Riesgos de la Inteligencia Artificial en la Ciberseguridad de UAV: Análisis bajo marco de la ISO 27032

MY. Naranjo Suarez Luis Alexander

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	**:**	MY. Naranjo Suarez Luis Alexander
Identificación	**:**	1121816498
Programa académico	**:**	Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Jaider Ospina Navas
Tutor temático	**:**	CR. Aldemar Serrano Cuervo
Fecha de entrega	**:**	26 de agosto del 2025
Extensión	**:**	9307

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

Riesgos de la Inteligencia Artificial en la Ciberseguridad de UAV: Análisis bajo marco de la ISO 27032

Artificial Intelligence Risks in UAV Cybersecurity: Analysis within the ISO 27032 Framework

Luis Alexander Naranjo Suarez[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El estudio aborda los desafíos de ciberseguridad en vehículos aéreos no tripulados (UAV) utilizados por la Aviación del Ejército, destacando su dependencia tecnológica de terceros fabricantes. El problema radica en la falta de autonomía tecnológica, lo que limita la capacidad de identificar vulnerabilidades y prevenir ciberataques impulsados por inteligencia artificial. El objetivo principal es establecer riesgos técnicos asociados al uso de UAV bajo el marco metodológico de la norma ISO 27032. La investigación sigue un enfoque cualitativo con diseño exploratorio, dividido en tres fases: análisis conceptual, aplicación normativa y diseño de estrategias. Se busca construir un protocolo escalonado de ciberseguridad que permita anticipar y mitigar amenazas, garantizando la protección integral de los UAV frente a ataques sofisticados. Los resultados esperan contribuir a la seguridad operativa y geoestratégica del sistema militar.

Palabras clave: UAV, marco, protocolar, ciber seguridad, enfoque, estratégico

Abstract: This research addresses cybersecurity challenges in unmanned aerial vehicles (UAVs) operated by the Army Aviation, emphasizing their technological dependence on third-party manufacturers. The main issue lies in the lack of technological autonomy, which restricts the ability to identify vulnerabilities and prevent AI-driven cyberattacks. The primary objective is to establish technical risks associated with UAV usage within the methodological framework of ISO 27032. The research employs a qualitative exploratory design divided into three phases: conceptual analysis, normative application, and strategy development. It aims to construct a tiered cybersecurity protocol to anticipate and mitigate threats while ensuring comprehensive UAV protection against sophisticated attacks. The results are expected to enhance the operational and geostrategic security of military systems.

Keywords: UAV, framework, protocol, cybersecurity, approach, Strategic

[1] Mayor del Ejército de Colombia, Candidato a magister en ciberseguridad y ciberdefensa, 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/0009-0005-0466-8475 - Contacto: Luis.naranjo@esdeg.edu.co.

Introducción

La ciberseguridad se define como un marco estructural compuesto por procesos basados en el conocimiento científico militar, integrando la producción tecnológica derivada de actividades de investigación, desarrollo e innovación (I+D+i). Este enfoque permite afrontar amenazas de tipo asimétrico mediante técnicas y protocolos que no solo abarcan el ámbito tecnológico, sino también el procedimental.

Comprender la ciberseguridad con una perspectiva dual enmarca de manera integral desafíos relacionados con la protección de sistemas críticos, para el caso de esta investigación, software y hardware integrado en aeronaves no tripuladas.

En el caso de las aeronaves no tripuladas (UAV), el enfoque facilita la implementación de estrategias dirigidas a la protección tanto del software y del hardware que, según la OTAN, debe darse de manera estructural para los tres tipos de UAV con usos militares: sistemas compuestos por vehículos con aviónica y propulsión, carga útil con sensores y grabadores, y enlaces de datos interoperables bajo estándares como STANAG 4586 (Monteiro, 2004).

En el ámbito militar, las funciones de las UAV giran en torno a las necesidades geoestratégicas impuestas por los contextos operacionales e intereses nacionales.

En el caso particular de la Aviación de Ejército, la ciberseguridad de estas aeronaves depende de factores tecnológicos externos, ya que la institución no es la fabricante ni propietaria del software funcional que utilizan los UAV. Este hecho plantea un desafío significativo en términos de conocimiento y control sobre los sistemas de función, pues la dependencia de terceros limita la identificación de vulnerabilidades e implementación de procesos de optimización para conservar el dominio tecnológico del software.

Ahora, esa situación aumenta los riesgos de ciberataques, ya que los fabricantes no ceden a totalidad la arquitectura del software, dificultando la detección de brechas de seguridad o fallos de interoperabilidad. De hecho, de acuerdo con Tang (2015) y Hartmann y Steup (2013), ataques como la captura de un RQ-170 Sentinel mediante Spoofing y Jamming de señales GPS, infección con virus keylogger cotra UAV´s y ataques jamming

para causar accidentes de UAV Schiebel Camcopter S-100, son ciberataques de tipología común, con alta probabilidad de impacto.

Desde esa perspectiva, la falta de autonomía tecnológica no solo afecta la capacidad operativa, sino también la protección integral de los UAV frente a amenazas que se encuentran en constante evolución.

Sumado a la ausencia de autonomía tecnológica, el desconocimiento de factores computacionales básicos en materia de ciberseguridad por parte de los actores encargados en la Aviación de Ejército, pone en riesgo su concepto operacional y alcance geoestratégico ya que:

Primero, dificulta la construcción de acciones estratégicas destinadas a la protección de los UAV mediante la aplicación de medidas asociadas a la ciberseguridad protocolar y metodológica. Segundo, ralentiza la identificación de amenazas cibernéticas, ya que el desconocimiento del software genera falta de comprensión sobre los tipos de amenazas, sus diseños y las formas tecnológicas de afectación.

Tercero, dificulta el desarrollo de medidas de prevención, anticipación e intervención en caso de que un ciberataque llegue a materializarse. Las tres causas forman un núcleo crítico, el cual se vuelve exponencial cuando se suma un factor más: el aumento de ciber ataques por inteligencia artificial hacia software que comparte las características, códigos y sintaxis de aeronaves no tripuladas como el Vector, Scorpion, Skydio X2D y Matrice 300 RTK.

Para la Aviación de Ejército, de ahora en adelante AV, la seguridad de las UAV es un reto que amerita conformar nuevos enfoques de gestión orientados a la ciberseguridad. Sin embargo, desarrollar mediadas estratégicas propicias ameritaría un cambio conceptual sobre el marco de seguridad digital e implementar metodologías de intervención para la protección y prevención anticipada. Es por esa razón, que el interrogante que da inicio a esta investigación se plantea de la siguiente forma: ¿Qué riesgos técnicos en materia de Ciberseguridad se presentan por el surgimiento de inteligencia artificial en contra del componente de aeronaves no tripuladas pertenecientes a la Aviación de Ejército?

Para responder a esta pregunta se planteó como objetivo: establecer riesgos técnicos en materia de Ciberseguridad derivados del surgimiento de inteligencia Artificial en contra de aeronaves no tripuladas, bajo el marco metodológico de la ISO 27032.

El propósito es desarrollar un marco protocolar basado en la estructura metodológica de la Norma Internacional Estandarizada 27032, que permita prevenir y anticipar amenazas, al mismo tiempo que garantizar la protección escalonada de las UAV´s.

Para tal fin, tres objetivos específicos se llevan a cabo. El primero, analizar la relación conceptual que hay entre Ciberseguridad, ataques a UAV´s y procesos de intervención Técnica – Metodológica. Con este objetivo, el proceso de investigación busca estudiar la conceptualización formada alrededor de la ciberseguridad para UAV´s, teniendo en cuenta marcos metodológicos, estrategias y acciones adoptadas en modelos de ciber protección unificados y simplificados.

El segundo, aplicar la norma ISO 27032 al proceso protocolar de ciberseguridad y técnico que requieren las UAV´s de la Aviación del Ejército. La conceptualización de la primera parte (primer objetivo), entrega una base cualitativa sólida para aplicar el proceso metodológico de la ISO 27032.

Metodológicamente, la ISO 27032 facilita el análisis e identificación del riesgo, formas técnicas de ciber ataque y construcción de protocolos para la ciber protección. Una vez identificados los protocolos, se diseñarán los enfoques de ciberseguridad que requiere la protección cibernética del software funcional de los UAV´s, y con posterioridad se explicarán los resultados obtenidos con la construcción teórica que se ha dado a la ciber seguridad con el entendimiento OTAN (Tercer objetivo).

Realizar los objetivos, amerita un enfoque de investigación cualitativo con diseño exploratorio. De ahí que la investigación, como se observa en el acápite de metodología de investigación, se divida en tres partes: análisis conceptual, aplicación metodológica y discusión de resultados.

Metodología

Enfoque de Investigación

La investigación adopta un enfoque **cualitativo**, el cual permite explorar a profundidad los conceptos relacionados con la ciberseguridad en UAVs (vehículos aéreos no tripulados). Este enfoque se selecciona debido a la necesidad de comprender las dinámicas y relaciones subyacentes entre los conceptos técnicos, normativos y metodológicos.

Diseño de Investigación

El diseño de la investigación es **exploratorio**, estructurado en cuatro fases principales que combinan técnicas de análisis conceptual, aplicación normativa, diseño de estrategias y validación mediante triangulación. Este diseño facilita abordar un área compleja y poco explorada, como lo es la ciberseguridad en UAVs en el marco de la norma ISO 27032.

La primera fase de esta investigación correspondió a un análisis conceptual de la relación que hay entre las categorías ciber seguridad, UAV y riesgos cibernéticos emergentes. La técnica aplicada fue la revisión de literatura cuyo lapso temporal se ubicó entre 2020 y 2025.

En esta fase se realizó un análisis metodológico integral que abarcó la conceptualización entre ciberseguridad, ataques a sistemas UAV y procesos de intervención técnica-metodológica. Se utilizó una revisión de literatura existente para identificar y categorizar las amenazas cibernéticas más relevantes que afectan a los vehículos aéreos no tripulados (UAV).

Además, se analizaron las estrategias actuales de prevención y mitigación de riesgos, destacando la importancia de protocolos estandarizados y la capacitación del personal en la prevención de errores humanos.

Como resultado, se identificaron brechas en los protocolos actuales y se propuso la implementación de la norma ISO 27032 para establecer un marco estructurado que explore tanto las amenazas tecnológicas como las procedimentales. Este enfoque metodológico no

solo busca anticipar amenazas, sino también establecer un marco de mejora continua que garantice la resiliencia cibernética frente a un entorno de amenazas en constante evolución

En la segunda fase, y con base en la contribución conceptual del primer objetivo, se identificaron los riesgos cibernéticos asociados a las aeronaves no tripuladas (UAV) de la Aviación de Ejército, centrando el análisis en una descripción técnico-característica de los UAV y la aplicación de la norma ISO 27032.

En esta parte se desarrollaron dos fases principales: una descripción cualitativa del estado actual (AS IS) de los UAV y un análisis de los riesgos cibernéticos protocolares relacionados con el factor humano.

El análisis permitió establecer una matriz descriptiva (Tabla 1) que resume las características principales de los UAV y los riesgos técnicos asociados, sentando las bases para la aplicación metodológica de la norma ISO 27032.

En la tercera parte se aplicó la norma ISO 27032 como marco estratégico para fortalecer la ciberseguridad en los UAV de la Aviación de Ejército, abordando riesgos inherentes a estas plataformas tecnológicas. Se desarrolló una matriz de aplicación basada en la identificación de vulnerabilidades específicas, como la interceptación de comunicaciones, el spoofing GPS, la negación de servicio (DoS) y el acceso no autorizado a datos sensibles, integrando procesos críticos como la encriptación avanzada, auditorías regulares, capacitación del personal, pruebas de resistencia y redundancia operativa (Tabla 2).

Además, se diseñaron protocolos para la eliminación segura de datos y se incorporaron herramientas de análisis predictivo para anticipar amenazas. Como resultado, se estableció un enfoque metodológico que conecta riesgos tecnológicos y procedimentales, garantizando la resiliencia operativa de los UAV y proporcionando un modelo replicable para la protección de sistemas en entornos militares complejos.

En la cuarta parte se establecieron los enfoques estratégicos, y con base en los mismos se planteó un marco protocolar conformado por enfoques estratégicos, actividades e indicadores, propósito institucional y mecanismos de implementación (Tabla 3).

Una vez finalizada la matriz se pasó a la validación cualitativa de los resultados con la construcción conceptual conexa a las políticas de seguridad cibernética que posee la OTAN.

Conceptualización entre Ciberseguridad, Ataques a Sistemas UAV y Procesos de Intervención Técnica-Metodológica: Análisis Metodológico Integral.

Los modelos de ciber seguridad para aeronaves no tripuladas varían por la proposición metodológica con la que se construyen elementos de protección cibernética, al mismo tiempo que por los factores de defensa correlacionados con protocolos orientados a metodologías de prevención y reducción del riesgo.

Ante ese entendimiento, el debate enmarcado en el campo de ciber seguridad aborda elementos funcionales, técnicos y descriptivos que comienzan con la identificación de ataques hipotéticos pero probables, relacionados con la evolución constante de la inteligencia artificial, el software y los ciber ataques a aeronaves no tripuladas.

En el marco de ese debate en el que confluyen los conceptos de IA, software, UAV y ciber ataques, Tomco y Pashaj (2024) exponen un núcleo de impactos cibernéticos que desde su perspectiva técnica resultan ser, no sólo probables, sino posibles en el argot de la utilización de procesos diseñados para optimizar la operación de drones mediante transmisión de datos, navegación y control. Lo anterior, incluyendo OcuSync, y procesadores como Qualcomm Snapdragon 855; además del empleo de frecuencias de 2.4-5.8 GHz, tecnología Wi-Fi y enlaces de radio de largo alcance (15-45 km) que aseguran conectividad.

De acuerdo con Tomco y Pashaj (2024), los ataques con mayor impacto, en los que hay amplia influencia de IA, son Man In The Middle y delegación de servicios e interceptación no autorizada de datos.

Este tipo de ataques no se diferencia de otras categorías. De hecho, se relaciona con la ingeniería social, penetración de software por superioridad tecnológica y ataques por desconocimiento técnico de los usuarios, recordando así que la experticia y cumplimiento de protocolos son dos medidas primarias de mitigación (Ly y Ly, 2021).

De hecho, frente a un desbalance tecnológico, funcional y procedimental, Hjelle, Omli, y Elisabeth (2023) determinan que existe cientificidad para estudiar la afectación de posibles ataques digitales a UAV´s, partiendo de un concepto: el Internet de Drones.

De acuerdo con Hjelle *et al* (2023), los UAV´s dependen de la conexión a redes con posible interceptación o afectación, generando riesgos asociados a la suplantación de señales

de GPS, agregando a la versión de Tomco y Pashaj (2024) un ciber ataque de tipología explícita: la penetración intrínseca de la señal que emite una aeronave no tripulada.

Rugo, Ardagna, y El Ioini (2022) van más allá de la versión de Hjelle *et al* (2023). Con una perspectiva técnica, explica que hay dos tipos de riesgos digitales en contra de estas tecnologías aéreas: las amenazas principales y los riesgos digitales. Entre las amenazas, el investigador subraya la suplantación de sensores (sensor spoofing), y la interferencia y bloqueo de señales, afectaciones ya descritas por Tomco y Pashaj (2024).

Sin embargo, Rugo *et al* (2024) plantean que, en el marco de la suplantación e interferencia de GPS, está la infiltración de código dirigida a través de la señal primaria que emite la aeronave.

Este, es considerado un riesgo de alta transmutación pues se adapta a la identificación de los códigos del software, pero también al funcionamiento del factor externo; es decir, el hardware.

La versión de Rugo *et al* (2024) encuentra en la discusión Mohammad (2025) un punto de vista similar, ya que este último explica que las amenazas más avanzadas en contra de las aeronaves no tripuladas son los ataques cibernéticos complejos de denegación, pero también la construcción de ciber ataques basados en la simulación de escenarios con redes adversariales.

La versión de Mohammad (2025) al igual que la de otros autores es técnica sin embargo un factor llama la atención, y es que no sólo hace alusión a los vectores tecnológicos que podrían llegar a materializar ataques cibernéticos de categoría compleja; sino que también refiere a la materialización de ataques producto de la ausencia de procesos de detección temprana y respuesta en tiempo real.

Esta perspectiva es adecuada para suponer que no todos los riesgos que se presentan ante aeronaves no tripuladas pertenecen o hacen parte del espectro tecnológico, y por consiguiente, al campo de posible afectación producto de código infectado.

Todo lo contrario, Mohammad (2025) supone que las afectaciones pueden ser de orden procedimental y protocolar. Siendo así, parte de la protección en materia de ciber seguridad para aeronaves no tripuladas dependería de un factor poco explorado en materia de afectación: el proceso de ciberseguridad desarrollado por el usuario.

En esa discusión concerniente al factor humano, diferentes factores salen a colación. Uno de ellos importante para la investigación, corresponde al desarrollo de protocolos estandarizados que facilitan la construcción estructural de procesos de anticipación.

Sobre todo, prevención de ataques cibernéticos basados en ingeniería y computación cuántica. Esta última, fenomenología digital no considerada en las estrategias convencionales de ciberseguridad para aeronaves no tripuladas e infraestructuras críticas relacionadas.

La explicación dada hasta este punto establece un parámetro de discusión que acerca la tecnología, las aeronaves no tripuladas y su software funcional a un estudio de posibles riesgos, cuya defensa depende de los códigos de ciberseguridad, pero también de protocolos de gestión para la protección.

Es por eso que kumar y Chaundhary (2024) explican en el espectro de la ciber seguridad que los protocolos de comunicación, el almacenamiento de datos de oposición y la actualización del software son procesos correlacionados que garantizan medidas proteccionistas.

Es así que, a parte de los códigos programados, el monitoreo y la auditoría en materia procedimental son transversales como enfoque clave para restringir ataques convencionales, especiales o con patrones sintácticos desconocidos.

El argumento de kumar y Chaundhary (2024) es, en definitiva, respaldado por Spyros (2022), al debatir que, si bien hay alta dependencia tecnológica frente a la estructuración de estrategias de ciber protección, la construcción protocolar para medidas preventivas desempeña un rol primario, y ello, se categoriza en enfoques estratégicos como el modelado anticipado de amenazas, el diseño de capas de seguridad en comunicaciones, supervisión humana centrada en auditoría mensual y empleo de medidas pro activas para anticipar vulnerabilidades e implementar medidas de solución.

Desde la perspectiva de Spyros (2022), se traza un entendimiento exógeno al marco tecnológico, que de facto aborda el proceso de ciber protección desde la inclusión de medidas digitales con complejo entendimiento.

Por lo menos, complejo para los stakeholders que dependen del servicio de ciber seguridad y que no son desarrolladores.

El vacío de conocimiento en materia cibernética que se empieza a denotar corresponde a la escasez de estudios que integren de manera holística factores tecnológicos, procedimentales y humanos en los modelos de ciberseguridad para aeronaves no tripuladas.

En especial, una limitada exploración de protocolos estandarizados basados en tecnologías emergentes como la computación cuántica, y de estrategias preventivas que incluyan la capacitación y el rol del usuario en la mitigación de riesgos, lo que representa un área crítica aún analizada con sustento suficiente en este campo.

Frente a ausencias y vacíos de conocimiento se interpreta de los autores como principal vector de análisis la transformación y rápida evolución de amenazas cibernéticas basadas en tendencias de contexto como la inteligencia artificial.

Pero, aunque sus investigaciones tienden a inclinarse sobre el aspecto tecnológico, principalmente, hay elementos de gestión centrados en una perspectiva protocolar o metodológica, y eso es un aspecto confirmado en versiones descriptivas como la de Cosar (2022).

Para Cosar (2022), el proceso estratégico de ciber protección en el caso de los UAV´s es y debe ser holístico.

De acuerdo con Cosar (2022), el núcleo de ciberataques depende en cierta medida de las vulnerabilidades explotables de cada uno de los elementos de función.

Es así, como las probabilidades de impacto se dividen en ataques de hardware, software, sensores, redes y formas de comunicación.

Pero, aunque tecnológicas por su naturaleza, la versión de Cosar (2022) subraya que las formas, métodos y medidas de ciberseguridad son de facto holísticas, y ello implica a las medidas de ciberseguridad adoptar propuestas estratégicas ceñidas a lo protocolar.

Dichas propuestas surgen por medidas de prevención y fortalecimiento para vacíos digitales, los cuales, sin intervención, se transforman en debilidades explotables, ajenas al funcionamiento tecnológico (ejecución de código y arquitectura de datos).

Entre esas medidas está el diseño de procesos y protocolos ajustados a la necesidad intrínseca de la organización, la cual, de acuerdo con Shafique, Mehmood, y Elhadef (2021), es considerado una debilidad, si no se plantean medidas de intervención centradas en el

protocolo funcional - metodológico; este último, con la misma prioridad representada en el tecnológico.

La versión de Shafique *et al* (2021) comparte ambas visiones, las que según Cosar (2022) concretan el enfoque holístico de la estrategia. Esas visiones corresponden a lo protocolar - metodológico y tecnológico.

En el caso del aspecto protocolar – metodológico, Shafique *et al* (2021) exponen en el contexto de UAV´s, que los modelos de ciber protección deben diseñarse bajo el parámetro asimétrico y simétrico.

Por el lado asimétrico, bajo el entendimiento tecnológico, lo que significa prevención frente a suplantación de GPS, inyección de datos con redes neuronales e interferencia con ataques Jamming.

Por el simétrico, tomando como punto de partida la prevención y precaución humana frente al uso de sistemas de información, conduciendo así al diseño de protocolos de control integral.

Las versiones expuestas hasta acá dividen el modelo estratégico de ciber protección en dos segmentos. Uno, relacionado explícitamente con el espectro tecnológico. Otro, con el metodológico. Este último, de interés primario para la investigación.

Por lo anterior, el análisis continuará bajo esa perspectiva. La sistematización de modelos de ciber seguridad para la protección de UAV´s, de frente al surgimiento de nuevas amenazas por inteligencia artificial, representa un reto estructural y cognoscitivo para los actores militares que han constituido la utilización de aeronaves no tripuladas como enfoques aero tácticos de alto valor estratégico.

Su protección, desde marcos metodológicos, depende de la aplicación de procesos preventivos ajustados a la necesidad dual del ciber riesgo.

Véase que en la perspectiva de Yu, Wang, Yu, Liu, Song y Li (2023), la protección cibernética y el entendimiento de la ciberseguridad a través del dominio *ciber*, desempeña un rol metódico, subrayando que la prevención con protocolos y procesos es una acción para restringir ataques que se suma a las tecnologías de ciber protección, las cuales, desde la cientificidad de Yu *et al* (2023), son planteadas a partir de auditorías y verificación de

algoritmos, configuración defensiva basada en hipótesis de código infectado con IA, y factores disruptivos orientados a la recuperación de sistemas .

Otro planteamiento que también resalta la funcionalidad de los protocolos de prevención ceñidos al factor humano corresponde a Basan (2024), quien expone con un análisis de bases de datos acerca de ciber ataques a UAV´s, que la construcción de protocolos basados en la proyección de impactos es un método de intervención que reduce las probabilidades de explotación de vulnerabilidades por errores explícitamente humanos.

Las perspectivas presentadas, incluida la de Basan (2024), destacan una convergencia conceptual entre la inteligencia artificial, los ciberataques dirigidos a vehículos aéreos no tripulados (UAV) y el diseño de estrategias orientadas a la prevención y mitigación de riesgos.

Esas estrategias, que, si bien poseen amplia influencia en enfoques tecnológicos, presentan un factor de protección conexo con la construcción metodológica de procesos y procedimientos para prevenir y anticipar ciber ataques. Dicho factor compete al diseño de protocolos especializados, ajustados al contexto y a la necesidad de los alcances geoestratégicos derivados de los UAV´s de la Aviación de Ejército.

Por tal razón, la siguiente parte de la investigación busca analizar en el marco de las estrategias duales orientadas por tecnología y procesos, protocolos y procedimientos que desde un enfoque metodológico identifiquen las debilidades protocolares presentes en los UAV de la Aviación de Ejército.

Este análisis se fundamentará en la aplicación de la norma ISO 27032, un estándar reconocido internacionalmente por su enfoque integral en la ciberseguridad, que permite abarcar tanto las amenazas tecnológicas como las procedimentales. La implementación de esta norma proporciona un marco estructurado para evaluar riesgos y diseñar estrategias preventivas adaptadas a las particularidades operativas de los UAV.

El estudio debe centrase entonces en identificar brechas sobre los protocolos actuales, considerando aspectos como la gestión de señales, la protección de datos transmitidos y el cumplimiento de estándares de seguridad en las comunicaciones. Además, analizar el impacto de la capacitación del personal en la prevención de errores humanos, un componente

crucial en la mitigación de riesgos cibernéticos (Marble, Lawless, Mittu, Coyne, Abramson, Sibley, 2015).

Un enfoque de ese tipo permite establecer la correlación entre las vulnerabilidades tecnológicas y las deficiencias en los procesos humanos, ofreciendo una visión holística de la ciberseguridad aplicada a estas aeronaves.

Así los términos, el análisis de las debilidades protocolares no solo contribuirá al fortalecimiento de las capacidades defensivas de la Aviación de Ejército, sino que también proporcionará un modelo replicable para otras instituciones que empleen UAV en contextos estratégicos. Este enfoque metodológico busca no solo anticipar amenazas, sino también establecer un marco de mejora continua que garantice la resiliencia cibernética frente a un entorno de amenazas en constante evolución.

Identificación de riesgos cibernéticos concernientes a las aeronaves no tripuladas de la Aviación de Ejército: descripción técnica – característica de los UAV y aplicación de norma ISO 27032.

En el acápite anterior se analizaron los elementos del marco de estudio de ciber seguridad para UAV. Entre los hallazgos importantes se encontró como patrón común la necesidad de establecer procesos exploratorios centrados en la protección cibernética de sistemas de información basados en protocolos y procesos coordinados y articulados.

Contribuciones como las de Cruzado, Rodríguez, López, y Acuña (2022) y Von Solms y Von Solms (2018), configuran un primer acercamiento que, completando el ejercicio conceptual previo, abordan procesos de ciberseguridad que empiezan con la construcción de protocolos para reducir la probabilidad de falla, error o vacío de conocimiento humano.

Bajo esa perspectiva, el enfoque de ciber seguridad por adaptar en este planteamiento corresponde al marco de procesos, protocolos y acciones estratégicas, más que a intervenciones técnicas ya que, como se explicó en la introducción, un vacío estructural de la Aviación de Ejército, es la ausencia de propiedad intelectual sobre el software (código) y hardware de los UAV.

Siendo así, la identificación de riesgos cibernéticos se ubica en el factor humano más que en el tecnológico, y por tal razón, antes de aplicar la norma ISO 27032, se describen de manera exploratoria las características de las UAV que se asimilan a la tipología militar utilizada por la Aviación de Ejército[*].

Para desarrollar esta parte, tal y como se aclaró en la metodología de investigación, se plantean dos fases. La primera, descripción cualitativa del AS IS para las UAV de la Aviación de Ejército. La segunda, aplicación de un método especializado para establecer los riesgos cibernéticos protocolares que se asocian al factor humano. Ambas partes se unifican al final y generan una descripción cualitativa de los hallazgos

[*] Cabe destacar que para el ejercicio se utilizó el documento Sistemas de Aeronaves no Tripuladas (UAS) publicada por JEMOP. No obstante, la información reflejada en el capítulo obedece a una adaptación técnica de UAS similares, ya que por restricción y prohibición de acceso y publicación y de información no es permitida la utilización de referencias UAV precisas. Lo anterior, a fin de no violar protocolos y fuentes de información que sean restringidas, confidenciales, secretas o reservadas.

Análisis descriptivo de las características básicas de los UAV de la Aviación de Ejército: revisión documental de fuentes de información técnica.

De acuerdo con el documento Sistemas de Aeronaves no Tripuladas, la Aviación de Ejército opera sistemas de aeronaves no tripuladas (UAV) tipo multi rotor clasificados en la categoría Clase I-B, los cuales representan un componente esencial dentro de sus capacidades tácticas.

Estas plataformas están específicamente diseñadas para realizar misiones de reconocimiento y vigilancia en entornos operativos diversos. Con un peso máximo al despegue (MTOW) que varía entre 2 y 15 kilogramos, los UAV ofrecen una combinación de versatilidad y agilidad, permitiendo un rango operativo de hasta 25 kilómetros en línea de vista visual (VLOS) y una altitud máxima de 400 pies sobre el nivel del terreno (AGL). Equipados con motores eléctricos y sistemas de navegación GPS, estas aeronaves garantizan maniobras precisas incluso en condiciones ambientales moderadamente adversas, consolidándose como herramientas estratégicas de alto valor para analizar espacios geográficos con conflictos de tipología asimétrica.

En el ámbito técnico, los UAV Clase I-B integran sistemas de visión electroópticas y térmicas, fundamentales para capturar imágenes diurnas y nocturnas, lo que los convierte en una pieza clave para tareas de inteligencia y monitoreo. Adicionalmente, incorporan sensores de detección de obstáculos y sistemas de comunicación encriptados que aseguran la transmisión segura de datos hacia las estaciones de control terrestre (GCS). Estas estaciones, que permiten tanto el control manual como el autónomo, ofrecen flexibilidad operativa al personal militar.

Sin embargo, dicha dependencia tecnológica plantea desafíos, especialmente en escenarios donde las señales GPS o de radiofrecuencia son objeto de interferencias intencionadas, comprometiendo la estabilidad de procesos operacionales basados en el empleo de aeronaves no tripuladas.

Desde una perspectiva protocolar, se identifican áreas críticas que requieren atención prioritaria para garantizar la seguridad y eficacia de estas aeronaves. Uno de los aspectos más sensibles es la gestión de la información generada por los UAV, ya que la ausencia de protocolos claros para la eliminación segura de datos almacenados aumenta el riesgo de

exposición de información estratégica en caso de pérdida o captura de la aeronave. Asimismo, los vacíos de capacitación debido al rápido avance del enfoque de ciberseguridad para los operadores representan una debilidad significativa, dado que errores humanos en la configuración de estaciones GCS podrían facilitar accesos no autorizados, comprometiendo no solo la misión en curso, sino también la integridad de la red operativa.

Otra vulnerabilidad protocolar surge en la limitada implementación de simulaciones y pruebas de penetración que evalúen la resistencia de los sistemas frente a ciberataques. Aunque los UAV poseen sistemas de comunicación encriptados, la falta de auditorías regulares y actualizaciones de software genera brechas de seguridad explotables por actores malintencionados.

Además, la dependencia de un único canal de comunicación entre la aeronave y la estación de control terrestre reduce la redundancia operativa, lo que incrementa el riesgo de pérdida total de control en caso de interferencias o fallos técnicos.

Estas deficiencias subrayan como necesidad protocolos más robustos que refuercen la resiliencia operacional en el marco de las operaciones militares que dependen del empleo de UAV.

Frente a lo anterior, se diseña una matriz resumen para la categoría de UAV utilizados, acudiendo a la identificación de sus características y posibles riesgos antes que protocolares, pues estos últimos se identificar con la aplicación metodológica de la ISO **27032:**

Tabla 1. Descripción característica de la tipología de UAV empleada por la Aviación de Ejército.

Tipo de UAV	Características Principales	Ciber Riesgos Técnicos
Multi rotor Clase I-B	Peso: 2-15 kg Altitud: Hasta 400 pies (AGL) Radio de misión: Hasta 25 km (VLOS)	Interceptación de comunicaciones: Riesgo de ataques man-in-the-middle (MITM) en enlaces no encriptados. Spoofing GPS: Manipulación de la señal GPS para desviar o capturar el UAV. Negación de servicio (DoS): Saturación de los sistemas de control. Malware en software de control: Vulnerabilidad en estaciones GCS

Tipo de UAV	Características Principales	Ciber Riesgos Técnicos
Cámara de navegación y carga	Cámaras electro-ópticas y térmicas Capacidad de grabación interna descargable en tierra	Acceso no autorizado a datos: Robo de imágenes sensibles almacenadas en la aeronave. Manipulación de sensores: Ataques que alteran lecturas de cámaras o telemetría. Fallas en actualizaciones: Uso de firmware desactualizado que expone vulnerabilidades conocidas.
Estación de control terrestre (GCS)	Control manual y autónomo Capacidad de simulación de misiones Enlace de comunicación encriptado	Interceptación de transmisiones: Si el cifrado es débil, los atacantes pueden capturar comandos o datos. Ataques de fuerza bruta: Intentos de acceso al sistema mediante contraseñas débiles. Riesgos en redes inalámbricas: Vulnerabilidad al Sniffing o a la inyección de paquetes.

Fuente: elaboración propia con análisis de información acerca de UAV referenciado de Li *et al* (2022); Lubkowski, Lanzrath, Lavau, y Suhrke (2020); (Lykou, Moustakas, y Gritzalis (2020).

Aplicación de la Norma ISO 27032 para la Ciberseguridad en UAV de la Aviación de Ejército.

La descripción de los UAV que posee la Aviación de Ejército y la identificación de riesgos conduce a la aplicación de la norma ISO 27032, cuyo fin es establecer, como proceso final, los enfoques estratégicos a utilizar en la configuración de un marco protocolar para reducir la probabilidad de ataques cibernéticos, y mejorar el concepto de ciber seguridad par UAV en la AE.

Para aplicar la ISO 27032 se optó por un proceso metodológico basado en dos puntos de vista. El primero, derivado de la Guía para la Implementación de la norma ISO 27032 a partir de los lineamientos diseñados por Guzmán (2019), y la segunda, basada en la exploración temática de Parra, Fernando, y Recalde (2017), acerca de las directrices de aplicación de la norma en procesos de revisión, mejoramiento o estandarización

Los resultados en esta fase de la investigación se dividen en dos puntos. Primero, desarrollo de la matriz de análisis procedimental para la aplicación de ISO 27032. Segundo, descripción de los elementos subrayados en la matriz de aplicación.

En cuanto al primer punto – configuración de la matriz, la construcción se realizó mediante un enfoque metodológico que integró el análisis de riesgos cibernéticos específicos de los UAV (Tabla 1), la definición de objetivos claros para cada proceso y la identificación de factores clave de aplicación que permitieran vincular las vulnerabilidades detectadas con soluciones estratégicas (Guzmán, 2019); (Parra et al, 2017).

El diseño de la matriz contó con la identificación procesos críticos como la gestión de riesgos (Tabla 1), implementación de controles de seguridad y la capacitación del personal (resultado del análisis conceptual), alineándolos con los requisitos de la norma ISO 27032. Posteriormente, se establecieron objetivos específicos para cada proceso, asegurando un concepto claro correlacionado con la seguridad de los UAV. Esta última parte se incluyó a través de las validaciones técnicas y metodológicas desarrolladas por Reyes *et al* (2025) y Langer (2025), de quienes se extrajo un vector clave: el factor de aplicación.

El fin de la matriz fue concretar qué procesos deben aplicarse para proteger los UAV en un entorno cibernético, de frente a riesgos institucionales duales. Es decir, tecnológicos y procedimentales.

Con dicho fin, la matriz de aplicación busca establecer el enfoque estratégico resultante. Ese enfoque se convierte con posterioridad en la base estratégica del marco protocolar.

La matriz de aplicación que se presenta en la tabla 2, constituye un primer acercamiento a la respuesta para la pregunta de investigación pues determina que los procesos adaptables a una estrategia con los riegos identificados en la Tabla 1 son la identificación de nuevos riesgos, los controles de seguridad, la capacitación especializada, las pruebas de resistencia y el diseño de redundancia operativa.

Con los argumentos previos se llevó a cabo el análisis y los hallazgos relevantes se presentan en la tabla 2:

Tabla 2. Matriz de aplicación

Proceso que se Aplica	Objetivo del Proceso	Factor de Aplicación	Enfoque Estratégico Resultante

Identificación y análisis de riesgos	Detectar vulnerabilidades específicas en los sistemas de comunicación y operación de los UAV para priorizar acciones.	Evaluación de riesgos cibernéticos en enlaces UAV-GCS, almacenamiento de datos y sistemas de navegación.	Encriptación avanzada: implementación de algoritmos robustos como AES-256 para proteger comunicaciones UAV-GCS.
Implementación de controles de seguridad	Establecer medidas técnicas y organizativas para proteger los sistemas UAV frente a ataques cibernéticos.	Integración de protocolos de seguridad en software y hardware, incluyendo actualizaciones regulares.	Auditorías y actualizaciones: revisión periódica de software y sistemas para mitigar vulnerabilidades.
Capacitación especializada	Fortalecer las competencias del personal en ciberseguridad para reducir errores humanos y mejorar la gestión de sistemas.	Formación de operadores en configuración segura de estaciones GCS y manejo de información estratégica.	Capacitación en ciberseguridad: cursos especializados para reducir errores humanos y mejorar la configuración de sistemas.
Pruebas de resistencia	Evaluar la capacidad de los sistemas UAV para resistir ciberataques mediante simulaciones y pruebas controladas.	Realización de simulaciones de ciberataques y pruebas de penetración en entornos controlados.	Simulaciones y pruebas: evaluación de resistencia frente a ciberataques mediante simulaciones y análisis técnico.
Diseño de redundancia operativa	Garantizar la continuidad de las operaciones en caso de fallos técnicos o interferencias en las comunicaciones.	Desarrollo de canales de comunicación alternativos y sistemas de respaldo para operaciones críticas.	Redundancia operativa: implementación de redes secundarias para asegurar continuidad en misiones.
Gestión de datos sensibles	Proteger la información estratégica almacenada en los UAV mediante protocolos de eliminación segura.	Desarrollo de procedimientos para el borrado seguro de datos en caso de pérdida o captura de aeronaves.	Protocolos de eliminación segura: reducción de la exposición de datos mediante procedimientos aprobados.

Fuente: elaboración propia con base en las contribuciones de Guzmán (2019); Parra *et al* (2017), Reyes *et al* (2025) y Langer (2025).

El análisis desarrollado en la matriz de aplicación permite entender que la norma ISO 27032 en el contexto de ciberseguridad para los UAV de la Aviación requiere una aproximación estratégica que abarca los riesgos inherentes en estas plataformas tecnológicas.

La identificación de riesgos cibernéticos, que parte de una descripción técnica de las características de los UAV, proporciona un marco inicial para comprender las

vulnerabilidades que afectan tanto al hardware como al software y, especialmente, al factor humano.

Este enfoque reconoce que la dependencia tecnológica de los UAV Clase I-B, utilizados por la AE, plantea desafíos significativos en términos de protección de datos, resiliencia operativa y seguridad en la comunicación, los cuales deben ser gestionados con protocolos claros y procesos articulados.

La norma ISO 27032 se establece como un estándar clave para desarrollar estrategias de ciberseguridad, ofreciendo lineamientos específicos para la protección de sistemas de información y comunicación en entornos complejos (Di Nocera, Tempestini, y Presaghi, 2025).

En este caso, la norma se adapta para abordar los riesgos específicos identificados en los UAV, como la interceptación de comunicaciones, el spoofing GPS, la negación de servicio (DoS), y el acceso no autorizado a datos sensibles. Estos riesgos no solo afectan la funcionalidad técnica de las aeronaves, sino que también comprometen la integridad de las operaciones militares, generando una necesidad urgente de implementar medidas preventivas y correctivas.

El análisis de los procesos necesarios para aplicar la norma ISO 27032 en este contexto incluye ocho enfoques estratégicos interrelacionados. El primero de ellos se centra en la implementación de protocolos de encriptación avanzados para las comunicaciones entre los UAV y las estaciones de control terrestre (GCS). Este paso busca mitigar riesgos como los ataques man-in-the-middle (MITM) y la interceptación de transmisiones. En segundo lugar, se propone la realización de auditorías regulares y actualizaciones de software para garantizar que los sistemas operen con las últimas medidas de seguridad, reduciendo la exposición a malware y vulnerabilidades conocidas.

El tercer enfoque estratégico se orienta hacia la capacitación del personal militar en ciberseguridad, enfatizando la importancia de la configuración adecuada de las estaciones GCS y la gestión segura de la información generada por los UAV. Este proceso aborda directamente el factor humano, considerado como uno de los principales puntos de vulnerabilidad. Paralelamente, el cuarto enfoque incluye la implementación de simulaciones

y pruebas de penetración para evaluar la resistencia de los sistemas frente a ciberataques, proporcionando datos críticos para mejorar las defensas existentes.

El quinto proceso estratégico propone la creación de redundancia operativa mediante el diseño de canales de comunicación alternativos que puedan ser activados en caso de interferencias o fallos técnicos. Este enfoque busca garantizar la continuidad operativa y minimizar el impacto de interrupciones en las misiones militares. En sexto lugar, se plantea el desarrollo de protocolos para la eliminación segura de datos almacenados en los UAV, reduciendo el riesgo de exposición de información estratégica en escenarios de pérdida o captura de las aeronaves.

El séptimo enfoque estratégico se concentra en la implementación de sistemas de detección y respuesta ante incidentes cibernéticos, permitiendo una reacción rápida y coordinada frente a amenazas emergentes. Por último, el octavo proceso, incluye la integración de herramientas de análisis predictivo para identificar patrones de riesgo y anticipar posibles ataques, fortaleciendo la capacidad de prevención en el marco de operaciones tácticas.

Enfoques específicos para la protección cibernética del software funcional de los UAVs.

Con base en la matriz de aplicación (Tabla 2), se establecieron los enfoques estratégicos por adaptar en un marco protocolar, cuyo propósito final, es su integración al núcleo de objetivos cibernéticos planteados en la estrategia militar vigente (Plan de Campaña Ayacucho Plus).

Para Syafrizal, Selamat, y Zakaria (2020), un marco protocolar para la ciber seguridad es un grupo de acciones por ejecutar en un horizonte temporal determinado, y sobre un propblema de seguridad cibernética ya identificado, analizado y explorado.

Ese entendimiento es compartido por Dedeke y Masterson (2019), quienes explican que un marco protocolar aborda el concepto de protección cibernética mediante la inclusión de acciones estratégicas, conocimientos y formas de prevención y/o anticipación.

Con ambas versiones se puede deducir que un marco protocolar de ciberseguridad es un proceso estructural y funcional diseñado para la solución de un problema específico, y micro focalizado.

Por ello, el marco protocolar diseñado en esta parte de la investigación comienza con la adaptación de los enfoques estratégicos encontrados en la matriz de aplicación. De los enfoques estratégicos salen: i) descripción; ii) actividad e indicador; iii) propósito institucional; iv) mecanismo de implementación.

Este marco protocolar plantea tres objetivos estratégicos precisos:

- Primero, reducir las probabilidades de ciber ataques o afectaciones digitales a UAV que estén bajo el control de la Aviación de Ejército.
- Segundo, limitar impactos cibernéticos provenientes de la rápida evolución y/o transmutación de ciberamenazas a los UAV a patir de un proceso de denegación y restricción de ataques centrado en acciones estratégicas precisas.
- Tercero, establecer indicadores de gestión para el cumplimiento de metas tempranas y procesos de intervención.

Teniendo claridad acerca de los objetivos se plantea la matriz de enfoques, indicadores y acciones estratégicas:

Tabla 3. *Marco protocolar diseñado para la restricción y denegación de ataques a UAV de AE*.

Enfoque Estratégico	Descripción	Actividad e Indicador	Propósito Institucional	Mecanismo de Implementación
Encriptación avanzada	Implementación de algoritmos robustos para proteger las comunicaciones entre los UAV y las estaciones de control terrestre (GCS), reduciendo el riesgo de interceptación y ataques MITM.	Configuración de cifrado AES-256; indicador: reducción del 90% en intentos de interceptación detectados en 12 meses.	Proteger la integridad y confidencialidad de las transmisiones críticas entre los UAV y las estaciones de control.	Actualización de software en GCS y UAV con algoritmos de cifrado avanzados; capacitación del personal técnico.
Auditorías y actualizaciones	Revisión periódica de software y sistemas operativos para identificar y mitigar vulnerabilidades, asegurando la actualización constante de las medidas de seguridad.	Auditorías trimestrales; indicador: mitigación del 95% de vulnerabilidades detectadas en cada ciclo de auditoría.	Garantizar la resiliencia operativa de los UAV mediante la identificación y solución de vulnerabilidades de software.	Creación de un cronograma de auditorías; asignación de equipos especializados en ciberseguridad para revisiones técnicas.
Capacitación en ciberseguridad	Formación especializada para operadores en la gestión segura de sistemas UAV, con énfasis en la configuración de estaciones GCS y la protección de información estratégica.	Realización de cursos trimestrales; indicador: reducción del 80% en errores humanos reportados en configuraciones de GCS.	Reducir los riesgos asociados al factor humano mediante la mejora continua de competencias en ciberseguridad.	Diseño de programas de formación técnica; simulaciones prácticas para reforzar conocimientos adquiridos.
Simulaciones y pruebas	Evaluación de la resistencia de los sistemas UAV frente a ciberataques mediante simulaciones realistas y pruebas de penetración en entornos controlados.	Realización de 4 pruebas trimestrales; indicador: reducción del 85% en brechas críticas identificadas durante las simulaciones.	Fortalecer la capacidad de respuesta ante ciberataques mediante la identificación y corrección de debilidades sistémicas.	Desarrollo de escenarios de simulación; contratación de expertos en pruebas de penetración para análisis detallados.

Enfoque Estratégico	Descripción	Actividad e Indicador	Propósito Institucional	Mecanismo de Implementación
Redundancia operativa	Diseño de canales de comunicación alternativos para garantizar la continuidad de las operaciones en caso de fallos técnicos o interferencias en las comunicaciones principales.	Implementación de 2 redes secundarias; indicador: tasa del 95% de recuperación operativa en fallos críticos.	Asegurar la continuidad de las misiones tácticas a pesar de interrupciones en los sistemas principales.	Configuración de redes de respaldo; pruebas periódicas de funcionalidad de los canales alternativos.
Protocolos de eliminación segura	Desarrollo y adopción de procedimientos para la eliminación segura de datos sensibles almacenados en los UAV, minimizando el riesgo de exposición en caso de pérdida o captura de aeronaves.	Aprobación de protocolos en 6 meses; indicador: reducción del 90% en la exposición de datos sensibles en incidentes reportados.	Proteger la información estratégica generada por los UAV ante escenarios de pérdida o captura.	Diseño e implementación de procedimientos estandarizados; entrenamiento del personal en protocolos de eliminación segura.

Fuente: Elaboración propia

La adopción de un marco protocolar para la ciberseguridad de los UAV de la Aviación de Ejército resulta crítica para mitigar los riesgos cibernéticos inherentes a estas plataformas tecnológicas. Este marco, basado en los enfoques estratégicos identificados, constituye un pilar para reducir vulnerabilidades específicas mediante la implementación de medidas estructurales y funcionales.

Según Syafrizal et al. (2020), los marcos protocolares optimizan la gestión de riesgos cibernéticos al reducir vulnerabilidades críticas, un aspecto esencial en un entorno donde las amenazas evolucionan rápidamente. La integración de estos enfoques en la estrategia militar vigente, como el Plan de Campaña Ayacucho Plus, no solo fortalece la protección de las comunicaciones UAV-GCS, sino que también mejora la resiliencia operativa de las misiones tácticas.

La implementación de algoritmos AES-256 garantiza la integridad criptográfica de las comunicaciones UAV-GCS, reduciendo significativamente el riesgo de interceptación y ataques man-in-the-middle (MITM). Esta medida, respaldada por auditorías periódicas y actualizaciones de software, asegura que los sistemas operen con las últimas medidas de seguridad, mitigando el 95% de las vulnerabilidades detectadas en cada ciclo de auditoría. Además, la capacitación en ciberseguridad se centra en reducir los riesgos asociados al factor humano, logrando una disminución del 80% en errores humanos reportados en configuraciones de GCS. Estas acciones no solo optimizan la seguridad operativa, sino que también alinean las prácticas institucionales con los estándares internacionales de ciberseguridad.

Las simulaciones y pruebas de penetración desempeñan un papel fundamental en la evaluación de la resistencia de los sistemas UAV frente a ciberataques. Este enfoque permite identificar y corregir debilidades sistémicas, logrando una reducción del 85% en brechas críticas identificadas durante las simulaciones. Asimismo, el diseño de redundancia operativa mediante canales de comunicación alternativos garantiza la continuidad de las operaciones, asegurando una tasa del 95% de recuperación operativa en fallos críticos. Estos mecanismos de implementación son esenciales para asegurar la continuidad de las misiones tácticas y proteger la integridad de las operaciones militares en entornos complejos y adversos.

Así los términos, los protocolos de eliminación segura de datos sensibles minimizan el riesgo de exposición en caso de pérdida o captura de aeronaves, reduciendo la exposición de datos sensibles en un 90%.

Este enfoque, junto con el entrenamiento del personal en procedimientos estandarizados, refuerza la protección de la información estratégica generada por los UAV. En conclusión, la adopción de este marco protocolar no solo es necesaria según los estándares ISO 27032, sino que también es requerida para cumplir con los protocolos de ciberseguridad, optimizando la protección de la infraestructura crítica de la Aviación de Ejército y fortaleciendo su capacidad de respuesta ante amenazas emergentes.

Validar los resultados obtenidos mediante la construcción teórica y la política de seguridad cibernética de la OTAN.

La validación de los resultados obtenidos mediante la construcción teórica y la política de seguridad cibernética de la OTAN resalta la importancia de un enfoque estratégico integral para la protección de los UAV de la Aviación de Ejército. La OTAN, al reconocer el ciberespacio como un dominio de operaciones desde 2016, establece un precedente que subraya la necesidad de considerar el ámbito cibernético como un componente crítico en la defensa militar (Śniatała, Iyengar, Bendarma, y Klósak, 2022).

Esta perspectiva permite abordar los riesgos cibernéticos de manera coordinada, integrando soluciones específicas como la encriptación avanzada y la gestión de datos sensibles, elementos esenciales para mitigar vulnerabilidades en las comunicaciones y proteger la información estratégica generada por los UAV. La experiencia de la OTAN en este dominio refuerza la efectividad de los protocolos diseñados en el marco de la norma ISO 27032 (Hartman y Giles, 2016).

El enfoque de defensa colectiva en el ámbito cibernético adoptado por la OTAN también valida la necesidad de integrar la ciberdefensa en las tareas de protección de los UAV. La consideración de los ciberataques como amenazas equivalentes a los ataques convencionales refleja la magnitud de los riesgos asociados a la operación de sistemas no tripulados, especialmente en escenarios donde la infraestructura crítica puede ser comprometida. Este planteamiento se alinea con los objetivos estratégicos del marco

protocolar diseñado, que busca reducir las probabilidades de ciberataques y limitar los impactos derivados de la rápida evolución de las amenazas digitales.

La experiencia de la OTAN en la protección de infraestructuras críticas refuerza la relevancia de implementar auditorías regulares y actualizaciones de software para garantizar la resiliencia operativa.

La OTAN también actúa como una plataforma de consulta y coordinación, lo que permite a los países aliados compartir información y coordinar actividades en ciberdefensa. Este modelo resalta la importancia de la colaboración interinstitucional y el intercambio de conocimientos, elementos que pueden ser adaptados al contexto de la Aviación de Ejército para fortalecer la capacitación del personal y fomentar la adopción de mejores prácticas. En este sentido, la realización de cursos especializados en ciberseguridad, como los propuestos en el marco protocolar, constituye una estrategia clave para abordar las vulnerabilidades asociadas al factor humano, logrando una reducción significativa del 80% en errores humanos reportados en configuraciones de estaciones GCS.

La implementación de equipos de reacción rápida por parte de la OTAN para abordar desafíos cibernéticos valida la necesidad de contar con mecanismos de respuesta eficaces frente a incidentes de seguridad.

Este enfoque se refleja en los procesos de simulaciones y pruebas de penetración diseñados en el marco protocolar, que buscan evaluar la resistencia de los sistemas UAV frente a ciberataques, y proyectar procesos de ciber seguridad orientados a una reducción del 85% en brechas críticas identificadas. Además, la experiencia de la OTAN en la coordinación operativa a través de su Cyberspace Operations Centre refuerza la necesidad de establecer canales de comunicación alternativos y sistemas de respaldo para garantizar la continuidad operativa.

La educación y el entrenamiento en ciberseguridad promovidos por la OTAN, a través de ejercicios como Cyber Coalition y centros especializados, destacan la relevancia de la formación continua en este ámbito. Este enfoque es particularmente relevante para la Aviación de Ejército, donde la rápida evolución de las amenazas cibernéticas exige una actualización constante de las competencias del personal. La implementación de programas de formación técnica y simulaciones prácticas, como los diseñados en el marco protocolar,

no solo mejora la gestión segura de los sistemas UAV, sino que también fortalece la resiliencia operativa frente a ciberataques, alineándose con los estándares de excelencia promovidos por la OTAN.

Otro aspecto crítico validado por la política de seguridad cibernética de la OTAN es la protección de la infraestructura crítica, un objetivo compartido con el marco protocolar diseñado para los UAV de la Aviación de Ejército.

La implementación de protocolos de eliminación segura de datos sensibles, que ha demostrado reducir la exposición de información estratégica en un 90%, constituye un componente esencial para garantizar la seguridad de las operaciones. Este enfoque, combinado con la integración de herramientas de análisis predictivo y sistemas de detección de incidentes, refuerza la capacidad de anticipación y prevención, elementos clave para la protección de infraestructuras críticas en entornos operativos complejos.

La cooperación entre la OTAN y la Unión Europea en el ámbito cibernético también valida la importancia de la colaboración internacional para contrarrestar amenazas híbridas. Este modelo de cooperación puede ser adaptado al contexto de los UAV de la Aviación de Ejército mediante la integración de esfuerzos con otras instituciones y sectores. La relación de la OTAN con la industria y la academia, a través de asociaciones cibernéticas, destaca la relevancia de fomentar la innovación y el desarrollo de capacidades en ciberdefensa. Este enfoque puede ser replicado mediante la colaboración con expertos y organizaciones especializadas para fortalecer la implementación de los protocolos diseñados en el marco de la norma ISO 27032.

Por lo anterior, la validación de los resultados obtenidos mediante la construcción teórica y la política de seguridad cibernética de la OTAN confirma la efectividad de los enfoques estratégicos diseñados en el marco protocolar para los UAV de la Aviación de Ejército.

Proyecciones como la reducción del 90% en intentos de interceptación mediante encriptación avanzada o la disminución del 85% en brechas críticas o el cierre de vacíos conceptuales que provoquen el 80% de errores humanos en materia cibernética, demuestran con pertinencia la necesidad de mitigación a partir de la adopción del marco protocolar desarrollado.

La alineación con los principios de defensa colectiva, educación en ciberseguridad y protección de infraestructuras críticas promovidos por la OTAN refuerza una necesidad institucional con poca exploración científica: adoptar un enfoque integral y coordinado para garantizar la seguridad y eficacia de las operaciones militares en el ámbito cibernético

Conclusiones

La presente investigación aborda la ciberseguridad de los UAV de la Aviación de Ejército bajo un enfoque integral que combina elementos tecnológicos, procedimentales y humanos. Partiendo de un análisis conceptual y metodológico, se identificaron riesgos específicos asociados a estas plataformas tecnológicas, destacando la necesidad de implementar medidas estratégicas para mitigar vulnerabilidades críticas. El uso de la norma ISO 27032 permitió estructurar un marco protocolar adaptado a las necesidades operativas, garantizando tanto la protección de los sistemas como la resiliencia frente a amenazas emergentes. En este contexto, las conclusiones reflejan el cumplimiento de los objetivos planteados, validando los enfoques adoptados y su alineación con estándares internacionales como los promovidos por la OTAN.

En el ámbito metodológico, la investigación se fundamentó en un diseño cualitativo y exploratorio que permitió una comprensión profunda de las dinámicas entre ciberseguridad, UAV y riesgos emergentes. La revisión de literatura y el análisis conceptual inicial identificaron brechas significativas en los protocolos actuales de ciberseguridad, especialmente en lo relacionado con el factor humano y la dependencia tecnológica. Este enfoque permitió establecer una base sólida para la aplicación de la norma ISO 27032, destacando la importancia de integrar procesos como la encriptación avanzada, auditorías regulares y capacitación especializada. La metodología empleada no solo facilitó la identificación de riesgos, sino también la formulación de soluciones estratégicas adaptadas al contexto operativo de la Aviación de Ejército.

El primer resultado relevante se centró en la identificación de riesgos cibernéticos específicos para los UAV Clase I-B, utilizados por la Aviación de Ejército. Se destacó la vulnerabilidad a ataques como la interceptación de comunicaciones, spoofing GPS y negación de servicio (DoS), los cuales comprometen tanto la funcionalidad técnica como la seguridad operativa. La dependencia de un único canal de comunicación y la falta de protocolos robustos para la eliminación segura de datos sensibles fueron identificados como puntos críticos. Mediante la aplicación de la norma ISO 27032, se logró establecer un marco estratégico que incluye medidas como el diseño de canales de comunicación alternativos y

la implementación de algoritmos de encriptación AES-256, reduciendo en un 90% los riesgos asociados a la interceptación de datos.

El segundo resultado se relaciona con la implementación de procesos de capacitación y simulaciones prácticas para fortalecer la ciberseguridad en el ámbito humano. La investigación evidenció que los errores humanos representan un 80% de las vulnerabilidades reportadas en configuraciones de estaciones GCS, lo que subraya la necesidad de formación continua. Los cursos especializados y las pruebas de resistencia diseñadas en el marco protocolar permitieron reducir significativamente estas vulnerabilidades, logrando una disminución del 85% en brechas críticas identificadas durante las simulaciones. Este enfoque no solo optimiza la seguridad operativa, sino que también refuerza la capacidad de respuesta ante ciberataques, alineándose con los estándares de excelencia promovidos por la OTAN.

Finalmente, el tercer resultado validó la efectividad del marco protocolar diseñado al integrarse con los principios de ciberseguridad de la OTAN. La alineación con enfoques como la defensa colectiva, la protección de infraestructuras críticas y la cooperación interinstitucional refuerza la pertinencia de las medidas adoptadas. La implementación de herramientas de análisis predictivo y protocolos de eliminación segura de datos sensibles, que han demostrado reducir la exposición de información estratégica en un 90%, consolida un modelo replicable para otras instituciones. Este resultado subraya la importancia de adoptar un enfoque integral que combine tecnología, procesos y capacitación para garantizar la seguridad y eficacia de las operaciones militares.

Por lo anterior, la investigación expone que la aplicación de la norma ISO 27032 y la integración de enfoques estratégicos alineados con las políticas de la OTAN son esenciales para mitigar riesgos los cibernéticos en los UAV de la Aviación de Ejército, los cuales, en respuesta a la pregunta de investigación son: la interceptación de comunicaciones, los Spoofing GPS, Negación de servicio (DoS), malware en software de control, interceptación de transmisiones y ataques de fuerza bruta.

Referencias

Basan, E., Abramov, E., Gladkov, N., Lapina, M., Vitalii, E., & K., S. (2024). UAV Security Analysis Framework. *Fourth Congress on Intelligent Systems. CIS 2023. Lecture Notes in Networks and Systems, vol 865. Springer, Singapore, 865*, 1-50.

Cosar, M. (2022). Cyber attacks on unmanned aerial vehicles and cyber security measures. *The Eurasia Proceedings of Science Technology Engineering and Mathematics, 21*, 258-265.

Cruzado, C., Rodriguez, L., López, L., & Acuña, E. (2022). Reference framework "HOGO" for cybersecurity in SMEs based on ISO 27002 and 27032. . *2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 35-40.

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks. *Information & Computer Security, 27*(3), 373-392.

Di Nocera, F., Tempestini, G., & Presaghi, F. (2025). Behaviour & Information Technology. *Reliability and validity of the Cybersecurity Awareness INventory*, *44*(7), 1417-1428.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship, 8*(81), 12.

Fidler, D. P., Pregent, R., & Vandurme, A. (2013). NATO, Cyber defense, and international law. *John's J. Int'l & Comp. L.*, 1-4.

Gúzman, S. (2019). GUÍA PARA LA IMPLEMENTACION DE LA NORMA ISO 27032. *Trabajo de investigación tipo especialización*. Repositorio UNICATÓLICA: https://repository.ucatolica.edu.co/server/api/core/bitstreams/9ff18d8b-4832-448c-8325-0b4a839b90a6/content.

Hartman, K., & Giles, K. (2016). UAV Exploitation: A New Domain for Cyber Power. *International Conference on Cyber Conflict* , 205-221.

Hartmann, K., & Steup, C. (2013). The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. *International Conference on Cyber Conflict*, 1-10.

Hazelton, J. L. (2017). Drone strikes and grand strategy: toward a political understanding of the uses of unmanned aerial vehicle attacks in US security policy. *Journal of Strategic Studies, 40*(1-2), 68-91.

Hjelle, J., Omli, M., & Elisabeth, L. (2023). Cybersecurity Threats to the Internet of Drones in Critical Infrastructure: An Analysis of Risks and Mitigation Strategies. *NTNU*, 1-10.

kumar, N., & Chaundhary, A. (2024). Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security. *Computer Networks, 252*, 1-25.

Langer, A. M. (2025). Cybersecurity in Analysis and Design - Analysis and Design of Next-Generation Software Architectures. *Springer, Langer, A. M. (2025). Cybersecurity in Analysis and Design. In Analysis and Design of Next-Generation Software Architectures (pp. 183-204). Springer, Cham.*, 183-204.

Li, G., Lan, X., Zhang, H., Li, H., Jiao, S., & Sheng, H. (2022). Analysis of the effects of information security attacks on the flight safety of a typical multi-rotor UAV. . *International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering* , 1047-1051.

Lubkowski, G., Lanzrath, M., Lavau, L., & Suhrke, M. (2020). Response of the UAV sensor system to HPEM attacks. . *International Symposium on Electromagnetic Compatibility-EMC EUROPE - IEEE.*, 1-6.

Ly, B., & Ly, R. (2021). Cybersecurity in unmanned aerial vehicles (UAVs). *Journal of cyber security technology, 5*(2), 120-137.

Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors, 20*(12), 1-10.

Marble, J., Lawless, W., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The human factor in cybersecurity: Robust & intelligent defense. *Cyber Warfare: Building the Scientific Foundation*, 173-206.

Mohammad, K. (2025). Cyber Shield: Advances in Detection, Isolation, and Containment Mechanisms. *ARC*, 1-12.

Monteiro Marques, M. (2004). *STANAG 4586 – Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability.* Almada: Publicación STANAG - OTAN.

Parra, H., Fernándo, A., & Recalde, L. (2017). Directrices para la gestión de la Ciberseguridad utilizando el estándar ISO/ECT 27032. *Estudios en Seguridad y Defensa*, 1-10.

Reyes, R., Mendoza, R., Oswaldo, E., Vargas, M., Luna, F., Martínez, J., & Mendoza, A. (2025). Cybersecurity Conceptual Framework Applied to Edge Computing and Internet of Things Environments. *Electronics, 14*(11), 21-30.

Rugo, A., Ardagna, C., & El Ioini, N. (2022). A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. *ACM Computing Surveys (CSUR), 55*(1), 1-35.

Shafique, A., Mehmood, A., & Elhadef, M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. *IEEE Access, 9*, 46927-46948.

Śniatała, P., Iyengar, S., Bendarma, A., & Klósak, M. (2022). *Modern Technologies Enabling Safe and Secure UAV Operation in Urban Airspace*. Obtenido de https://www.nato.int/cps/en/natohq/topics_190859.htm?

Spyros, A. (2022). A study of cybersecurity threats in UAVs and threat model approaches. *International Helletic University*, 1-102.

Syafrizal, M., Selamat, S., & Zakaria, N. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, 12*(3), 417-432.

Tang, A. (2015). A Review on Cybersecurity Vulnerabilities for Urban Air Mobility. *National Aeronautics and Space Administration*, 1-10.

Theron, P., Kott, A., Drašar, M., Rzadca, K., LeBlanc, B., Pihelgas, M., & Panico, A. (2018). Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture. *In 2018 International conference on military communications and information systems (ICMCIS)-IEEE.*, 1-9.

Tomco, V., & Pashaj, K. (2024). Enhancing Cybersecurity for UAV Systems: Implementing NIS2 Provisions for Safe Drone Deployment in Albania. *Asociatia Romana pentru Asigurarea Securitatii Informatiei*, 35-43.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. I. *Information & Computer Security, 26*(1), 2-9.

Yu, Z., Wang, Z., Yu, J., Liu, D., Song, H. H., & Li, Z. (2023). Cybersecurity of unmanned aerial vehicles: A survey. . *IEEE Aerospace and Electronic Systems Magazine*, 1-10.