodríguez-Ramírez, L., Urrego-Mendoza, Z., Samacá-Samacá, D., Garzón-Orjuela, N. y Eslava-Schmalbach, J. (2022). Mental health consequences of armed conflicts in adults: An overview. *Actas Españolas de Psiquiatría, 50*(2), 68-91. https://actaspsiquiatria.es/index.php/actas/article/view/114

Muñoz-Burbano, A. X. y Toro-López, A. D. (2021). *Síntomas del trastorno por estrés postraumático en soldados profesionales del Batallón de Infantería N.º 7 General José Hilario López, a partir de su experiencia en combates terrestres* [Tesis de pregrado, Fundación Universitaria de Popayán]. Repositorio Institucional FUP. https://fupvirtual.edu.co/repositorio/s/repositorio/item/12927

Naeem, A., Sikder, I., Wang, S., Barrett, E. S., Fiedler, N., Ahmad, M., Nguyen, U.-S. D. T., Martsenkovskyi, D., Holovanova, I., Hicks, M. H.-R. y Haque, U. (2025). Parent-child mental health in Ukraine in relation to war trauma and drone attacks. *Comprehensive Psychiatry, 139*, 152590. https://doi.org/10.1016/j.comppsych.2025.152590 PMid:40090214

Ortiz, R. D. (2015). El concepto de guerra híbrida y su relevancia para América Latina. Revista Ensayos Militares, 1(2), 131-148. https://revistaensayosmilitares.cl/index.php/acague/article/view/110

Patiño-Camargo, J. E. (2024). Los drones letales en la estrategia militar moderna: un análisis desde la teoría clásica. *Revista Estrategia, Poder y Desarrollo, 3*(6), 133-154. https://doi.org/10.25062/2955-0289.4874

Pineda-Julio, L. P. y Bonilla-Córdoba, M. F. (2017). *Trastorno de estrés postraumático en personal de las fuerzas militares y policía, revisión sistemática* [Tesis de maestría, Universidad del Rosario]. Repositorio Institucional EdocUR. https://doi.org/10.48713/10336_13504

Ramos-Del Río, B. y Martí-Noguera, J. J. (2022). *Experiencias en ciberpsicología: hacia una nueva era de la psicología.* Universidad Nacional Autónoma de México.

Resolución 8430 de 1993 [Ministerio de Salud de Colombia]. Por la cual se establecen las normas científicas, técnicas y administrativas para la investigación en salud. 4 de octubre de 1993. https://normograma.invima.gov.co/compilacion/docs/resolucion_minsalud_r8430_93.htm

Resolución 2764 de 2022 [Ministerio de Trabajo de Colombia]. Por la cual se adopta la Batería de instrumentos para la evaluación de factores de Riesgo Psicosocial, la Guía Técnica General para la promoción, prevención e intervención de los factores psicosociales y sus efectos en la población trabajadora y sus protocolos específicos y se dictan otras disposiciones. 18 de julio de 2022. D.O. No. 52106. https://observapsicosocialcol.com/resolucion-2764-de-2022/

Rivera-López, E. (2017). Los drones, la moralidad profunda y las convenciones de la guerra. *Isonomía. Revista de Teoría y Filosofía del Derecho,* (46), 11-28. https://doi.org/10.5347/46.2017.51

Rodríguez, J. D. (15 de junio de 2026). Incautan drones, explosivos y material de guerra de Disidencias Farc en López de Micay. *Caracol.com.co.* https://caracol.com.co/2026/06/16/incautan-drones-explosivos-y-material-de-guerra-de-la-jaime-martinez-en-cauca/

Saini, R. K., Raju, M. S. y Chail, A. (2021). Cry in the sky: Psychological impact on drone operators. *Industrial Psychiatry Journal, 30*(Supl. 1), S15-S19. https://doi.org/10.4103/0972-6748.328782 PMid:34908658 PMCid:PMC8611566

Sohr, R. (2025). La era del dron. Mensaje. https://www.mensaje.cl/edicion-impresa/la-era-del-dron/

The Lancet. (2025). Understanding the health threats of drone warfare (editorial). *The Lancet, 406*(10516), 2191. https://doi.org/10.1016/S0140-6736(25)02261-5 PMid:41206155

Vargas-Cano, C. A., Gil-Osorio, J. F. y Jiménez-Reina, J. (2025). El uso de drones en seguridad y defensa: impactos y retos para el cumplimiento del DIH y la protección de los derechos humanos. *Estudios en Seguridad y Defensa, 20*(39), 67-88. https://doi.org/10.25062/1900-8325.4905

Williamson, L., Dell, C. A., Osgood, N., Chalmers, D., Lohnes, C., Carleton, N. y Asmundson, G. (2021). Examining changes in posttraumatic stress disorder symptoms and substance use among a sample of Canadian veterans working with service dogs: An exploratory patient-oriented longitudinal study. *Journal of Veterans Studies, 7*(1), 1-13. https://doi.org/10.21061/jvs.v7i1.194

Wirtz, J. J. (2016). *Understanding intelligence failure: Warning, response and deterrence*. Routledge. https://doi.org/10.4324/9781315673295

Wolf, E. J., Mitchell, K. S., Koenen, K. C. y Miller, M. W. (2014). Combat exposure severity as a moderator of genetic and environmental liability to post-traumatic stress disorder. *Psychological Medicine, 44*(7), 1499-1509. https://doi.org/10.1017/S0033291713002286

Zueger, R., Niederhauser, M., Utzinger, C., Annen, H. y Ehlert, U. (2022). Effects of resilience training on mental, emotional, and physical stress outcomes in military officer cadets. *Military Psychology, 35*(6), 566-576. https://doi.org/10.1080/08995605.2022.2139948

Zulaika, J. (2022). La guerra de drones: caza, fantasía y el arte de asesinar. Disparidades. *Revista de Antropología, 77*(1), e003. https://doi.org/10.3989/dra.2022.003

Revista Perspectivas en Inteligencia
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 18, Número 27, enero - junio de 2026
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web:https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Exposición al combate en escenarios de amenaza por UAS y salud mental operacional en soldados del Ejército Nacional desplegados en el Cauca (2024)

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Jorge Luis Forero-Herrera es Magister en Sistemas Integrados de Gestión de la Prevención de Riesgos Laborales, la Calidad, el Medio Ambiente y la Responsabilidad Social Corporativa de la Universidad Internacional de La Rioja (España), Magíster en Inteligencia Estratégica de la Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Colombia), con Especialización en Gestión de la Seguridad y Salud en el Trabajo de la Universidad Internacional de La Rioja (España), Especialización Tecnológica en Gestión Aeronáutica de la Escuela de Suboficiales Fuerza Aeroespacial colombiana "CT. Andrés M. Díaz" (Colombia), es psicólogo de la Institución Universitaria Politécnico Grancolombiano (Colombia).

https://orcid.org/0000-0003-0868-5000 - Contacto: joforero8@poligran.edu.co

Esta página queda intencionalmente en blanco

EDITORIAL

ARTÍCULOS

Revista Científica Perspectivas en Inteligencia
"BG. Ricardo Charry Solano" (ESICI)
(Revista científica en Ciencias Sociales e Interdisciplinaria)

ISSN 2145-194X (impreso) • ISSN 2745-1690 (en línea)
Vol.18- N° 27• pp. 15-167 • Enero- Junio/ 2026

Bogotá, D.C., Colombia

Sección de Publicaciones del Ejército Nacional

Visítanos en el Portal de la Revista Académica
Escuela de Inteligencia y Contrainteligencia
Institución Universitaria
Vigilada Mineducación