Ciberseguridad en la operación y protección de las aeronaves BELL del Ejército Nacional

Mayor (EJC) Luis Alberto Chavarro Gutiérrez

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

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

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Luis Alberto Chavarro Gutiérrez
Identificación	**:**	1032396466
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Jairo Andrés Becerra Cuervo
Tutor temático	**:**	Jaider Ospina Navas
Fecha de entrega	**:**	16 Octubre 2025
Extensión	**:**	8000 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

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

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

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

AUTORIZACIÓN DE PUBLICACIÓN

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

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

Ciberseguridad en la operación y protección de las aeronaves BELL del Ejército Nacional

Cybersecurity in the Operation and Protection of BELL Aircraft of the Colombian Army

Luis Alberto Chavarro Gutiérrez[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente artículo analiza el papel de la ciberseguridad en la protección y operación de las aeronaves BELL del Ejército Nacional de Colombia. Desde un enfoque cualitativo y con base en análisis documental, se describen las principales amenazas cibernéticas que enfrentan estos sistemas, así como los mecanismos de protección implementados o requeridos. El estudio identifica factores normativos, tecnológicos y operativos que inciden en la seguridad digital de las aeronaves, con especial énfasis en la articulación interinstitucional y la adaptación de estándares internacionales. Como resultado, se destaca la necesidad de fortalecer las capacidades en ciberdefensa, implementar medidas preventivas y consolidar un modelo integral que permita responder eficazmente ante riesgos emergentes, contribuyendo a la continuidad operativa y la soberanía tecnológica nacional.

Palabras clave: Aeronaves militares; ciberdefensa; ciberseguridad; Ejército Nacional; infraestructura crítica; seguridad informática.

Abstract: This article analyzes the role of cybersecurity in the protection and operation of BELL aircraft used by the Colombian Army. Through a qualitative approach and based on documentary analysis, the main cyber threats affecting these systems are described, as well as the protection mechanisms implemented or needed. The study identifies regulatory, technological, and operational factors that influence the digital security of aircraft, with a focus on institutional coordination and the adaptation of international standards. The findings highlight the need to strengthen cyber defense capabilities, adopt preventive measures, and consolidate an integrated model to effectively address emerging risks, thus ensuring operational continuity and national technological sovereignty.

Keywords: Critical infrastructure; cyber defense; cybersecurity; military aircraft; national army; information security.

.

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

Introducción

En el contexto de la defensa nacional, la protección de infraestructuras críticas ha dejado de ser un concepto exclusivo del ámbito físico. Hoy en día, el ciberespacio se ha consolidado como un dominio estratégico donde las amenazas digitales pueden comprometer la estabilidad operativa de los sistemas militares (Madrigal & García , 2021). Las aeronaves BELL del Ejército Nacional, por su creciente digitalización, se han convertido en activos tácticos vulnerables a riesgos cibernéticos, abriendo un nuevo frente de atención en la ciberseguridad aeronáutica militar, tal cual como lo indica Salamanca et al., (2022).

En las dos últimas décadas, el incremento en los niveles de tecnificación e interdependencia digital en el sector defensa ha multiplicado las superficies de ataque. Eventos internacionales como los ciberataques a Georgia (2008), Irán (2010) o Ucrania (2017), han demostrado el poder disruptivo del ciberespacio sobre plataformas militares (VIU, 2025). En el caso colombiano, a esto se suman factores como la obsolescencia tecnológica de ciertos equipos, las limitaciones presupuestales, y la necesidad de fortalecer una doctrina nacional de ciberdefensa alineada con estándares internacionales.

En este contexto, se hace necesario analizar cómo la ciberseguridad puede fortalecer la operación y protección de las aeronaves BELL del Ejército Nacional, abordando los desafíos técnicos, organizacionales y normativos que enfrenta la institución. Este artículo, basado en una metodología cualitativa de revisión documental, responde a esta inquietud mediante tres objetivos: describir las principales amenazas cibernéticas, identificar los mecanismos de protección actuales o requeridos, y analizar los factores operativos y tecnológicos que inciden en su seguridad digital (Rivas, 2025).

Metodología

El presente estudio adopta un enfoque cualitativo, alineado con los principios expuestos por Altamirano y Meléndez (2021), el cual busca explorar y comprender a profundidad fenómenos complejos como la ciberseguridad aplicada a la protección de infraestructuras críticas. Este enfoque se basa en análisis metódico de fuentes documentales y normativas, permitiendo identificar relaciones, patrones y riesgos específicos del entorno militar.

El diseño de investigación es de tipo exploratorio-descriptivo, ideal para abordar temas poco investigados en el contexto nacional, como la protección cibernética de las aeronaves BELL del Ejército Nacional. La revisión documental estructurada se compone de estudios previos, marcos normativos nacionales e internacionales, y experiencias de ciberdefensa relevantes, lo que facilita el desarrollo de un análisis detallado y contextualizado.

Igualmente, el proceso de selección sigue un criterio de pertinencia y se basa en la revisión de bases de datos académicas como Scopus y Google Scholar, además de informes gubernamentales. Este proceso no sigue un muestreo probabilístico, sino un criterio de selección no probabilístico intencional, donde se priorizan fuentes relevantes y actuales. El instrumento de recolección de datos es la ficha de análisis documental, estructurada para clasificar y sistematizar la información obtenida. Cada ficha se organiza según categorías clave: identificación de amenazas, medidas de ciberdefensa, y buenas prácticas aplicables al entorno de la aviación militar (Ortiz, 2022).

Describir las principales amenazas cibernéticas asociadas a las aeronaves BELL en el contexto actual del Ejército Nacional.

Los helicópteros tipo BELL del Ejército Nacional de Colombia desempeñan un papel determinante en las operaciones militares, tanto en tareas de movilidad táctica, evacuaciones aeromédicas, transporte logístico como en misiones de seguridad territorial (Tovar & Figueroa, 2021). Por sus capacidades versátiles, estas plataformas aéreas representan activos estratégicos de alto valor que deben mantenerse operativos incluso en escenarios de conflicto híbrido o guerra irregular. Sin embargo, en el contexto actual de creciente digitalización de los sistemas embarcados y de interdependencia tecnológica, la superficie de exposición cibernética de estas aeronaves se ha ampliado considerablemente, haciendo imperativa su protección no solo física, sino también digital.

En este marco, la ciberseguridad emerge como una dimensión prioritaria dentro de las políticas de defensa y mantenimiento operativo. Las amenazas cibernéticas contra plataformas aéreas pueden comprometer no solo la confidencialidad y disponibilidad de los datos, sino también la integridad funcional de sistemas críticos como navegación, comunicaciones, sensores o software de misión (Acuña & Blanco, 2023). A pesar de ello, las estrategias de protección en muchos entornos militares, especialmente en países en vías de desarrollo, aún no han alcanzado un nivel de madurez suficiente para mitigar estos riesgos de forma integral y continua.

La flota BELL enfrenta retos particulares: la obsolescencia de varios de sus componentes, la ausencia de protocolos de ciberdefensa específicos para aviación, y la limitada conciencia situacional sobre ciberamenazas entre parte del personal técnico y

operativo. A esto se suma la falta de blindaje digital en sistemas de apoyo en tierra, como las estaciones de mantenimiento o las redes de planificación de vuelo, los cuales están conectados directa o indirectamente con las aeronaves (Blanquicet, 2025).

En este primer capítulo se abordan estos desafíos a partir de una descripción sistemática de las principales amenazas cibernéticas asociadas al uso y operación de las aeronaves BELL. La identificación de estas amenazas no solo permite anticipar posibles vectores de ataque, sino que también sirve como base para diseñar estrategias preventivas, adaptativas y sostenibles en el tiempo.

Características operacionales y tecnológicas de las aeronaves BELL

Las aeronaves BELL en operación dentro del Ejército Nacional de Colombia entre ellas los modelos BELL UH-1H-II y UH-1N constituyen plataformas multipropósito que han sido adaptadas para cumplir con diversas misiones militares en terrenos complejos y bajo condiciones de alta exigencia operacional. Estas aeronaves son ampliamente utilizadas por su maniobrabilidad, versatilidad y capacidad de despliegue táctico (Lombardo, 2024).

Los helicópteros BELL incorporan sistemas críticos como el sistema de navegación GPS, radios de comunicación táctica, transpondedores, sensores de misión y, en algunos casos, enlaces digitales de datos para interoperabilidad. Estos componentes están interconectados entre sí y, en ciertos escenarios, con nodos externos como centros de comando, unidades terrestres o plataformas de mantenimiento. Aunque su diseño original no contemplaba plenamente los actuales requisitos de seguridad cibernética, muchos de estos sistemas han sido modernizados parcialmente, lo que ha dado paso a configuraciones híbridas con componentes nuevos coexistiendo con otros más antiguos situación que puede aumentar las vulnerabilidades técnicas, tal cual como lo menciona Díaz et al., (2020).

Uno de los principales vectores de riesgo se encuentra en los sistemas de mantenimiento y carga de datos, que permiten actualizar información de vuelo, cargar planes de misión, verificar condiciones técnicas y diagnosticar fallos. Estos sistemas, al interactuar con computadores portátiles, memorias externas u otros dispositivos móviles, pueden actuar como canales inadvertidos de intrusión si no se implementan medidas de control, autenticación y monitoreo. Tal como lo advertía Benítez (2019), la ausencia de autenticación en las comunicaciones inalámbricas o de cifrado en actualizaciones de software embarcado puede facilitar el ingreso de código malicioso que afecte el comportamiento de los sistemas de navegación o control.

A esto se suma el uso de componentes COTS (Commercial Off-The-Shelf) hardware y software disponibles en el mercado civil que, aunque reducen costos y tiempos de integración, pueden no cumplir con los estándares de ciberresiliencia exigidos en entornos militares. El ciclo de vida corto de estos componentes (hardware de 18 meses, software de 3 a 5 años) contrasta con la vida útil esperada de las aeronaves (más de 25 años), generando brechas técnicas que dificultan su actualización o reacreditación frente a nuevas amenazas (OACI, 2020).

Desde una perspectiva operativa, los helicópteros BELL también pueden verse afectados por la exposición indirecta a sistemas de apoyo en tierra como redes logísticas, estaciones de planificación de vuelo, o centros de comunicación táctica, que, al estar conectados a infraestructuras más amplias (redes militares o civiles), se convierten en puntos de entrada potenciales para ataques cibernéticos que luego escalen hasta las aeronaves.

En este sentido, las imágenes técnicas proporcionadas por el usuario, que muestran vistas estructurales de los helicópteros tipo BELL, permiten visualizar los posibles puntos de

conexión física y lógica: interfaces de mantenimiento ubicadas en cabina, antenas de comunicación no protegidas o compartimientos de acceso a los módulos de software. Estos puntos pueden ser clave para diseñar estrategias defensivas, tanto físicas como cibernéticas, y para establecer una segmentación efectiva entre sistemas vitales (comunicaciones, control de vuelo) y no vitales (multimedia, sensores auxiliares).

De esa manera, las características operacionales y tecnológicas de las aeronaves BELL combinadas con su contexto de uso en zonas de conflicto, su obsolescencia progresiva y su interconexión con sistemas externos las convierten en objetivos vulnerables que requieren una estrategia específica de protección cibernética basada en estándares, monitoreo continuo y capacitación del personal técnico.

En el análisis de las aeronaves BELL como activos estratégicos del Ejército Nacional, se identifican múltiples componentes y subsistemas que, por su naturaleza digital y nivel de interconectividad, representan puntos vulnerables frente a amenazas cibernéticas. En la siguiente tabla se presentan los puntos críticos más relevantes en términos de ciberseguridad, organizados según el tipo de vulnerabilidad asociada y su posible impacto operacional.

Tabla 1 Puntos críticos de ciberseguridad en aeronaves BELL

Componente o Subsistema	Tipo de Vulnerabilidad	Impacto Potencial
Sistema de navegación GPS	Spoofing / Jamming de señal	Pérdida de navegación precisa
Transpondedor ADS-B	Inyección de tráfico / Phantom aircraft	Alteración del espacio aéreo percibido
Estación de mantenimiento en tierra	Malware por equipos no aislados	Compromiso del mantenimiento seguro
Puertos de acceso físico (USB, Ethernet)	Acceso no autorizado / introducción de código malicioso/ SQL injection	Puerta de entrada directa al sistema Modificación de libros históricos de aeronaves Q.C.
Sistema de comunicación táctica (VHF/UHF)	Intercepción o denegación de servicio	Interrupción de comunicaciones críticas
Software de misión	Manipulación o corrupción del código embarcado	Comportamiento anómalo en vuelo

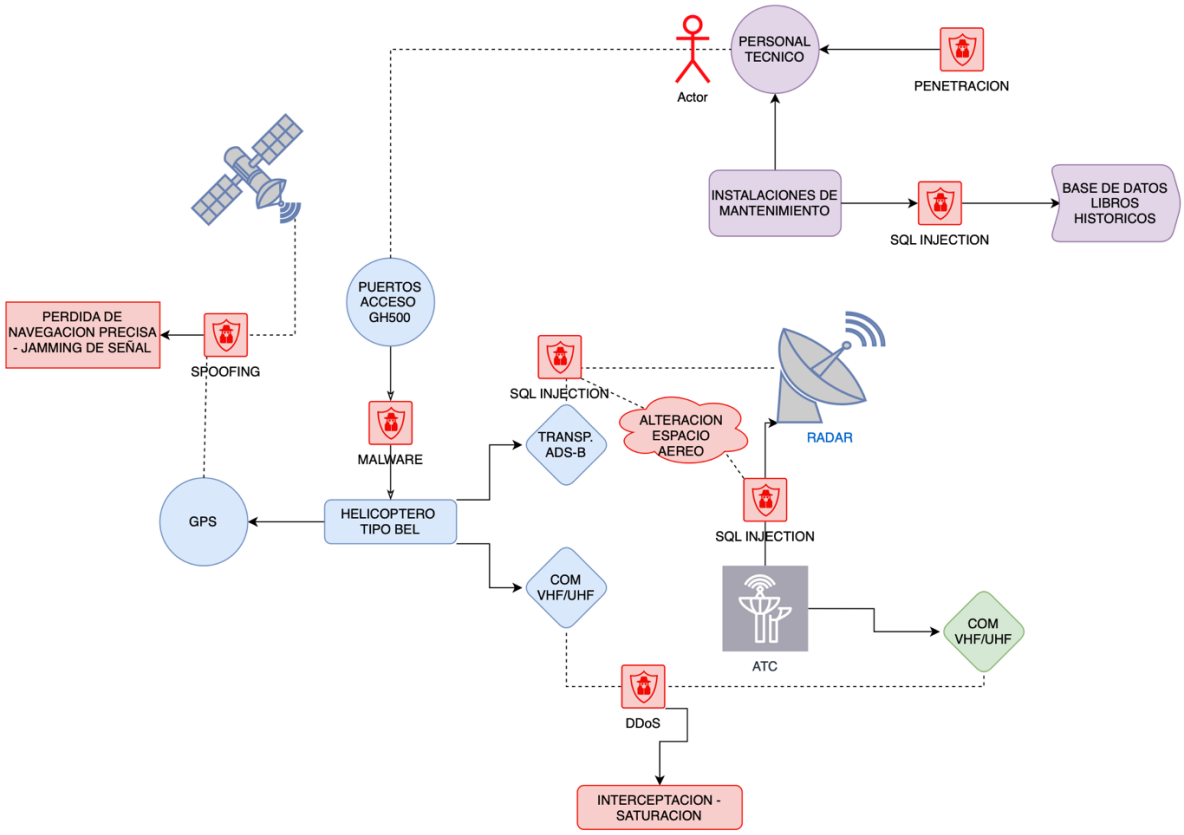
Dispositivos COTS integrados	Obsolescencia técnica / backdoors	Exposición a amenazas sin soporte técnico
Actualizaciones vía memoria portátil	Fuga de datos / infección cruzada	Ingreso de malware persistente
Interfaz hombre-máquina (HMI)	Manipulación de instrucciones por ingeniería social	Decisiones erróneas del piloto

Fuente: Elaboración propia con base en Pérez Benítez, Bonilla y documentación técnica aeronáutica.

Las amenazas cibernéticas que enfrentan las aeronaves BELL incluyen desde interferencias en la navegación por spoofing y jamming, hasta ataques sofisticados como la inyección de datos falsos en el ADS-B o la explotación de accesos físicos no controlados, como puertos USB o ranuras microSD, especialmente en sistemas críticos como el GH-500. Estas vulnerabilidades evidencian la necesidad de un modelo integral de protección que contemple tanto los sistemas embarcados como la infraestructura y los procedimientos de apoyo en tierra (Echeverria, 2023).

El siguiente diagrama de representa la arquitectura integral de los sistemas del helicóptero BELL UH-1H/ UH-1N del Ejército Nacional de Colombia, analizado desde la perspectiva de ciberseguridad operacional.

El modelo ilustra cómo los sistemas críticos de las aeronaves BELL como control de vuelo, navegación y comunicaciones se interrelacionan con elementos de misión y mantenimiento, identificando puntos vulnerables ante amenazas como el spoofing GPS o la inyección de malware. Al mostrar cómo un ataque desde sistemas no vitales puede escalar a componentes esenciales, resalta la urgencia de implementar medidas de segmentación y refuerzo técnico, apoyado en manuales operativos y en los riesgos expuestos en la Tabla 1.



Amenazas cibernéticas en aviación militar según la literatura.

La ciberseguridad en el entorno aeronáutico ha evolucionado rápidamente en los últimos años, principalmente debido al aumento de la interconectividad de los sistemas embarcados y de apoyo en tierra. Este fenómeno ha sido ampliamente documentado por autores como Pérez Benítez (2019) y Ramón Bonilla (2022), quienes coinciden en que la aviación tanto civil como militar enfrenta una creciente exposición a vectores de ataque digital, muchos de ellos invisibles hasta que se materializa una intrusión con consecuencias operacionales.

Entre las amenazas más relevantes identificadas en la literatura se encuentran los ataques de Spoofing, los cuales buscan falsificar las señales de GPS para inducir errores en

la navegación de la aeronave. En un escenario operativo, esto podría significar la desviación intencionada de un helicóptero tipo BELL de su trayectoria original, con riesgos evidentes para la misión y la seguridad de la tripulación. De igual forma, los ataques tipo Jamming pueden inutilizar las señales de navegación satelital mediante interferencias dirigidas, generando pérdida de referencia geoespacial en tiempo real (Blanquicet, 2025).

Por otra parte, el transpondedor ADS-B, encargado de transmitir información de posición y altitud de la aeronave, es vulnerable a la inyección de tráfico falso que puede crear "aeronaves fantasma" en las pantallas de control aéreo, como lo explican las investigaciones de Safe Skies (2018). Esto genera desinformación táctica y eleva el riesgo de colisión o errores en la toma de decisiones.

Los ataques de denegación de servicio distribuido (DDoS) también han sido mencionados por Bonilla (2022) como una amenaza significativa. Aunque estos ataques suelen ser catalogados de complejidad media, su impacto puede ser desproporcionado si afectan sistemas de información aeronáutica como NOTAMs, que son avisos oficiales que comunican información esencial sobre el estado o cambios en instalaciones, servicios o procedimientos aeronáuticos y que pueden afectar la seguridad de las operaciones de vuelo, así como también a los sistemas de mantenimiento o servidores de planificación de vuelo.

El ejemplo del ataque sufrido por la FAA en enero de 2023, donde miles de vuelos fueron cancelados o retrasados debido a la caída de su base de datos, ilustra cómo una interrupción en los sistemas de información puede generar un efecto cascada con consecuencias operativas y políticas (Madrigal & García , 2021).

Otra amenaza emergente identificada es la posible interferencia de tecnologías civiles como el 5G con los sistemas de navegación embarcados. La Organización de Aviación Civil

Internacional (OACI) ha manifestado preocupación por esta interferencia, que podría alterar las señales satelitales utilizadas por las aeronaves durante las fases más críticas del vuelo: despegue y aterrizaje. Este tipo de incidentes no solo compromete la integridad de la operación, sino que representa una amenaza latente de tipo estructural, al estar relacionada con el ecosistema tecnológico circundante.

Por último, los ataques persistentes avanzados (APT, por sus siglas en inglés) representan la amenaza más compleja para los sistemas militares. Estos ataques son desarrollados por actores estatales o grupos con alta capacidad técnica, y buscan infiltrarse en los sistemas de las aeronaves o sus centros de control con fines de espionaje, sabotaje o recopilación de inteligencia. Parra (2024) define estos ataques como conjuntos de tácticas y técnicas diseñadas para mantenerse ocultos en el sistema objetivo durante largos períodos, lo que dificulta su detección y neutralización.

Aunque no se han reportado públicamente ataques APT dirigidos específicamente contra aeronaves BELL, casos como el ocurrido en 2023 contra un avión ruso Beriev A-50, dañado por un ataque coordinado del grupo BYPOL, evidencian la vulnerabilidad de aeronaves militares frente a amenazas cibernéticas y físicas combinadas, lo que refuerza la necesidad de medidas preventivas robustas. (Infobae, 2023).

Además, El grupo TA2541, vinculado a ciberamenazas persistentes avanzadas, ha atacado al sector aeroespacial y de defensa desde 2017 mediante troyanos de acceso remoto (RATs), lo que evidencia la necesidad urgente de fortalecer la ciberseguridad en todas las plataformas aéreas militares, incluidas las aeronaves BELL, frente a amenazas sofisticadas y persistentes. (Payo, 2022).

Factores operativos y tecnológicos en seguridad cibernética.

La protección de activos estratégicos en el ámbito militar, particularmente en lo que respecta a las plataformas aéreas, ha evolucionado en las últimas décadas hacia una dimensión que trasciende lo físico y lo mecánico. La ciberseguridad, entendida como la capacidad de prevenir, detectar, responder y recuperarse frente a amenazas digitales, se ha convertido en un pilar fundamental para la defensa nacional (Suarez, 2023). En el caso específico de las aeronaves BELL del Ejército Nacional de Colombia, la creciente dependencia de sistemas electrónicos, software embarcado y redes de comunicación ha ampliado considerablemente la superficie de exposición a riesgos cibernéticos.

El primer capítulo permitió identificar amenazas clave como el spoofing, jamming, inyecciones de datos falsos y vulnerabilidades en sistemas de mantenimiento, evidenciando que la seguridad cibernética de las aeronaves BELL no solo requiere barreras tecnológicas, sino también una gestión integral de factores internos que fortalezcan su resiliencia operativa.

Dentro de estas variables, los factores operativos y tecnológicos juegan un papel determinante. En el ámbito operativo, las prácticas del personal, el cumplimiento de los procedimientos establecidos y la cultura organizacional en materia de seguridad informática influyen de manera directa en la exposición o mitigación de los riesgos. Por otro lado, los factores tecnológicos, como el estado de los sistemas, la infraestructura de soporte y el nivel de obsolescencia de los componentes electrónicos, determinan la capacidad de respuesta de la plataforma ante posibles ataques.

La obsolescencia tecnológica, por ejemplo, ha sido señalada en diversos estudios como un facilitador de ciberataques, al limitar la implementación de actualizaciones de

seguridad y aumentar la vulnerabilidad frente a técnicas de explotación modernas. Simultáneamente, la falta de cultura cibernética y la ausencia de protocolos claros para el manejo de información digital en ambientes operacionales son elementos que incrementan el riesgo de incidentes (Ospina & Sanabria, 2020).

En este sentido, este capítulo tiene como propósito identificar y analizar los factores operativos y tecnológicos que afectan la seguridad cibernética de las aeronaves BELL del Ejército Nacional, mediante un enfoque cualitativo y documental. El análisis permitirá evidenciar no solo vulnerabilidades técnicas, sino también deficiencias procedimentales y organizacionales que pueden comprometer la operatividad y protección de estos activos estratégicos.

Factores operativos: procedimientos, personal y cultura organizacional.

La ciberseguridad en el entorno militar no solo depende de la implementación de tecnologías avanzadas o de sistemas de protección digital, sino que también se fundamenta en la manera como las personas, los procedimientos y la cultura organizacional interactúan dentro de la institución (Rivera & Ardila, 2022). En el caso de las aeronaves BELL del Ejército Nacional, estos factores operativos constituyen un elemento determinante en la prevención y mitigación de riesgos cibernéticos.

Como primer escenario, los procedimientos operativos estándar (SOP) relacionados con la manipulación de equipos, la actualización de software y la gestión de datos son esenciales para minimizar vulnerabilidades. Tal como lo plantea Acuña y Blanco (2023), la ausencia de procedimientos claros o la falta de actualización de estos puede generar brechas que sean fácilmente explotables por actores malintencionados. Ejemplos como el uso inadecuado de dispositivos de almacenamiento externo, la falta de control en el acceso físico

a los sistemas de navegación o la omisión de verificaciones de integridad de software representan riesgos latentes.

Asimismo, el factor humano, considerado uno de los eslabones más débiles en la cadena de ciberseguridad, adquiere especial relevancia en el contexto militar. Correa, Ortiz y Peña (2022) destacan que la formación y sensibilización del personal son claves para fortalecer la postura defensiva de las unidades operativas. La falta de conocimiento en ciberseguridad por parte del personal técnico y de vuelo puede derivar en errores operativos, como la conexión de dispositivos no autorizados, el uso de contraseñas débiles o el incumplimiento de protocolos de respuesta ante incidentes.

En este sentido, la implementación de programas continuos de concienciación y entrenamiento en ciberseguridad es una necesidad urgente para el Ejército Nacional. Acorde a Correa et al., (2017) modelos como el desarrollado en la Escuela Militar de Aviación (EMAVI), basado en metodologías de gamificación, han demostrado ser efectivos para interiorizar buenas prácticas de seguridad entre el personal operativo.

Otro aspecto crítico es la cultura organizacional frente a la ciberseguridad. Como señalan Anabalón et al., (2020), muchas instituciones militares aún perciben la ciberseguridad como un tema exclusivamente técnico, desestimando su dimensión humana y organizacional. Esta visión limitada genera ambientes donde los riesgos cibernéticos son subestimados y donde no se promueven comportamientos seguros entre el personal.

Asimismo, el análisis realizado por Sancho (2017) resalta la importancia de integrar la gestión del riesgo cibernético dentro de la planificación operativa de las unidades militares. Esto implica que las decisiones estratégicas sobre el empleo de aeronaves, como las BELL,

consideren también las variables asociadas a la seguridad digital, evaluando posibles escenarios de ataque y sus impactos operacionales.

De ese modo, el fortalecimiento del liderazgo en ciberseguridad dentro de las unidades aéreas se presenta como una acción prioritaria. Tal como lo plantea Lara (2025), es necesario que los comandantes de unidad y los responsables de mantenimiento tecnológico asuman un rol proactivo en la implementación y supervisión de políticas de ciberdefensa. Esto incluye desde la asignación de recursos para capacitación, hasta la exigencia del cumplimiento estricto de protocolos de seguridad.

En síntesis, los factores operativos asociados a procedimientos, personal y cultura organizacional constituyen un pilar fundamental en la protección cibernética de las aeronaves BELL. Sin un enfoque integral que considere estos elementos, cualquier inversión tecnológica podría verse anulada por errores humanos o fallas organizativas que expongan a la flota a incidentes de alto impacto.

Factores tecnológicos: sistemas, infraestructura y obsolescencia.

La dimensión tecnológica representa uno de los pilares más sensibles dentro del análisis de la ciberseguridad en plataformas aéreas como las aeronaves BELL del Ejército Nacional. La interacción entre sistemas embarcados, infraestructura de apoyo en tierra y redes de comunicación configura un entorno de alta complejidad técnica, donde la identificación de vulnerabilidades requiere un enfoque integral.

Desde una primera perspectiva, resulta indispensable analizar los sistemas de misión y navegación. Estos componentes, esenciales para la operatividad de las aeronaves, presentan una serie de riesgos asociados a la falta de actualizaciones, el uso de software no validado o la ausencia de mecanismos de autenticación robusta. Tal como advierten Acuña y Blanco

(2023), muchos de estos sistemas carecen de una gestión de ciclo de vida orientada a la ciberseguridad, lo que dificulta la aplicación de parches de seguridad y la ode configuraciones seguras.

También, la infraestructura de comunicaciones constituye otro punto crítico. Sistemas como el ACARS, el transpondedor ADS-B y los radios de comunicación táctica dependen de redes de datos que, si no están adecuadamente protegidas, pueden ser interceptadas o alteradas. Benítez (2019) destaca que la falta de cifrado en las comunicaciones aeronáuticas es una de las debilidades más explotadas por actores malintencionados, lo que podría permitir la inyección de información falsa o la interrupción de enlaces críticos durante el vuelo.

Adicionalmente, la infraestructura de soporte en tierra, como las estaciones de mantenimiento y los servidores de planificación de vuelo, también representan un eslabón vulnerable. Bonilla (2022) documenta que la falta de segmentación de redes y la coexistencia de entornos operativos con redes administrativas pueden facilitar movimientos laterales de atacantes una vez que logran acceso inicial a la infraestructura.

Uno de los problemas más evidentes en el caso colombiano es la obsolescencia tecnológica de parte de la flota BELL. Como indica Blanquicet (2025), el retiro reciente de varias aeronaves debido a limitaciones técnicas y presupuestales refleja el estado crítico de actualización tecnológica en este segmento. La presencia de sistemas operativos antiguos, hardware sin soporte de fabricante y software desactualizado crea un terreno propicio para la explotación de vulnerabilidades conocidas.

La integración de componentes COTS (Commercial Off-The-Shelf) agrava esta situación. Aunque estos dispositivos son utilizados para reducir costos y facilitar el mantenimiento, su uso sin las debidas medidas de control y endurecimiento de seguridad

puede abrir nuevas vías de ataque, como lo señalan Díaz et al. (2020). Los riesgos incluyen desde la presencia de backdoors hasta la imposibilidad de aplicar actualizaciones de seguridad debido a incompatibilidades con otros sistemas embarcados.

Otro factor tecnológico relevante es la ausencia de un sistema de monitoreo continuo de seguridad cibernética a bordo de las aeronaves. Mientras que en otros países se han implementado soluciones basadas en análisis de tráfico de red interno y detección de anomalías en tiempo real (Anabalón et al., 2020), en el caso de las aeronaves BELL esta capacidad aún no ha sido plenamente desarrollada.

La ausencia de políticas robustas de hardening, la falta de control en la configuración de sistemas y la escasa adopción de marcos internacionales como el NIST Cybersecurity Framework o la norma ISO/IEC 27001 incrementan las vulnerabilidades en las aeronaves BELL. Según la OACI (2020), es indispensable que los sistemas aeronáuticos se diseñen bajo el principio de seguridad desde su origen (security by design), una práctica que no se aplica consistentemente en plataformas heredadas.

A su vez, factores como la obsolescencia tecnológica, la limitada inversión en infraestructura crítica y la falta de una política de actualización integral generan un entorno de riesgo acumulativo. En línea con lo señalado por Lara (2025), esta realidad demanda una estrategia de ciberdefensa proactiva que no solo modernice los sistemas actuales, sino que también incorpore tecnologías emergentes orientadas a proteger la integridad, disponibilidad y confidencialidad de la información operacional (Cubillos, 2022).

Análisis de casos y experiencias relevantes.

La incorporación de experiencias previas y el análisis de casos documentados constituyen una fuente invaluable de aprendizaje para la formulación de estrategias de ciberdefensa aplicables a las aeronaves BELL del Ejército Nacional. Las lecciones aprendidas de incidentes reales en el ámbito de la aviación militar permiten comprender cómo los factores operativos y tecnológicos, cuando no son gestionados adecuadamente, pueden derivar en vulnerabilidades críticas.

Uno de los casos más relevantes en el contexto internacional fue el ataque al sistema de control de aeronaves no tripuladas de la Fuerza Aérea de los Estados Unidos en 2011, conocido como el "Virus en Creech Air Force Base". Según Durán (2011), este incidente expuso la falta de controles internos en las estaciones de operación remota, permitiendo la infección por malware que afectó la recolección y transmisión de datos de vuelo. Este caso demuestra cómo un error en la gestión de estaciones terrestres puede comprometer la seguridad de las plataformas aéreas, analogía aplicable al contexto de las aeronaves BELL y sus estaciones de mantenimiento (Infodron, 2011).

En el ámbito civil, el ciberataque de tipo ransomware que afectó a la empresa Garmin en 2020 también proporciona valiosas enseñanzas (Mitnicksecurity, 2020). Este incidente paralizó temporalmente los servicios de navegación y comunicación de miles de aeronaves alrededor del mundo (Bonilla, 2022). La afectación de sistemas de soporte y la imposibilidad de acceder a datos críticos para el vuelo son elementos que deben ser considerados en la evaluación de riesgos del Ejército Nacional.

Desde una perspectiva regional, el trabajo de Suárez (2023) destaca la creciente preocupación por las capacidades ofensivas cibernéticas de actores no estatales en América

Latina. El estudio señala que estos grupos han comenzado a explorar vulnerabilidades en infraestructuras militares, incluyendo sistemas de comunicación y control aéreo, lo que evidencia la necesidad de fortalecer la vigilancia y defensa cibernética de activos como la flota BELL.

Un caso documentado por Parra (2024) hace referencia a las campañas de ataques avanzados persistentes (APT) dirigidas contra industrias aeroespaciales y de defensa, donde se identificaron intrusiones prolongadas con fines de espionaje. Aunque no existen registros públicos de ataques APT específicos contra aeronaves BELL, la experiencia internacional evidencia que sistemas de aviación militar con características tecnológicas similares han sido objetivos prioritarios para grupos de ciberamenazas avanzadas.

Otra experiencia relevante es la implementación de programas de concienciación y formación en ciberseguridad en fuerzas aéreas aliadas. El estudio de Correa et al. (2017), desarrollado en la Escuela Militar de Aviación de Colombia, demostró que las estrategias de capacitación basada en juegos formativos contribuyen significativamente a reducir el riesgo humano en incidentes cibernéticos. Este enfoque puede ser adaptado para el personal técnico y operativo vinculado a la operación y mantenimiento de las aeronaves BELL.

En ese orden, la revisión del marco regulatorio chileno, analizado por Anabalón et al. (2020), aporta elementos sobre la importancia de actualizar las políticas nacionales de ciberseguridad en entornos críticos. Este estudio destaca la necesidad de establecer estándares mínimos de seguridad, procedimientos de respuesta ante incidentes y auditorías permanentes, aspectos todos aplicables al contexto colombiano.

Gracias a todo lo anterior, el análisis de casos y experiencias previas confirma que los factores operativos y tecnológicos son elementos centrales en la protección cibernética de

plataformas aéreas. La revisión de estos eventos permite fortalecer la toma de decisiones, anticipar posibles escenarios de riesgo y establecer medidas concretas que garanticen la seguridad y la continuidad operativa de la flota BELL del Ejército Nacional.

Mecanismos de protección cibernética en las aeronaves BELL: formulación integral para el Ejército Nacional

En el contexto colombiano, caracterizado por amenazas híbridas persistentes, las aeronaves BELL del Ejército Nacional desempeñan un papel estratégico esencial en operaciones como reconocimiento, evacuación médica, infiltración y apoyo aéreo. Su creciente dependencia de sistemas digitales integrados como GPS, navegación inercial (INS), enlaces aire-tierra y módulos de diagnóstico ha optimizado su rendimiento, pero también las ha expuesto a vectores de ciberataque cada vez más sofisticados. Esta digitalización, aunque necesaria, incrementa el riesgo sobre la disponibilidad, confiabilidad y control seguro de las plataformas, haciendo imprescindible una visión integral de ciberseguridad para garantizar su operatividad.

De acuerdo con la Agencia de Ciberseguridad de la Unión Europea (ENISA, 2022), el sector aeronáutico presenta múltiples puntos de vulnerabilidad, desde el software de vuelo hasta la cadena de suministro digital. La Organización de Aviación Civil Internacional (2021) y la OTAN (2025) han señalado que las plataformas aéreas militares, como las BELL, enfrentan desafíos específicos al operar en entornos hostiles, con redes de comunicación expuestas, sistemas embarcados de difícil actualización y dependencia de proveedores internacionales. En este sentido, el presente capítulo propone una formulación técnica, estratégica y contextualizada de los mecanismos de protección cibernética que deben ser

aplicados o reforzados en la flota BELL, partiendo de un diagnóstico realista de su situación actual.

Desde una perspectiva de pensamiento sistémico y sociotécnico (Leveson, 2012), la ciberseguridad no puede limitarse a soluciones tecnológicas. Es necesario integrar procedimientos de gobernanza, capacitación del talento humano, mecanismos de detección temprana, segmentación de redes embarcadas, y controles estrictos en el mantenimiento y actualización de software. Además, organismos como el MITRE (2024) y el SANS Institute (2025) han planteado marcos metodológicos como ATT&CK y CMMC que permiten identificar patrones de ataque y reducir la superficie expuesta de los sistemas aeronáuticos.

El capítulo se estructura en tres apartados. En el primero, se describe el estado actual de los mecanismos de protección implementados en la flota BELL, destacando sus fortalezas y limitaciones. En el segundo, se presentan estándares internacionales y buenas prácticas en ciberseguridad aeronáutica aplicables al contexto colombiano. Por último, en el tercer apartado, se formulan recomendaciones prácticas orientadas a fortalecer la ciberdefensa de estas aeronaves, con base en el análisis documental y la experiencia operacional acumulada en el entorno nacional.

Esta formulación cobra especial importancia si se considera la amenaza creciente de ataques DDoS, spoofing, jamming, malware persistente y manipulación de transpondedores y enlaces de datos, tal como lo alertan estudios recientes del Departamento de Defensa de los EE.UU. (2024) (2022) y la FAA (2017). Por tanto, dotar a la flota BELL de mecanismos robustos de protección cibernética no solo preserva su capacidad de misión, sino que asegura la vida del personal militar y la continuidad de las operaciones en defensa de la soberanía nacional.

Diagnóstico actual de medidas de protección implementadas

Las aeronaves BELL del Ejército Nacional son esenciales para misiones tácticas y logísticas; sin embargo, su creciente digitalización ha ampliado las superficies de ataque cibernético, lo que exige un diagnóstico riguroso de las medidas de protección actuales para garantizar su operatividad segura. (Ejército, 2023). De manera general, la protección cibernética de estas aeronaves ha estado supeditada a protocolos de seguridad física, controles de acceso y restricciones en la modificación de software.

Algunas aeronaves BELL, especialmente las modernizadas en los últimos cinco años, han sido equipadas con sistemas redundantes de navegación y comunicación, lo que permite mitigar parcialmente ataques de interferencia o spoofing (Lawler, 2024). Adicionalmente, se han implementado controles para el acceso físico a los sistemas de misión, así como restricciones para el uso de dispositivos USB y actualizaciones únicamente bajo supervisión de personal autorizado.

Aun así, estudios como el de Kaspersky ICS-CERT (2022) han evidenciado que estas medidas, aunque necesarias, no son suficientes ante ataques avanzados y persistentes. Aún persisten vulnerabilidades estructurales, como la falta de segmentación entre redes embarcadas (comunicación, navegación y mantenimiento), la carencia de mecanismos de detección en tiempo real, y la baja frecuencia de auditorías técnicas específicas en ciberseguridad. En este sentido, el modelo tradicional de seguridad reactiva resulta insuficiente para un entorno operacional donde actores como el ELN o estructuras residuales de las FARC han demostrado capacidad para ejecutar operaciones cibernéticas disruptivas.

Asimismo, la falta de una política institucional robusta que establezca requerimientos de ciberseguridad específicos para plataformas aéreas también representa un vacío

estratégico. Según la Agencia de Ciberseguridad de la Unión Europea (ENISA, 2022), la inexistencia de protocolos diferenciados para plataformas embarcadas limita la capacidad de respuesta ante incidentes y dificulta la trazabilidad de intrusiones. En Colombia, el marco legal está representado por documentos como el CONPES 3701 y la Estrategia Nacional de Ciberseguridad, pero estos aún no descienden con suficiente precisión al ámbito de la aviación militar (CONPES, 2011).

Además, desde el punto de vista técnico, un punto crítico identificado es la obsolescencia de algunos sistemas embarcados. Como lo plantea ICAO (2021), muchos componentes electrónicos instalados en aeronaves militares tienen más de una década de funcionamiento, y sus sistemas operativos ya no reciben soporte de seguridad. Esta situación no solo limita la capacidad de actualización, sino que incrementa la exposición frente a exploits conocidos.

Entonces, un aspecto adicional es el mantenimiento técnico. Durante las rutinas de inspección y diagnóstico de las aeronaves BELL, se utilizan laptops de escaneo y consolas especializadas que, en algunos casos, no están aisladas de redes administrativas o carecen de protocolos de "air gap". Esto representa una vulnerabilidad crítica, ya que un dispositivo contaminado podría infectar sistemas embarcados sin ser detectado. El SANS Institute (2021) advierte que este tipo de vectores son altamente efectivos y difíciles de rastrear cuando no existe una separación física entre ambientes operativos y administrativos.

El nivel de formación del personal también influye directamente en la eficacia de las medidas actuales. Según Correa et al. (2017), aunque existen capacitaciones básicas en seguridad de la información, todavía no se incluye una doctrina específica sobre ciberseguridad embarcada para los operadores, técnicos o comandantes de aeronave. Esto

limita la capacidad de respuesta ante eventos como alertas falsas, manipulación de transpondedores o anomalías digitales en sistemas de navegación.

En cuanto al monitoreo continuo, actualmente no se dispone de un Centro de Operaciones de Seguridad (SOC) dedicado al monitoreo de sistemas aéreos o a la detección de anomalías en los vuelos. Aunque se han hecho avances en la implementación del Comando Conjunto Cibernético, su alcance aún no permite una supervisión específica de la flota de ala rotatoria.

Así las cosas, un aspecto crítico del diagnóstico es la dependencia tecnológica de proveedores extranjeros, principalmente estadounidenses. Esta dependencia limita la autonomía en la identificación de puertas traseras (backdoors), y dificulta la validación interna del código fuente de ciertos sistemas. La doctrina de "seguridad por diseño" (secure by design), propuesta por Lockheed Martin (2021), todavía no se implementa completamente en el proceso de adquisición y modernización de aeronaves en Colombia.

En síntesis, si bien se han dado pasos iniciales en la protección cibernética de las aeronaves BELL, las medidas actuales son fragmentadas, reactivas y carentes de una arquitectura de ciberdefensa integral. El diagnóstico evidencia la necesidad urgente de avanzar hacia una protección proactiva, basada en estándares internacionales, detección continua, segregación de redes, control del ciclo de vida del software embarcado y fortalecimiento doctrinal del personal.

Estándares internacionales y buenas prácticas aplicables.

Para fortalecer los mecanismos de protección cibernética en aeronaves como las BELL del Ejército Nacional, es indispensable revisar los estándares internacionales y buenas prácticas adoptadas por fuerzas armadas, organismos de aviación y agencias de ciberseguridad de

referencia global. Estas directrices permiten establecer un marco técnico confiable, adaptable al contexto colombiano, y garantizar la interoperabilidad con socios estratégicos en operaciones conjuntas o misiones de cooperación.

Uno de los marcos de referencia más consolidados es el NIST Cybersecurity Framework (NIST CSF), desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos. Este modelo se organiza en cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar (NIST, 2022). Su aplicación al entorno aeronáutico permite desarrollar controles específicos como el análisis de riesgos en sistemas embarcados, la segmentación de redes internas, y la gestión del ciclo de vida del software de navegación. Además, el NIST CSF recomienda realizar ejercicios de simulación y recuperación ante fallos, clave en misiones tácticas de ala rotatoria.

En paralelo, la Organización de Aviación Civil Internacional (ICAO) ha emitido el documento Doc 9985 Manual sobre Ciberseguridad en Aviación, el cual establece una taxonomía de amenazas y vulnerabilidades aplicables a aeronaves y sistemas de control. La ICAO enfatiza la necesidad de aplicar medidas de protección integradas al diseño de sistemas, como la redundancia lógica, validación de autenticidad en transmisiones y protocolos de criptografía embarcada (ICAO, 2021). En Colombia, este estándar aún no ha sido adoptado plenamente en plataformas militares, lo que genera una brecha de seguridad relevante.

Otra fuente relevante es la iniciativa MITRE ATT&CK for ICS, que identifica tácticas, técnicas y procedimientos (TTPs) usados por adversarios contra sistemas de control industrial y, por extensión, sistemas aeronáuticos. Esta matriz clasifica ataques comunes como la explotación de vulnerabilidades en firmware, modificación de configuraciones, y

suplantación de identidades en canales de comunicación (MITRE, 2022). Adaptar esta matriz al contexto BELL permitiría desarrollar un "perfil de amenazas" específico para cada tipo de operación (inserción, CASEVAC, reconocimientos), permitiendo anticipar vectores de ataque.

Asimismo, la Agencia de Ciberseguridad de la Unión Europea (ENISA) ha propuesto el modelo Cybersecurity for Aviation – Sectoral Baseline, que establece medidas de gobernanza, gestión de riesgos y respuesta a incidentes. Entre sus recomendaciones figura la asignación de responsables de ciberseguridad embarcada, la actualización regular de parches, el control de acceso basado en funciones, y auditorías periódicas. ENISA también promueve el principio de defensa en profundidad: no depender de un único control, sino de múltiples capas de seguridad técnica y procedimental (ENISA, 2022).

En el ámbito militar, la OTAN a través de su centro CCDCOE ha desarrollado el documento Cyber Defence Capability Development Framework (CDCDF), que propone una integración de la ciberdefensa en cada fase del ciclo de adquisición y operación de plataformas. Este marco recomienda realizar análisis de misión y pruebas de penetración antes de desplegar aeronaves, así como establecer una arquitectura segura desde el diseño ("security by design") (NATO CCDCOE, 2023). En Colombia, esta lógica podría ser integrada a los procesos logísticos de modernización o compra de componentes para los BELL.

La norma DO-326A/ED-202A de la RTCA/EUROCAE establece criterios para la protección de aeronaves civiles contra amenazas cibernéticas, incluyendo evaluación de impacto, mitigación de vulnerabilidades y verificación continua del sistema. Aunque diseñada para aviación civil, su estructura es útil para establecer controles embarcados en

ambientes militares, como la autenticación de dispositivos de mantenimiento o la verificación de integridad del software en tiempo real (RTCA, 2021).

El Center for Internet Security (CIS) ha publicado listas de verificación específicas para sistemas operativos usados en contextos militares (Windows Embedded, Linux Hardened, etc.), útiles para proteger las consolas de mantenimiento empleadas en hangares y bases aéreas (CIS, 2025). También promueve políticas de gestión de credenciales y monitoreo centralizado, que podrían implementarse en el Comando Conjunto Cibernético para monitorear en tiempo real la seguridad de la flota aérea.

Por otra parte, la guía CMMC (Cybersecurity Maturity Model Certification) desarrollada por el Departamento de Defensa de EE.UU. establece cinco niveles de madurez en seguridad. Este modelo exige que los contratistas militares adopten prácticas como control de medios removibles, cifrado en tránsito y repositorios seguros. Si bien Colombia no está obligada por el CMMC, su adopción voluntaria en la Fuerza Aérea o Ejército Nacional marcaría un avance importante en prácticas de gobernanza y auditoría (Defense Department , 2024).

Propuestas de mejora y recomendaciones para el Ejército Nacional.

La protección cibernética de las aeronaves BELL del Ejército Nacional no debe abordarse como una tarea fragmentada o meramente técnica, sino como un esfuerzo articulado que integre procedimientos operacionales, capacidades tecnológicas y resiliencia organizacional. En este sentido, se propone una estrategia dividida en tres ejes fundamentales: prevención, detección y respuesta, conforme a los principios establecidos en marcos como el NIST CSF, la guía DO-326A/ED-202A y los lineamientos doctrinales del Comando Conjunto Cibernético.

Figura 1 Estructura jerárquica de ciberdefensa aérea para la operación segura de aeronaves BELL en el Ejército Nacional de Colombia.

Nota: Figura de elaboración propia, basada en el análisis documental de los lineamientos del Comando Conjunto Cibernético, el marco técnico del NIST Cybersecurity Framework, los manuales operativos de la División de Aviación Asalto Aéreo del Ejército Nacional de Colombia y las recomendaciones de MITRE (2022) y Safe Skies (2018).

El primer paso en una defensa efectiva es prevenir. Para ello, se recomienda:

- **Aislamiento de redes críticas embarcadas (air gap controlado):** Separar lógicamente los sistemas de navegación, comunicación y mantenimiento para reducir la posibilidad de que una intrusión comprometa múltiples subsistemas. Esta medida es aplicable incluso en plataformas de vuelo legacy, mediante el uso de gateways especializados y controladores de tráfico interno.
- **Control de acceso biométrico a interfaces críticas:** Sustituir el acceso basado en contraseña por mecanismos biométricos o tokens criptográficos, especialmente en las estaciones de mantenimiento en tierra, donde suelen conectarse dispositivos externos.
- **Política de dispositivos autorizados (Device Whitelisting):** Todo dispositivo USB, laptop o herramienta digital que interactúe con el sistema debe estar registrado,

verificado y actualizado. Esto previene ataques tipo "injection" o introducción de malware en puntos de mantenimiento (Safe Skies, 2018).

- **Firmware integrity validation:** Establecer un protocolo de revisión y autenticación del firmware instalado en los BELL antes y después de cada misión. Esto se puede implementar a través de checksum o códigos hash validados contra un servidor seguro en la base aérea.
- **Cifrado extremo a extremo en comunicaciones tierra-aeronave:** Sustituir protocolos no cifrados por mecanismos con criptografía simétrica o híbrida, como AES-256 o RSA, para proteger la transmisión de coordenadas, instrucciones o telemetría en tiempo real (MITRE, 2022).

Una estrategia de protección efectiva debe contar con herramientas que permitan identificar anomalías antes de que generen impacto. Se proponen las siguientes acciones:

- **Sistema de detección de intrusiones (IDS) embarcado:** Este sistema, adaptado al entorno aeronáutico, debe monitorear la integridad de los archivos del sistema, la ejecución de procesos inusuales y el acceso a redes internas.
- **Análisis de tráfico interno con IA:** Emplear algoritmos de aprendizaje automático para identificar patrones inusuales de comportamiento, como un cambio inesperado en la trayectoria o tiempos atípicos de transmisión de datos.
- **Monitoreo remoto por parte del Comando Conjunto Cibernético:** La creación de un centro de vigilancia cibernética dedicado exclusivamente a plataformas aéreas permitiría alertas tempranas, respuesta inmediata y centralización de reportes de ciberincidentes.

- **Registro de eventos e integridad de logs:** Se debe garantizar la inalterabilidad de los registros de vuelo y de mantenimiento, así como los eventos digitales relacionados con cada operación.

Dado que ningún sistema es completamente inmune a los ataques, es imprescindible contar con procedimientos de respuesta robustos y entrenados:

- **Protocolos de contingencia en vuelo:** Los pilotos y oficiales técnicos deben recibir entrenamiento específico sobre cómo actuar ante pérdida de comunicación, alteración de datos GPS, fallas en el sistema de navegación o anomalías en el sistema de control de misión. Estos protocolos deben estar integrados en los manuales tácticos.
- **Desactivación segura de subsistemas no esenciales:** En caso de un ataque confirmado, debe poder activarse una función que limite automáticamente los subsistemas a los esenciales para el vuelo seguro, desconectando aquellos que puedan estar comprometidos.
- **Backups cifrados de configuración operativa:** Disponer de respaldos digitales seguros del sistema de misión, sistemas de armas (si aplica), e interfaces de navegación para su restauración inmediata una vez asegurado el entorno.
- **Simulacros periódicos de ciberincidentes:** Al igual que se entrenan fallas mecánicas o evacuaciones, las tripulaciones y técnicos de tierra deben realizar ejercicios de cibercrisis. Esto incluye simulaciones de spoofing, jamming, ataques DDoS al centro de control o fallas en el enlace satelital.

Conclusiones

Las aeronaves BELL del Ejército Nacional se han consolidado como plataformas tácticas de alta relevancia en las operaciones militares, pero su nivel de tecnificación y dependencia de sistemas digitales las hace especialmente vulnerables a amenazas cibernéticas. Ataques como el spoofing, jamming, DDoS, inyecciones en ADS-B y el uso de tecnologías civiles como el 5G representan vectores reales de riesgo que podrían afectar gravemente la seguridad operacional y la eficacia de la misión en escenarios de conflicto interno.

El análisis de los factores operativos y tecnológicos reveló debilidades estructurales que aumentan la superficie de exposición cibernética. La carencia de protocolos especializados, la baja cultura organizacional en temas de ciberdefensa y la escasa formación del personal aéreo en entornos digitales impiden una respuesta efectiva ante incidentes. A esto se suma la presencia de sistemas obsoletos, la falta de segmentación de redes embarcadas y el uso de tecnologías mixtas (militares y civiles), lo cual eleva el nivel de riesgo frente a actores hostiles.

La formulación de mecanismos de protección para las aeronaves BELL permitió identificar soluciones prácticas, adaptadas a las condiciones operacionales del Ejército Nacional. Medidas como la instalación de firewalls embarcados, la autenticación biométrica, el cifrado de comunicaciones, la segmentación de redes, la creación de un centro de monitoreo cibernético y la capacitación continua del personal constituyen una ruta concreta hacia el fortalecimiento de la seguridad cibernética de la flota.

La ciberdefensa en el ámbito aéreo debe ser concebida como una disciplina independiente de las políticas convencionales de tecnología de la información. Esto implica

su inclusión transversal en todo el ciclo operacional aéreo, desde la planeación de la misión hasta las fases posteriores al vuelo, con una perspectiva doctrinal que articule las amenazas híbridas actuales, el rol estratégico de las aeronaves BELL y la necesidad de resiliencia institucional frente a ataques cibernéticos.

Por último, se identificó la ausencia de lineamientos normativos específicos en las políticas nacionales de ciberseguridad para el componente aéreo militar. Documentos como el CONPES 3701 o la Estrategia Nacional de Ciberseguridad no abordan de manera diferenciada las necesidades del entorno operacional aéreo. Por tanto, se recomienda al Comando Conjunto Cibernético, en articulación con la División de Aviación Asalto Aéreo, desarrollar una política integral de ciberdefensa aérea que incluya doctrina, interoperabilidad, entrenamiento y protocolos de protección adaptados a la realidad de las aeronaves BELL.

Pese a los avances puntuales en concientización y algunos esfuerzos técnicos, la realidad actual de la ciberseguridad aplicada a la flota BELL del Ejército Nacional revela una brecha considerable frente al nivel óptimo requerido para operar en entornos híbridos y de alta complejidad. El estado actual se caracteriza por una débil estandarización de protocolos, limitada infraestructura tecnológica adaptada al entorno aeronáutico militar, escasa articulación doctrinal con el Comando Conjunto Cibernético y bajos niveles de entrenamiento especializado en ciberdefensa aérea. En contraste, el estado deseado exige una estructura integral, escalable y sostenida que integre desde el diseño de políticas institucionales hasta la implementación táctica, con énfasis en prevención, monitoreo, respuesta y recuperación.

Referencias

Acuña, G. B., & Blanco, V. (2023). *Mejora de Procesos de la Ciberseguridad Aeronáutica mediante un Marco de Trabajo*. Obtenido de https://revistas.unal.edu.co/index.php/dyna/article/view/107420

Altamirano, A. E., & Meléndez, L. (2021). *Los paradigmas y las metodologías usadas en el proceso de investigación: una breve revisión*. Obtenido de https://rua.ua.es/dspace/handle/10045/119978

Anabalón, J., Bobadilla, C., & Tobar , A. (2020). *Una Contribución de ISSA Chile a la Nueva Normativa de Ciberseguridad de la Subsecretaría de Telecomunicaciones*. Obtenido de https://www.researchgate.net/profile/Juan-Anabalon/publication/342159180_ISSA_CHILE_WORKING_PAPER_1_Una_Contribucion_de_ISSA_Chile_a_la_Nueva_Normativa_de_Ciberseguridad_de_la_Subsecretaria_de_Telecomunicaciones/links/5ee7b1ec299bf1faac561821/ISSA-CHILE-W

Benítez, J. I. (2019). *Ciberdefensa Aeroespacial*. Obtenido de http://revista.unade.edu.do/index.php/rscd/article/view/65/80

Blanquicet, J. A. (2025). *Nueve helicópteros UH1-N del Ejército salen de circulación: quedan 99 aeronaves funcionales*. Obtenido de https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/nueve-helicopteros-uh1-n-del-ejercito-salen-de-circulacion-quedan-99-aeronaves-funcionales-3422708

Bonilla, G. D. (2022). *Riesgos cibernéticos para la aviación regular "el 11 de septiembre cibernético"*. Obtenido de https://esdegrevistas.edu.co/index.php/rcit/article/view/4775

CIS. (2025). *¿Quieres saber más sobre los Puntos de Referencia del CIS? Mira nuestro video a continuación.* Obtenido de https://learn.cisecurity.org/benchmarks

CONPES. (2011). *CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa*. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Correa, J. A., Ortiz, L., & Peña, N. (2017). *Desarrollo de un Juego Formativo para Aportar a la Concienciación en Cibersegu-ridad al Personal de la Escuela Militar de Aviación (Emavi) "Marco Fidel Suárez" de la Fuerza Aérea Colombiana en la ciudad de Cali*. Obtenido de https://www.redalyc.org/pdf/6735/673571175011.pdf

Cubillos, A. E. (2022). *Riesgos de las Aeronaves Remotamente Tripuladas Bajo el Enfoque de Ciberseguridad*. Obtenido de https://repository.unipiloto.edu.co/handle/20.500.12277/12519

Defense Department . (2024). *Programa de Certificación del Modelo de Madurez de Ciberseguridad (CMMC)*. Obtenido de https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

Defense Department. (2024). *Cybersecurity Maturity Model Certification (CMMC) Program*. Obtenido de https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

Díaz, J. E., González, E., Pérez, J., Medina, R., & Rangel, A. (2020). *Complemento al simulador de vuelo del helicóptero Bell 206, para las prácticas en la formación de pilotos de la ESAVI.* Obtenido de http://www.scielo.org.co/scielo.php?pid=S1794-12372020000200113&script=sci_arttext

Durán, J. J. (2011). *La Ciberseguridad en el Ámbito Militar*. Obtenido de https://dialnet.unirioja.es/descarga/articulo/3837348.pdf

Echeverria, G. (2023). *Amenazas cibernéticas: Tipos, riesgos y estrategias de protección para empresas y usuarios*. Obtenido de https://www.tecnologia-informatica.com/amenazas-ciberneticas/

Ejército. (2023). *Boletin No. 80 Seguridad de aeronaves en helipuerto*. Obtenido de https://www.ejercito.mil.co/boletin-no-80-seguridad-de-aeronaves-en-helipuerto/

ENISA. (2022). *The NIS2 directive highlights the importance of bolstering cybersecurity in the transport sector to protect critical infrastructure across aviation, maritime, rail, and road transport.* Obtenido de https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/transport

FAA. (2017). *Cybersecurity*. Obtenido de https://www.faa.gov/about/plansreports/cybersecurity

ICAO. (2021). *Aviation Cybersecurity Strategy*. Obtenido de https://www.icao.int/aviation-cybersecurity-strategy

Infobae. (2023). *Un grupo opositor bielorruso destruyó un avión espía de Rusia de USD 300 millones.* Obtenido de https://www.infobae.com/america/mundo/2023/02/27/un-grupo-opositor-bielorruso-destruyo-un-avion-espia-del-kremlin-de-usd-300-millones-en-minsk/

Infodron. (2011). *Un virus informático afecta a la flota de UAV de la Fuerza Aérea de Estados Unidos*. Obtenido de https://www.infodron.es/texto-diario/mostrar/3532163/virus-informatico-afecta-flota-uav-fuerza-aerea-estados-unidos

Lara, N. C. (2025). *El ciberespacio como escenario de conflicto en el siglo XXI. ¿Hacia la militarización de la ciberseguridad?* Obtenido de https://revistas.utadeo.edu.co/index.php/razoncritica/article/view/ciberespacio-como-escenario-conflicto-siglo-xxi/2183

Lawler, K. (2024). *Astronautics providing badger pro+™ integrated flight display system in bell basix-pro glass cockpit retrofit kit for 412 helicopters*. Obtenido de https://www.astronautics.com/tag/bell-helicopter/

Leveson, N. G. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. Obtenido de https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied

Lombardo, O. M. (2024). *La renovación de Bell con soluciones eficientes y modernas: Bell 505, 412 EPi y 407 GXi/M*. Obtenido de https://helosmag.com/helos-magazine/la-renovacion-de-bell-con-soluciones-eficientes-y-modernas-bell-505-412-epi-y-407-gxi-m/

Madrigal, G. D., & García , R. (2021). *CyberDrone: una plataforma de ciberseguridad para detección de ataques a drones*. Obtenido de http://www.scielo.org.co/scielo.php?pid=S0122-34612021000100044&script=sci_arttext

Mitnicksecurity. (2020). *An Overview of the 2020 Garmin Ransomware Attack*. Obtenido de https://www.mitnicksecurity.com/blog/2020-garmin-ransomware-attack

MITRE. (2024). *ICS Matrix*. Obtenido de https://attack.mitre.org/matrices/ics/

OACI. (2020). *Webinario sobre la implementación de ciberseguridad de la aviación OACI/CANSO/AIRBUS*. Obtenido de https://n9.cl/twpaw

Ortiz, T. L. (2022). *El ciberespacio: nuevo dominio de la guerra y el crimen*. Obtenido de https://doi.org/10.25062/2955-0270.4792

Ospina, M. R., & Sanabria, P. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*. Obtenido de http://scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

OTAN. (2025). *The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub*. Obtenido de https://ccdcoe.org/

Parra, P. A. (2024). *¿Cómo los ciberdelincuentes usan tecnologías avanzadas en IA para crear Deepfakes y Deepvoices para suplantar las identidades y estafar?* Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-los-ciberdelincuentes-usan-tecnologias-avanzadas-en-ia-para-crear-deepfakes-y-deepvoices-para-suplantar-las-identidades-y-estafar-3393101

Payo, A. (2022). *Alertan de la existencia de un grupo de hackers centrado en la aviación y la defensa.* Obtenido de https://www.escudodigital.com/ciberseguridad/grupo-hackers-centrado-en-aviacion-defensa_50935_102.html

Rivas, S. (2025). *El Ejército de Colombia y el reemplazo de sus UH-1N y Huey 2, una necesidad urgente*. Obtenido de https://n9.cl/b3i62

Rivera, O. M., & Ardila, J. (2022). *El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia*. Obtenido de https://revistascedoc.com/index.php/pei/article/view/333/730

RTCA. (2021). *DO-326A / ED-202A Introducción a la ciberseguridad en la aviación*. Obtenido de https://afuzion.com/do-326a-ed-202a-aviation-cyber-security/

Salamanca, E. A., Cabrera, F., & Reith, S. (2022). *Estrategia de Seguridad de la Infraestructura Crítica Nacional 2022-2032*. Obtenido de https://esdeglibros.edu.co/index.php/editorial/catalog/book/163

Sancho, C. (2017). *Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier*. Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/view/2859

SANS. (2025). *Industrial Control Systems Security Training*. Obtenido de https://www.sans.org/cybersecurity-focus-areas/industrial-control-systems-security

Suarez, J. S. (2023). *Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital*. Obtenido de https://revistascedoc.com/index.php/pei/article/view/628

Tovar, G. A., & Figueroa, E. (2021). *El helicóptero como factor decisivo para la movilidad táctica: el caso colombiano (1997-2012)*. Obtenido de http://scielo.org.co/scielo.php?script=sci_arttext&pid=S1900-65862021000200308

VIU. (2025). *TIC en Colombia: Cómo impulsan el futuro y desarrollo del país*. Obtenido de https://www.universidadviu.com/co/actualidad/nuestros-expertos/tic-en-colombia-como-impulsan-el-futuro-y-desarrollo-del-pais