



ESCUELA DE
POSTGRADOS
DE LA FAC - EPFAC



MAESTRÍA EN
DIRECCIÓN Y GESTIÓN
DE LA SEGURIDAD INTEGRAL



COLADCA
INTERNACIONAL

MEMORIAS – III SIMPOSIO DE
INVESTIGACIÓN
FORMATIVA – MADGSI
14 de mayo de 2026



Aeropuertos y Ciberentornos Seguros:
Modelos de Protección y Competencias para la
Seguridad de la Aviación Civil y de Estado

Directivos

CR. Yerim Andrés Rozo Cepeda
Director Escuela de Postgrados de la FAC
TC. Alberto Moreno Abril
Comandante Grupo Académico
TC. Andrea Esther Villafrades Gómez
Comandante Escuadrón Educación Superior

Editor

Escuela de Posgrados FAC “Capitán José Edmundo Sandoval”
Nit. 899999102-2
Cra 11 No. 102-50
+57(601) 3159816 Extensión 72500
Correspondencia@epfac.edu.co

Comité Organizador

MY. Iván Alonso Flórez Rozo
OD18. David Enrique López Cortés
OD18. Jaquelin Castillo García
OD15. Rosa Margoth Orjuela Rivera
CTO. Siham Natalia Torres Márquez

Diseño

Aldemar Zambrano Torres

Comité Revisor

MY. Iván Alonso Flórez Rozo
OD18. David Enrique López Cortés
OD18. Jaquelin Castillo García
OD15. Rosa Margoth Orjuela Rivera
CTO. Siham Natalia Torres Márquez

Autores

MY. Marco Antonio Abril Morales
MY. César Augusto Álvarez Duque
CT. Marino Gómez Rodríguez
CT. Gabriel Enrique Useche Ramos
CT. Elizabeth Corredor Guerrero
TE. Edgar Darío Pérez Díaz
T2. Javier Palacio Suárez
TJ(RA) Carlos Héctor Quinchía Wilches
TE(RA) John Wilder Parada Guzmán
Isleny López Chaquea

Periodo anual

Sitio web

<https://www.epfac.edu.co/es/eventos-academicos/eventos-academicos-seguridad-integral>

Contáctanos

Cra. 11 No. 102-50 Edificio ESDEGUE, Escuadrón de Investigaciones.

Oficina 411. Bogotá D.C., Colombia. A.A.110111.

Teléfonos (057-1) 637 8927 – 6206518 Ext. 1700, 1719, 1722.

Correo electrónico: admisiones.madgsi@epfac.edu.co

Información Técnica Publicación Producto de Investigación Grupo de investigación en Ciencias Militares Aeronáuticas y Administrativas – GICMA COL0140489.

Tercera Edición, mayo 2026. ISSN 3073-0325 Periodicidad anual, publicación digital Sitio Web:

[https://cdn227724.fac.mil.co/sites/epfac/files/Docs-EPFAC/](https://cdn227724.fac.mil.co/sites/epfac/files/Docs-EPFAC/Memorias%20III%20Simposio%20ISSN%203073-0325%20MADGSI%202026.pdf)

[Memorias%20III%20Simposio%20ISSN%203073-0325%20MADGSI%202026.pdf](https://cdn227724.fac.mil.co/sites/epfac/files/Docs-EPFAC/Memorias%20III%20Simposio%20ISSN%203073-0325%20MADGSI%202026.pdf)

Bogotá, Colombia 2026 ©2026.

Está permitida la reproducción total o parcial de los escritos aquí contenidos para uso personal o con fines académicos e investigativos, siempre y cuando se haga la respectiva cita o referencia a la ponencia, autor(es), y a la publicación de las Memorias en el marco del segundo Simposio de Investigación Formativa, y su impacto en Seguridad Integral en el sector aeronáutico, organizado por la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana. Bogotá, Colombia (Suramérica). En caso de querer reproducir esta obra para otros fines, en cualquiera de sus formatos, deberá contar con el permiso escrito de la entidad editora.

Copyright (c) 2026. Escuela de Postgrados de la Fuerza Aeroespacial Colombiana.

Introducción

La investigación formativa constituye un eje fundamental en la educación posgradual, al promover el desarrollo de competencias analíticas, críticas y propositivas que permiten abordar de manera integral los desafíos contemporáneos de la seguridad. En este contexto, la Maestría en Dirección y Gestión de la Seguridad Integral fomenta espacios académicos orientados a la generación, socialización y fortalecimiento del conocimiento científico, contribuyendo a la formación de profesionales capaces de responder a las dinámicas cambiantes de los entornos organizacionales y estratégicos.

Por ello, el Tercer Simposio de Investigación Formativa: Aeropuertos y ciberentornos seguros: Modelos de protección y competencias para la seguridad de la aviación civil y de Estado, fue el escenario académico en el que los estudiantes de la cohorte VIII presentaron los avances de sus proyectos de investigación. Este encuentro permitió la divulgación de resultados preliminares, el intercambio de experiencias investigativas y la discusión de problemáticas emergentes relacionadas con la seguridad integral, fortaleciendo la calidad y pertinencia de los procesos de investigación desarrollados en el programa.

Así mismo, se propició la interacción entre estudiantes, docentes, expertos invitados y miembros del comité evaluador, quienes aportaron observaciones y recomendaciones orientadas al fortalecimiento metodológico y conceptual de los trabajos de grado. De igual manera, la participación de conferencistas especializados en ciberseguridad seguridad e inteligencia artificial, enriqueció el análisis de los retos actuales que enfrentan las organizaciones y los Estados en materia de protección, prevención y gestión de riesgos aeroportuarios.

Este boletín de investigación tiene como propósito documentar el desarrollo del evento y los avances investigativos socializados, destacando su importancia para la comunidad académica, la producción de conocimiento y la formulación de soluciones innovadoras que contribuyan al fortalecimiento de la seguridad integral en diversos ámbitos de aplicación.

Tercer Simposio de Investigación Formativa MADGSI

Objetivo General

Dar a conocer los resultados de proyectos de investigación de la Maestría en Dirección y Gestión de la Seguridad Integral a la comunidad en general que se desempeña o demuestra interés en el área de seguridad de instalaciones, protección de activos, gestión de riesgos y administración del talento humano.

Objetivos Específicos

1. Presentar a los participantes y evaluadores los avances de los proyectos de investigación de los estudiantes de cuarto semestre de la cohorte VIII, de la Maestría en Dirección y Gestión de la Seguridad Integral.
2. Proponer a los expositores un análisis objetivo y de acciones de mejora con el ánimo de fortalecer su trabajo de grado.
3. Socializar los avances de la investigación del programa de Maestría ante un comité científico y comunidad académica.
4. Fortalecer el proceso de investigación formativa de los estudiantes de la octava cohorte de la Maestría.

Seguridad de la aviación civil como capacidad estratégica aeroespacial

TE (R) John Wilder Parada Guzmán

John Wilder Parada Guzmán: Oficial retirado del Ejército Nacional, con especialización en Administración de la Seguridad de la Universidad Militar Nueva Granada, Maestrando en Dirección y Gestión de la Seguridad Integral de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana. Director de operaciones a nivel nacional de la empresa de seguridad Serviconi Ltda con base en Barranquilla.

Correo electrónico institucional: john.parada@epfac.edu.co

Correo personal: john.parada13@hotmail.com

Línea de investigación: Dirección y Gestión de la Seguridad Integral

Resumen

Esta investigación abordó la transición desde la seguridad aeroportuaria hacia la seguridad de la aviación civil, entendida como la protección de la aviación civil contra actos de interferencia ilícita mediante medidas, procedimientos, recursos humanos y materiales. Este contexto permitió comprender que la aviación civil no se limitó a una actividad comercial o de transporte, sino que constituyó un sistema estratégico para la conectividad, la movilidad, la economía, la gobernabilidad y la seguridad nacional. Desde el Convenio de Chicago ya se había advertido que el uso indebido de la aviación civil podía afectar la seguridad general, y el Anexo 17 consolidó una visión internacional orientada a prevenir interferencias ilícitas contra aeronaves, aeropuertos, pasajeros, tripulaciones, personal en tierra y servicios de navegación aérea (Organización de Aviación Civil Internacional [OACI], 1944, 2022).

El problema específico investigado consistió en la confusión conceptual y doctrinal entre seguridad aeroportuaria y seguridad de la aviación civil. En la práctica institucional y académica ambos términos habían sido empleados como equivalentes, aunque su alcance no fue el mismo. La seguridad aeroportuaria se había relacionado principalmente con controles locales dentro del aeropuerto, tales como vigilancia, inspección, protección de áreas restringidas, control de accesos y aplicación de procedimientos en instalaciones aeroportuarias.

En contraste, la seguridad de la aviación civil tuvo una dimensión más amplia, estatal, normativa, preventiva e interinstitucional, orientada a proteger todo el sistema aeronáutico frente a actos deliberados. Esta ambigüedad redujo la precisión del análisis del riesgo, debilitó la claridad doctrinal y dificultó la formulación de respuestas frente a amenazas que evolucionaron desde la piratería aérea, el secuestro de aeronaves hasta el sabotaje, el terrorismo, el uso de explosivos, las amenazas internas, los drones y los ataques híbridos (Klenka, 2019; OACI, 2022; Pyrgies, 2019).

El objetivo general fue analizar la evolución conceptual, histórica y normativa de la seguridad aeroportuaria hacia la seguridad de la aviación civil, así como sus implicaciones doctrinales para la Fuerza Aeroespacial Colombiana. Para alcanzar este propósito, el estudio revisó la evolución de los actos de interferencia ilícita, diferenció los conceptos centrales del campo AVSEC, examinó la respuesta normativa internacional y colombiana, e identificó los aportes de dicha transición para la protección del espacio aéreo, la defensa de infraestructura crítica, la interoperabilidad institucional, la inteligencia preventiva, la gestión del riesgo y la respuesta frente a amenazas emergentes. El alcance se delimitó a una revisión documental, histórica, normativa y analítica, sin pretender formular un modelo operacional cerrado, sino aportar una lectura doctrinal útil para la seguridad integral del sistema aeronáutico nacional.

La recopilación y análisis de información se realizó mediante instrumentos como una revisión documental que se aplicó bajo un enfoque cualitativo. Se usó una matriz de revisión normativa como el Convenio de Chicago, los convenios de Tokio, La Haya y Montreal, el Anexo 17, el Doc. 8973 y el RAC 160; una ficha de análisis conceptual para comparar seguridad aeroportuaria, seguridad de la aviación civil, seguridad física, AVSEC y actos de interferencia ilícita; una matriz histórico-analítica para ubicar eventos internacionales y colombianos asociados con secuestro, sabotaje, narcoterrorismo, uso de explosivos y amenazas tecnológicas; y una ficha de implicaciones doctrinales para relacionar los hallazgos con la misión de la Fuerza Aeroespacial Colombiana.

Estos instrumentos se utilizaron mediante lectura selectiva, categorización, comparación normativa y análisis de contenido, lo que permitió estudiar cada fuente en su contexto, contrastarla con otras fuentes y construir inferencias doctrinales fundamentadas, de acuerdo con la lógica de la investigación cualitativa y documental (Hernández-Sampieri & Mendoza, 2018).

Los hallazgos evidenciaron que la seguridad de la aviación civil evolucionó desde controles locales centrados en el aeropuerto hacia una política estatal de protección integral del sistema aeronáutico. Se encontró que los actos de interferencia ilícita no fueron estáticos: en una

primera etapa predominaron la piratería aérea y el apoderamiento ilícito de aeronaves; luego aparecieron el sabotaje y los explosivos como medios de alto impacto; posteriormente, los atentados del 11 de septiembre de 2001 demostraron que una aeronave civil podía ser utilizada como arma estratégica; y, en el presente, surgieron riesgos asociados con drones, amenazas internas, ciberamenazas y ataques híbridos.

También se encontró que la respuesta internacional de la organización de aviación civil internacional (OACI) consolidó un marco preventivo mediante el Convenio de Chicago, los convenios especializados, el Anexo 17 y el Doc. 8973, mientras que Colombia incorporó progresivamente dichos estándares por medio de programas nacionales y reglamentos aeronáuticos hasta llegar al RAC 160. Este tránsito fortaleció el tratamiento de la seguridad de la aviación civil, aunque conservó algunos usos funcionales del término seguridad aeroportuaria en contextos regulatorios específicos (OACI, 2023; Unidad Administrativa Especial de Aeronáutica Civil [UAEAC], 2025).

Se concluyó que la diferencia entre seguridad aeroportuaria y seguridad de la aviación civil no fue solo terminológica, sino estratégica. La primera operó como una dimensión de aplicación en el aeropuerto, mientras la segunda representó una responsabilidad estatal amplia para proteger aeronaves, instalaciones, servicios, pasajeros, tripulaciones, personal en tierra y público frente a actos deliberados. Para la Fuerza Aeroespacial Colombiana, estos resultados significarán un aporte doctrinal porque permitirán integrar el AVSEC a una visión ampliada de defensa aeroespacial, alerta temprana, inteligencia, gestión del riesgo e interoperabilidad con Aerocivil, explotadores aeroportuarios, autoridades territoriales y organismos de seguridad. Los hallazgos significaron que la aviación civil debía comprenderse como infraestructura crítica y como componente estratégico de la seguridad nacional.

El impacto de la investigación consistió en fortalecer la comprensión doctrinal del sistema aeronáutico y en generar productos académicos asociados: el capítulo de libro, Seguridad en instalaciones aeronáuticas críticas: un enfoque interdisciplinario – 100 años con la mejor seguridad en tierra, propuesto para los 100 años de la Jefatura de Seguridad y Defensa de la Fuerza Aeroespacial Colombiana, el paper para el Simposio MADGSI y el póster de sustentación fue orientado a divulgar la transición de la seguridad aeroportuaria hacia la seguridad de la aviación civil.

Palabras clave: Actos de interferencia ilícita, AVSEC, drones, gestión del riesgo, seguridad aeroportuaria, seguridad de la aviación civil.

Abstract

This research addressed the transition from airport security to civil aviation security, understood as the protection of civil aviation against acts of unlawful interference through measures, procedures, human resources, and material resources. This context made it possible to understand that civil aviation was not limited to a commercial or transportation activity, but rather constituted a strategic system for connectivity, mobility, the economy, governance, and national security. Since the Chicago Convention, it had already been recognized that the misuse of civil aviation could affect general security, and Annex 17 consolidated an international approach aimed at preventing unlawful interference against aircraft, airports, passengers, crews, ground personnel, and air navigation services (International Civil Aviation Organization [ICAO], 1944, 2022).

The specific problem investigated consisted of the conceptual and doctrinal confusion between airport security and civil aviation security. In institutional and academic practice, both terms had been used as equivalents, although their scope was not the same. Airport security had been mainly associated with local controls within the airport, such as surveillance, screening, protection of restricted areas, access control, and the implementation of procedures in airport facilities. In contrast, civil aviation security had a broader state-level, regulatory, preventive, and interinstitutional dimension, aimed at protecting the entire aeronautical system against deliberate acts. This ambiguity reduced the precision of risk analysis, weakened doctrinal clarity, and hindered the formulation of responses to threats that evolved from air piracy and aircraft hijacking to sabotage, terrorism, the use of explosives, insider threats, drones, and hybrid attacks (Klenka, 2019; ICAO, 2022; Pyrgies, 2019).

The general objective was to analyze the conceptual, historical, and regulatory evolution from airport security to civil aviation security, as well as its doctrinal implications for the Colombian Aerospace Force. To achieve this purpose, the study reviewed the evolution of acts of unlawful interference, differentiated the core concepts of the AVSEC field, examined the international and Colombian regulatory response, and identified the contributions of this transition to the protection of airspace, the defense of critical infrastructure, institutional interoperability, preventive intelligence, risk management, and the response to emerging threats. The scope was limited to a documentary, historical, regulatory, and analytical review, without intending to formulate a closed

operational model, but rather to provide a doctrinal interpretation useful for the comprehensive security of the national aeronautical system.

The collection and analysis of information were carried out through instruments such as a documentary review applied under a qualitative approach. A regulatory review matrix was used, including the Chicago Convention, the Tokyo, Hague, and Montreal Conventions, Annex 17, Doc. 8973, and RAC 160; a conceptual analysis sheet to compare airport security, civil aviation security, physical security, AVSEC, and acts of unlawful interference; a historical-analytical matrix to locate international and Colombian events associated with hijacking, sabotage, narcoterrorism, the use of explosives, and technological threats; and a doctrinal implications sheet to relate the findings to the mission of the Colombian Aerospace Force. These instruments were used through selective reading, categorization, regulatory comparison, and content analysis, which made it possible to study each source in its context, contrast it with other sources, and construct well-founded doctrinal inferences, in accordance with the logic of qualitative and documentary research (Hernández-Sampieri & Mendoza, 2018).

The findings showed that civil aviation security evolved from local controls centered on the airport toward a state policy for the comprehensive protection of the aeronautical system. It was found that acts of unlawful interference were not static: in an initial stage, air piracy and the unlawful seizure of aircraft predominated; later, sabotage and explosives emerged as high-impact means; subsequently, the attacks of September 11, 2001, demonstrated that a civil aircraft could be used as a strategic weapon; and, at present, risks associated with drones, insider threats, cyber threats, and hybrid attacks have emerged. It was also found that the international response of the International Civil Aviation Organization (ICAO) consolidated a preventive framework through the Chicago Convention, specialized conventions, Annex 17, and Doc. 8973, while Colombia progressively incorporated these standards through national programs and aeronautical regulations up to RAC 160. This transition strengthened the treatment of civil aviation security, although it retained some functional uses of the term airport security in specific regulatory contexts (ICAO, 2023; Special Administrative Unit of Civil Aeronautics [UAEAC], 2025).

It was concluded that the difference between airport security and civil aviation security was not merely terminological, but strategic. The former operated as an application dimension within the airport, while the latter represented a broad state responsibility to protect aircraft, facilities, services, passengers, crews, ground personnel, and the public against deliberate acts. For the Colombian Aerospace Force, these results will constitute a doctrinal contribution because they

will make it possible to integrate AVSEC into an expanded vision of aerospace defense, early warning, intelligence, risk management, and interoperability with Aerocivil, airport operators, territorial authorities, and security agencies.

The findings meant that civil aviation should be understood as critical infrastructure and as a strategic component of national security. The impact of the research consisted of strengthening the doctrinal understanding of the aeronautical system and generating associated academic products: the book chapter *Security in Critical Aeronautical Facilities: An Interdisciplinary Approach – 100 Years with the Best Security on the Ground*, proposed for the 100th anniversary of the Security and Defense Directorate of the Colombian Aerospace Force; the paper for the MADGSI Symposium; and the defense poster aimed at disseminating the transition from airport security to civil aviation security.

Keywords: Acts of unlawful interference, airport security, AVSEC, civil aviation security, drones, risk management.

Referencias

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill.

Klenka, M. (2019). Major incidents that shaped aviation security. *Journal of Transportation Security*, 12(1-2), 39-56. <https://doi.org/10.1007/s12198-019-00201-2>

Organización de Aviación Civil Internacional. (1944). Convenio sobre Aviación Civil Internacional (Doc. 7300). OACI.

Organización de Aviación Civil Internacional. (2022). Anexo 17: Seguridad: Protección de la aviación civil internacional contra actos de interferencia ilícita (12.^a ed.). OACI.

Organización de Aviación Civil Internacional. (2023). Manual de seguridad de la aviación (Doc. 8973). OACI.

Pyrgies, J. (2019). The UAVs threat to airport security: Risk analysis and mitigation. *Journal of Airline and Airport Management*, 9(2), 63-96. <https://doi.org/10.3926/jairm.127>

Unidad Administrativa Especial de Aeronáutica Civil. (2025). Seguridad de la aviación civil y facilitación en la aviación civil internacional. Aerocivil.

**Liderazgo de la Autoridad Aeronáutica en la gestión de Seguridad y la
Normatividad de la Aviación Estatal**

MY. César Augusto Álvarez Duque

César Augusto Álvarez Duque: Oficial de la Fuerza Aeroespacial Colombiana con 16 años de experiencia en seguridad y defensa de bases aéreas, con una sólida trayectoria en seguridad y defensa de bases y liderazgo organizacional en los cargos laborados. Profesional en Administración de Empresas de la Universidad Cooperativa de Colombia, con cargo actual Especialista en Análisis de Riesgo, orgánico del Comando Aéreo de Combate No 1. Actualmente es investigador en formación, cursa la Maestría en Dirección y Gestión de la Seguridad Integral de la Escuela de Posgrados de la Fuerza Aeroespacial Colombiana, enfocando su trabajo académico en *la Gobernanza de la Seguridad en la Aviación de Estado Rol Estratégico de la Autoridad Aeronáutica*.

Correo electrónico institucional: cesar.alvarez@fac.mil.co

Correo electrónico institucional: cesar.alvarez@epfac.edu.co

Línea de investigación: Dirección y Gestión de la Seguridad Integral

Resumen

La seguridad de la aviación de Estado en Colombia enfrenta un panorama de amenazas sin precedentes, donde la convergencia de riesgos tradicionales y emergentes exige una transformación en la forma en que se protege la infraestructura crítica aeroportuaria. El problema central que motivó esta investigación es la insuficiente definición y consolidación del rol de la Autoridad Aeronáutica de la Aviación de Estado (AAAES) en materia de seguridad (seguridad física) y su gobernanza dentro del sistema aeronáutico nacional.

A pesar de contar con un sustento normativo, se evidencia una desarticulación entre los sectores civil y militar, una posible falta de estandarización en los programas de seguridad física de las guarniciones de las fuerzas militares con operaciones aéreas y una integración limitada de respuestas ante amenazas híbridas, ciberataques y el actual uso de sistemas aéreos no tripulados (UAS por sus siglas en inglés) hostiles.

Estas debilidades limitan la capacidad institucional para salvaguardar la soberanía y los activos estratégicos frente a actores no estatales y tecnologías disruptivas que comprometen la seguridad nacional. Para abordar este fenómeno, la investigación adoptó una metodología cualitativa fundamentada en la revisión documental exhaustiva y el análisis comparativo. Se examinaron marcos normativos internacionales, como el Anexo 17 de la OACI y el Doc 10108, contrastándolos con la legislación colombiana, específicamente el Decreto 2937 de 2010 y el RACAE 160.

Por otra parte, la recolección de datos se complementó con el estudio de modelos de gobernanza en potencias aéreas como Estados Unidos, Israel y la Unión Europea, lo que permitió identificar brechas y mejores prácticas en la protección de activos aeronáuticos militares. Este enfoque comparativo facilitó la estructuración de recomendaciones estratégicas basadas en la gestión del riesgo y la adaptación tecnológica. Los hallazgos principales revelaron que la seguridad (security) en la aviación de Estado ha pasado de un enfoque de protección física perimetral a una gestión integral que incluye la ciberseguridad y medios tecnológicos.

Se encontró que, aunque Colombia posee una base operativa sólida derivada de su conflicto interno, persiste una fragmentación normativa que genera espacios vacíos en la supervisión de la seguridad de las instalaciones. El análisis de riesgos permitió identificar siete amenazas críticas, destacando los ataques directos a bases, la infiltración interna, el sabotaje y los ataques asimétricos con drones. Asimismo, se evidenció que la adopción de tecnologías como la inteligencia artificial y el análisis predictivo es aún incipiente, lo que frena la capacidad de anticipación ante incidentes de interferencia ilícita sofisticada.

Estos resultados significaron que la Autoridad Aeronáutica de la Aviación de Estado (AAAES), en cabeza de la Fuerza Aeroespacial Colombiana, según decreto 2937 del año 2010, debe trascender su función reguladora tradicional para convertirse en un actor proactivo y preventivo. El fortalecimiento de la seguridad no depende únicamente de la acumulación de normas, sino de una gobernanza eficaz que armonice los estándares de la aviación civil con las necesidades operativas militares.

La investigación sugirió que el éxito de la seguridad (Security) aeronáutica estatal radica en el equilibrio entre la eficiencia operativa de las misiones y el rigor de las medidas de protección. Se requiere, por tanto, una cultura de seguridad institucionalizada que integre la inteligencia militar con la supervisión técnica, garantizando que la infraestructura aeronáutica sea resiliente ante un entorno global cada vez más interconectado y volátil.

El impacto de esta investigación radica en proporcionar una hoja de ruta estratégica para que la Fuerza Aeroespacial Colombiana lidere la modernización de la seguridad aeronáutica

estatal en la región. Los productos asociados incluyen una propuesta de seguir actualizando el RACAE 160 según contextos tanto nacionales como regionales y mundiales, circulares regulatorias, así como el diseño de metodologías de evaluación de riesgos multicapadas y alineadas con estándares globales de la OACI.

Palabras clave: Aeródromo, Amenazas, UAS, Reglamento, Seguridad.

Abstract

State aviation security in Colombia faces an unprecedented threat landscape, where the convergence of traditional and emerging risks demands a transformation in how critical airport infrastructure is protected. The central issue that prompted this research is the insufficient definition and consolidation of the role of the State Aviation Authority (AAAES) in matters of security (physical security) and its governance within the national aviation system.

Despite having a regulatory framework, there is evidence of a disconnect between the civil and military sectors, a potential lack of standardization in the physical security programs of military garrisons with air operations, and limited integration of responses to hybrid threats, cyberattacks, and the current use of hostile unmanned aerial systems (UAS).

These weaknesses limit the institutional capacity to safeguard sovereignty and strategic assets against non-state actors and disruptive technologies that threaten national security. To address this phenomenon, the research adopted a qualitative methodology based on an exhaustive literature review and comparative analysis. International regulatory frameworks, such as ICAO Annex 17 and Doc 10108, were examined and compared with Colombian legislation, specifically Decree 2937 of 2010 and RACAE 160.

Furthermore, data collection was complemented by a study of governance models in aviation powers such as the United States, Israel, and the European Union, which allowed for the identification of gaps and best practices in the protection of military aviation assets. This comparative approach facilitated the formulation of strategic recommendations based on risk management and technological adaptation. The main findings revealed that security in state aviation has shifted from a perimeter physical protection approach to a comprehensive management approach that includes cybersecurity and technological means.

The study found that, although Colombia has a solid operational foundation stemming from its internal conflict, regulatory fragmentation persists, creating gaps in the oversight of facility security. The risk analysis identified seven critical threats, highlighting direct attacks on bases, internal infiltration, sabotage, and asymmetric attacks using drones. Furthermore, it was evident that the adoption of technologies such as artificial intelligence and predictive analytics is still in its infancy, which hinders the ability to anticipate incidents of sophisticated unlawful interference.

These findings meant that the State Aviation Authority (AAAES), under the leadership of the Colombian Aerospace Force, pursuant to Decree 2937 of 2010, must move beyond its traditional regulatory role to become a proactive and preventive actor. Strengthening security depends not only on the accumulation of regulations but also on effective governance that harmonizes civil aviation standards with military operational needs.

The research suggested that the success of state aviation security lies in striking a balance between the operational efficiency of missions and the rigor of protective measures. An institutionalized safety culture is therefore required, one that integrates military intelligence with technical oversight, ensuring that aviation infrastructure remains resilient in an increasingly interconnected and volatile global environment.

The impact of this research lies in providing a strategic roadmap for the Colombian Aerospace Force to lead the modernization of state aviation security in the region. Related outputs include a proposal to continue updating RACAE 160 in accordance with national, regional, and global contexts and regulatory circulars, as well as the design of multi-layered risk assessment methodologies aligned with global ICAO standards.

Keywords: Aerodrome, Threats, UAS, Regulations, Safety.

Referencias

Aeronáutica Civil de Colombia. (2022). Reglamento Aeronáutico Colombiano - RAC 160 Programa Nacional de Seguridad de la Aviación Civil.

Alemanno, A. (2018). *The governance of disasters and risk regulation in aviation security*.

Fuerza Aeroespacial Colombiana. (2020). *Reglamento Aeronáutico Colombiano de Aviación de Estado RACAE 160 SEGURIDAD Y DEFENSA DE LA AVIACIÓN DE ESTADO*. Diario Oficial No. 51.461.

International Air Transport Association (IATA). (2021). *Aviation Cybersecurity Guidance Material*.

Organización de Aviación Civil Internacional (OACI). (2022). *Anexo 17 al convenio sobre Aviación Civil Internacional, Seguridad de la aviación*.

Pardo Posada. (2021). *Metodologías de análisis de riesgo en la aviación*.

Presidencia de la República de Colombia. (2010). *Decreto 2937 de 2010*.

Thomas, A. R. (2019). *Aviation Security Management*.

Educación en seguridad de la aviación de Estado para la protección de bases aéreas

CT. Marino Gómez Rodríguez

Marino Gómez Rodríguez: Oficial de la Fuerza Aeroespacial Colombiana, con 13 años de servicio en la Institución y perteneciente a la especialidad de Defensa de Bases. Administrador de Empresas de la Universidad Militar Nueva Granada y candidato a Magíster en Dirección y Gestión de la Seguridad Integral de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana, actualmente se desempeña como Jefe de la Sección Táctica de Gestión Humana y Administrativa del Escuadrón de Seguridad y Defensa de Bases N° 205, orgánico del Grupo Aéreo del Oriente (GAORI). Su experiencia profesional se ha orientado al liderazgo, administración del talento humano, gestión operativa y fortalecimiento de capacidades relacionadas con la protección de instalaciones, personal y activos estratégicos de la Fuerza Aeroespacial Colombiana.

Correo electrónico institucional: marino.gomez@fac.mil.co

Correo electrónico académico: marino.gomez@epfac.edu.co

Línea de investigación: Dirección y Gestión de la Seguridad Integral

Resumen

La protección de bases aéreas constituye una condición esencial para preservar el poder aeroespacial, asegurar la continuidad operacional y proteger el componente humano, las aeronaves, la infraestructura crítica y la información asociada a la aviación de Estado. El problema específico que orientó el estudio de la investigación fue la posible brecha entre la formación recibida por el personal de Seguridad y Defensa de Bases de la Fuerza Aeroespacial Colombiana y las exigencias normativas, doctrinales y operacionales propias de la seguridad de la aviación de Estado. Aunque la Institución cuenta con un marco regulatorio y educativo relevante, soportado en el Decreto 2937 de 2010, el RACAE 160 y referentes internacionales como el Anexo 17 de la OACI, se identificó que la existencia de normas, manuales y programas no garantizaba por sí sola su apropiación práctica ni su traducción en capacidad real de protección (Organización de Aviación Civil Internacional, 2017; Presidencia de la República de Colombia, 2010; Fuerza Aérea Colombiana, 2020). En ese sentido, el estudio plantea la educación no como un requisito administrativo, sino como una capacidad estratégica orientada a convertir la doctrina, la

regulación y los procedimientos en criterio profesional, cultura de seguridad y respuesta operacional.

La investigación se desarrolló desde un enfoque mixto con predominio cualitativo, de alcance analítico, descriptivo y propositivo. La recolección de datos combinó revisión documental de normas, doctrina, programas académicos y literatura especializada; análisis de los procesos de formación de oficiales y suboficiales; encuesta digital aplicada a personal de la especialidad; entrevista semiestructurada orientada al ámbito académico de la Escuela de Suboficiales; y observación participante derivada de la experiencia institucional en Seguridad y Defensa de Bases. La población de referencia correspondió a oficiales y suboficiales de la especialidad. El análisis se organizó alrededor de tres ejes: educación y doctrina, programas y estrategias de formación, y lineamientos para fortalecer la relación entre formación y cumplimiento normativo.

Los hallazgos demostraron que la dificultad principal no se encontraba en una ausencia absoluta en la formación, sino en su nivel de alineación con la realidad operacional. En los datos disponibles, el 100 % de los encuestados valoró en nivel alto o muy alto la necesidad de fortalecer los programas de formación en seguridad de la aviación de Estado. Al mismo tiempo, las variables con menor valoración promedio estuvieron relacionadas con la inclusión de normativa nacional e internacional, el conocimiento adecuado del RACAE 160, la disponibilidad de recursos y materiales didácticos, el entrenamiento mediante simulacros o ejercicios tácticos y la actualización doctrinal de los programas.

En contraste, se observaron fortalezas en la percepción sobre el dominio de los instructores, la cultura de seguridad en las unidades, la pertinencia de la formación para las funciones del personal y la influencia directa de la formación en el cumplimiento de los procedimientos. Estos resultados sugirieron que la formación existente fue reconocida como útil, pero aún demanda mayor profundidad normativa, actualización recurrente, escenarios prácticos, recursos de apoyo y conexión con amenazas emergentes.

La entrevista semiestructurada permitió profundizar esta interpretación. Desde la perspectiva académica consultada, el RACAE 160 sí fue abordado en los procesos formativos, pero no siempre con la profundidad práctica necesaria para que el personal lo incorporara plenamente en su desempeño diario. También se identificó una brecha parcial entre lo enseñado en las escuelas y lo exigido por la práctica en una base aérea, especialmente en gestión de crisis, liderazgo bajo presión, ciberseguridad aplicada, drones hostiles, análisis de amenazas, uso de tecnologías, evaluación por competencias y simulaciones complejas.

Esta evidencia coincidió con los planteamientos de la doctrina de protección de la fuerza, según la cual la supervivencia y efectividad del personal, los recursos y la infraestructura

dependen de la preparación integral frente al entorno de amenaza (United States Air Force, 2023). Asimismo, en concordancia con estudios sobre defensa de bases aéreas, los cuales advierten que la vulnerabilidad de una base afecta la generación de poder aéreo y su protección exige organización, previsión, entrenamiento especializado y coordinación interinstitucional (Vick et al., 2020).

Estos hallazgos permitieron establecer que la educación en seguridad de la aviación de Estado debía comprenderse como un puente entre la norma y la operación. Desde las teorías del aprendizaje, se interpretó que el conocimiento adquiría valor institucional cuando se relacionaba con experiencias previas, se aplicaba en escenarios reales o simulados y fortalecía la capacidad de actuar con criterio en situaciones de incertidumbre (Díaz Barriga & Hernández, 2002; Schunk, 2012).

Por tanto, una formación centrada únicamente en la exposición normativa resultaba insuficiente frente a amenazas dinámicas. La seguridad de bases aéreas demanda un modelo educativo más aplicado, con simulaciones, análisis de casos, entrenamiento recurrente, actualización anual de contenidos críticos, articulación entre escuelas y unidades operativas, y evaluación de competencias observables.

El impacto de la investigación radicó en haber aportado una lectura estratégica sobre la educación en seguridad de aviación de Estado como condición necesaria para fortalecer la protección de bases aéreas, la continuidad de las operaciones y la preservación del poder aeroespacial de la Fuerza Aeroespacial Colombiana. Sus hallazgos permitieron comprender que formar al personal de Seguridad y Defensa de Bases no es únicamente un asunto académico, sino una decisión institucional orientada a convertir la norma, la doctrina y la experiencia operacional en capacidad real de protección.

Como producto asociado, se desarrolló el capítulo de libro **“Formar para defender: La educación en seguridad de aviación de Estado como eje de la protección de bases aéreas”**, en el cual se profundizó esta discusión desde una mirada más amplia, integrando fundamentos doctrinales, educativos, normativos y operacionales. Dicho capítulo invita al lector a comprender por qué la defensa de una base aérea no depende solo de medios físicos o procedimientos escritos, sino de la preparación del talento humano encargado de interpretar amenazas, actuar con criterio y sostener la misión en escenarios cada vez más complejos.

Palabras clave: Aviación de Estado, bases aéreas, doctrina militar, educación militar, protección, seguridad.

Abstract

The protection of air bases constitutes an essential condition for preserving aerospace power, ensuring operational continuity, and safeguarding personnel, aircraft, critical infrastructure, and information associated with State aviation. The specific problem that guided the research study was the possible gap between the training received by Air Base Security and Defense personnel of the Colombian Aerospace Force and the regulatory, doctrinal, and operational requirements of State aviation security. Although the Institution has a relevant regulatory and educational framework, supported by Decree 2937 of 2010, RACAE 160, and international references such as ICAO Annex 17, the study identified that the existence of regulations, manuals, and programs did not, by itself, guarantee their practical appropriation or their translation into real protection capability (Organización de Aviación Civil Internacional, 2017; Presidencia de la República de Colombia, 2010; Fuerza Aérea Colombiana, 2020). In this regard, the study presents education not as an administrative requirement, but as a strategic capability aimed at transforming doctrine, regulation, and procedures into professional judgment, security culture, and operational response.

The research was developed through a mixed approach with qualitative predominance and an analytical, descriptive, and propositional scope. Data collection combined documentary review of regulations, doctrine, academic programs, and specialized literature; analysis of officer and non-commissioned officer training processes; a digital survey applied to personnel of the specialty; a semi-structured interview focused on the academic field of the Non-Commissioned Officers School; and participant observation derived from institutional experience in Air Base Security and Defense. The reference population corresponded to officers and non-commissioned officers of the specialty. The analysis was organized around three axes: education and doctrine, training programs and strategies, and guidelines to strengthen the relationship between training and regulatory compliance.

The findings showed that the main difficulty was not an absolute absence of training, but rather its level of alignment with operational reality. In the available data, 100% of respondents rated the need to strengthen State aviation security training programs as high or very high. At the same time, the variables with the lowest average ratings were related to the inclusion of national and international regulations, adequate knowledge of RACAE 160, availability of didactic resources and materials, training through drills or tactical exercises, and doctrinal updating of programs. In contrast, strengths were observed in the perception of instructor expertise, security culture within units, the relevance of training for personnel duties, and the direct influence of training on compliance with procedures. These results suggested that existing training was

recognized as useful, but still required greater regulatory depth, recurring updates, practical scenarios, support resources, and connection with emerging threats.

The semi-structured interview allowed this interpretation to be deepened. From the academic perspective consulted, RACAE 160 was addressed in training processes, but not always with the practical depth needed for personnel to fully incorporate it into their daily performance. A partial gap was also identified between what was taught in schools and what was required in practice at an air base, especially in crisis management, leadership under pressure, applied cybersecurity, hostile drones, threat analysis, use of technologies, competency-based assessment, and complex simulations. This evidence was consistent with force protection doctrine, according to which the survival and effectiveness of personnel, resources, and infrastructure depend on comprehensive preparation for the threat environment (United States Air Force, 2023). It was also consistent with studies on air base defense, which warn that the vulnerability of an air base affects the generation of airpower and that its protection requires organization, foresight, specialized training, and interinstitutional coordination (Vick et al., 2020).

These findings made it possible to establish that education in State aviation security should be understood as a bridge between regulation and operation. From learning theories, the study interpreted that knowledge acquires institutional value when it is connected to previous experience, applied in real or simulated scenarios, and used to strengthen the ability to act with judgment in situations of uncertainty (Díaz Barriga & Hernández, 2002; Schunk, 2012). Therefore, training focused only on regulatory exposition proved insufficient in the face of dynamic threats. Air base security demands a more applied educational model, with simulations, case analysis, recurring training, annual updating of critical content, articulation between schools and operational units, and assessment of observable competencies.

The impact of the research lay in having provided a strategic interpretation of State aviation security education as a necessary condition to strengthen air base protection, operational continuity, and the preservation of the aerospace power of the Colombian Aerospace Force. Its findings made it possible to understand that training Air Base Security and Defense personnel is not only an academic matter, but an institutional decision aimed at transforming regulation, doctrine, and operational experience into real protection capability. As an associated product, the book chapter **“Training to Defend: State Aviation Security Education as an Axis for Air Base Protection”** was developed, deepening this discussion from a broader perspective by integrating doctrinal, educational, regulatory, and operational foundations. This chapter invites readers to understand why the defense of an air base does not depend solely on physical means or written

procedures, but on the preparation of personnel responsible for interpreting threats, acting with judgment, and sustaining the mission in increasingly complex scenarios.

Keywords: State aviation, air bases, military doctrine, military education, protection, security.

Referencias

Díaz Barriga Arceo, F., & Hernández Rojas, G. (2002). *Estrategias docentes para un aprendizaje significativo: Una interpretación constructivista*. McGraw-Hill.

Fuerza Aérea Colombiana. (2020). *RACAE 160: Seguridad y defensa de la aviación de Estado*. Autoridad Aeronáutica de Aviación de Estado.

Organización de Aviación Civil Internacional. (2017). *Anexo 17 al Convenio sobre Aviación Civil Internacional: Seguridad. Protección de la aviación civil internacional contra los actos de interferencia ilícita* (10.^a ed.). OACI.

Presidencia de la República de Colombia. (2010, 5 de agosto). *Decreto 2937 de 2010. Por el cual se designa a la Fuerza Aérea Colombiana como autoridad aeronáutica de la aviación de Estado y ente coordinador ante la autoridad aeronáutica civil colombiana*.

Schunk, D. H. (2012). *Teorías del aprendizaje: Una perspectiva educativa* (6.^a ed.). Pearson Educación.

United States Air Force. (2023). *Air Force Doctrine Publication 3-10: Force Protection*. Department of the Air Force.

Vick, A. J., Zeigler, S. M., Brackup, J., & Meyers, J. S. (2020). *Air base defense: Rethinking Army and Air Force roles and functions*. RAND Corporation.

La Seguridad en la Aviación de Estado y sus Capacidades Operacionales

Técnico Segundo Javier Palacio Suárez

Javier Palacio Suárez: Suboficial de la Fuerza Aeroespacial Colombiana, Administrador de Empresas del Politécnico Grancolombiano, Tecnólogo en Talento Humano del Servicio Nacional de Aprendizaje (SENA), Especialista Tecnológico en Administración de Operaciones para la Seguridad Aeroportuaria de la Escuela de Suboficiales de la Fuerza Aeroespacial Colombiana (ESUFA). Maestrando de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana (EPFAC) en el programa de Dirección y Gestión de la Seguridad Integral, Su formación académica y profesional se encuentra orientada a la gestión organizacional, administración del talento humano y dirección de operaciones de seguridad.

Actualmente se desempeña como Suboficial Técnico Comandante de Escuadra Control de Acceso en el Comando Aéreo de Transporte Militar (CATAM), liderando procesos relacionados con la seguridad física, supervisión de personal y control de ingreso a instalaciones militares. Su experiencia integra la ejecución de procedimientos operacionales, coordinación de recursos humanos y aplicación de protocolos de seguridad institucional, contribuyendo al fortalecimiento de la disciplina, la eficiencia operativa y la protección de activos vitales e infraestructura crítica.

Se destaca por su liderazgo, compromiso institucional y capacidad para la toma de decisiones en entornos de alta exigencia, articulando conocimientos administrativos con competencias estratégicas, tácticas y operacionales, orientadas a la mejora continua en la seguridad aeroportuaria de las unidades militares.

Correo electrónico institucional: Javier.palacio@fac.mil.co

Correo electrónico institucional: jajoparo27@gmail.com

Línea de investigación: Modelos de Seguridad Integral

Resumen

La seguridad en la aviación de Estado representó un componente estratégico de la seguridad nacional, debido a su función en la protección de misiones gubernamentales, infraestructuras críticas y el core business institucional. En este sentido, la Organización de

Aviación Civil Internacional (OACI, 2017) estableció que la seguridad aeronáutica constituyó un elemento esencial para proteger las operaciones aéreas frente a actos de interferencia ilícita. No obstante, el problema central que abordó la investigación radicó en la aplicación insuficiente de modelos de seguridad diseñados para la aviación civil, los cuales no respondieron adecuadamente a las particularidades operacionales, estratégicas y de riesgos propios de la aviación estatal. Esta situación generó brechas en la gestión de amenazas, en la formulación de estrategias especializadas y en el desarrollo de capacidades operacionales necesarias para enfrentar escenarios complejos y dinámicos. De acuerdo con Carrasquilla (2021), las capacidades distintivas de la Fuerza Aérea Colombiana constituyeron elementos fundamentales para fortalecer la disuasión estratégica y la protección de los intereses nacionales.

La investigación tuvo como objetivo analizar la seguridad en la aviación de Estado a partir de sus capacidades operacionales, identificando sus componentes distintivos, las amenazas emergentes y las principales vulnerabilidades que afectaron su eficacia. El alcance del estudio se centró en la revisión y análisis de marcos normativos, doctrinales y operativos, así como en la evaluación de riesgos en el contexto de la aviación estatal, considerando su relación directa con la soberanía, la defensa y la continuidad del Estado. Según la OACI (2023a), los sistemas modernos de seguridad aeronáutica debieron adoptar enfoques basados en gestión del riesgo para responder eficazmente a amenazas emergentes y escenarios de alta complejidad.

Para la recolección de información se empleó una metodología cualitativa basada en el análisis documental y la consulta a expertos a través de cuestionarios. En primer lugar, se realizó una revisión de fuentes normativas internacionales, tales como los lineamientos de la Organización de Aviación Civil Internacional (OACI), junto con regulaciones nacionales y doctrinas institucionales del sector defensa. En segundo lugar, se aplicó la técnica de entrevistas a especialistas en seguridad de la aviación de Estado, lo cual permitió obtener información precisa sobre capacidades, amenazas y debilidades del sistema.

Finalmente, se utilizó una matriz de riesgo como herramienta de análisis para clasificar las amenazas en función de su probabilidad e impacto, lo que facilitó la priorización de acciones estratégicas. En relación con ello, Peñaloza Cabanzo (2021) destacó que la gestión del riesgo cibernético en plataformas de comando y control constituyó un factor determinante para garantizar la seguridad de las operaciones aéreas estatales.

Los resultados evidenciaron que la seguridad en la aviación de Estado requirió capacidades operacionales propias y diferenciadas, que superaron los enfoques tradicionales de la seguridad aeronáutica. Entre las principales capacidades identificadas se encontraron la inteligencia y contrainteligencia aérea, el comando y control, la gestión del riesgo estratégico, la seguridad física especializada, la capacidad de búsqueda y salvamento, y la ciberseguridad aeronáutica. Estas capacidades no operaron de forma aislada, sino que conformaron un sistema integrado orientado a la anticipación, prevención y respuesta frente a amenazas complejas. De igual forma, la Fuerza Aérea Colombiana (2018), mediante el Reglamento Aeronáutico Colombiano de la Aviación de Estado (RACAE 160), estableció la necesidad de implementar medidas específicas de protección y control para las operaciones estatales.

De igual manera, los hallazgos mostraron que el entorno de amenazas evolucionó hacia escenarios híbridos, en los cuales convergieron riesgos físicos, tecnológicos y ciberespaciales. Se identificaron como amenazas prioritarias los actos de sabotaje, el terrorismo, las amenazas internas asociadas al factor humano, el uso malicioso de drones y los ciberataques contra sistemas críticos. Estas amenazas adquirieron mayor relevancia en la aviación de Estado debido a la naturaleza estratégica de sus operaciones, lo que incrementó su impacto potencial sobre la seguridad nacional. La OACI (2023c) señaló que las amenazas contemporáneas exigieron capacidades integradas de prevención, detección y respuesta frente a incidentes de seguridad aeronáutica.

En cuanto a las vulnerabilidades, se evidenciaron debilidades en tres dimensiones principales. En el ámbito normativo, se observó una dependencia de marcos diseñados para la aviación civil, lo que generó vacíos en su aplicación al contexto estatal. En el ámbito tecnológico, se identificaron limitaciones frente a la rápida evolución de las amenazas cibernéticas. En el ámbito organizacional, persistieron fallas en la coordinación interinstitucional y en la gestión del talento humano, lo que pudo afectar la eficacia de la respuesta ante incidentes de seguridad.

Los resultados obtenidos a partir de las entrevistas a expertos confirmaron que la seguridad en la aviación de Estado debía concebirse como un sistema estratégico basado en capacidades, y no únicamente como un conjunto de medidas operativas. Existió consenso en que dichas capacidades debieron desarrollarse de manera integral, articulando inteligencia, tecnología, doctrina y gestión del riesgo. Así mismo, se identificó una brecha entre el nivel de amenaza existente y el grado de preparación institucional, especialmente en el ámbito de la

ciberseguridad aeronáutica. En concordancia con ello, la OACI (2023a) enfatizó la importancia de fortalecer la resiliencia institucional mediante modelos preventivos y adaptativos.

Estos hallazgos permitieron concluir que la seguridad en la aviación de Estado debía evolucionar hacia un modelo preventivo, sistémico y adaptable, capaz de enfrentar amenazas multidimensionales en un entorno de alta incertidumbre. La gestión del riesgo se consolidó como un elemento transversal para la toma de decisiones estratégicas, permitiendo priorizar amenazas, optimizar recursos y fortalecer la resiliencia institucional. En este contexto, resultó fundamental fortalecer la articulación entre los marcos normativos, doctrinales y operativos, así como promover la innovación tecnológica y la capacitación especializada del talento humano.

En consecuencia, la seguridad en la aviación de Estado no solo se constituyó como una función operativa, sino también como una capacidad estratégica que contribuyó directamente a la protección de la soberanía y la estabilidad del Estado. El desarrollo de capacidades operacionales propias permitió garantizar la continuidad de las misiones estatales y enfrentar de manera efectiva los desafíos emergentes del entorno de seguridad contemporáneo.

Finalmente, la investigación tuvo como impacto el fortalecimiento del enfoque estratégico de la seguridad en la aviación de Estado, lo cual contribuyó a la mejora en la toma de decisiones y en la formulación de políticas de seguridad aeronáutica. Como producto del estudio, se desarrolló una matriz de riesgo comparativa, un análisis integral de capacidades operacionales, orientadas a fortalecer la seguridad en la aviación de Estado.

Adicionalmente, como producto derivado del proceso investigativo, se elaboró un capítulo de libro, destacando las “Capacidades Operacionales de la Seguridad de Aviación de Estado”, el cual fue incorporado en una obra académica conmemorativa de los cien años de la especialidad de seguridad y defensa de bases de la Fuerza Aeroespacial Colombiana. Este aporte permitió consolidar la relación entre la producción científica, la generación de conocimiento especializado y el fortalecimiento institucional del sector aeronáutico y de defensa.

Palabras clave: aviación de Estado, capacidades operacionales, ciberseguridad aeronáutica, gestión del riesgo, inteligencia estratégica.

Abstract

State aviation security represented a strategic component of national security due to its role in protecting governmental missions, critical infrastructure, and the institutional core business. In this regard, the International Civil Aviation Organization (ICAO, 2017) established that aviation security constituted an essential element in protecting air operations against acts of unlawful interference. Nevertheless, the central issue addressed by the research lay in the insufficient application of security models designed for civil aviation, which failed to adequately respond to the operational, strategic, and risk-related particularities inherent to state aviation. This situation generated gaps in threat management, in the formulation of specialized strategies, and in the development of operational capabilities necessary to address complex and dynamic scenarios. According to Carrasquilla (2021), the distinctive capabilities of the Colombian Air Force constituted fundamental elements for strengthening strategic deterrence and the protection of national interests.

The research aimed to analyze state aviation security through its operational capabilities by identifying its distinctive components, emerging threats, and the main vulnerabilities that affected its effectiveness. The scope of the study focused on the review and analysis of normative, doctrinal, and operational frameworks, as well as on risk assessment within the context of state aviation, considering its direct relationship with sovereignty, defense, and state continuity. According to ICAO (2023a), modern aviation security systems were required to adopt risk-management-based approaches in order to respond effectively to emerging threats and highly complex scenarios.

For data collection, a qualitative methodology based on documentary analysis and expert consultation through questionnaires was employed. First, a review of international regulatory sources was conducted, including the guidelines issued by the International Civil Aviation Organization (ICAO), together with national regulations and institutional doctrines from the defense sector. Second, interviews were conducted with specialists in state aviation security, which made it possible to obtain precise information regarding capabilities, threats, and weaknesses within the system. Finally, a risk matrix was used as an analytical tool to classify threats according to their probability and impact, thereby facilitating the prioritization of strategic actions. In this regard, Peñaloza Cabanzo (2021) emphasized that cyber risk management within command and control platforms constituted a determining factor in guaranteeing the security of state air operations.

The results demonstrated that state aviation security required its own differentiated operational capabilities that surpassed traditional aviation security approaches. Among the main capabilities identified were air intelligence and counterintelligence, command and control, strategic risk management, specialized physical security, search and rescue capability, and aviation cybersecurity. These capabilities did not operate independently; rather, they formed an integrated system aimed at anticipating, preventing, and responding to complex threats. Likewise, the Colombian Air Force (2018), through the Colombian State Aviation Regulation (RACAE 160), established the need to implement specific protection and control measures for state operations.

Similarly, the findings showed that the threat environment evolved toward hybrid scenarios in which physical, technological, and cyberspace-related risks converged. Sabotage, terrorism, insider threats associated with the human factor, malicious use of drones, and cyberattacks against critical systems were identified as priority threats. These threats gained greater relevance in state aviation due to the strategic nature of its operations, which increased their potential impact on national security. ICAO (2023c) indicated that contemporary threats required integrated prevention, detection, and response capabilities against aviation security incidents.

Regarding vulnerabilities, weaknesses were identified in three main dimensions. In the normative sphere, dependence on frameworks designed for civil aviation was observed, which generated gaps in their application to the state context. In the technological sphere, limitations were identified in addressing the rapid evolution of cyber threats. In the organizational sphere, failures persisted in interinstitutional coordination and human talent management, which could affect the effectiveness of responses to security incidents.

The results obtained from expert interviews confirmed that state aviation security had to be conceived as a strategic capability-based system rather than merely as a set of operational measures. There was consensus that such capabilities had to be developed comprehensively by integrating intelligence, technology, doctrine, and risk management. Likewise, a gap was identified between the existing threat level and the degree of institutional preparedness, particularly in the field of aviation cybersecurity. In line with this, ICAO (2023a) emphasized the importance of strengthening institutional resilience through preventive and adaptive models.

These findings led to the conclusion that state aviation security had to evolve toward a preventive, systemic, and adaptable model capable of addressing multidimensional threats in a highly uncertain environment. Risk management became consolidated as a cross-cutting element for strategic decision-making, enabling threat prioritization, resource optimization, and the

strengthening of institutional resilience. In this context, it became essential to strengthen the articulation among normative, doctrinal, and operational frameworks, as well as to promote technological innovation and specialized training of human talent.

Consequently, state aviation security not only constituted an operational function but also a strategic capability that directly contributed to the protection of sovereignty and state stability. The development of operational capabilities of its own made it possible to guarantee the continuity of state missions and to effectively address emerging challenges within the contemporary security environment.

Finally, the research had an impact on strengthening the strategic approach to state aviation security, which contributed to improving decision-making processes and the formulation of aviation security policies. As products of the study, a comparative risk matrix, a comprehensive analysis of operational capabilities, and strategic guidelines aimed at strengthening state aviation security were developed.

Additionally, as a complementary product derived from the research process, a book chapter focused on the “Operational Capabilities of State Aviation Security” was prepared and incorporated into an academic commemorative publication marking the one hundredth anniversary of the security and base defense specialty of the Colombian Aerospace Force. This contribution strengthened the relationship between scientific production, specialized knowledge generation, and the institutional development of the aviation and defense sector.

Keywords: aviation cybersecurity, aviation security, operational capabilities, risk management, state aviation, strategic intelligence.

Referencias

Carrasquilla, P. A. (2021). Capacidades distintivas de la Fuerza Aérea Colombiana como elementos de disuasión en el marco de cooperación con la OTAN. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, 16(1), 49–76. <https://doi.org/10.18359/ries.5255>

Fuerza Aérea Colombiana. (2018). Reglamento Aeronáutico Colombiano de la Aviación de Estado (RACAE 160). Fuerza Aérea Colombiana. https://aaaes.fac.mil.co/sites/aaaes/files/AAAES/documentos/racae_2017.pdf

Organización de Aviación Civil Internacional. (2017). Anexo 17: Seguridad de la aviación. Organización de Aviación Civil Internacional. https://www.dgac.gob.bo/wp-content/uploads/2018/05/Anexo_17.pdf

Organización de Aviación Civil Internacional. (2023a). Global Aviation Security Plan (GASeP). Organización de Aviación Civil Internacional. <https://www.icao.int/Security/GASeP/Pages/default.aspx>

Organización de Aviación Civil Internacional. (2023c). Manual de seguridad de la aviación (Doc 8973). Organización de Aviación Civil Internacional.

Peñaloza Cabanzo, J. (2021). Gestión del riesgo cibernético para la plataforma de Sistema Integrado de Comando y Control de la Aviación del Ejército (SICCA) [Trabajo de grado, Escuela Superior de Guerra]. Repositorio Institucional ESG. <https://www.esdegrepositorio.edu.co/handle/20.500.14205/11073>

Rol de la Fuerza Aeroespacial Colombiana ante interferencia ilícita en pistas compartidas

CT. Elizabeth Corredor Guerrero

CT. Elizabeth Corredor Guerrero: Oficial de la Fuerza Aeroespacial Colombiana, Administradora Aeronáutica, con Diplomado Dirección y Gestión de la Seguridad Integral, candidata a Magister en Dirección y Gestión de la Seguridad Integral de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana. Actualmente se desempeña como comandante Escuadrón Control Táctico y Medios Electrónicos del Grupo de Seguridad y Defensa de Bases Aéreas No. 15. Cuenta con 10 años de experiencia institucional ejerciendo en la especialidad de Defensa de Bases.

Correo electrónico institucional: elizabeth.corredor@fac.mil.co

Correo electrónico institucional: elicorredor1795@hotmail.co

Línea de investigación: Dirección y Gestión de la Seguridad Integral

Resumen

La seguridad de la aviación civil frente a actos de interferencia ilícita constituye un asunto estratégico para Colombia, especialmente en pistas donde concurren operaciones civiles y de la aviación de Estado. En los escenarios conocidos como pistas compartidas, la presencia simultánea de autoridades civiles, operadores aeroportuarios, Fuerza Pública y unidades militares genera una dinámica operacional compleja que exige mecanismos robustos de coordinación, claridad de responsabilidades y capacidades de respuesta articuladas. El problema específico que orientó este análisis radicó en que, aunque el marco normativo nacional e internacional establece lineamientos para prevenir y responder ante actos de interferencia ilícita, persisten desafíos estructurales en la interoperabilidad institucional, la actualización de procedimientos, el entrenamiento conjunto y la ejecución táctica en campo (Unidad Administrativa Especial de Aeronáutica Civil, 2025).

Los actos de interferencia ilícita comprenden amenazas deliberadas contra la aviación, como lo es el apoderamiento ilícito de aeronaves, sabotaje, intrusión en áreas restringidas, introducción de armas o artefactos explosivos, toma de rehenes, ataques contra infraestructura aeroportuaria, comunicación de información falsa y uso hostil de sistemas aéreos no tripulados y que no solo comprometen la operación aérea, sino que también afecta la vida humana, la infraestructura crítica, la continuidad del servicio y la seguridad nacional. Por esta razón, la

Organización de Aviación Civil Internacional establece que los Estados deben adoptar medidas para proteger la aviación civil contra actos de interferencia ilícita, mediante programas, procedimientos y acciones coordinadas de prevención y respuesta (Organización de Aviación Civil Internacional, 2022).

Así mismo, la Fuerza Aeroespacial Colombiana desempeña un rol estratégico en su condición de Autoridad Aeronáutica de Aviación de Estado y a través de la especialidad de Defensa de Bases Aéreas y sus capacidades operativas la participación resulta indispensable en escenarios donde la aviación civil y la aviación de Estado convergen en un mismo entorno operacional, lo que exige la implementación de medidas coordinadas para prevenir, mitigar o contener amenazas que puedan afectar la seguridad de la aviación (Fuerza Aérea Colombiana, 2020).

El alcance de esta investigación se centró en unidades aéreas con operación compartida, tomando como referencia los lineamientos de la Organización de Aviación Civil Internacional, el Reglamento Aeronáutico de Colombia 160, el Decreto 2937 de 2010, el Plan Nacional de Contingencia y la doctrina institucional de la Fuerza Aeroespacial Colombiana. Se desarrolló bajo un enfoque cualitativo y descriptivo, sustentado en revisión documental y recolección de información con expertos. La revisión documental permitió examinar normas, doctrina y procedimientos relacionados con la seguridad de la aviación civil, la aviación de Estado y la respuesta frente a actos de interferencia ilícita con el fin de identificar la regulación de la seguridad en la aviación civil.

La recolección de información se realizó mediante un instrumento de encuestas estructuradas a comandantes de grupos o escuadrones de seguridad con responsabilidad en unidades que operan pistas compartidas, así como a personal con experiencia en capacidades especializadas de reacción. Se analizaron tres categorías: operacional, táctico y organizacional; las cuales permitieron caracterizar de manera integral los factores que influyen en la respuesta ante interferencia ilícita.

Los resultados de las encuestas evidenciaron que las pistas compartidas representan entornos de alta complejidad, debido a la coexistencia de operaciones civiles y militares. Esta condición incrementa la exposición a riesgos, exige mayor control sobre áreas restringidas y demanda coordinación permanente entre la Aeronáutica Civil, la Fuerza Aeroespacial Colombiana, la Policía Nacional, operadores aeroportuarios y demás entidades responsables de la seguridad.

Al realizar el análisis de la revisión documental frente a las encuestas se logró identificar las amenazas de mayor impacto con respecto a interferencia ilícita dirigidas contra infraestructura

crítica, aeronaves, pistas, sistemas esenciales para la operación aérea y áreas de acceso restringido. Entre las amenazas más relevantes se destacaron el sabotaje, las incursiones no autorizadas, el apoderamiento ilícito de aeronaves, el empleo de artefactos explosivos y el uso hostil de drones comerciales o adaptados. Este hallazgo demostró que la seguridad de la aviación civil debe abordarse desde una perspectiva integral, combinando medidas preventivas, vigilancia permanente, gestión del riesgo y capacidades de reacción ante amenazas tradicionales y emergentes.

No obstante, se identificaron brechas que limitan la efectividad de la respuesta; entre ellas se encontró la necesidad de actualizar y socializar los procedimientos institucionales, la falta de estandarización plena entre unidades con pistas compartidas, las limitaciones en comunicaciones interoperables, baja periodicidad y falta de estandarización en los simulacros conjuntos y la necesidad de fortalecer la cultura organizacional de seguridad frente a actos de interferencia ilícita. Estas brechas pueden generar respuestas desiguales, demoras en la reacción y dificultades para coordinar acciones entre entidades civiles y militares.

Como conclusión esta investigación permitió entender que el rol de la Fuerza Aeroespacial Colombiana a través de la especialidad de Defensa de Bases Aéreas ante interferencia ilícita en pistas compartidas es estratégico y operativo, pero requiere fortalecimiento continuo. Su contribución depende de la integración entre doctrina, entrenamiento, comunicaciones, tecnología y coordinación interinstitucional. Así mismo, que esta especialidad.

Palabras clave: Actos de interferencia ilícita, Aviación civil, Fuerza Aeroespacial Colombiana, Interoperabilidad institucional, Pistas compartidas, Seguridad aeronautica.

Abstract

Civil aviation security against acts of unlawful interference is a strategic issue for Colombia, especially at airfields where civil and government aviation operations coexist. In scenarios known as shared airfields, the simultaneous presence of civil authorities, airport operators, law enforcement, and military units creates a complex operational dynamic that requires robust coordination mechanisms, clear lines of responsibility, and coordinated response capabilities. The specific problem that guided this analysis stemmed from the fact that, although the national and international regulatory framework establishes guidelines for preventing and responding to acts of unlawful interference, structural challenges persist in institutional interoperability, the updating of procedures, joint training, and tactical execution in the field (Special Administrative Unit of Civil Aviation, 2025).

Acts of unlawful interference include deliberate threats to aviation, such as the unlawful seizure of aircraft, sabotage, trespassing in restricted areas, the introduction of weapons or explosive devices, hostage-taking, attacks on airport infrastructure, the dissemination of false information, and the hostile use of unmanned aerial systems—all of which not only compromise aviation operations but also endanger human life, critical infrastructure, service continuity, and national security. For this reason, the International Civil Aviation Organization stipulates that States must adopt measures to protect civil aviation against acts of unlawful interference through coordinated prevention and response programs, procedures, and actions (International Civil Aviation Organization, 2022).

Likewise, the Colombian Aerospace Force plays a strategic role as the State Aviation Authority, and through its Air Base Defense unit and operational capabilities, its participation is indispensable in scenarios where civil aviation and state aviation converge in the same operational environment, which requires the implementation of coordinated measures to prevent, mitigate, or contain threats that may affect aviation safety (Colombian Air Force, 2020).

The scope of this research focused on air units with shared operations, using as a reference the guidelines of the International Civil Aviation Organization, Colombian Aeronautical Regulation 160, Decree 2937 of 2010, the National Contingency Plan, and the institutional doctrine of the Colombian Air Force. It was conducted using a qualitative and descriptive approach, based on a literature review and data collection from experts. The literature review allowed for the examination of regulations, doctrine, and procedures related to civil aviation security, state aviation, and the response to acts of unlawful interference, with the aim of identifying civil aviation security regulations.

Data collection was conducted using a structured survey administered to commanders of security groups or squadrons responsible for units operating on shared airstrips, as well as to personnel with experience in specialized response capabilities. Three categories were analyzed: operational, tactical, and organizational; these categories enabled a comprehensive characterization of the factors influencing the response to unlawful interference.

The survey results showed that shared runways represent highly complex environments due to the coexistence of civilian and military operations. This situation increases exposure to risks, requires greater control over restricted areas, and demands constant coordination among the Civil Aviation Authority, the Colombian Air Force, the National Police, airport operators, and other entities responsible for security.

An analysis comparing the literature review with survey data identified the most significant threats of unlawful interference targeting critical infrastructure, aircraft, runways, systems essential

to flight operations, and restricted-access areas. Among the most significant threats were sabotage, unauthorized incursions, the unlawful seizure of aircraft, the use of explosive devices, and the hostile use of commercial or modified drones. This finding demonstrated that civil aviation security must be addressed from a comprehensive perspective, combining preventive measures, continuous surveillance, risk management, and response capabilities against both traditional and emerging threats.

However, gaps were identified that limit the effectiveness of the response; these included the need to update and disseminate institutional procedures, the lack of full standardization among units sharing runways, limitations in interoperable communications, infrequent and non-standardized joint drills, and the need to strengthen the organizational security culture in the face of acts of unlawful interference. These gaps can lead to inconsistent responses, delays in reaction, and difficulties in coordinating actions between civilian and military entities.

In conclusion, this research has shown that the role of the Colombian Aerospace Force, through its Air Base Defense specialty, in addressing unlawful interference at shared airfields is both strategic and operational, but requires continuous strengthening. Its effectiveness depends on the integration of doctrine, training, communications, technology, and interagency coordination. Likewise, this specialty.

Keywords: Acts of unlawful interference, Civil aviation, Colombian Aerospace Force, Institutional interoperability, Shared runways, Aviation security.

Referencias

Fuerza Aérea Colombiana. (2020). Manual de doctrina básica aérea, espacial y ciberespacial.

Organización de Aviación Civil Internacional. (2022). Anexo 17 al Convenio sobre Aviación Civil Internacional: Seguridad. Protección de la aviación civil internacional contra los actos de interferencia ilícita.

Presidencia de la República de Colombia. (2010, 5 de agosto). Decreto 2937 de 2010. Por el cual se designa a la Fuerza Aérea Colombiana como autoridad aeronáutica de la aviación de Estado y ente coordinador ante la autoridad aeronáutica civil colombiana. Diario Oficial No. 47.793.

Unidad Administrativa Especial de Aeronáutica Civil. (2025). Reglamento Aeronáutico de Colombia RAC 160: Seguridad de la aviación civil. Unidad Administrativa Especial de Aeronáutica Civil.

Inteligencia militar para prevenir amenazas en instalaciones aeronáuticas

TE. Edgar Darío Pérez Díaz

Edgar Darío Pérez Díaz: Oficial de la Fuerza Aeroespacial Colombiana, en el grado de Teniente Efectivo, perteneciente al cuerpo de Seguridad y Defensa de Bases, en la especialidad de Inteligencia, con seis años de servicio en la institución. Maestrando de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana (EPFAC) en el programa de Dirección y Gestión de la Seguridad Integral.

Actualmente se desempeña como Comandante de la Escuadrilla de Inteligencia Aérea N.º 2021 en el Escuadrón de Inteligencia Aérea N.º 202 del Grupo Aéreo del Oriente, liderando procesos orientados a la obtención, análisis y producción de inteligencia para la identificación temprana de amenazas que puedan afectar la seguridad operacional, el cumplimiento de la misión y la protección de instalaciones estratégicas.

Su experiencia integra la dirección de actividades de inteligencia militar, análisis del entorno operacional y territorial, coordinación de capacidades de recolección de información y apoyo a la toma de decisiones en escenarios de seguridad y defensa.

Correo electrónico institucional: edgar.perez@fac.mil.co

Correo electrónico personal: eddapedi1997@hotmail.com

Línea de investigación: Modelos de Seguridad Integral

Resumen

En el contexto colombiano, las instalaciones aeronáuticas concentran capacidades críticas para la defensa, la soberanía, el control del espacio aéreo, la respuesta a emergencias y la proyección del poder aeroespacial. Por ello, su afectación no solo compromete bienes materiales o la continuidad operacional, sino también la legitimidad estatal, la confianza pública y la capacidad de respuesta institucional. Esta investigación se enfocó en la protección de instalaciones aeronáuticas militares de la FAC como infraestructura crítica del Estado.

En ese escenario, la seguridad de dichas instalaciones no se redujo al perímetro físico, porque muchas Unidades Militares Aéreas se encuentran ubicadas en entornos urbanos, rurales o mixtos donde confluyeron predios civiles, rutas de acceso y dinámicas sociales que incidieron en el riesgo. Asimismo, el estudio reconoció que la evolución de las amenazas, desde acciones convencionales hasta terrorismo, sabotaje, crimen organizado y modalidades híbridas, exigió integrar la normativa aeronáutica, la doctrina militar y la inteligencia territorial en un enfoque

preventivo de seguridad integral (Organización de Aviación Civil Internacional [OACI], 2017; Unidad Administrativa Especial de Aeronáutica Civil [UAEAC], 2020).

En consecuencia, la investigación se enfocó en analizar y generar una herramienta para identificar, caracterizar y gestionar predios concurrentes o colindantes en los límites de las Unidades Militares Aéreas, conforme a las exigencias del Capítulo A del RAC 160 y a las necesidades propias de instalaciones de uso militar. La seguridad aplicada se había concentrado principalmente en medidas físicas, tecnológicas y procedimentales internas, mientras que el entorno territorial inmediato no siempre fue tratado como una fuente permanente de amenaza.

Esta situación generó brechas de anticipación frente a actores hostiles que podían utilizar zonas civiles, vías públicas, predios vecinos o dinámicas comunitarias para observar, aproximarse, infiltrar, sabotear o ejecutar acciones violentas contra infraestructuras aeronáuticas. Dentro de los últimos antecedentes, como el ataque contra la Base Aérea Marco Fidel Suárez, fue utilizado como referente de análisis porque evidenció la importancia de ampliar la seguridad más allá del cerramiento físico, fortalecer la alerta temprana y vincular la inteligencia militar con la gestión del riesgo en espacios de interacción civil-militar (Fuerza Aeroespacial Colombiana [FAC], 2025; Función Pública, 2013).

Por esta razón, la investigación tuvo como objetivo analizar la incorporación de la inteligencia militar en la implementación del Capítulo A del RAC 160, con el propósito de fundamentar una matriz de seguridad integral preventiva aplicable a la protección de instalaciones aeronáuticas militares. Para ello, la investigación delimitó su alcance en tres niveles complementarios. En primer lugar, se diagnosticó la aplicación normativa y doctrinal del RAC 160 en instalaciones de la FAC, con énfasis en la gestión de predios concurrentes y en la integración de capacidades de inteligencia.

En segundo lugar, se seleccionaron parámetros técnicos tentativos para aplicar inteligencia militar en la protección de bases aéreas, considerando criterios normativos, operacionales y territoriales. En tercer lugar, se planteó la validación de dichos parámetros mediante entrevistas a expertos, lo que permitió identificar de manera detallada las capacidades existentes, las amenazas potenciales y las vulnerabilidades presentes en el sistema.

Para la recolección y el análisis de los datos se empleó una metodología cualitativa basada en el análisis documental y las entrevistas a expertos. Se empleó una matriz de análisis normativo-doctrinal para comparar las disposiciones del RAC 160, el Anexo 17, el Doc. 8973, la Ley 1621 de 2013 y referentes de seguridad integral con las necesidades de protección de bases aéreas. Esta matriz permitió organizar obligaciones, criterios de seguridad, conceptos de infraestructura crítica, control de accesos, protección perimetral, gestión del riesgo e inteligencia.

De igual manera, se diseñaron entrevistas semiestructuradas a expertos en seguridad, inteligencia y gestión del riesgo para recoger percepciones sobre prácticas, limitaciones y oportunidades de integración. Finalmente, se utilizó una matriz de riesgo como herramienta de análisis para evaluar y categorizar las amenazas de acuerdo con su nivel de probabilidad e impacto, permitiendo priorizar acciones estratégicas orientadas al fortalecimiento de la seguridad y la mitigación de riesgos (Bernal, 2010; Hernández-Sampieri & Mendoza, 2018).

Los resultados evidenciaron que la protección de las instalaciones aeronáuticas militares exigió el desarrollo de capacidades operacionales y de inteligencia diferenciadas, capaces de superar los enfoques tradicionales de la seguridad aeronáutica civil. Aunque el RAC 160 constituyó una base normativa relevante para la protección de la aviación, su aplicación en escenarios militares requirió una adaptación doctrinal y operacional, debido a que el entorno de amenaza de una base aérea presentó características estratégicas distintas a las de un aeropuerto civil. En este contexto, se identificó que la seguridad de las bases aéreas no podía limitarse únicamente a controles perimetrales, accesos restringidos y vigilancia interna, sino que debía integrar capacidades orientadas a la anticipación y comprensión del entorno territorial.

Entre los principales hallazgos se estableció que los predios concurrentes y zonas colindantes constituyeron espacios de vulnerabilidad estratégica, debido a la convergencia de usos civiles y militares, la movilidad de población, las dinámicas territoriales y la posibilidad de actividades de vigilancia hostil o infiltración por parte de actores adversarios. Estas condiciones incrementaron la exposición de las instalaciones aeronáuticas frente a amenazas híbridas, en las cuales convergieron riesgos físicos, tecnológicos, criminales y de inteligencia.

De igual manera, se evidenció que las amenazas evolucionaron hacia escenarios multidimensionales, donde coexistieron el terrorismo, el sabotaje, las amenazas internas asociadas al factor humano, el empleo malicioso de drones, la obtención clandestina de información y los riesgos cibernéticos contra sistemas críticos. En consecuencia, la inteligencia militar se consolidó como un eje articulador fundamental para la seguridad integral preventiva, al permitir comprender el entorno operacional, identificar patrones de riesgo y apoyar la toma de decisiones estratégicas mediante la integración de capacidades, dentro de los principios de legalidad, necesidad y proporcionalidad establecidos en el marco jurídico colombiano (Ley 1621 Función Pública, 2013).

Asimismo, los hallazgos demostraron que la protección efectiva de las instalaciones aeronáuticas militares requirió una articulación permanente entre la Fuerza Aeroespacial Colombiana, la Aeronáutica Civil, la Policía Nacional y las autoridades territoriales, con el fin de reducir vacíos de control, fortalecer el intercambio de información y mejorar la coordinación frente

a riesgos que afectaran simultáneamente la defensa nacional, la seguridad pública y la aviación (OACI, 2020; UAEAC, 2020). En este sentido, la coordinación interinstitucional y la sinergia civil-militar se identificaron como factores determinantes para consolidar esquemas de seguridad más resilientes y adaptativos.

Las entrevistas realizadas a expertos permitieron concluir que la seguridad de las instalaciones aeronáuticas debía concebirse como un sistema estratégico basado en capacidades, y no únicamente como un conjunto de medidas físicas u operativas aisladas. Existió consenso en que dichas capacidades debían desarrollarse de manera integral, articulando doctrina, inteligencia, tecnología, gestión del riesgo y análisis territorial, con el propósito de fortalecer la anticipación estratégica y reducir la sorpresa operacional frente a amenazas emergentes.

En consecuencia, la investigación permitió concluir que la protección de bases aéreas debía evolucionar desde modelos predominantemente reactivos hacia un enfoque preventivo, sistémico y adaptable, sustentado en la inteligencia territorial, la defensa en profundidad y la gestión integral del riesgo.

Finalmente, el impacto de la investigación se proyectó en el fortalecimiento doctrinal de la Fuerza Aeroespacial Colombiana, mediante la generación de insumos para la construcción de un modelo sinérgico de seguridad integral preventiva aplicable a instalaciones aeronáuticas militares. Como productos asociados al estudio se desarrollaron capítulo de libro titulado “Prevención De Amenazas En Instalaciones Aeronáuticas: Una Aproximación Desde La Inteligencia Militar”, una matriz normativo-doctrinal, los parámetros técnicos tentativos para la gestión de predios concurrentes y la propuesta de lineamientos estratégicos orientados a fortalecer la protección de activos vitales e infraestructura crítica aeronáutica.

Palabras clave: Seguridad integral preventiva, instalaciones aeronáuticas militares, predios concurrentes, infraestructura crítica, RAC 160.

Abstract

In the Colombian context, aviation facilities house critical capabilities for defense, sovereignty, airspace control, emergency response, and the projection of aerospace power. Therefore, any disruption to these facilities not only jeopardizes physical assets or operational continuity but also state legitimacy, public trust, and institutional response capacity. This research focused on the protection of the FAC's military aeronautical facilities as critical state infrastructure.

In this scenery, the security of these facilities was not limited to the physical perimeter, as many Air Force units are located in urban, rural, or mixed environments where civilian properties, access routes, and social dynamics converged, all of which influenced the risk. Likewise, the study recognized that the evolution of threats—ranging from conventional actions to terrorism, sabotage, organized crime, and hybrid forms—required the integration of aviation regulations, military doctrine, and territorial intelligence into a preventive approach to comprehensive security (International Civil Aviation Organization [ICAO], 2017; Special Administrative Unit of Civil Aviation [UAEAC], 2020).

Consequently, the research focused on analyzing and developing a tool to identify, characterize, and manage adjacent or neighboring properties within the boundaries of Air Force bases, in accordance with the requirements of Chapter A of RAC 160 and the specific needs of military facilities. Security measures had primarily focused on physical, technological, and internal procedural measures, while the immediate territorial environment was not always treated as a constant source of threat.

This situation created gaps in anticipation regarding hostile actors who could use civilian areas, public roads, neighboring properties, or community dynamics to observe, approach, infiltrate, sabotage, or carry out violent actions against aeronautical infrastructure. Among recent incidents, the attack on the Marco Fidel Suárez Air Base was used as a case study because it highlighted the importance of extending security beyond physical perimeters, strengthening early warning systems, and integrating military intelligence with risk management in areas of civil-military interaction (Colombian Aerospace Force [FAC], 2025; Civil Service, 2013).

For this reason, the study aimed to analyze the integration of military intelligence into the implementation of Chapter A of RAC 160, with the goal of establishing a comprehensive preventive security framework applicable to the protection of military aviation facilities. To this end, the study defined its scope across three complementary levels. First, the normative and doctrinal application of RAC 160 at FAC facilities was assessed, with an emphasis on the management of shared premises and the integration of intelligence capabilities.

Second, tentative technical parameters were selected for applying military intelligence to the protection of air bases, taking into account regulatory, operational, and territorial criteria. Third, the validation of these parameters was addressed through interviews with experts, which allowed for a detailed identification of existing capabilities, potential threats, and vulnerabilities present in the system.

A qualitative methodology based on document analysis and expert interviews was used for data collection and analysis. A normative-doctrinal analysis matrix was used to compare the

provisions of RAC 160, Annex 17, Doc. 8973, Law 1621 of 2013, and comprehensive security benchmarks with the protection needs of air bases. This matrix enabled the organization of obligations, security criteria, concepts of critical infrastructure, access control, perimeter protection, risk management, and intelligence.

Similarly, semi-structured interviews were designed with experts in security, intelligence, and risk management to gather insights on practices, limitations, and opportunities for integration. Finally, a risk matrix was used as an analytical tool to assess and categorize threats according to their level of probability and impact, enabling the prioritization of strategic actions aimed at strengthening security and mitigating risks (Bernal, 2010; Hernández-Sampieri & Mendoza, 2018).

The results showed that protecting military aviation facilities required the development of specialized operational and intelligence capabilities capable of going beyond traditional approaches to civil aviation security. Although RAC 160 provided a relevant regulatory framework for aviation security, its application in military settings required doctrinal and operational adaptation, as the threat environment of an air base presented strategic characteristics distinct from those of a civil airport. In this context, it was determined that airbase security could not be limited solely to perimeter controls, restricted access, and internal surveillance, but must integrate capabilities aimed at anticipating and understanding the territorial environment.

Among the main findings, it was established that adjacent properties and surrounding areas constituted spaces of strategic vulnerability due to the convergence of civilian and military uses, population mobility, territorial dynamics, and the possibility of hostile surveillance or infiltration by adversarial actors. These conditions increased the exposure of aviation facilities to hybrid threats, in which physical, technological, criminal, and intelligence risks converged.

Similarly, it became evident that threats had evolved into multidimensional scenarios, where terrorism, sabotage, internal threats associated with human factors, the malicious use of drones, clandestine information gathering, and cyber risks targeting critical systems coexisted. Consequently, military intelligence established itself as a fundamental coordinating pillar for comprehensive preventive security, enabling an understanding of the operational environment, the identification of risk patterns, and support for strategic decision-making through the integration of capabilities, within the principles of legality, necessity, and proportionality established in the Colombian legal framework (Law 1621 on Public Service, 2013).

Likewise, the findings demonstrated that the effective protection of military aeronautical facilities required ongoing coordination between the Colombian Aerospace Force, the Civil Aviation Authority, the National Police, and territorial authorities, in order to reduce control gaps, strengthen information sharing, and improve coordination in the face of risks that simultaneously

affect national defense, public safety, and aviation (ICAO, 2020; UAEAC, 2020). In this regard, inter-institutional coordination and civil-military synergy were identified as key factors in consolidating more resilient and adaptive security frameworks.

Interviews with experts led to the conclusion that aviation facility security should be viewed as a strategic, capability-based system, rather than merely as a set of isolated physical or operational measures. There was consensus that these capabilities should be developed in a comprehensive manner, integrating doctrine, intelligence, technology, risk management, and territorial analysis, with the aim of strengthening strategic foresight and reducing operational surprise in the face of emerging threats.

Consequently, the research led to the conclusion that the protection of air bases should evolve from predominantly reactive models toward a preventive, systemic, and adaptive approach, grounded in territorial intelligence, defense in depth, and comprehensive risk management.

Finally, the research contributed to strengthening the doctrinal framework of the Colombian Aerospace Force by providing input for the development of a synergistic model of comprehensive preventive security applicable to military aviation facilities. As outputs of the study, a book chapter titled “Threat Prevention at Aeronautical Facilities: An Approach from Military Intelligence” was developed, along with a normative-doctrinal matrix, tentative technical parameters for the management of adjacent properties, and a proposal for strategic guidelines aimed at strengthening the protection of vital assets and critical aeronautical infrastructure.

Keywords: Comprehensive preventive security, military aviation facilities, adjacent properties, critical infrastructure, RAC 160.

Referencias

Bernal, C. A. (2010). Metodología de la investigación (4.^a ed.). Pearson Educación.

Función Pública. (2013). Ley 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. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706>

Fuerza Aeroespacial Colombiana. (2025). Comunicado 004/2025. <https://www.fac.mil.co/es/comunicados/comunicado-0042025>

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill.

Organización de Aviación Civil Internacional. (2017). Anexo 17: Seguridad de la aviación civil internacional. OACI.

Organización de Aviación Civil Internacional. (2020). Manual de seguridad de la aviación (Doc. 8973). OACI.

Unidad Administrativa Especial de Aeronáutica Civil. (2020). RAC 160: Seguridad de la aviación civil. Aerocivil.

Seguridad física de la aviación civil colombiana: fortalecimiento de la gestión del riesgo

TJ (RA) Carlos Héctor Quinchía Wilches

Carlos Héctor Quinchía Wilches: Suboficial en uso de buen retiro en el grado Técnico Jefe en uso de buen retiro de la Fuerza Aeroespacial Colombiana (FAC). Administrador de empresas de la Universidad Nacional Abierta y a Distancia – UNAD. Tecnólogo en Seguridad Aeroportuaria y maestrando actualmente la Maestría en Dirección y Gestión de la Seguridad Integral (MADGSI).

Correo electrónico institucional: carlos.quinchia@epfac.edu.co

Correo electrónico personal: carlos.quinchia.co@gmail.com

Línea de investigación: Dirección y Gestión de la Seguridad Integral

Resumen

La seguridad de la aviación civil es un sistema crítico donde confluyen factores regulatorios, operacionales, tecnológicos y humanos (Leveson, 2011; Hollnagel, 2014; OACI, 2020). A pesar de la consolidación de estándares internacionales liderada por la Organización de Aviación Civil Internacional (OACI), el problema central que abordó esta investigación radica en la importante brecha entre la solidez del marco regulatorio y la efectividad de su implementación en la gestión de riesgos dentro de la seguridad física de la aviación civil colombiana.

Esta brecha limita la capacidad del sistema para anticipar prevenir y responder a amenazas tradicionales y emergentes, afectando la resiliencia y confiabilidad del transporte aéreo (OACI, 2024). La evidencia histórica, tanto a nivel internacional como nacional, demostró que los incidentes de seguridad no se explican por la ausencia de regulaciones, sino más bien por fallas en la coordinación del sistema, deficiencias en la gobernanza y limitaciones en la aplicación práctica de enfoques basados en riesgo (Reason, 1997; OACI, 2020).

Para abordar este problema, la investigación adoptó un enfoque cualitativo y documental basado en el análisis sistemático y comparativo de fuentes regulatorias, técnicas y académicas. El Corpus documental incluyó instrumentos internacionales como el Anexo 17, el Documento 8973 Manual de Seguridad de la Aviación y el Plan Global de Seguridad de la Aviación Civil (GASeP), así como el marco regulatorio colombiano, representado principalmente por el RAC

160 y sus programas complementarios, entre los cuales se encuentran: Programa Nacional de Instrucción en Seguridad de la Aviación Civil (PNISAC), Programa Nacional de Control de Calidad de la Seguridad de la Aviación Civil (PNCC) y Programa Nacional de Facilitación del Transporte Aéreo (PNFTA).

La metodología se estructuró en etapas de selección de documentos, lectura analítica, categorización y comparación, apoyadas en técnicas de análisis de contenido. Este enfoque permitió identificar conceptos clave, relaciones regulatorias y discrepancias entre el diseño regulatorio y su aplicación operativa, sin recurrir a mediciones estadísticas, sino priorizando la interpretación crítica del sistema Seguridad de la Aviación o por sus siglas en Inglés AVSEC (Aviation Security) dentro de su contexto (OACI, 2020; OACI, 2022; OACI, 2024; UAEAC, 2025).

Los hallazgos demostraron que Colombia cuenta con un marco regulatorio sólido, alineado con los estándares internacionales, lo que constituye una fortaleza estructural del sistema. Sin embargo, la investigación identificó varias brechas críticas: primero, se observó una debilidad en la gobernanza del sistema AVSEC, particularmente en la coordinación interinstitucional, donde la existencia de estructuras formales no garantiza procesos de toma de decisiones efectivos ni mecanismos de evaluación del desempeño. Segundo, se evidenció una brecha entre la reglamentación y la práctica; manifestada en la limitada incorporación de evaluaciones de riesgo en las operaciones diarias y la persistencia de enfoque reactivos y prescriptivos. Tercero, se identificaron desafíos en la gestión de amenazas contextuales e internas tales como la corrupción, la infiltración del crimen organizado y la heterogeneidad territorial, factores que complican la aplicación de modelos internacionales estandarizados (OACI 2020; OACI 2024).

Además, el estudio subrayó la importancia del factor humano como elemento fundamental en la gestión de riesgos (OACI, 2024). Si bien existen programas de capacitación y certificación, persisten las dudas sobre su impacto real en el desempeño operativo, especialmente en lo que respecta a la capacidad del personal para interpretar riesgos, tomar decisiones bajo presión y mantener una cultura de seguridad eficaz (OACI 2020). Esta situación demostró que la seguridad no se supedita solo a controles técnicos o normativos, sino también de la interacción dinámica entre personas, procesos y tecnología. En este sentido y ampliando el concepto, los hallazgos confirmaron que la seguridad de la aviación civil debe entenderse como un sistema sociotécnico complejo, es decir, que es un sistema donde la seguridad depende de la interacción entre personas, tecnología, normas y procesos, dentro de un entorno dinámico y cambiante; donde las fallas surgen de la interacción de múltiples factores y no de errores aislados (Leveson, 2011).

Otro resultado relevante se sustentó en el análisis comparativo entre los estándares internacionales y el marco normativo nacional, el cual evidenció que, aunque el enfoque sistémico y basado en riesgo promovido por la OACI, particularmente a través del Anexo 17, el Documento 8973 Manual de Seguridad de la Aviación y el Plan Global para la Seguridad de la Aviación Doc. 10118 (GASep), ha sido formalmente incorporado en instrumentos como el RAC 160 Seguridad de la Aviación Civil y sus programas complementarios, la literatura normativa y el análisis documental identifican limitaciones en su implementación operativa (UAEAC, 2025; OACI, 2022).

Estas limitaciones se reflejan en debilidades en la coordinación interinstitucional, la incorporación efectiva del análisis de riesgos en la toma de decisiones y las capacidades técnicas para evaluaciones dinámicas, lo que pone de manifiesto una tensión entre el enfoque conceptual de la seguridad y su materialización en la operación diaria, confirmando la existencia de una brecha estructural en el sistema AVSEC colombiano (OACI, 2020; OACI, 2024).

Estos hallazgos sugirieron que la optimización de la gestión de riesgos en la seguridad física de la aviación civil colombiana no depende de la creación de nuevas regulaciones, sino del fortalecimiento de la capacidad institucional para implementar eficazmente los marcos existentes; esto implica mejorar la coordinación interinstitucional, integrar el análisis de riesgos en la toma de decisiones operativas, fortalecer la cultura de seguridad, desarrollar capacidades técnicas y adaptar los modelos internacionales al contexto nacional. En términos prácticos, la gestión de riesgos debe evolucionar de un enfoque reactivo a uno preventivo, sistémico y basado en la evidencia. (OACI, 2020; OACI, 2024).

En este contexto, la investigación ofreció una visión integral del sistema colombiano de seguridad de la aviación (AVSEC), permitiendo comprender sus fortalezas, limitaciones y oportunidades de mejora. Su impacto se refleja en la generación de una base analítica para la toma de decisiones estratégicas, el fortalecimiento institucional y la formulación de mejores prácticas en la gestión de riesgos (OACI, 2024). Entre los resultados asociados se incluyeron recomendaciones aplicables al diseño de políticas públicas, la mejora de los programas de capacitación, el fortalecimiento del control de calidad y la optimización de la coordinación interinstitucional, contribuyendo así al desarrollo de un sistema de seguridad de la aviación más resiliente y eficiente, adaptado a la dinámica de riesgos contemporánea (OACI, 2020; OACI, 2024; UAEAC, 2025).

En conclusión, la investigación demostró que la seguridad de la aviación civil en Colombia ha transitado desde un enfoque predominantemente normativo hacia un modelo de gestión del

riesgo más sistémico, dinámico y alineado con las directrices internacionales, consolidado en el RAC 160 y en la adopción progresiva del SeMS. Sin embargo, la persistencia de brechas entre la regulación y la práctica, sumada a la complejidad de las amenazas emergentes, evidencia que la eficacia del sistema AVSEC no depende únicamente del cumplimiento normativo, sino de su capacidad para integrar tecnología, procesos y cultura de seguridad en entornos operativos reales.

En este sentido, el futuro de la seguridad de la aviación civil colombiana exige avanzar hacia esquemas de seguridad inteligente, consolidar el SeMS como núcleo de decisión estratégica y fortalecer una gobernanza basada en la cooperación y el intercambio oportuno de información, como condiciones indispensables para garantizar un sistema resiliente, adaptable y sostenible frente a los desafíos contemporáneos. En suma, y también como producto de este proceso investigativo, se elaboró el capítulo de libro “Gestión del riesgo de la seguridad física de la aviación civil colombiana: revisión documental”, el cual se integra a la obra conmemorativa de los cien años de la especialidad de seguridad y defensa de bases de la Fuerza Aeroespacial Colombiana, fortaleciendo el vínculo entre la producción académica y el desarrollo institucional del sector.

Palabras clave: Aviación civil, gestión del riesgo, gobernanza, implementación operativa, seguridad AVSEC, SeMS.

Abstract

Civil aviation security is a critical system where regulatory, operational, technological, and human factors converge (Leveson, 2011; Hollnagel, 2014; ICAO, 2020). Despite the consolidation of international standards led by the International Civil Aviation Organization (ICAO), the central problem addressed by this research lies in the significant gap between the robustness of the regulatory framework and the effectiveness of its implementation regarding risk management within the physical security of Colombian civil aviation.

This gap limits the system's capacity to anticipate, prevent, and respond to both traditional and emerging threats, thereby affecting the resilience and reliability of air transport (ICAO, 2024). Historical evidence at both the international and national levels has demonstrated that security incidents are not explained by an absence of regulations, but rather by failures in system

coordination, deficiencies in governance, and limitations in the practical application of risk-based approaches (Reason, 1997; ICAO, 2020).

To address this problem, the research adopted a qualitative and documentary approach based on the systematic and comparative analysis of regulatory, technical, and academic sources. The documentary corpus included international instruments such as Annex 17, Document 8973 (Aviation Security Manual), and the Global Aviation Security Plan (GASeP), as well as the Colombian regulatory framework represented primarily by RAC 160 and its complementary programs. These complementary programs include the National Civil Aviation Security Training Program (PNISAC), the National Civil Aviation Security Quality Control Program (PNCC), and the National Air Transport Facilitation Program (PNFTA).

The methodology was structured into stages involving document selection, analytical reading, categorization, and comparison, supported by content analysis techniques. This approach enabled the identification of key concepts, regulatory relationships, and discrepancies between regulatory design and its operational application without resorting to statistical measurements by instead prioritizing a critical interpretation of the Aviation Security system (or AVSEC) within its specific context (ICAO, 2020; ICAO, 2022; ICAO, 2024; UAEAC, 2025).

The findings demonstrated that Colombia possesses a robust regulatory framework aligned with international standards, constituting a structural strength of the system. However, the research identified several critical gaps: First, a weakness was observed in the governance of the AVSEC system particularly regarding inter-institutional coordination where the existence of formal structures does not guarantee effective decision-making processes or performance evaluation mechanisms. Second, a gap was evident between regulation and practice, manifested in the limited integration of risk assessments into daily operations and the persistence of reactive and prescriptive approaches. Third, challenges were identified in managing contextual and internal threats such as corruption, organized crime infiltration, and territorial heterogeneity factors that complicate the application of standardized international models (ICAO, 2020; ICAO, 2024).

Furthermore, the study underscored the importance of the human factor as a fundamental element in risk management (ICAO, 2024). While training and certification programs do exist, doubts persist regarding their actual impact on operational performance particularly concerning personnel's capacity to interpret risks, make decisions under pressure, and maintain an effective safety culture (ICAO, 2020). This situation demonstrated that safety is not contingent solely upon technical or regulatory controls, but also upon the dynamic interaction among people, processes, and technology. In this regard and by broadening the concept the findings confirmed that civil aviation security must be understood as a complex sociotechnical system; that is, a system

wherein safety depends on the interplay among people, technology, regulations, and processes within a dynamic and ever-changing environment, and where failures arise from the interaction of multiple factors rather than from isolated errors.

Another relevant result was grounded in a comparative analysis between international standards and the national regulatory framework. This analysis revealed that, although the systemic and risk-based approach promoted by ICAO specifically through Annex 17, Document 8973 (the Aviation Security Manual), and Document 10118 (the Global Aviation Security Plan or GAsEP) (ICAO, 2022; ICAO, 2020; ICAO, 2024) has been formally incorporated into instruments such as RAC 160 (Civil Aviation Security) and its complementary programs, both regulatory literature and documentary analysis identify limitations regarding its operational implementation (UAEAC, 2025; ICAO, 2022).

These limitations are reflected in weaknesses regarding inter-institutional coordination, the effective incorporation of risk analysis into decision-making, and technical capabilities for dynamic assessments; this highlights a tension between the conceptual approach to security and its realization in daily operations, thereby confirming the existence of a structural gap within the Colombian AVSEC system (ICAO, 2020; ICAO, 2024).

These findings suggested that optimizing risk management within the physical security of Colombian civil aviation does not depend on the creation of new regulations, but rather on strengthening institutional capacity to effectively implement existing frameworks. This entails improving inter-institutional coordination, integrating risk analysis into operational decision-making, strengthening safety culture, developing technical capabilities, and adapting international models to the national context. In practical terms, risk management must evolve from a reactive approach to one that is preventive, systemic, and evidence-based (ICAO, 2020; ICAO, 2024).

In this context, the research offered a comprehensive overview of the Colombian aviation security (AVSEC) system, facilitating an understanding of its strengths, limitations, and opportunities for improvement. Its impact is reflected in the establishment of an analytical foundation for strategic decision-making, institutional strengthening, and the formulation of best practices in risk management (ICAO, 2024). Associated outcomes included recommendations applicable to public policy design, the enhancement of training programs, the strengthening of quality control, and the optimization of inter-institutional coordination thereby contributing to the development of a more resilient and efficient aviation security system, tailored to contemporary risk dynamics (ICAO, 2020; ICAO, 2024; UAEAC, 2025).

In conclusion, the research demonstrated that civil aviation safety in Colombia has shifted from a predominantly regulatory approach toward a more systemic and dynamic risk management

model aligned with international guidelines, as enshrined in RAC 160 and reflected in the progressive adoption of the SeMS. However, the persistence of gaps between regulation and practice, coupled with the complexity of emerging threats, demonstrates that the effectiveness of the AVSEC system does not depend solely on regulatory compliance, but on its ability to integrate technology, processes, and a safety culture into real-world operational environments.

In this regard, the future of Colombian civil aviation security requires moving toward smart security frameworks, consolidating the SeMS as the core of strategic decision-making, and strengthening governance based on cooperation and the timely exchange of information—all of which are essential conditions for ensuring a resilient, adaptable, and sustainable system capable of addressing contemporary challenges. In summary, and also as a result of this research process, the book chapter “Risk Management of Physical Security in Colombian Civil Aviation: A Literature Review” was written, which is included in the commemorative volume marking the centennial of the Colombian Aerospace Force’s base security and defense specialty, thereby strengthening the link between academic output and the sector’s institutional development.

Keywords: Civil aviation, risk management, governance, operational implementation, AVSEC security, SeMS.

Referencias

Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate.

Leveson, N. G. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press.

Organización de Aviación Civil Internacional. (2020). Manual de seguridad de la aviación (Doc 8973, 12.^a ed.).

Organización de Aviación Civil Internacional. (2022). Anexo 17 al Convenio sobre Aviación Civil Internacional: Seguridad. Protección de la aviación civil internacional contra los actos de interferencia ilícita.

Organización de Aviación Civil Internacional. (2024). Plan global para la seguridad de la aviación (Doc 10118, 2.^a ed.).

Reason, J. (1997). Managing the risks of organizational accidents (1st ed.). Routledge

Unidad Administrativa Especial de Aeronáutica Civil. (2025). Reglamento Aeronáutico de Colombia RAC 160: Seguridad de la aviación civil. Aerocivil.

Gestión del talento humano para fortalecer la protección de bases aéreas

MY. Marco Antonio Abril Morales

Marco Antonio Abril Morales: Oficial de la Fuerza Aeroespacial Colombiana, Licenciado en Educación Física, Recreación y Deportes de la Universidad Cooperativa de Colombia, candidato a Magister en Dirección y Gestión de la Seguridad Integral de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana. Actualmente se desempeña como Jefe de la Sección Planeamiento del Grupo de Seguridad y Defensa de Bases Aéreas No. 35. Cuenta con 17 años de experiencia institucional en cargos de mando, planeamiento, talento humano y seguridad de bases aéreas. Su trayectoria profesional se ha orientado al liderazgo de personal militar, la administración del talento humano, la protección de instalaciones estratégicas y el fortalecimiento de capacidades operacionales en escenarios de seguridad integral.

Correo electrónico institucional: marco.abril@fac.mil.co

Correo electrónico institucional: maam.10@hotmail.com

Línea de investigación: Dirección y Gestión de la Seguridad Integral

Resumen

La seguridad y defensa de bases aéreas constituye una función estratégica para la protección del componente físico del poder aéreo, espacial y ciberespacial, debido a que estas instalaciones concentran infraestructura crítica, aeronaves, sistemas de comando y control, capacidades tecnológicas, información sensible y personal indispensable para la continuidad operacional. En este escenario, el talento humano cumple un papel determinante, pues es el encargado de ejecutar funciones críticas como la vigilancia, el control de accesos, la reacción, la defensa activa y la protección de activos estratégicos. Por tanto, la efectividad de la seguridad de una base aérea no depende únicamente de medios físicos, tecnológicos o doctrinales, sino también de la forma en que se administra, prepara, lidera y acompaña al personal responsable de cumplir la misión.

A partir de este contexto, el problema de investigación se relacionó con la necesidad de comprender cómo los procesos de selección, capacitación, motivación, bienestar, liderazgo y asignación del personal inciden en la efectividad de las operaciones de seguridad y defensa de bases aéreas. Esta situación adquiere especial importancia en escenarios donde las amenazas son dinámicas y las exigencias operacionales requieren personal confiable, competente, disciplinado, motivado y con capacidad de respuesta. En consecuencia, se identificó que una

administración del talento humano limitada únicamente a la asignación de cargos, sin evaluación de competencias, seguimiento permanente o fortalecimiento del bienestar, puede generar vulnerabilidades humanas que afectan la seguridad física, tecnológica y operacional de las instalaciones.

En atención a esta problemática, el objetivo general de la investigación adquirió especial relevancia, porque permitió ubicar al personal no como un simple recurso de apoyo, sino como un eje decisivo para la protección de activos estratégicos. En ese sentido, el estudio buscó analizar la administración del talento humano como factor clave para fortalecer la protección de bases aéreas, a partir de la revisión teórica, doctrinal, normativa e institucional, así como de la percepción del personal perteneciente a la Especialidad de Seguridad y Defensa de Bases Aéreas. Este objetivo permitió establecer la relación entre talento humano, liderazgo, bienestar, capacitación, gestión por competencias y efectividad operacional en el cumplimiento de funciones críticas de seguridad.

Para el desarrollo del estudio se utilizaron como instrumentos la revisión teórica, doctrinal, normativa e institucional y una encuesta aplicada a 104 integrantes de la Especialidad de Seguridad y Defensa de Bases Aéreas. La revisión teórica permitió articular aportes sobre talento humano, gestión por competencias, liderazgo, seguridad operacional y factor humano. En este sentido, Chiavenato (2011) comprende el talento humano como un conjunto de conocimientos, habilidades, actitudes y valores que aportan valor estratégico a la organización; Dessler (2015) resalta la importancia de la selección, capacitación y evaluación del personal con base en competencias; Ulrich et al. (2007) vinculan la gestión humana con la estrategia institucional; Reason (2016) advierte sobre la incidencia del factor humano en los riesgos organizacionales; y Hollnagel (2014) destaca la capacidad adaptativa de las personas para sostener la seguridad en entornos complejos.

De manera complementaria, la encuesta permitió reconocer percepciones del personal frente a motivación, bienestar, liderazgo, capacitación, capacidad de respuesta y condiciones de recuperación. No obstante, como fase pendiente de la investigación, se proyectó la realización de un grupo focal con personal experto en seguridad y defensa de bases aéreas, activo y retirado, con experiencia institucional, con el propósito de profundizar los hallazgos preliminares, contrastar la información recolectada y fortalecer la propuesta final del estudio, la cual se encuentra en proceso de tabulación.

Los hallazgos preliminares evidenciaron que el talento humano no debe entenderse únicamente como un recurso administrativo, sino como un componente estratégico del sistema de seguridad y defensa. La encuesta mostró que la motivación y el bienestar incidieron en el

rendimiento operativo y en la capacidad de reacción del personal; asimismo, permitió identificar percepciones menos favorables frente al respeto de los compensatorios posteriores al servicio, aspecto que pudo afectar la recuperación física y mental. También se encontró que el liderazgo militar, la capacitación continua y la gestión por competencias influyeron en la cohesión, la disciplina, el compromiso institucional y la reducción de vulnerabilidades humanas, físicas, tecnológicas y operacionales.

En consecuencia, se concluyó que la protección de bases aéreas no inicia en la cámara, el sensor, la barrera o el sistema de reacción; inicia en la persona que observa, interpreta, decide y actúa cuando la misión lo exige. Esta investigación evidenció que el talento humano no es un apoyo secundario del sistema de seguridad, sino el punto donde la doctrina, la tecnología, el liderazgo y la operación se convierten en capacidad real de protección. Por ello, fortalecer la selección, la capacitación, la motivación, el bienestar y el liderazgo del personal de Seguridad y Defensa de Bases significa reducir vulnerabilidades antes de que se materialicen, aumentar la capacidad de respuesta y proteger con mayor solidez los activos estratégicos de la Fuerza Aeroespacial Colombiana. El aporte central del estudio consistió en demostrar que cuidar y gestionar mejor al personal no solo mejora el desempeño individual, sino que fortalece la defensa del poder aéreo, espacial y ciberespacial de la Nación. Como producto asociado, esta investigación aportó al capítulo de libro titulado Administración del talento humano en la seguridad y defensa de bases aéreas, del libro propuesto Seguridad en Instalaciones Aeronáuticas Críticas: un enfoque interdisciplinario – cien años con la mejor seguridad en tierra, elaborado en el marco de la conmemoración de los 100 años de la Especialidad de Seguridad y Defensa de Bases, así como al proceso de investigación formativa de la Maestría en Dirección y Gestión de la Seguridad Integral de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana.

Palabras clave: bases aéreas, bienestar institucional, gestión por competencias, liderazgo militar, seguridad integral, talento humano.

Abstract

The security and defense of air bases constitute a strategic function for the protection of the physical component of air, space, and cyberspace power, since these facilities concentrate critical infrastructure, aircraft, command and control systems, technological capabilities, sensitive information, and personnel essential for operational continuity. In this scenario, human talent plays a decisive role, as it is responsible for carrying out critical functions such as surveillance, access control, response, active defense, and the protection of strategic assets. Therefore, the

effectiveness of air base security does not depend solely on physical, technological, or doctrinal means, but also on the way the personnel responsible for accomplishing the mission are managed, trained, led, and supported.

Based on this context, the research problem was related to the need to understand how personnel selection, training, motivation, welfare, leadership, and assignment processes influenced the effectiveness of air base security and defense operations. This situation becomes especially important in scenarios where threats are dynamic and operational demands required reliable, competent, disciplined, motivated personnel with response capacity. Consequently, it was identified that human talent management limited only to job assignment, without competency assessment, permanent follow-up, or welfare strengthening, can create human vulnerabilities that affect the physical, technological, and operational security of these facilities.

In response to this problem, the general objective of the research acquired special relevance because it made it possible to position personnel not as a simple support resource, but as a decisive axis for the protection of strategic assets. In this sense, the study sought to analyze human talent management as a key factor in strengthening the protection of air bases, based on theoretical, doctrinal, regulatory, and institutional review, as well as on the perceptions of personnel belonging to the Air Base Security and Defense Specialty. This objective made it possible to establish the relationship between human talent, leadership, welfare, training, competency-based management, and operational effectiveness in the performance of critical security functions.

For the development of the study, theoretical, doctrinal, regulatory, and institutional review, as well as a survey applied to 104 members of the Air Base Security and Defense Specialty, were used as instruments. The review made it possible to articulate contributions on human talent, competency-based management, leadership, operational safety, and the human factor. In this regard, Chiavenato (2011) understands human talent as a set of knowledge, skills, attitudes, and values that provide strategic value to the organization; Dessler (2015) highlights the importance of personnel selection, training, and evaluation based on competencies; Ulrich et al. (2007) link human management to institutional strategy; Reason (2016) warns about the influence of the human factor on organizational risks; and Hollnagel (2014) emphasizes people's adaptive capacity to sustain safety in complex environments.

In addition, the survey made it possible to identify personnel perceptions regarding motivation, welfare, leadership, training, response capacity, and recovery conditions. However, as a pending phase of the research, a focus group with active and retired experts in air base security

and defense, with institutional experience, was planned in order to deepen the preliminary findings, contrast the information collected, and strengthen the final proposal of the study.

The preliminary findings showed that human talent should not have been understood merely as an administrative resource, but as a strategic component of the security and defense system. The survey showed that motivation and welfare influenced operational performance and personnel response capacity; it also identified less favorable perceptions regarding respect for compensatory rest periods after service, an aspect that could affect physical and mental recovery. It was also found that military leadership, continuous training, and competency-based management influenced cohesion, discipline, institutional commitment, and the reduction of human, physical, technological, and operational vulnerabilities.

Consequently, it is concluded that the protection of air bases does not begin with the camera, the sensor, the barrier, or the response system; it begins with the person who observes, interprets, decides, and acts when the mission requires it. This research shows that human talent is not a secondary support element of the security system, but the point where doctrine, technology, leadership, and operations become a real protection capability. Therefore, strengthening the selection, training, motivation, welfare, and leadership of Air Base Security and Defense personnel means reducing vulnerabilities before they materialize, increasing response capacity, and more solidly protecting the strategic assets of the Colombian Aerospace Force. The central contribution of the study consists of demonstrating that caring for and better managing personnel not only improves individual performance, but also strengthens the defense of the Nation's air, space, and cyberspace power. As an associated product, this research contributes to the book chapter entitled Human Talent Management in the Security and Defense of Air Bases, prepared within the framework of the commemoration of the 100th anniversary of the Security and Defense of Bases Specialty, as well as to the formative research process of the Master's Degree in Direction and Management of Comprehensive Security at the Colombian Aerospace Force Postgraduate School.

Keywords: air bases, competency-based management, comprehensive security, human talent, institutional welfare, military leadership.

Referencias

Chiavenato, I. (2011). Administración de recursos humanos: El capital humano de las organizaciones. McGraw-Hill.

Dessler, G. (2015). Administración de recursos humanos. Pearson Educación.

Fuerza Aérea Colombiana. (2020). Doctrina básica aérea, espacial y ciberespacial. Fuerza Aérea Colombiana.

Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate.

Organización de Aviación Civil Internacional. (2018). Manual de gestión de la seguridad operacional. OACI.

Organización del Tratado del Atlántico Norte. (2016). AJP-3.14 Allied joint doctrine for force protection. NATO Standardization Office.

Reason, J. (2016). Managing the risks of organizational accidents. Routledge.

Ulrich, D., Brockbank, W., Johnson, D., Sandholtz, K., & Younger, J. (2007). HR competencies: Mastery at the intersection of people and business. Society for Human Resource Management.

Modelo de vigilancia estatal de ciberseguridad para proveedores de servicios de tránsito aéreo

Ing. Isleny López Chaquea

Isleny López Chaquea: Ingeniera Industrial, candidata a Magíster en Dirección y Gestión de la Seguridad Integral, Escuela de Postgrados de la Fuerza Aeroespacial Colombiana (EPFAC). Inspectora de seguridad de la aviación civil de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC — Aerocivil), adscrita a la Dirección de Autoridad a la Seguridad de Aviación Civil de la Secretaría de Autoridad Aeronáutica. Su trabajo de grado se enfoca en el diseño de un modelo de vigilancia de la ciberseguridad aplicado a los sistemas CNS-MET de los Proveedores de Servicios de Tránsito Aéreo (ATSP), en coherencia con los estándares de la Organización de Aviación Civil Internacional (OACI) en el dominio AVSEC.

Correo electrónico institucional: isleny.lopez@aerocivil.gov.co

Correo electrónico personal: islenycha@hotmail.com

Línea de investigación: Modelos de Seguridad Integral

Resumen

La presente investigación abordó la ausencia de una herramienta técnica formalizada que permitiera a la Dirección de Autoridad a la Seguridad de Aviación Civil de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC) ejercer vigilancia estructurada, sistemática y continua sobre la ciberseguridad de los sistemas de Comunicaciones, Navegación, Vigilancia y Meteorología (CNS-MET) de los Proveedores de Servicios de Tránsito Aéreo (ATSP) en Colombia. Si bien el Reglamento Aeronáutico Colombiano (RAC) 160 (UAEAC, 2025a) y su Adjunto de Ciberseguridad (UAEAC, 2025b) establecen los requisitos de ciberseguridad que los ATSP deben cumplir, la autoridad aeronáutica carecía del instrumento necesario para verificar dicho cumplimiento de manera estructurada. Esta brecha resultó crítica en un contexto en el que, durante 2025, se registraron más de veintisiete millones de intentos de ciberataques contra los sistemas aeronáuticos colombianos, según datos de la Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea (DTANA), evidenciando un entorno de amenazas persistente y sofisticado.

La investigación adoptó un enfoque mixto, predominantemente cualitativo, de tipo descriptivo y aplicado (Bernal, 2022), con un componente cuantitativo en la fase de validación del modelo. La recolección de información se estructuró mediante seis instrumentos

complementarios. El primero consistió en una matriz de correspondencia normativa construida en Excel y procesada computacionalmente en Python mediante Google Colab, que cruzó los requisitos del Adjunto de Ciberseguridad al RAC 160 con los marcos ISO/IEC 27001 (ISO, 2022), NIST CSF 2.0 (NIST, 2024), IEC 62443 (IEC, 2022), NIST SP 800-53 Rev. 5 y AS/NAS 9933, mediante análisis descriptivo, mapas de calor, dendrograma de clustering jerárquico y similitud Jaccard.

El segundo correspondió a una ficha de benchmarking documental aplicada a las autoridades de mayor madurez en vigilancia de ciberseguridad aeronáutica —CAA UK (CAP1753), EASA (Part-IS) y TSA—, en proceso de análisis. El tercero fue una encuesta estructurada con preguntas mixtas —escala Likert y preguntas abiertas— diseñada para expertos de autoridades aeronáuticas de la región SAM de la OACI (Sur America), adoptada en lugar de la entrevista semiestructurada dada la complejidad logística de coordinar agendas internacionales (Hernández-Sampieri et al., 2018; Creswell & Creswell, 2023), en proceso de aplicación.

El cuarto instrumento correspondió a entrevistas semiestructuradas aplicadas a ocho de los trece inspectores de seguridad de la aviación civil certificados de la UAEAC, analizadas mediante codificación cualitativa en tres niveles: abierta, axial y selectiva. El quinto fue una entrevista en profundidad por sesiones (Kvale & Brinkmann, 2015) aplicada al informante clave de la jefatura responsable de la ciberseguridad de los sistemas CNS-MET del ATSP colombiano, en calidad de actor objeto de vigilancia. El sexto instrumento, un cuestionario de validación tipo Likert con análisis de consistencia interna mediante alfa de Cronbach, se encontraba pendiente de aplicación a los ocho inspectores AVSEC como jueces de expertos, una vez diseñado el modelo.

El análisis de la matriz normativa identificó un núcleo común de requisitos de ciberseguridad presentes en todos los marcos —gestión de riesgos, control de accesos, gestión de incidentes, continuidad operacional y formación del personal—, y reveló que la cadena de suministro tecnológica, la segmentación de redes IT/OT y la verificación de controles específicos para entornos de Tecnología Operacional (OT) constituían los dominios con mayor brecha normativa en el marco colombiano. Las entrevistas a los inspectores AVSEC permitieron identificar siete categorías centrales: experiencia y rol del inspector, enfoques de vigilancia, importancia de la ciberseguridad, retos y limitaciones, capacidades y herramientas, elementos deseables del modelo e implementación gradual.

Los hallazgos más relevantes incluyeron la coexistencia de enfoques de vigilancia sin articulación metodológica formal, la ausencia de herramientas específicas para entornos OT/CNS-MET y brechas significativas en la formación técnica de los inspectores. La entrevista a

la jefatura del ATSP reveló que dicha entidad contaba con una infraestructura de ciberseguridad más robusta de lo que los inspectores percibían —con centro de operaciones de seguridad (SOC/NOC) operativo las veinticuatro horas, herramientas especializadas y convenios con el Centro de Comando Cibernético—, y confirmó un hallazgo crítico: el área de ciberseguridad del ATSP no conocía completamente los sistemas OT/CNS-MET que protegía, evidenciando una brecha de integración interna IT/OT directamente relacionada con el problema de investigación. La triangulación entre ambos instrumentos aplicados confirmó la brecha de vigilancia desde las dos perspectivas y validó el enfoque basado en riesgo con priorización de la disponibilidad sobre la confidencialidad, propio de los entornos OT aeronáuticos.

Estos hallazgos permiten concluir que la ausencia de un modelo de vigilancia específico generaba una brecha entre los compromisos internacionales asumidos por Colombia ante la OACI —evaluados mediante el Programa Universal de Auditoría de Seguridad de la Aviación con Enfoque de Monitoreo Continuo (USAP-CMA) (OACI, 2023)— y la capacidad operativa de la autoridad aeronáutica para garantizar su cumplimiento.

La revisión documental comparada indicó que las autoridades de mayor madurez habían evolucionado de modelos de auditoría estática hacia esquemas de vigilancia basada en riesgo con monitoreo continuo, lo que constituyó la dirección metodológica del modelo propuesto. El producto principal de la investigación es un modelo de vigilancia estatal de la ciberseguridad para los ATSP, articulado en dimensiones de proceso, madurez y referencia normativa, con seis dominios funcionales de evaluación: gobernanza, protección de redes y sistemas IT/OT, monitoreo y detección continua, respuesta a incidentes y continuidad operacional, gestión de la cadena de suministro tecnológico, y formación y cultura de ciberseguridad el cual está en construcción.

Su impacto se proyectó en tres planos: en el regulatorio, dotando a la Dirección de Autoridad a la Seguridad de Aviación Civil de una herramienta operativa para ejercer su función AVSEC conforme al RAC 160; en el técnico, fortaleciendo la resiliencia de los sistemas aeronáuticos colombianos frente a ciberamenazas; y en el académico, aportando un marco metodológico replicable en otros Estados de la región SAM de la OACI y en contextos de infraestructura crítica.

Palabras clave: ATSP, AVSEC, ciberseguridad, CNS-MET, tránsito aéreo, vigilancia estatal.

Abstract

This study addressed the lack of a formalized technical tool that would enable the Civil Aviation Safety Authority Directorate of the Special Administrative Unit for Civil Aviation (UAEAC) to conduct structured, systematic, and continuous oversight of the cybersecurity of the Communications, Navigation, Surveillance, and Meteorology (CNS-MET) systems of Air Traffic Service Providers (ATSPs) in Colombia. Although Colombian Aeronautical Regulation (RAC) 160 (UAEAC, 2025a) and its Cybersecurity Annex (UAEAC, 2025b) establish the cybersecurity requirements that ATSPs must meet, the aeronautical authority lacked the necessary instrument to verify such compliance in a structured manner. This gap proved critical in a context where, during 2025, more than twenty-seven million cyberattack attempts were recorded against Colombian aeronautical systems, according to data from the Directorate of Telecommunications and Air Navigation Aids (DTANA), highlighting a persistent and sophisticated threat environment.

The research adopted a mixed-methods approach, predominantly qualitative, descriptive, and applied in nature (Bernal, 2022), with a quantitative component during the model validation phase. Data collection was structured using six complementary instruments. The first consisted of a regulatory correspondence matrix built in Excel and processed computationally in Python using Google Colab, which cross-referenced the requirements of the Cybersecurity Annex to RAC 160 with the ISO/IEC 27001 (ISO, 2022), NIST CSF 2.0 (NIST, 2024), IEC 62443 (IEC, 2022), NIST SP 800-53 Rev. 5, and AS/NAS 9933, using descriptive analysis, heat maps, hierarchical clustering dendrograms, and Jaccard similarity.

The second involved a documentary benchmarking checklist applied to the most mature authorities in aviation cybersecurity oversight—CAA UK (CAP1753), EASA (Part-IS), and TSA—currently under analysis. The third was a structured survey with mixed questions—Likert scale and open-ended questions—designed for experts from aviation authorities in the ICAO SAM region (South America), adopted in place of the semi-structured interview given the logistical complexity of coordinating international schedules (Hernández-Sampieri et al., 2018; Creswell & Creswell, 2023), currently being administered.

The fourth instrument consisted of semi-structured interviews conducted with eight of the thirteen certified civil aviation security inspectors from the UAEAC, which were analyzed using three levels of qualitative coding: open, axial, and selective. The fifth was a session-based in-depth interview (Kvale & Brinkmann, 2015) conducted with the key informant from the department responsible for cybersecurity of the CNS-MET systems at the Colombian ATSP, in his capacity as a subject of surveillance. The sixth instrument, a Likert-type validation questionnaire with internal

consistency analysis using Cronbach's alpha, was pending administration to the eight AVSEC inspectors as expert judges, once the model had been designed.

The analysis of the regulatory matrix identified a common core of cybersecurity requirements present in all frameworks—risk management, access control, incident management, business continuity, and staff training— and revealed that the technology supply chain, IT/OT network segmentation, and verification of specific controls for Operational Technology (OT) environments constituted the domains with the greatest regulatory gaps in the Colombian framework. Interviews with AVSEC inspectors identified seven key categories: inspector experience and role, monitoring approaches, the importance of cybersecurity, challenges and limitations, capabilities and tools, desirable elements of the model, and phased implementation.

The most significant findings included the coexistence of monitoring approaches lacking formal methodological coordination, the absence of specific tools for OT/CNS-MET environments, and significant gaps in the technical training of inspectors. The interview with ATSP leadership revealed that the agency had a more robust cybersecurity infrastructure than inspectors perceived—with a security operations center (SOC/NOC) operating 24 hours a day, specialized tools, and agreements with the Cyber Command Center—and confirmed a critical finding: the ATSP's cybersecurity division did not fully understand the OT/CNS-MET systems it was protecting, highlighting an internal IT/OT integration gap directly related to the investigation's findings. The triangulation of the two applied methodologies confirmed the oversight gap from both perspectives and validated the risk-based approach prioritizing availability over confidentiality, which is characteristic of aviation OT environments.

These findings lead to the conclusion that the absence of a specific oversight model created a gap between the international commitments made by Colombia to the ICAO—assessed through the Universal Safety Audit Program with a Continuous Monitoring Approach (USAP-CMA) (ICAO, 2023)—and the aviation authority's operational capacity to ensure compliance.

The comparative literature review indicated that more mature authorities had evolved from static audit models toward risk-based oversight schemes with continuous monitoring, which constituted the methodological direction of the proposed model. The main output of the research is a state cybersecurity oversight model for ATSPs, structured around process, maturity, and regulatory reference dimensions, with six functional assessment domains: governance, IT/OT network and system protection, continuous monitoring and detection, incident response and operational continuity, technology supply chain management, and cybersecurity training and culture, which is currently under development.

Its impact was felt on three levels: at the regulatory level, by providing the Civil Aviation Security Authority with an operational tool to carry out its AVSEC functions in accordance with RAC 160; technically, by strengthening the resilience of Colombia's aeronautical systems against cyber threats; and academically, by providing a methodological framework that can be replicated in other States of the ICAO SAM region and in critical infrastructure contexts.

Keywords: ATSP, AVSEC, cybersecurity, CNS-MET, air traffic, state oversight.

Referencias

Bernal, C. A. (2022). *Metodología de la investigación: administración, economía, humanidades y ciencias sociales* (5.^a ed.). Pearson Educación.

Civil Aviation Authority. (2024). *CAA cyber security oversight strategy 2024–2026 (CAP1753)*. Civil Aviation Authority. <https://www.caa.co.uk/publication/download/21294>

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2018). *Metodología de la investigación* (6.^a ed.). McGraw-Hill Education.

International Electrotechnical Commission. (2022). *IEC 62443 series: Security for industrial automation and control systems*. IEC. <https://www.iec.ch/taxonomy/term/778>

International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. <https://www.iso.org/standard/27001>

Kvale, S., & Brinkmann, S. (2015). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE Publications.

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework 2.0 (NIST CSWP 29)*. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

Organización de Aviación Civil Internacional. (2022). *Plan de acción de ciberseguridad de la aviación — Cybersecurity action plan (CyAP, 2.^a ed.)*. OACI. <https://www.icao.int/aviation-cybersecurity/action-plan>

Organización de Aviación Civil Internacional. (2023). *Programa Universal de Auditoría de Seguridad de la Aviación con Enfoque de Monitoreo Continuo (USAP-CMA)*. OACI. <https://www.icao.int/security/avsec/Pages/USAP.aspx>

Unidad Administrativa Especial de Aeronáutica Civil. (2025a). Resolución 0189 de 2025, por la cual se modifica la norma RAC 160 — Seguridad de la aviación civil de los Reglamentos Aeronáuticos de Colombia. *Diario Oficial de Colombia*. <https://www.suin-juriscol.gov.co/clp/contenidos.dll/Resolucion/30054525>

Unidad Administrativa Especial de Aeronáutica Civil. (2025b). *Adjunto de ciberseguridad al RAC 160 — Seguridad de la aviación civil* [Documento de información pública reservada conforme al artículo 74 de la Constitución Política de Colombia y al numeral 2.14 del Anexo 17 de la OACI]. UAEAC — Aerocivil.

Alineación de la Fuerza Aeroespacial Colombiana ante la Organización del Tratado del Atlántico Norte

CT. Gabriel Enrique Useche Ramos

Gabriel Enrique Useche Ramos: Administrador Aeronáutico, Maestrante en Dirección y Gestión de la Seguridad Integral de la Escuela de Postgrados de la Fuerza Aeroespacial Colombiana (EPFAC). Actualmente se desempeña como comandante del Escuadrón de Comandos Especiales Aéreos del Grupo de Operaciones Especiales Aéreas de la Fuerza Aeroespacial Colombiana (FAC). Cuenta con amplia experiencia operativa y técnica en procesos de estandarización e interoperabilidad, destacándose su participación en las fases de evaluación y certificación de capacidades institucionales bajo el programa Operational Capability Concept Evaluation and Feedback (OCC E&F) de la OTAN, con énfasis en el área de Protección a la Fuerza (Force Protection).

Correo electrónico institucional: gabriel.useche@fac.mil.co

Línea de investigación: Modelos de Seguridad Integral

Resumen

La presente investigación abordó el desafío estratégico que enfrentó la Fuerza Aeroespacial Colombiana (FAC) en su proceso de alineación e interoperabilidad con los estándares de la Organización del Tratado del Atlántico Norte (OTAN), el alcance del estudio se delimitó específicamente en el área de Protección a la Fuerza (Force Protection) bajo el programa Operational Capability Concept Evaluation and Feedback (OCC E&F) (Supreme Headquarters Allied Powers Europe [SHAPE], 2024). El problema central identificado radicó en la existencia de brechas críticas en términos de estandarización doctrinal, entrenamiento, procedimientos y documentación que dificultaron el cumplimiento de los requisitos de certificación para capacidades estratégicas como el reabastecimiento aéreo (AAR), la búsqueda y rescate en combate (C-SAR) y los servicios de tránsito aéreo (ATS). Esta problemática comprometió la interoperabilidad táctica y restringió la proyección internacional de la institución como socio global de la Alianza. (Carrasquilla & Acevedo, 2021).

Metodológicamente, la investigación se fundamentó en un enfoque mixto con un diseño de triangulación concurrente, lo que permitió la recolección y el análisis simultáneo de datos cuantitativos y cualitativos para efectuar una validación cruzada (Hernández-Sampieri & Mendoza, 2018). La población del estudio estuvo integrada por 55 funcionarios vinculados al proceso de certificación, de los cuales se seleccionó una muestra no probabilística dirigida a 16 expertos (Subject matter expert) con experiencia real en evaluaciones nacionales e internacionales de la OTAN.

Los instrumentos aplicados incluyeron una exhaustiva revisión de 47 Acuerdos de Estandarización (STANAG) y Publicaciones Tácticas Aliadas, así como 82 documentos de la doctrina nacional, entrevistas semiestructuradas y matrices de análisis de brechas con listas de verificación. Este diseño proporcionó la realidad objetiva de los requisitos técnicos y la realidad subjetiva de las experiencias y buenas prácticas del personal durante las evaluaciones.

Los resultados de la investigación permitieron identificar como primera medida, los requisitos técnicos para la certificación del área de Force Protection, definiendo una estructura jerárquica de 293 componentes de evaluación, desglosados en 8 tareas, 35 subtareas y 250 elementos de verificación (FAC,2025). El análisis cuantitativo reveló que la tarea de recuperación (Recovery) fue la más extensa de la evaluación, seguida por las habilidades básicas individuales comunes (ICCS), lo que ratificó que la protección a la fuerza es una responsabilidad transversal de todo el personal.

En segundo lugar, mediante la comparación de la doctrina nacional frente a la Publicación Conjunta Aliada 3.14, (NATO, 2024) se determinó una brecha real de interoperabilidad del 28.7 %. Este hallazgo evidenció una disparidad crítica entre la autoevaluación de nivel uno SEL-1, que reportó un cumplimiento del 94.5%, y la evaluación de la OTAN de nivel uno NEL-1, que evidenció un cumplimiento del 71.3%. Dicha discrepancia obedeció a la mayor rigurosidad y al juicio profesional de los evaluadores internacionales, quienes demandaron precisión en la jerarquía doctrinal y años de experticia en el área de Force Protection. (FAC,2024).

En tercer lugar, como respuesta a los vacíos identificados, se consolidó un conjunto de 13 buenas prácticas unificadas adaptadas al contexto colombiano. Entre las propuestas más relevantes destacaron la implementación de una gobernanza y sincronización operativa para articular las áreas de operaciones (OPS), logística (LOG) y protección a la fuerza (FP); la adopción del bilingüismo aplicado bajo el estándar del Acuerdo de Estandarización (STANAG 6001) (NATO, 2024) para la elaboración de reportes y comunicaciones de mando y control (C2); y el fortalecimiento del entrenamiento en habilidades básicas individuales comunes (ICCS) con trazabilidad digital y énfasis en competencias observables y evaluables. Asimismo, se identificó

la necesidad de una secuenciación de evaluación de las capacidades para evitar la sobreextensión institucional al intentar certificar múltiples áreas simultáneamente sin el soporte suficiente de recursos y personal.

El significado de estos hallazgos sugirió que alcanzar la certificación requerirá una transformación cultural y operativa profunda que convertirá los estándares internacionales en hábitos institucionales cotidianos a todo nivel. La brecha detectada indicó que la institución deberá transitar hacia una estandarización inteligente, donde la doctrina sea homogénea, los procesos de mando y control deben ser resilientes y el talento humano cuente con las competencias necesarias para operar sin barreras idiomáticas. En conclusión, la implementación de estas 13 buenas prácticas que no han sido implementadas permitirá una hoja de ruta estratégica que fortalecerá la seguridad física, la resiliencia y la credibilidad de la Fuerza Aeroespacial Colombiana, en su proceso de posicionamiento como un socio global confiable capaz de proyectar su poder aéreo y espacial en misiones de coalición multinacional con los más altos estándares internacionales.

El impacto de esta investigación residió en proporcionar a la Fuerza Aeroespacial Colombiana una hoja de ruta estratégica y técnica de alto valor institucional para cerrar las brechas de interoperabilidad detectadas en el área de Force Protection y garantizar el éxito en futuras evaluaciones internacionales bajo el programa OCC E&F. El estudio también facilitó la transición de una doctrina empírica hacia un modelo sólido de Force Protection que se armonizó con el estándar AJP-3.14, permitiendo la protección efectiva del componente físico del Poder Aéreo, Espacial y Ciberespacial. (FAC, 2020).

Como productos asociados derivados de esta investigación se generó un conjunto de trece buenas prácticas unificadas adaptadas al contexto operativo nacional y un Handbook enfocado a ICCS bajo los estándares de la OTAN, diseñados para transformar la experiencia operativa en una capacidad institucional transferible. Asimismo, se suministró una matriz de análisis de brechas (GAP) , una Matriz SWOT-DOFA, una matriz de clasificación documental nacional y de la OTAN las cuales fueron un insumo para la estandarización de necesidades de las unidades evaluadas en las capacidades AAR, C-SAR y ATS, Estos instrumentos se posicionaron como herramientas de planeamiento y supervisión esenciales para alcanzar una estandarización inteligente que proyectara a la institución como un referente regional en seguridad y defensa estratégica.

Palabras clave: Interoperabilidad, certificación, OTAN, Protección a la fuerza, Programa de Evaluación y Retroalimentación del Concepto de Capacidades Operativas.

Abstract

This research addressed the strategic challenge faced by the Colombian Aerospace Force (FAC) in its process of alignment and interoperability with the standards of the North Atlantic Treaty Organization (NATO). The scope of the study was specifically delimited to the area of Force Protection under the Operational Capability Concept Evaluation and Feedback (OCC E&F) Programme (Supreme Headquarters Allied Powers Europe [SHAPE], 2024). The central problem identified was the existence of critical gaps in doctrinal standardization, training, procedures, and documentation, which hindered compliance with certification requirements for strategic capabilities such as Air-to-Air Refuelling (AAR), Combat Search and Rescue (C-SAR), and Air Traffic Services (ATS). This issue compromised tactical interoperability and restricted the institution's international projection as a global partner of the Alliance (Carrasquilla & Acevedo, 2021).

Methodologically, the research was based on a mixed-methods approach with a concurrent triangulation design, which enabled the simultaneous collection and analysis of quantitative and qualitative data for cross-validation purposes (Hernández-Sampieri & Mendoza, 2018). The study population consisted of 55 personnel directly involved in the certification process, from which a purposive non-probability sample of 16 Subject Matter Experts (SMEs) was selected, all with real experience in national and international evaluations conducted under the North Atlantic Treaty Organization framework. The instruments applied included an exhaustive review of 47 Standardization Agreements (STANAGs) and Allied Tactical Publications, as well as 82 national doctrine documents, semi-structured interviews, and gap analysis matrices supported by checklists. This design provided both the objective reality of the technical requirements and the subjective reality of the experiences and best practices of personnel during the evaluation processes.

The research findings first enabled the identification of the technical requirements for certification in the Force Protection area, defining a hierarchical structure of 293 evaluation components, broken down into 8 tasks, 35 subtasks, and 250 verification elements (FAC, 2025). The quantitative analysis revealed that the Recuperation task was the most extensive component of the evaluation, followed by Individual Common Core Skills (ICCS), confirming that Force Protection is a cross-cutting responsibility of all personnel. Secondly, through the comparison of national doctrine against Allied Joint Publication 3.14 (NATO, 2024), an actual interoperability gap of 28.7% was determined. This finding revealed a critical disparity between the Self-Evaluation

Level 1 (SEL-1), which reported 94.5% compliance, and the NATO Evaluation Level 1 (NEL-1), which reflected 71.3% compliance. This discrepancy was attributed to the greater rigor and professional judgment of international evaluators, who required accuracy in doctrinal hierarchy and years of expertise in the field of Force Protection (FAC, 2024).

Thirdly, in response to the gaps identified, a set of 13 unified best practices adapted to the Colombian context was consolidated. Among the most relevant proposals were the implementation of governance and operational synchronization mechanisms to articulate the areas of Operations (OPS), Logistics (LOG), and Force Protection (FP); the adoption of applied bilingualism under Standardization Agreement STANAG 6001 (NATO, 2024) for the preparation of reports and command and control (C2) communications; and the strengthening of Individual Common Core Skills (ICCS) training through digital traceability and an emphasis on observable and assessable competencies. Likewise, the need for a sequenced capability evaluation process was identified in order to prevent institutional overextension when attempting to certify multiple areas simultaneously without sufficient resource and personnel support.

The significance of these findings suggested that achieving certification required a deep cultural and operational transformation, converting international standards into routine institutional practices at all levels. The gap identified indicated that the institution had to transition toward intelligent standardization, where doctrine was homogeneous, command and control processes were resilient, and human talent possessed the required competencies to operate without language barriers. In conclusion, the implementation of these 13 best practices constituted a strategic roadmap that strengthened the physical security, resilience, and credibility of the Colombian Aerospace Force in its process of positioning itself as a reliable global partner capable of projecting its air and space power in multinational coalition missions under the highest international standards.

The impact of this research lay in providing the Colombian Aerospace Force with a high-value strategic and technical roadmap to close the interoperability gaps identified in the Force Protection area and to ensure success in future international evaluations under the OCC E&F Programme. The study also facilitated the transition from an empirical doctrine toward a robust Force Protection model harmonized with AJP-3.14, enabling the effective protection of the physical component of Air, Space, and Cyberspace Power (FAC, 2020).

As associated products derived from this research, a set of thirteen unified best practices adapted to the national operational context was delivered, designed to transform operational experience into a transferable institutional capability. Likewise, a Gap Analysis Matrix, a SWOT-DOFA Matrix, and a national and NATO documentary classification matrix were provided, serving

as inputs for the standardization of the needs of the evaluated units in the AAR, C-SAR, and ATS capabilities. These instruments were positioned as essential planning and supervision tools to achieve intelligent standardization, projecting the institution as a regional benchmark in strategic security and defense.

Keywords: Interoperability, certification, NATO, Force Protection, Operational Capability Concept Evaluation and Feedback Programme.

Referencias

Carrasquilla Acevedo, P. A. (2021). Capacidades distintivas de la FAC como elementos de disuasión en el marco de cooperación con la OTAN. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, 16(1), 49–76. <https://doi.org/10.18359/ries.5255>

Fuerza Aeroespacial Colombiana. (2024). *Informe de autoevaluación SEL-1 del Programa OCC E&F*. Oficina de Asuntos Internacionales.

Fuerza Aeroespacial Colombiana. (2025). *Informe de evaluación NEL-1 del Programa OCC E&F*. Oficina de Asuntos Internacionales.

Fuerza Aérea Colombiana. (2020). Manual de doctrina básica aérea, espacial y ciberespacial -DBAEC- (5.^a ed.). Departamento Estratégico de Doctrina Aérea y Espacial

Hernández-Sampieri, R., y Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.

NATO Standardization Office. (2024, 21 de octubre). *Allied joint publication-3.14: allied joint doctrine for force protection* (Edición B, Versión 1). NSO.

Supreme Headquarters Allied Powers Europe. (2024, abril). *Operational Capabilities Concept Evaluation and Feedback (OCC E&F) programme handbook* (Versión 5.1). SHAPE.