Implementación de sistemas de defensa en instalaciones militares frente a amenazas en Colombia

Mayor (EJC) Iván Camilo González Rada

Artículo para optar al título profesional:

Magister en Seguridad y Defensa Nacional

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Iván Camilo González Rada
Identificación	**:**	1032396914
Programa académico	**:**	Maestría en Seguridad y Defensa Nacionales
Tutor metodológico	**:**	DO. Jonnathan Jiménez Reina
Tutor temático	**:**	Mayor (EJC) David Núñez Capacho
Fecha de entrega	**:**	
Extensión	**:**	

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Implementación de sistemas de defensa en instalaciones militares frente a amenazas en Colombia

Implementation of defense systems at military installations against threats in Colombia

Iván Camilo González Rada[*]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este articulo analiza la necesidad y los desafíos de implementar sistemas de defensa anti-dron en las instalaciones militares colombianas frente a amenazas emergentes como los drones armados utilizados por grupos ilegales. A través de un enfoque cualitativo y documental, se identifican vulnerabilidades estructurales, tecnológicas y normativas que afectan la capacidad de respuesta de las Fuerzas Militares ante incursiones aéreas no tripuladas. Se revisan casos recientes de ataques con drones en Colombia, así como las iniciativas adoptadas por el Ministerio de Defensa desde 2024, incluyendo adquisiciones tecnológicas como el sistema Skylock Dome. De modo que, el estudio concluye que una defensa efectiva requiere no solo inversión en tecnología, sino también entrenamiento especializado, interoperabilidad entre Fuerzas y adaptación a la geografía colombiana. Se ofrecen recomendaciones estratégicas para mejorar la resiliencia militar en un contexto de guerra híbrida.

Palabras clave: Colombia; Defensa aérea; Drones; Guerra Híbrida; Resiliencia Militar; Seguridad Nacional.

Abstract: This article analyzes the need and challenges of implementing anti-drone defense systems in Colombian military installations in the face of emerging threats such as armed drones used by illegal groups. Through a qualitative and documentary approach, structural, technological, and regulatory vulnerabilities that affect the Armed Forces' response capacity to unmanned aerial incursions are identified. Recent cases of drone attacks in Colombia are reviewed, as well as initiatives adopted by the Ministry of Defense since 2024, including technological acquisitions such as the Skylock Dome system. The study concludes that effective defense requires not only investment in technology, but also specialized training, interoperability between forces, and adaptation to

[*] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0003-2004-7466 - Contacto: landinezj@esdeg.edu.co.

Colombia's geography. Strategic recommendations are offered to improve military resilience in a hybrid warfare context.

Keywords: Air Defense;Colombia; Drones; Hybrid Warfare; Military Resilience; National Security.

[T1] Introducción

La temática propuesta en esta investigación gira en torno a la implementación de sistemas de defensa anti-dron en instalaciones militares colombianas, en respuesta a las amenazas emergentes derivadas del uso de aeronaves no tripuladas por parte de grupos armados ilegales. En los últimos años, el uso de drones ha dejado de ser exclusivo de operaciones militares de Estados con alta capacidad tecnológica y se ha expandido hacia actores no estatales, quienes los emplean para actividades delictivas y ataques asimétricos. La facilidad de acceso a tecnología comercial, sumada a la capacidad de modificarla para fines ofensivos, ha puesto en evidencia una nueva dimensión del conflicto armado interno en Colombia.

El problema central que se pretende abordar radica en el incremento alarmante de ataques con drones por parte de estructuras armadas ilegales en departamentos como Cauca, Putumayo y Caquetá. Según un artículo publicado en Prensa Latina (2025), en el año 2024 se registraron al menos 115 ataques con drones, muchos de ellos dirigidos contra instalaciones militares y población civil. Estos dispositivos han sido utilizados para lanzar explosivos, espiar posiciones del Ejército y vulnerar la seguridad perimetral de bases estratégicas. La situación ha sido agravada por la limitada capacidad tecnológica de las Fuerzas Militares para detectar y neutralizar estas amenazas en tiempo real, tal como lo reconoció el Ministerio de Defensa en diciembre de 2024, cuando anunció una inversión de 20.000 millones de pesos en tecnología antidrones (Semana, 2024).

En consecuencia, la pertinencia de esta investigación radica en la urgencia de evaluar la efectividad de estas tecnologías emergentes, no solo como una necesidad táctica sino como una estrategia de seguridad nacional. La incorporación de sistemas de defensa anti-dron permitirá prevenir ataques, proteger al personal militar y civil, salvaguardar infraestructura crítica y recuperar el control del espacio aéreo de baja altura. Además, en términos estratégicos, posiciona a Colombia en la vanguardia regional en la respuesta ante amenazas tecnológicas no convencionales.

Diversos autores han abordado esta problemática en escenarios internacionales. Rodríguez (2023), analiza cómo drones como el Shahed-136 han sido utilizados por Rusia para debilitar la infraestructura crítica ucraniana. Escobar (2024), documenta el uso de drones por parte de cárteles mexicanos y grupos criminales brasileños para fines de ataque y vigilancia. A nivel nacional, informes de prensa (El País, 2024), detallan incidentes en zonas como El Plateado (Cauca), donde drones con explosivos causaron heridas a militares y civiles, resaltando la inminente necesidad de fortalecer las capacidades defensivas del Estado ante este tipo de amenazas. Para ello se formularon los siguientes objetivos específicos:

- Identificar las principales amenazas emergentes de tipo operacional y tecnológico que enfrentan las instalaciones militares en Colombia y su relación con el uso de drones hostiles.
- Describir la efectividad de los sistemas de defensa anti-dron implementados en instalaciones militares colombianas, considerando su capacidad de detección, neutralización y respuesta ante incursiones no autorizadas.

- Proponer estrategias de optimización en la adopción e implementación de tecnologías anti-dron en instalaciones militares, con base en análisis de mejores prácticas y marcos normativos aplicables.

Por lo tanto, la presente investigación se desarrolla en el marco de un conflicto interno persistente, donde la seguridad de instalaciones militares y civiles se ve amenazada por nuevas tecnologías que escapan al control tradicional del Estado. El actual contexto de violencia armada en Colombia, especialmente en regiones del suroccidente del país, ha generado un escenario crítico: las disidencias de las FARC, el ELN y bandas criminales emplean drones para realizar ataques selectivos, reconocimiento aéreo, e incluso vigilancia de tropas gubernamentales. Por ende, ha llevado a un desequilibrio táctico en las operaciones de seguridad y defensa, al cual las instituciones deben responder con rapidez, precisión e innovación tecnológica. Para ello, se formuló la siguiente pregunta de investigación:

¿Cuál es el efecto de la implementación de un sistema de defensa anti-dron frente a amenazas operacionales y tecnológicas emergentes en instalaciones militares en Colombia?

En el ámbito nacional, existen documentos rectores como la Política de Seguridad y Defensa (2022–2030) que instan a la modernización de las capacidades militares, reconociendo la necesidad de incorporar tecnologías de cuarta revolución industrial para enfrentar amenazas híbridas. A nivel institucional, el Plan Estratégico del Ministerio de Defensa contempla el fortalecimiento de la inteligencia técnica y la protección de instalaciones, especialmente en regiones de alta complejidad. Sin embargo, el avance normativo aún es incipiente en materia de regulación del uso y neutralización de drones en

conflictos armados internos, lo que amplifica la vulnerabilidad del aparato estatal frente a este fenómeno.

Desde la academia, abordar esta problemática permite contribuir a un campo emergente en los estudios de seguridad y defensa tecnológica, generando conocimiento estratégico que puede aplicarse a la toma de decisiones operativas. Además, permite integrar enfoques interdisciplinarios como ingeniería, ciencia política y estudios militares para comprender los efectos de los sistemas anti-dron y su implementación táctica en el terreno.

Desde la perspectiva institucional, esta investigación cobra especial relevancia para las Fuerzas Militares de Colombia, que enfrentan diariamente las consecuencias del uso ofensivo de drones por parte de actores armados. Proponer una estrategia integral basada en evidencia para enfrentar esta amenaza representa una oportunidad para aumentar la eficacia operativa, proteger la vida del personal militar y civil, y preservar la infraestructura clave del Estado.

A largo plazo, superar este problema permitirá consolidar la doctrina militar frente a amenazas tecnológicas, fomentar el desarrollo de capacidades nacionales en ciberseguridad y guerra electrónica, y contribuir al fortalecimiento de la defensa soberana del país. Asimismo, se abre la posibilidad de generar alianzas estratégicas internacionales para la innovación en sistemas antidron y el desarrollo de un marco normativo moderno.

[T1] Metodología

Este estudio se enmarca en un enfoque cualitativo de tipo exploratorio y descriptivo, cuyo objetivo es analizar los efectos de la implementación de sistemas de defensa anti-dron

en instalaciones militares frente a amenazas emergentes en Colombia. La investigación se basa en el análisis documental y contextual de fuentes secundarias, lo que permite caracterizar el fenómeno desde una perspectiva técnico-operativa, doctrinal y legal.

Al respecto, se empleó el método de análisis documental, que consiste en revisar de forma sistemática documentos oficiales, estudios académicos, reportes técnicos, normativa vigente y artículos de prensa especializada. Este método es adecuado para el abordaje de fenómenos recientes y en transformación, como lo es el uso ofensivo de drones por parte de actores armados ilegales.

De la misma manera, la principal herramienta utilizada fue una matriz de análisis de contenido, la cual permitió organizar las fuentes según categorías temáticas como: tipos de amenazas, capacidades tecnológicas existentes, vacíos normativos, sistemas implementados y recomendaciones estratégicas. Esta herramienta facilitó la comparación entre distintos enfoques doctrinales y experiencias nacionales e internacionales.

Por ende, se utilizaron instrumentos como fichas de análisis documental, guías de revisión técnica por ejemplo la Guía C-UAS 2024 de la Fuerza Aérea Colombiana, y declaraciones oficiales recogidas en entrevistas y reportes periodísticos. Estos instrumentos permitieron triangular información y validar patrones, percepciones y respuestas institucionales. Se analizaron, por ejemplo, los comunicados del Ministerio de Defensa sobre la adquisición de sistemas como Skylock Dome y las experiencias operativas en eventos como la COP16.

Por último, esta metodología es pertinente dado el carácter emergente de la amenaza analizada. La limitada disponibilidad de estudios empíricos y la dispersión de información justifican un enfoque exploratorio y documental. A través de esta aproximación, se logró

construir una visión integrada del problema, identificar vacíos críticos y fundamentar las recomendaciones que se presentan en el desarrollo del artículo.

[T1] Amenazas emergentes en instalaciones militares

A pesar de los avances en seguridad, la irrupción de drones hostiles ha puesto de manifiesto vulnerabilidades significativas en la defensa de las instalaciones militares colombianas. Estas vulnerabilidades se pueden clasificar en tres ámbitos principales: estructurales, normativas y tecnológicas, las cuales convergen para crear brechas que pueden ser explotadas por actores ilegales(Patiño, 2024). A continuación, se analizan dichas debilidades, sustentadas en incidentes recientes y evaluaciones oficiales.

Dicho de otra manera, los grupos armados organizados han incorporado drones comerciales modificados con capacidad de transportar explosivos y ejecutar ataques precisos contra objetivos militares y civiles.

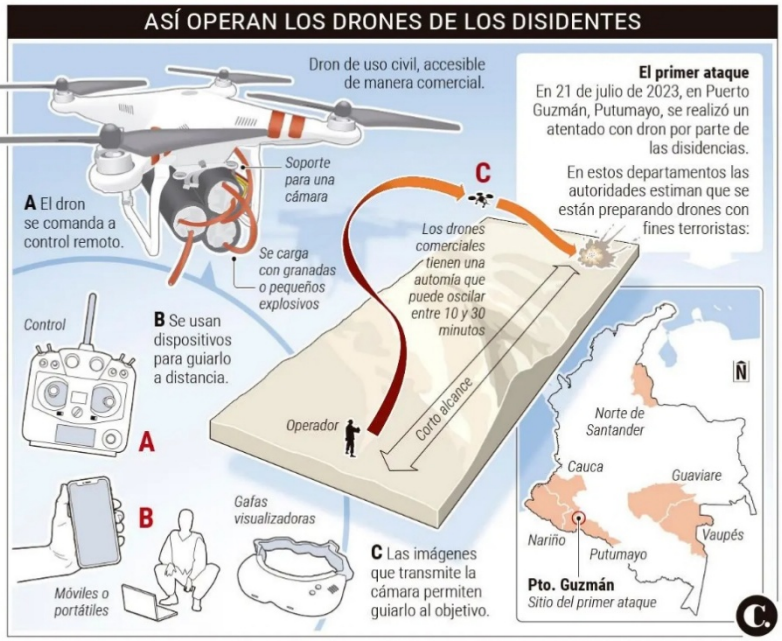
Figura 1. *Drones Que lanzan explosivos*

Nota. Fuente: (El País, 2024)

La presente figura, evidencia a soldados del Ejército Colombiano desactivando explosivos montados en un dron, las instalaciones militares tradicionalmente han sido diseñadas para enfrentar amenazas convencionales, principalmente terrestres o de aeronaves tripuladas, pero no estaban preparadas para agresiones con pequeños drones. En términos estructurales, muchas bases y puestos avanzados cuentan con amplios perímetros abiertos y pocos obstáculos contra incursiones aéreas de baja altura. Esto significa que un dron comercial modificado puede sobrevolar o ingresar al espacio de una guarnición sin ser detectado a tiempo, dejando expuestos a personal, arsenales y edificaciones críticas. Incidentes ocurridos en 2024 ilustran esta situación: por ejemplo, en El Plateado (Cauca) se reportó que "explosivos cayeron del cielo" sobre tropas y civiles, lanzados mediante drones artesanales por disidencias armadas(El País, 2024).

En efecto, esto evidencia que no existían barreras físicas ni defensas activas capaces de impedir que un artefacto volador pequeño logre lanzar explosivos dentro de las instalaciones militares y haga afectaciones a las tropas e incluso la población civil.

Figura 2 . *Drones comerciales con fines terroristas*



Fuente. (El País, 2024)

La figura con datos de AFP y las Fuerzas Militares, ofrece una representación gráfica clara y detallada del modo en que grupos armados organizados en Colombia están utilizando drones comerciales con fines terroristas. Esta infografía es particularmente útil para visualizar el funcionamiento técnico y táctico de estas amenazas emergentes, así como su impacto geográfico.

En la parte superior izquierda se observa un dron de uso civil, comúnmente disponible en el mercado, al cual se le ha adaptado un mecanismo para portar granadas o pequeños explosivos en lugar de la cámara habitual. Este tipo de dron es manipulado a través de controles remotos convencionales (etiqueta A), los cuales pueden ser del tipo tradicional con joysticks o mediante dispositivos móviles o portátiles (etiqueta B). Además, algunos operadores utilizan gafas de realidad aumentada o visores de primera persona (FPV), lo que

les permite una visualización directa de las imágenes transmitidas por la cámara del dron y guiarlo con mayor precisión hacia su objetivo (etiqueta C).

Al mismo tiempo, la figura resalta la autonomía limitada de estos drones comerciales, que suele oscilar entre 10 y 30 minutos, lo que les otorga un alcance relativamente corto, pero suficiente para realizar ataques rápidos y dirigidos desde distancias seguras. En efecto, la trayectoria que sigue el dron desde el punto de despegue hasta el blanco es representada mediante una flecha curva que concluye con la detonación del artefacto explosivo.

En la parte derecha inferior se incorpora un mapa de Colombia en el que se señalan departamentos críticos como Nariño, Putumayo, Cauca, Norte de Santander, Guaviare y Vaupés, donde las autoridades han detectado actividades relacionadas con la preparación de drones para ataques. Se destaca Puerto Guzmán (Putumayo) como el sitio del primer ataque confirmado de este tipo, ocurrido el 21 de julio de 2023, lo que marcó un precedente preocupante sobre el uso bélico de esta tecnología accesible.

[T2] Uso de drones en operaciones de grupos armados organizados en Colombia

El uso de drones representa una amenaza creciente para bases militares, arsenales y otras infraestructuras críticas, exponiendo vulnerabilidades en los sistemas de defensa aérea. En el plano normativo y doctrinal, hasta fechas recientes, Colombia carecía de un marco jurídico y procedimental robusto para enfrentar el uso malicioso de drones. Si bien la Aeronáutica Civil ha emitido regulaciones (RAC 91 y 100) que prohíben volar drones en zonas restringidas, por ejemplo, sobre instalaciones militares, policiales o carcelarias.

Igualmente, dichas normas se orientan al uso recreativo o comercial legítimo y su cumplimiento por parte de actores ilegales es nulo. Previo a 2023-2024, no existían leyes específicas que sancionaran penalmente el empleo de drones como armas, ni que facultaran explícitamente a la Fuerza Pública a *detectar e inhabilitar* drones sospechosos en el espacio aéreo nacional. Esta laguna legal representó una vulnerabilidad: ante la ausencia de un **marco** legal claro, las Fuerzas Militares y de policía enfrentaban ambigüedades sobre la autoridad para neutralizar un dron en vuelo, por ejemplo, el uso de inhibidores de frecuencia, que en tiempos de paz podría entrar en conflicto con normas de telecomunicaciones, o el derribo de drones civiles, que podría generar responsabilidades si no está claramente autorizado.

Adicionalmente, la falta de regulación en la venta y tenencia de drones facilitó que grupos armados accedieran a esta tecnología sin mayores obstáculos. Un estudio resaltó que en Colombia la documentación y registro de drones civiles ha sido históricamente laxa, y existe poco respeto por la normatividad en el uso de VANT (vehículos aéreos no tripulados) . Esto derivó en un mercado donde disidencias y otros actores pudieron adquirir fácilmente drones comerciales (incluso a través de plataformas en línea internacionales, como evidenció la incautación de un dron DJI en manos de disidencias, comprado por Internet)(Ministerio de Defensa Nacional, 2024). La situación contrasta con países donde el uso de drones está estrictamente licenciado; en Colombia esa ausencia de controles legales y administrativos permitió la proliferación de dispositivos en manos indebidas.

Ante los ataques con drones sufridos, el Gobierno reconoció esta vulnerabilidad normativa y comenzó a subsanarla. En 2024, las autoridades impulsaron por primera vez iniciativas legales específicas para contrarrestar este fenómeno. El comandante de la Policía Nacional, general William Salamanca, anunció el impulso de un *proyecto de ley* en el

Congreso orientado a regular el uso de drones en Colombia, a raíz de la preocupación generada por los ataques de grupos criminales (particularmente las disidencias de las FARC)(Mazo, 2024). Esta propuesta elaborada con apoyo del Ministerio de Defensa busca establecer diferenciaciones entre usos legítimos (recreativos, comerciales, estatales) y actividades ilícitas con drones, creando sanciones y controles a la comercialización y empleo de estos aparatos.

Igualmente, el Ministerio de Defensa expidió doctrinas internas y protocolos operacionales para que las Fuerzas Militares y de Policía actúen coordinadamente ante incursiones de drones hostiles, algo que antes no estaba formalizado. Cabe destacar que, con la formulación de la Política de Ciencia, Tecnología e Innovación en Defensa en 2024, se incorporó oficialmente la defensa contra drones como una línea prioritaria, lo cual proporciona sustento normativo para la asignación de recursos y desarrollo de capacidades antidron por ejemplo, se destinaron más de 20.000 millones de pesos a la adquisición de estos sistemas, según el Ministerio de Defensa(Patiño, 2024). No obstante, mientras dichas reformas legales se materializan, sigue presente la vulnerabilidad de un vacío normativo que por años dejó a las fuerzas del Estado con herramientas jurídicas limitadas para anticipar y perseguir la amenaza de los drones. La pronta aprobación e implementación de la nueva legislación será crucial para cerrar esta brecha y respaldar las operaciones de defensa anti-dron dentro de un estado de derecho claro y legítimo.

Figura 3. *Drones Grupos Armados*

Nota. Fuente: (Cano, 2023)

La dispersión geográfica de las unidades militares en Colombia introduce una dimensión estructural adicional, ya que muchas de ellas están localizadas en regiones selváticas o montañosas donde el control del espacio aéreo a baja altitud(Cano, 2023). Las líneas de visión obstruidas por la topografía y la vegetación espesa, pueden dificultar tanto la vigilancia humana como la eficacia de sensores (radares terrestres, cámaras) si es que estos existen. En puestos remotos, el personal en guardia carece de medios específicos para detectar un dron más allá de la observación visual o auditiva medios claramente insuficientes dada la velocidad y el tamaño reducido de estos aparatos. Asimismo, la ausencia histórica de ataques aéreos no convencionales hizo que muchas instalaciones no contaran con protocolos de respuesta ante la presencia de drones: no existían procedimientos estandarizados sobre qué hacer si se avista un dron sobrevolando una base, lo que genera confusión y retrasos en la reacción inicial.

Consecuentemente, los grupos armados ilegales han explotado estas brechas estructurales. Las estadísticas oficiales muestran que en 2024 se registraron 115 incidentes de ataques con drones en el país, perpetrados en su mayoría por organizaciones criminales o terroristas, afectando a personal militar e instalaciones estratégicas sin que las defensas existentes pudieran impedirlo. El hecho de que estas agresiones hayan tenido éxito relativo (causando heridos, daños a infraestructura e incluso muertes) indica que la arquitectura actual de seguridad perimetral y aérea de las bases es vulnerable y requiere ser replanteada para esta nueva clase de amenaza (Patiño, 2024).

[T1] Efectividad de los Sistemas de Defensa Anti-Dron

En Colombia, la efectividad de los sistemas de defensa anti-dron ha sido hasta ahora limitada, debido a la escasa disponibilidad de tecnología especializada, la dispersión geográfica de las unidades militares y la complejidad del terreno nacional. Hasta finales de 2024, la mayoría de las instalaciones militares no contaban con sensores específicos para la detección y neutralización de drones de bajo vuelo. Por ende, esta carencia permitió que grupos armados ilegales llevaran a cabo múltiples ataques sin oposición efectiva. Debido a que, las amenazas fueron particularmente evidentes en regiones como el Cauca y el Putumayo, donde drones comerciales modificados fueron usados para lanzar explosivos y realizar operaciones de vigilancia. La inexistencia de sistemas C-UAS integrados (radares, inhibidores, cámaras ópticas, entre otros) dejó en evidencia una brecha tecnológica que el Estado colombiano ha comenzado a abordar mediante inversiones recientes.

A partir del segundo semestre de 2024, el Ministerio de Defensa inició la adquisición de sistemas avanzados como Skylock Dome, así como equipos portátiles de interferencia electrónica (jammers) y sensores RF. Estos sistemas permiten detectar y neutralizar drones hostiles mediante perturbación de señales o identificación visual. Sin embargo, su despliegue aún es limitado y no ha cubierto todas las instalaciones críticas. Además, el desempeño de los sistemas ha demostrado variabilidad en zonas con selva densa o topografía montañosa, lo que plantea el reto de adaptar la tecnología a las condiciones del entorno colombiano. Por tanto, aunque se han dado avances relevantes, la efectividad general de los sistemas antidron dependerá de su cobertura total, su interoperabilidad entre fuerzas y su sostenibilidad logística, así como del entrenamiento especializado del personal encargado de operarlos.

[T2] Sistemas anti-dron implementados en Colombia

En el frente tecnológico, las vulnerabilidades provienen de la insuficiente capacidad instalada para detectar, rastrear e interceptar drones hostiles, así como de limitaciones técnicas de los equipos disponibles frente a las condiciones operativas en Colombia. Hasta antes del plan nacional antidron lanzado a finales de 2024, las Fuerzas Militares contaban con muy pocos sistemas dedicados de *Counter-UAS*. La defensa antiaérea convencional radares militares y armamento antiaéreo está concebida para aeronaves de mayor tamaño y velocidad, por lo que un dron pequeño, de plástico y bajo vuelo, podía fácilmente escapar del radar y volar por debajo del umbral de detección.

El ministro de Defensa Iván Velásquez admitió en junio de 2024 que era necesario incrementar capacidades en esta materia, reflejando que los medios tecnológicos existentes

no bastaban para proteger plenamente las instalaciones militares. En varios ataques reportados, los drones lograron alcanzar sus blancos sin oposición efectiva, lo que sugiere que no había sensores tempranos ni contramedidas electrónicas funcionando en esas ubicaciones en el momento del incidente(Patiño, 2024).

Otro aspecto crítico es la adaptación de la tecnología al terreno. Colombia presenta terrenos complejos (cordilleras, selvas) que plantean retos técnicos para los sistemas antidron. Algunos equipos probados por el Ejército inicialmente mostraron un desempeño adecuado en zonas planas (por ejemplo, en Bogotá o en la sabana de Tolemaida), pero al llevarlos al Cauca no funcionan, según explicó el general Emilio Cardozo, señala una vulnerabilidad importante: no todos los sistemas comerciales contra drones son eficaces en entornos montañosos o selváticos, donde las señales de radio pueden tener interferencias y la detección por radar o línea visual se dificulta(Nomesqui, 2025). Ahora bien, la lección aprendida por las Fuerzas Militares es que se requieren soluciones tecnológicas calibradas para las condiciones locales; de lo contrario, una falsa sensación de seguridad podría dejar expuestas a las unidades desplegadas en regiones agrestes.

El plan de defensa anti-UAV colombiano busca combinar detección y neutralización. Entre las tecnologías evaluadas figuran sistemas integrales como *Skylock Dome* (israelí), que usa radares avanzados y sensores ópticos (detecta hasta 400 drones y con IA evalúa sus cargas útiles). En 2024 el Ejército expresó interés en Skylock Dome precisamente por su capacidad de repeler enjambres y proteger infraestructura crítica. También se han obtenido equipos más sencillos: por ejemplo, en septiembre de 2024 fuerzas del Valle del Cauca recibieron un paquete de antidrones portátiles (drones modificados con jammers de largo alcance) para las operaciones de la COP16. Estos dispositivos, según autoridades locales, "identifican" drones

hostiles a varios kilómetros (gracias a su antena inhibidora) y emiten señales de interferencia para cortar el enlace de control y hacerlos aterrizar(Saumeth, 2024a).

En la práctica, los métodos de neutralización en Colombia se basan principalmente en interferencia electrónica (jamming). Los equipos entregados cuentan con inhibidores de radiofrecuencia de largo alcance que, una vez detectan un dron armado, envían pulsos que rompen el enlace de control remoto. Así los pilotos pierden el control del dispositivo hasta que aterriza y se evita el ataque. Además, la Policía Nacional ha explorado el uso de fusiles antidrón (tipo DroneGun") que lanzan señales de bloqueo local o redes para derribar UAVs. Colombia también impulsa alianzas con la industria: por ejemplo, la empresa española Indra creó en 2024 un hub regional en Colombia para desplegar sistemas de guerra electrónica y antidrón en América Latina(Saumeth, 2023).

Asimismo, existía hasta hace poco personal entrenado y unidades especializadas en guerra electrónica enfocada en drones. La respuesta inicial a la amenaza recayó en métodos convencionales (intentar derribar el dron a tiros, evacuar al personal, etc.), los cuales no siempre son efectivos ni seguros. La falta de integración entre las Fuerzas –por ejemplo, conectar los radares y defensa aérea de la Fuerza Aérea con las alertas en bases del Ejército en tierra– también constituía una brecha tecnológica-organizativa: cada fuerza manejaba por separado la situación, lo que podía causar demoras en la reacción ante un dron enemigo.

De la misma manera, entre 2023-2024 el perfil tecnológico antidron de Colombia presentaba carencias notables: escasez de sensores especializados desplegados, ausencia de sistemas de neutralización en la mayoría de las guarniciones, y limitada operatividad en terreno difícil de los pocos equipos probados. Esta situación motivó la asignación de recursos

de emergencia a finales de 2024 para la compra e implementación de sistemas antidron de última generación, (Deutsche Welle, 2024).

No obstante, hasta que dichos sistemas estén plenamente operativos en todas las instalaciones sensibles, persiste la vulnerabilidad tecnológica que podría seguir siendo explotada por grupos ilegales mediante drones para espionaje, contrabando o ataques. La evidencia de 115 incidentes en un año confirma que el enemigo supo aprovechar la brecha tecnológica existente, lo que urge a superarla con inversión e innovación rápida (analizado en el siguiente apartado)(Patiño, 2024).

[T3] Capacidades futuras y líneas estratégicas para una defensa anti-dron integral

La experiencia reciente en Colombia frente al uso de drones por parte de grupos armados ilegales ha dejado en evidencia la urgente necesidad de construir capacidades robustas y sostenibles para enfrentar esta amenaza. Hasta 2024, los 115 incidentes documentados de ataques o sobrevuelos no autorizados con drones, particularmente en departamentos como Cauca, Arauca y Norte de Santander, demostraron que el país carecía de un sistema integral para prevenir y neutralizar incursiones aéreas no tripuladas (Patiño, 2024). A partir de ello, se delinean cinco capacidades clave que deben ser desarrolladas para consolidar una defensa antidron eficaz.

En primer lugar, la construcción de una doctrina unificada y normativa C-UAS es indispensable. En Colombia, cada fuerza Ejército, Fuerza Aérea, Armada y Policía ha operado de forma independiente en cuanto a la respuesta antidron. Por ejemplo, en el ataque ocurrido en mayo de 2024 contra una base del Ejército en el Putumayo, se comprobó que la

base no estaba conectada a ningún sistema de alerta temprana de la Fuerza Aérea, lo que impidió una reacción coordinada. En contraste, países como Israel y Estados Unidos han desarrollado doctrinas conjuntas que permiten respuestas articuladas en tiempo real entre fuerzas terrestres, aéreas y de inteligencia, con protocolos estandarizados de reacción ante distintas clases de drones (comerciales, tácticos, de enjambre, etc.).

En segundo lugar, se requiere la incorporación de inteligencia artificial y autonomía en los sistemas de detección y respuesta. Los drones utilizados por los grupos armados en Colombia, como los DJI Phantom modificados o los Matrice 300, vuelan a baja altura y pueden cambiar rutas con rapidez. Los sistemas tradicionales, como radares militares convencionales, no están diseñados para detectar estos objetivos. Por eso, el Ejército de Colombia inició pruebas con el sistema Skylock Dome en 2024, un equipo israelí que emplea sensores ópticos e inteligencia artificial para identificar drones, analizar su comportamiento y activar inhibidores de señal automáticamente. No obstante, su uso aún está limitado a pocas instalaciones piloto en Tolemaida, La Guajira y Tumaco. La experiencia de Arabia Saudita también es relevante: tras el ataque con drones a su refinería de Aramco en 2019, desarrollaron sistemas de IA que hoy permiten neutralizar amenazas en menos de 7 segundos(Sheu et al., 2019).

En tercer lugar, la cobertura territorial debe ir más allá de los perímetros militares. El uso de drones para vigilancia y ataques se ha extendido a zonas rurales, corredores de narcotráfico y pasos ilegales fronterizos. Por ejemplo, en el Catatumbo, se han reportado sobrevuelos sospechosos sobre instalaciones de la Policía, y en la frontera con Venezuela, el ELN habría usado drones para monitorear movimientos del Ejército (Deutsche Welle, 2024).

Para hacer frente a esto, se requiere desplegar una red de sensores terrestres y aéreos, integrados a un sistema nacional de vigilancia que conecte estaciones fijas y móviles, radares de corto alcance, y drones de patrullaje propios, como se ha hecho en México a lo largo del muro fronterizo con EE.UU., mediante el programa "Tecnología Fronteriza Integral".

Una cuarta línea clave es el fortalecimiento de la industria nacional de defensa y la reducción de la dependencia tecnológica externa. Hasta ahora, Colombia ha adquirido sistemas antidron mediante importaciones (Skylock Dome de Israel, DroneGun de Australia, jammers de origen chino), pero no cuenta con desarrollo propio. Esto encarece los costos, dificulta el mantenimiento y limita la personalización de soluciones para el terreno nacional. En 2024, la empresa española Indra abrió en Colombia un centro regional de guerra electrónica, lo cual representa una oportunidad para que la industria local incluyendo empresas como CIAC o Codaltec participe en el desarrollo de sensores, software de detección y plataformas móviles de defensa antidron adaptadas a la selva, la montaña y las zonas costeras.

Por último, la capacitación del recurso humano es una condición sine qua non. La operación de estos sistemas requiere personal entrenado en guerra electrónica, análisis de señales, ciberdefensa y mantenimiento técnico. En la actualidad, solo el Batallón de Guerra Electrónica del Ejército y algunos operadores de la Fuerza Aérea cuentan con formación específica en C-UAS. En 2023, en el ataque con dron explosivo contra una estación policial en Jamundí, los uniformados desconocían los protocolos para reportar, rastrear o mitigar la amenaza, lo que resultó en fallas graves de respuesta. A diferencia de esto, países como Alemania y Francia capacitan permanentemente a sus tropas en simuladores C-UAS y han

creado unidades permanentes dedicadas a operaciones antidron, con entrenamiento conjunto entre ejército, policía y cuerpos civiles.

[T1] Estrategias para la Optimización de la implementación de tecnologías anti-dron

Frente a las vulnerabilidades descritas, resulta imperativo incorporar innovaciones tecnológicas que fortalezcan la defensa anti-dron en Colombia. A nivel global, el campo de los sistemas *C-UAS* ha avanzado rápidamente, ofreciendo un abanico de soluciones que van desde radares especializados hasta armas de energía dirigida. En el contexto colombiano, la adopción de estas tecnologías debe adaptarse a las realidades operativas locales (terreno, tipo de amenaza, recursos disponibles) y complementarse con desarrollos propios e iniciativas de cooperación internacional(Departamento de Seguridad Nacional de los Estados Unidos, 2024). A continuación, se presentan las principales innovaciones tecnológicas relevantes y su aplicabilidad para mejorar la seguridad y resiliencia de las instalaciones militares en Colombia.

[T2] Detección temprana y seguimiento

La primera capa de un sistema antidron eficaz es la capacidad de *descubrir* la presencia de vehículos no tripulados hostiles a la mayor distancia y con la mayor anticipación posible. Para ello, se cuenta con radares de alta resolución diseñados específicamente para objetos de baja firma radar (drones pequeños, a baja altura). Por ejemplo, el sistema español Crow

(adquirido recientemente por la Fuerza Aérea Colombiana) emplea radares capaces de identificar drones de tamaño reducido a largas distancias, (El País, 2024).

Por lo tanto, este tipo de radar especializado puede distinguir un dron incluso cuando vuela bajo o entre obstáculos, algo esencial para el paisaje colombiano. Junto a los radares, se integran sensores electroópticos e infrarrojos de última generación: cámaras de gran alcance y resolución que, apoyadas por algoritmos de inteligencia artificial, permiten identificar visualmente el objeto detectado y evaluar si representa una amenaza real (por ejemplo, determinando si porta algún paquete sospechoso). Estas cámaras también ayudan a hacer seguimiento continuo del dron una vez detectado, lo cual es vital para dirigir las contramedidas.

Al respecto, otra innovación en detección es el uso de sensores de radiofrecuencia (RF) que escanean el espectro electromagnético en busca de las señales de control o enlace de datos que emiten los drones. Muchos drones comerciales operan en bandas conocidas (2.4 GHz, 5.8 GHz); un receptor RF avanzado puede captar estas emisiones y *localizar la fuente*, incluso eventualmente identificar el modelo de dron por su firma electrónica.

En efecto, la empresa francesa Cerbair, cuyo sistema móvil contra-drones fue seleccionado por Colombia en 2019, basa su tecnología precisamente en la detección RF combinada con perturbación electrónica. La FAC (Fuerza Aeroespacial Colombiana) integró unidades móviles de Cerbair para proteger bases aéreas, indicando desde entonces la búsqueda de innovaciones que detecten e inhiban drones de forma portátil y rápida. Tales sistemas RF son especialmente útiles en entorno urbano o selvático donde el radar tradicional puede fallar: al captar la señal del dron o su operador, ofrecen una alerta temprana complementaria a la del radar y cámaras, (Prensa Latina, 2025).

Al respecto, la tendencia tecnológica es hacia sistemas multisensor integrados. Colombia ya demostró las ventajas de esta aproximación durante la COP16 (Conferencia de Biodiversidad de la ONU en 2024) en Cali, donde desplegó el sistema Crow combinado con otros sensores, logrando detectar más de 300 drones y bloquear 90 actividades no autorizadas, (Saumeth, 2024b).

La integración de múltiples unidades coordinadas permitió cubrir un amplio espacio aéreo de manera consistente. Esta experiencia pionera en un evento internacional puede trasladarse ahora a la protección permanente de instalaciones militares: dotar a cada base importante de una burbuja de vigilancia 360° con radar, óptica y análisis de radiofrecuencia interconectados, gestionados por un centro de control que fusione esas fuentes de datos (tecnología de fusión de sensores). De esta forma, se incrementa exponencialmente la probabilidad de detección temprana, incluso si el adversario emplea técnicas de sigilo o drones autónomos.

[T3] Neutralización y contramedidas

Una vez identificado un dron intruso, el siguiente paso innovador es su neutralización segura y efectiva. Aquí destacan varias tecnologías aplicables: la inhibición por radiofrecuencia, las contramedidas cinéticas de precisión y, en el futuro próximo, sistemas de energía dirigida. En el corto plazo, la opción más viable y ya en proceso de adopción en Colombia es la inhibición (jamming) de las comunicaciones del dron. Consiste en emitir señales electromagnéticas potentes en las mismas frecuencias que utiliza el dron, para interrumpir el enlace con su operador o con los satélites de navegación GPS. El efecto típico

es que el dron quede desorientado o regrese automáticamente a su punto de origen, desactivando así la amenaza.

Los nuevos *"sistemas antidrones"* adquiridos por el Ministerio de Defensa incluyen seguramente esta capacidad: el propio ministro Velásquez explicó que están *"diseñados para detectar y neutralizar"* drones manejados ilegalmente. De hecho, el sistema Crow de Indra, ya citado, integra un bloque de tecnología de interferencia (jamming) que, una vez confirmada la amenaza, bloquea las guías de control del dron. Esta clase de contramedida electrónica es especialmente útil porque evita daños colaterales: el dron atacado por jamming normalmente aterrizará o caerá fuera de control antes de llegar a su objetivo, sin necesidad de dispararle munición real sobre áreas pobladas(Patiño, 2024).

Sin embargo, la inhibición RF puede no ser suficiente en todos los casos, por ejemplo, si el dron vuela de manera autónoma con una ruta preprogramada, o si opera en modo totalmente autoguiado sin depender de señales externas. Para esos casos, se exploran contramedidas cinéticas. Aquí también hay innovaciones interesantes: desde drones interceptores (drones defensivos que persiguen y chocan o atrapan al intruso con redes) hasta municiones especiales anti-dron disparadas desde escopetas o fusiles(Çetin et al., 2021). Sobre esto último, destaca el desarrollo de cartuchos anti-dron presentados en 2024 por la corporación rusa Rostec, diseñados para ser usados en armas ligeras y capaces de derribar drones pequeños.

En efecto, tales municiones expelen una suerte de perdigones o proyectiles optimizados para alcanzar blancos aéreos diminutos, incrementando la probabilidad de derribo con escopetas a rangos cortos. Si bien esta tecnología rusa es reciente y su eficacia real está por probarse, ilustra cómo la innovación se extiende incluso a equipamiento

convencional adaptado para la amenaza dron(Rostec, 2024). En el contexto colombiano, donde muchas patrullas en terreno no tendrían a mano sistemas complejos, disponer de medios cinéticos sencillos (pero especializados) como escopetas con cartuchos antidron o rifles de aire comprimido de alta potencia con miras automatizadas podría brindar una última línea de defensa para neutralizar un artefacto enemigo que haya evadido otras capas de protección. El Ejército Nacional ha estado probando algunas novedosas armas antidrones en 2024, cuyos detalles se mantienen reservados, pero que apuntan justamente a contar con opciones portátiles de neutralización.

A mediano y largo plazo, están emergiendo tecnologías más futuristas como los láseres de alta energía dirigidos. Estos sistemas pueden *"quemar"* o incapacitar físicamente a un dron a velocidad de la luz, y ya se han ensayado en otros países contra blancos aéreos pequeños. Colombia, a través de su política de innovación, podría explorar convenios para probar armas de energía dirigida en escenarios controlados, dado que sus características (precisión y ausencia de munición tradicional) serían ideales para proteger bases sin riesgo de metralla. No obstante, por ahora estos sistemas son costosos y complejos, por lo que las soluciones implementables a corto plazo seguirán siendo combinaciones de detección multi-sensor + inhibición RF + métodos cinéticos selectivos (Ver figura 1).

Figura 4. *Sistema tecnológico de defensa anti-dron*

Nota. Fuente: (Wuhan, 2024)

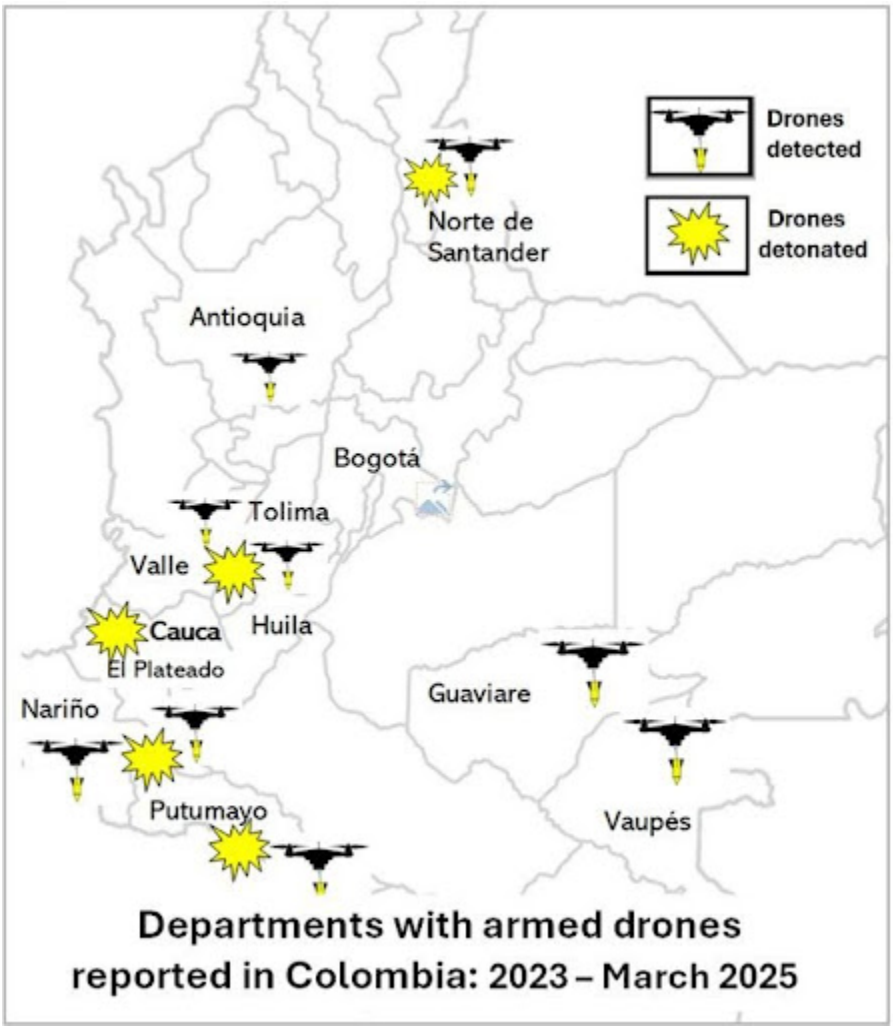
La figura presenta un sistema tecnológico de defensa anti-dron desplegado en un entorno abierto, posiblemente como parte de una prueba o una instalación temporal de vigilancia aérea. En primer plano, se observan dos dispositivos montados sobre trípodes, que parecen corresponder a componentes clave de un sistema C-UAS (Counter-Unmanned Aerial System), utilizado para la detección, seguimiento y neutralización de drones no autorizados(NUST, 2024).

Los sensores RF que operan en frecuencias 2.4G y 5.8G están diseñados para detectar drones comerciales con precisión, lo que implica componentes sofisticados y algoritmos de inteligencia artificial. Su capacidad para hacer detección pasiva sin interferir con otras señales los convierte en herramientas valiosas para defensa y seguridad(Departamento de Seguridad Nacional de los Estados Unidos, 2024). A valores de 2025, este rango equivale aproximadamente a 240-400 millones de pesos colombianos por unidad, lo cual representa una inversión significativa para entidades públicas. Esto puede requerir licitaciones, convenios interinstitucionales o cooperación internacional para adquirir varias unidades, (Wuhan, 2024).

De la misma manera, el dispositivo a la izquierda, de forma cilíndrica y superficie lisa, corresponde muy probablemente a una antena de radar omnidireccional o a un sensor de radiofrecuencia diseñado para detectar señales emitidas por drones comerciales y sus controladores. Su diseño cerrado y aerodinámico sugiere resistencia a condiciones climáticas adversas y eficiencia en la captación de frecuencias electromagnéticas en un rango amplio.

A la derecha, el equipo más complejo montado sobre un trípode robusto parece integrar múltiples tecnologías. La parte superior incluye dos antenas verticales que posiblemente sirven para la interferencia de señal (*jamming*), mientras que el módulo rectangular adosado puede corresponder a un radar de escaneo electrónico o un sistema de control de dirección para rastrear objetos voladores(Alexandra, 2015). En la parte inferior del conjunto hay otros componentes que podrían incluir cámaras ópticas o térmicas para identificación visual, junto con un sistema de soporte y estabilización. Este tipo de dispositivo compuesto se asemeja a los sistemas móviles multisensor, diseñados para actuar como plataformas de vigilancia táctica en eventos o zonas sensibles, brindando detección temprana, geolocalización y respuesta activa.

Figura 5. *Incidentes con drones armados entre 2023 y marzo de 2025*



Nota. Fuente: (Hide, 2025)

Como se evidencia, la figura muestra un mapa de Colombia destacando los departamentos donde se han reportado incidentes con drones armados entre 2023 y marzo de 2025. Los íconos indican tanto detecciones como detonaciones de drones, siendo más críticos los departamentos de Cauca, Putumayo, Nariño, Valle del Cauca y Norte de Santander, donde se han registrado explosiones confirmadas. La concentración de estos eventos en regiones con alta presencia de grupos armados ilegales revela una expansión del uso de tecnologías

como los drones con explosivos en el conflicto armado, especialmente en zonas rurales del suroccidente del país (Hide, 2025).

De la misma manera, Colombia debe evaluar alternativas tecnológicas viables conforme a los análisis técnicos realizados por las Fuerzas Militares, con el objetivo de fortalecer los sistemas de seguridad de sus unidades. Estas decisiones deben priorizar criterios como eficiencia operativa, sostenibilidad logística, capacidad de integración con sistemas existentes y potencial de desarrollo tecnológico a mediano y largo plazo.

[T4] Adaptación al contexto colombiano

Una constante en la aplicación de cualquier tecnología nueva es la necesidad de adaptarla al contexto local. Las Fuerzas Militares han aprendido esto empíricamente en las pruebas de sistemas antidron: ningún equipo será adquirido si no demuestra funcionar en el terreno colombiano real. Por ello, una innovación clave ha sido el desarrollo de protocolos de evaluación técnica in situ: antes de desplegar masivamente un sistema, se realizan pruebas en distintas regiones (llanos, montañas, selva) para calibrar su rendimiento(Tavera, 2024). Esta práctica asegura que las inversiones se hagan en equipos cuyo diseño y software puedan ajustarse a las necesidades (por ejemplo, algoritmos de radar configurados para ignorar el "ruido" de aves en la jungla, o para distinguir drones de helicópteros en zonas donde opera la aviación militar).

La transferencia tecnológica también juega un rol: Colombia está buscando no solo comprar equipos, sino aprender de los fabricantes y aliados cómo mantenerlos y mejorarlos. El programa antidrones anunciado incluye componentes de economía de escala y proyectos

de uso dual, para optimizar recursos y obtener beneficios colaterales en sectores civiles(Patiño, 2024). Un ejemplo es aprovechar las mismas cámaras y drones defensivos para tareas como vigilancia agrícola, control ambiental o atención de desastres cuando no estén en uso militar, maximizando así el retorno de la inversión tecnológica.

En términos organizacionales, una innovación importante ha sido la creación de equipos especializados interinstitucionales. Bajo el liderazgo de la Fuerza Aeroespacial Colombiana, el país avanzó en 2024 en una hoja de ruta que coordina esfuerzos de las Fuerzas Militares y la Policía en materia de defensa contra drones(Prensa Latina, 2025). Esto incluye centros de comando conjuntos para monitorear el espacio aéreo de bajo nivel en tiempo real, compartiendo información entre la FAC (que opera radares y aeronaves) y el Ejército/Armada (que protegen las instalaciones en tierra) y la Policía (que aporta inteligencia sobre posibles planes de ataque con drones y maneja la seguridad urbana).

La cooperación internacional es otro pilar: se está trabajando con países aliados con años de experiencia en amenazas similares (se menciona colaboración con agencias de Estados Unidos en entrenamiento y dotación de equipo), así como con fabricantes de renombre global para adaptar soluciones a Colombia. Gracias a ello, Colombia se perfila como pionera regional en la adopción de la tecnología antidron, habiendo incursionado tempranamente en su uso desde 2006 y ahora integrando sistemas avanzados que muchos vecinos apenas comienzan a considerar(Saumeth, 2024b).

[T4] Propuesta Estratégica

La creciente amenaza que representan los vehículos aéreos no tripulados (UAVs) empleados por grupos armados ilegales en Colombia exige el diseño de una propuesta estratégica integral que oriente la implementación de sistemas de defensa anti-dron (C-UAS) a nivel nacional. Dicha propuesta debe estructurarse en fases secuenciales y complementarias, articulando el marco legal, las capacidades tecnológicas, la coordinación interinstitucional y el desarrollo industrial nacional. Esto garantizará no solo la neutralización efectiva de amenazas aéreas, sino también la sostenibilidad operativa y tecnológica de las Fuerzas Militares (Patiño, 2024).

El primer paso consiste en consolidar un marco normativo y doctrinal que otorgue a las Fuerzas Militares y de Policía la autoridad expresa para detectar, interferir y neutralizar drones no autorizados en el espacio aéreo colombiano, en consonancia con el Derecho Internacional Humanitario y las regulaciones de la Aeronáutica Civil. Este marco debe incluir protocolos claros sobre el uso de inhibidores de señal, armas cinéticas y otros métodos de neutralización, así como reglas de enfrentamiento (ROE) adaptadas al contexto de la amenaza drónica (Mazo, 2024). A nivel doctrinal, es fundamental desarrollar manuales tácticos C-UAS que integren las lecciones aprendidas en operaciones nacionales y buenas prácticas internacionales, como las doctrinas OTAN sobre protección de instalaciones críticas frente a UAVs (Marrone, 2022).

La segunda fase requiere el despliegue progresivo de sistemas de detección y neutralización en las regiones con mayor incidencia de ataques, como Cauca, Nariño, Putumayo y Norte de Santander (Hide, 2025). Esto implica la instalación de sensores

multisectoriales (radares de baja firma, sensores RF, cámaras ópticas e infrarrojas) integrados en redes de vigilancia 24/7, así como la provisión de equipos de neutralización portátiles y fijos. La priorización geográfica permitirá cubrir primero las instalaciones estratégicas y luego expandir la cobertura hacia áreas rurales de alto riesgo. Experiencias internacionales, como el uso del sistema Skylock Dome en entornos urbanos y rurales, evidencian la necesidad de calibrar los sistemas a las condiciones topográficas y climáticas locales para maximizar su efectividad (Saumeth, 2024a).

La tercera fase contempla la creación de unidades antidron especializadas en cada división y brigada, integradas por personal entrenado en guerra electrónica, ciberdefensa y operación de sistemas C-UAS. Este personal debe recibir formación continua, incluyendo simulacros de ataques y ejercicios conjuntos con la Fuerza Aeroespacial, la Armada y la Policía Nacional (Ministerio de Defensa Nacional, 2024). Asimismo, es imprescindible establecer centros de comando y control unificados que integren la información procedente de todos los sensores y permitan una respuesta coordinada en tiempo real. La experiencia de países como Israel demuestra que la interoperabilidad entre fuerzas y agencias civiles es clave para neutralizar amenazas aéreas no tripuladas de forma eficiente (Sheu et al., 2019).

La última fase busca garantizar la sostenibilidad de la defensa antidron a través del fortalecimiento de la industria nacional de defensa. Colombia debe fomentar alianzas entre las Fuerzas Militares, empresas tecnológicas (como CIAC y Codaltec) y universidades para desarrollar sensores, software de detección e interceptores propios adaptados a entornos selváticos, montañosos y costeros. Iniciativas como el hub regional de guerra electrónica de

Indra en Colombia constituyen una oportunidad para transferir tecnología y reducir la dependencia de proveedores extranjeros (Saumeth, 2023). Este enfoque no solo disminuirá costos a largo plazo, sino que incrementará la autonomía tecnológica del país, alineándose con la Política de Ciencia, Tecnología e Innovación en Defensa (Ministerio de Defensa Nacional, 2024).

[T1] Conclusiones

Se recomienda agilizar la adquisición y despliegue de sistemas antidron en todas las instalaciones militares de importancia estratégica. La prioridad debe darse a aquellas unidades en zonas de alto riesgo (Cauca, Nariño, Catatumbo, entre otras) donde los grupos armados tienen presencia y han ensayado ataques con drones. Estos sistemas deben incluir capacidades de detección 24/7 (radares, sensores RF) y de respuesta inmediata (jammers, drones interceptores), integrados en una red nacional de vigilancia. Asimismo, se sugiere establecer un centro de monitoreo unificado que reciba en tiempo real las alertas de todos los sensores desplegados en el país, evitando así vacíos de cobertura. Dado que las pruebas han mostrado variaciones de rendimiento en distinto terreno, es crucial que los sistemas escogidos se calibren en el terreno antes de su compra definitiva; esto garantizará su efectividad operativa.

Aunque está en trámite legislación para regular el uso de drones y facultar su control, es vital acelerar la aprobación de este marco legal. Se recomienda que la nueva ley defina claramente la autoridad de las Fuerzas Militares y de Policía para detectar, interferir y

derribar drones no autorizados en espacio aéreo colombiano, incluyendo las responsabilidades en tiempos de paz y en zonas rurales apartadas. Igualmente, la ley debe imponer controles a la venta de drones de ciertas características (carga útil, alcance, autonomía) y sanciones ejemplares al uso ilícito de estos aparatos, de modo que actúe como disuasivo legal. En paralelo, deben actualizarse las reglas de enfrentamiento (ROE) internas: cada comandante debe tener lineamientos precisos sobre cómo actuar ante un dron hostil, minimizando la ambigüedad legal. Un marco robusto no solo habilitará la acción oportuna, sino que protegerá a los efectivos que actúen en legítima defensa antiaérea contra eventuales litigios.

La incorporación de tecnología avanzada debe ir acompañada de un intenso programa de capacitación. Se recomienda crear unidades o equipos antidron especializados en cada división o brigada, compuestos por personal entrenado en operación de equipos C-UAS y en tácticas de respuesta. Estos equipos deben recibir instrucción continua, incluyendo simulacros de ataques con drones para ensayar la coordinación entre los operadores de sensores, tiradores designados y cadena de mando. Adicionalmente, integrar módulos sobre amenazas drónicas en los currículos de las escuelas militares (de oficiales y suboficiales) y en los centros de entrenamiento de la Policía Nacional.

A nivel doctrinal, es necesario desarrollar manuales tácticos propios sobre defensa contra drones, ajustados a las lecciones aprendidas localmente y a las mejores prácticas internacionales (por ejemplo, protocolos de la OTAN u otros países aliados adaptados a la realidad colombiana). Esta doctrina deberá abarcar no solo la defensa de instalaciones fijas sino también la protección de tropas en operaciones móviles (patrullas, convoyes) frente a posibles ataques desde el aire(Marrone, 2022).

Recomendar modificaciones en la infraestructura militar para reducir la efectividad de posibles ataques con drones. Por ejemplo, en polvorines y depósitos de municiones, implementar cubiertas o mallas de protección aérea que impidan la caída directa de artefactos explosivos lanzados desde drones. En alojamientos de personal y puestos de guardia, considerar techos reforzados o refugios cercanos a los puestos centinela donde el personal pueda cubrirse rápidamente si se detecta un dron armado. Del mismo modo, despejar vegetación demasiado cercana a los perímetros que pueda facilitar la ocultación de drones en aproximación, e instalar iluminación y sensores de movimiento que dificulten operaciones nocturnas de aparatos enemigos. Estas medidas pasivas de fortificación aumentarán la resiliencia incluso si un dron logra infiltrarse, mitigando sus posibles daños. Cada instalación debería realizar un estudio de vulnerabilidad física enfocado en amenazas aéreas pequeñas, y ejecutar las mejoras estructurales recomendadas.

Aprovechando la base industrial y académica nacional, se recomienda fomentar proyectos de I+D locales para soluciones antidron innovadoras. Universidades, centros de investigación militar (como CIDES en el Ejército o CIAC en la FAC) y empresas colombianas de tecnología podrían trabajar conjuntamente en el desarrollo de prototipos adaptados: por ejemplo, sistemas acústicos de detección temprana aptos para selva, software de inteligencia artificial entrenado con datos de drones usados en Colombia, o mejoras a drones militares existentes para convertirlos en interceptores.

Además, impulsar concursos o convocatorias (posiblemente con financiación del Ministerio de Ciencia o el Departamento de Prosperidad Digital) para startups que presenten soluciones creativas en este campo. En línea con la política de *transferencia tecnológica*, todo equipo comprado del exterior debe venir acompañado de capacitación técnica y, cuando

sea posible, participación de ingenieros colombianos en su mantenimiento y eventual producción bajo licencia. Esto no solo reducirá costos a largo plazo, sino que aumentará la autonomía tecnológica del país en materia de defensa anti-dron.

Referencias

Alexandra, L. N. S. (2015). Sistema de interferencia de señal celular en dispositivos con tecnología GSM. *Universidad Técnica de Ambato . Facultad de Ingeniería En Sistemas, Electrónica e Industrial*.

Cano, C. (2023). La inteligencia artificial en el pos-acuerdo colombiano: el caso de los drones de combate para operaciones sostenidas contra grupos armados organizados. . *Universidad Externado de Colombia.* https://bdigital.uexternado.edu.co/entities/publication/bcf16cfa-693f-4938-9251-39a1b0fad0a6

Çetin, E., Barrado, C., & Pastor, E. (2021). Improving real-time drone detection for counter-drone systems. *Aeronautical Journal*, *125*(1292). https://doi.org/10.1017/aer.2021.43

Departamento de Seguridad Nacional de los Estados Unidos. (2024). *Dirección de Ciencia y Tecnología. Sistemas antiaéreos no tripulados (C-UAS) [Counter-Unmanned Aircraft Systems (C-UAS)].* https://www.dhs.gov/science-and-technology/counter-unmanned-aircraft-systems-c-uas

Deutsche Welle. (2024). *ELN se atribuye ataque contra una base militar colombiana. DW*. https://www.dw.com/es/eln-se-atribuye-ataque-contra-una-base-militar-colombiana-que-dej%C3%B3-3-muertos-y-26-heridos/a-70288149#:~:text=La%20guerrilla%20del%20Ej%C3%A9rcito%20de,de%20paz%20con%20esa%20agrupaci%C3%B3n.

El País. (2024). Drones que lanzan bombas: la nueva etapa del conflicto colombiano. *El País*. https://elpais.com/america-colombia/2024-06-19/drones-que-lanzan-bombas-la-nueva-etapa-del-conflicto-colombiano.html

Hide, S. (2025). Drone attacks increasingly affect civilians in Colombia's conflict. . *Al Jazeera.* https://latinamericareports.com/drone-attacks-increasingly-affect-civilians-in-colombias-conflict/10839/#:~:text=In%20July%2C%20a%2010,others%20were%20injured%2C%20some%20seriously

Marrone, A. (2022). El nuevo Concepto Estratégico de la OTAN: novedades y prioridades. . *Revista de Pensamiento Estratégico y Seguridad CISDE.* . https://www.centroculturalsol.com/El%20nuevo%20Concepto%20Estrat__gico%20de%20la%20OTAN.pdf

Mazo, G. D. (2024). *Policía Nacional buscará que se regulen los drones en Colombia tras ataques aéreos de grupos armados*. https://www.infobae.com/colombia/2024/07/06/policia-nacional-buscara-que-se-regulen-los-drones-en-colombia-tras-ataques-aereos-de-grupos-armados/#:~:text=El%20general%20William%20Salamanca%2C%20director,Nari%C3%B1o%20y%20Valle%20del%20Cauca.

Ministerio de Defensa Nacional. (2024). Colombia refuerza su seguridad con sistemas avanzados de defensa contra drones para proteger a la comunidad, la fuerza pública y el territorio nacional. . *Ministerio de Defensa Nacional de Colombia.* https://www.mindefensa.gov.co/prensa/noticia-visualizacion/noticias-prensa-colombia-refuerza-su-seguridad

Nomesqui, R. J. (2025). *Comandante del Ejército Nacional expuso detalles de la "guerra tecnológica" que se registra en Colombia*. https://www.infobae.com/colombia/2025/04/24/comandante-del-ejercito-nacional-expuso-detalles-de-la-guerra-tecnologica-que-se-registra-en-el-pais/

NUST. (2024). *NUST College of Electrical & Mechanical Engineering Project thesis: Chapter 1 – Introduction. Rawalpindi, Pakistán: National University of Sciences and Technology (NUST).* file:///C:/Users/USER/Downloads/DesignandDevelopmentofAIBasedAutonomousDrone%20(1).pdf

Patiño. (2024). *Gobierno anuncia la llegada de sistemas avanzados "antidrones" para combatir ataques de grupos ilegales. Colprensa.* https://cambiocolombia.com/conflicto-armado-en-colombia/gobierno-refuerza-seguridad-con-sistemas-avanzados-para-ataques-con

Prensa Latina. (2025). Colombia busca fortalecer seguridad nacional con sistema antidrones. *Prensa Latina*. https://www.prensa-latina.cu/2025/01/08/colombia-busca-fortalecer-seguridad-nacional-con-sistema-antidrones/

Rostec. (2024). *Rostec demonstrates special-purpose gun cartridges for UAV engagement. Research Institute of Applied Chemistry.* https://rostec.ru/en/media/news/rostec-demonstrates-special-purpose-gun-cartridges-for-uav-engagement/#start

Saumeth. (2024a). *El Ejército colombiano está interesado en el sistema antidrones Skylock Dome*. https://www.infodefensa.com/texto-diario/mostrar/4939464/13x-colombia-colombia-interesada-sistema-anti-drones-skylock-dome#:~:text=El%20Skylock%20Dome%20ofrece%20adem%C3%A1s,soluciones%20terrestres%2C%20a%C3%A9reas%20y%20mar%C3%ADtimas

Saumeth, E. (2023). Colombia contrata sistemas de guerra electrónica por 92 millones de dólares. *Infodefensa*. https://www.infodefensa.com/texto-diario/mostrar/4125472/colombia-adquiere-sistemas-guerra-electronica-92-millones-dolares

Saumeth, E. (2024b). Colombia comprará antidrones para proteger a los 12.000 visitantes de la COP 16. . *InfoDefensa.* https://www.infodefensa.com/texto-diario/mostrar/4936193/130-colombia-colombia-comprara-anti-drones-cop-16

Sheu, B. H., Chiu, C. C., Lu, W. T., Huang, C. I., & Chen, W. P. (2019). Development of UAV tracing and coordinate detection method using a dual-axis rotary platform for an anti-UAV system. *Applied Sciences (Switzerland)*, *9*(13). https://doi.org/10.3390/app9132583

Tavera, F. (2024). ¿Cómo han transformado las tecnologías emergentes el panorama de las aeronaves no tripuladas en el ámbito militar y de seguridad nacional? . *Escuela Superior de Guerra "General Rafael Reyes Prieto"*. https://www.esdegrepositorio.edu.co/bitstream/handle/20.500.14205/11253/Ariculo%20de%20Revision%20V3-%20My%20Tavera.pdf?sequence=1

Wuhan. (2024). *La detección de drones por RF utiliza sensores de radiofrecuencia (RF) que escuchan y monitorean de manera pasiva 2.4G 5.8G las frecuencias para las transmisiones de drone*. https://es.made-in-china.com/co_a5250379796602ad/product_RF-Drone-Detection-Uses-Radio-Frequency-RF-Sensors-That-Passively-Listen-and-Monitor-2-4G-5-8g-Frequencies-for-Transmissions-of-Drones_uoynysiogy.html