ANÁLISIS DE RIESGOS CIBERNÉTICOS PARA SISTEMAS ADS-B (AUTOMATIC DEPENDENT SURVEILLANCE BROADCAST) DURANTE OPERACIONES AÉREAS

Mayor (FAC) Víctor Alfonso López Salguero

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 (FAC) Víctor Alfonso López Salguero
Identificación	**:**	94542963
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	PhD. Jairo Andrés Becerra Cuervo
Tutor temático	**:**	PhD. Jimmy Anderson Flórez
Fecha de entrega	**:**	11 de agosto de 2025
Extensión	**:**	11.467 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

ANÁLISIS DE RIESGOS CIBERNÉTICOS PARA SISTEMAS ADS-B (AUTOMATIC DEPENDENT SURVEILLANCE BROADCAST) DURANTE OPERACIONES AÉREAS

Analysis of Cyber Risks in the Use of the ADS-B System During Air Operations

Víctor Alfonso López Salguero[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El sistema ADS-B (Automatic Dependent Surveillance-Broadcast) ha fortalecido la vigilancia aérea al ofrecer actualizaciones de mayor precisión y en tiempo real de la posición de aeronaves, mejorando la gestión del tráfico aéreo. Sin embargo, su diseño abierto, sin mecanismos de cifrado ni autenticación, se han expuesto vulnerabilidades frente a ciberataques como la inyección de mensajes, GPS spoofing, modificación y eliminación de mensajes. Este artículo analiza mencionadas vulnerabilidades, su impacto en la operación aérea y las posibles estrategias de mitigación basadas en los modelos FAST y STRIDE. Se propone además el procedimiento C.A.R.E. (Coordinación, Autenticación, Respuesta y Evaluación) como iniciativa para fortalecer la resiliencia cibernética del sistema en Colombia, complementado con un modelo híbrido de gestión de riesgos utilizando FAST y mapas cognitivos difusos.

Palabras clave: ADS-B; ciberseguridad; FAST y STRIDE; procedimiento C.A.R.E.; Riesgos, Vulnerabilidades.

Abstract: The Automatic Dependent Surveillance-Broadcast (ADS-B) system has strengthened air traffic surveillance by providing more accurate and real-time updates of aircraft positions, enhancing air traffic management. However, its open design, lacking encryption and authentication mechanisms, has exposed vulnerabilities to cyberattacks such as message injection, GPS spoofing, message modification, and deletion. This article analyzes these vulnerabilities, their impact on air operations, and possible mitigation strategies based on the FAST and STRIDE models. Additionally, the C.A.R.E. protocol (Coordination, Authentication, Response, and Evaluation) is proposed as an initiative to enhance the cyber resilience of the system in Colombia, complemented by a hybrid risk management model using fuzzy cognitive maps.

Keywords: ADS-B; C.A.R.E. protocol; cybersecurity; FAST and STRIDE model; risks; vulnerabilities.

[1] Mayor de la Fuerza Aeroespacial Colombiana. Candidato a magíster en ciberseguridad y ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Ing. Informático, Escuela Militar de Aviación "Marco Fidel Suárez", Colombia. https://orcid.org/0009-0009-6001-6198 - Contacto: victor.lopez@esdeg.edu.co.

Introducción

En el contexto de la aviación moderna, el uso del sistema ADS-B (Automatic Dependent Surveillance-Broadcast) ha supuesto un avance en la vigilancia del tráfico aéreo al permitir un control más preciso y actualizado de la posición de las aeronaves, facilitando la transmisión automática de información aeronáutica, como la posición, velocidad y altitud de aeronaves, tanto a los controladores del tráfico aéreo como a otras aeronaves equipadas con ADS-B. Sin embargo, su diseño y arquitectura, basado en la emisión continua de datos sin mecanismos de cifrado ni autenticación, expone al sistema ante vulnerabilidades cibernéticas que pueden comprometer la integridad, disponibilidad y autenticidad de la información transmitida mediante el mismo. Estas vulnerabilidades han sido objeto de múltiples estudios y análisis, evidenciando que algunos ciberataques como la inyección de mensajes falsos, alteran o desaparecen mensajes que podrían comprometer la seguridad durante el vuelo.

En este contexto, el presente artículo analiza las principales vulnerabilidades cibernéticas asociadas al sistema ADS-B durante las operaciones aéreas, enfatizando en aquellos vectores de ataque que afectan directamente la continuidad operativa.

De igual forma, se propone una clasificación de las vulnerabilidades y análisis de cada uno de los riesgos mediante la metodología FAST (Functional Analysis System Technique) y posteriormente se plantea un nuevo modelo híbrido dentro del análisis de los riesgos asociados con relación a las variables identificadas para tal fin con la creación de Mapas Cognitivos Difusos. Así mismo, se propone el procedimiento C.A.R.E. (Coordinación,

Autenticación, Respuesta y Evaluación), una iniciativa procedimental diseñada para fortalecer la resiliencia del sistema ADS-B en el contexto colombiano.

Metodología

La investigación adopta un enfoque cualitativo, orientado al análisis comprensivo de vulnerabilidades cibernéticas asociados al uso del sistema ADS-B en operaciones aéreas en el contexto colombiano. El método empleado es de carácter deductivo, donde se iniciará con la identificación y clasificación de las vulnerabilidades del sistema mediante la recopilación de información basada en revisión bibliográfica de fuentes científicas, documentos técnicos de organismos internacionales (OACI, FAA, EASA), normativas nacionales (RAC 91, Resolución 02217 de 2023) y literatura reciente sobre ciberseguridad en sistemas ADS-B.

Se va a realizar un estudio estructurado de las principales vulnerabilidades encontradas en el estado del arte, además de realizar pruebas de laboratorio en la validación de la vulnerabilidad de message injection de forma simulada y real, mediante el uso de un HackRF y un RTL-SDR, usando el sistema operativo Linux-Ubunto y lenguaje de programación Python, posteriormente se realiza la categorización de los ataques del sistema ADS-B con base en la confidencialidad, integridad, disponibilidad y autenticación.

Para la clasificación de los riesgos del sistema, primero se hará una clasificación de las vulnerabilidades con base a su severidad y probabilidad para determinar el nivel de riesgo, luego se llevará a cabo el análisis de estos mediante la revisión de distintas metodologías, para poder identificarlos y luego usar modelos existentes en ciberseguridad (FAST y STRIDE) para la evaluación de los riesgos del sistema.

Con la finalidad de abordar de manera holística los riesgos del sistema ADS-B en el contexto aeronáutico colombiano, se propone un modelo híbrido que combina distintos resultados (enfoque FAST, información de la red de coocurrencia y los resultados obtenidos de la metodología Delphi efectuada a expertos) junto con técnicas de mapas conceptuales difusos, con la finalidad de fortalecer la modelación de los riesgos asociados.

Finalmente, se desarrolla como iniciativa, el Procedimiento C.A.R.E (Coordinación, Autenticación, Respuesta y Evaluación), la cual actúa como respuesta operativa y estructurada, proponiendo soluciones aplicables en escenarios operativos reales, para fortalecer la seguridad operacional en el entorno aéreo colombiano.

1. Estado del Arte

A lo largo de los últimos años, diversos incidentes han evidenciado la vulnerabilidad cibernética del sector aeronáutico ante ataques cibernéticos, desde la interrupción de servicios en torres de control hasta la infección de dispositivos electrónicos de vuelo y la filtración de información confidencial. En el contexto colombiano, la situación no ha sido ajena, se han presentado ataques de ransomware que comprometieron a la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC) en 2021 y a la aerolínea Viva Air en 2022, poniendo en evidencia la necesidad de implementar medidas efectivas de ciberseguridad para proteger los sistemas aeronáuticos del país. A continuación, se presentan algunos casos que ilustran el impacto de los ciberataques en la aviación (Pantoja Viveros, 2016, p. 13):

Tabla 1 Casos de Ciberataques en Aviación

Año	Descripción
1997	Un hacker irrumpió en un sistema informático de Bell Atlantic, lo que provocó la caída de la torre de control de la Administración Federal de Aviación (FAA) y el apagado de las luces de la pista de aterrizaje.
2008	Se detectaron 800 alertas de incidentes cibernéticos en instalaciones de control del tráfico aéreo, y más de 150 incidentes aún no han sido resueltos.
2009	Un conductor de camión que transportaba un inhibidor de señal GPS causó accidentalmente interrupciones en el sistema de aumento basado en tierra (GBAS) del Aeropuerto Internacional Newark Liberty.
2014	Muchos aviones desaparecieron de las pantallas de radar en Austria, Alemania, República Checa y Eslovaquia. Se sospecha que el incidente estuvo relacionado con ejercicios de guerra electrónica.
2021	phishing mediante un correo malicioso introdujo un ransomware que afectó los sistemas internos de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC) (Arias, 2023, p. 45).
2022	Phishing dirigido a la aerolínea Viva Air resultó en el robo y filtración de 18.25 GB de información confidencial (Arias, 2023, p. 45).

Fuente: Elaboración propia.

La siguiente tabla presenta una síntesis de casos documentados y simulaciones avanzadas en los que se han materializado riesgos cibernéticos sobre el sistema ADS-B. Se describe el tipo de amenaza empleada, desde inyecciones de mensajes falsos hasta interferencias electromagnéticas reales, así como la técnica específica utilizada por los atacantes. Esta recopilación permite evidenciar la vulnerabilidad del sistema ante diversos vectores de ataque y subraya la necesidad urgente de fortalecer su arquitectura de seguridad:

Tabla 2 Casos Ataques al Sistema ADS-B

Caso	Técnica Utilizada	Descripción del Ataque	Fecha y Lugar de Ocurrencia
Ghost Aircraft Injection	Inyección de mensajes	Creación de aeronaves falsas mediante transmisión ADS-B falsa (Haines & Foster, 2012)	2012, DefCon 20 (EE. UU.)
Spoofing GNSS en zonas de conflicto	Spoofing GPS	Desviación de trayectoria vía señales GPS falsas (Ronen & Ben-Moshe, 2021)	2022, Siria / Mar Negro
Inyección de mensajes SDR	SDR con dump1090	Emisión de datos no auténticos desde SDR casero (Strohmeier et al., 2014)	2018, Alemania (Experimento SDR)
Simulación de spoofing académico	GPS spoofing simulado	Experimentos académicos simulando spoofing (Jafarnia-Jahromi et al., 2012)	2019, Corea del Sur (Simulación spoofing)
Prueba controlada de spoofing GPS	Spoofing con señales falsas	Prueba de spoofing con dron y GNSS controlado (Humphreys, 2020)	2020, Texas, EE. UU.
Spoofing en Mar Negro	Spoofing de señal GNSS	Análisis OSINT revela manipulación GNSS en Mar Negro (GPSJam.org, 2023)	2023, Mar Negro
Estudio sobre manipulación de RF	Interferencia por SDR	Estudio sobre modificación de señales RF vía SDR (Costin & Francillon, 2015)	2021, España
Interferencia satelital en Ucrania	Denegación satelital GNSS	Bloqueo intencional de señal GNSS en zona de combate (NATO, 2022)	2022, Ucrania
Simulación MLAT Ginebra	Inyección controlada y validación MLAT	Verificación por multilateración en entorno controlado (Monteiro et al., 2015)	2016, Ginebra, Suiza

Fuente: Elaboración propia a partir de la bibliografía

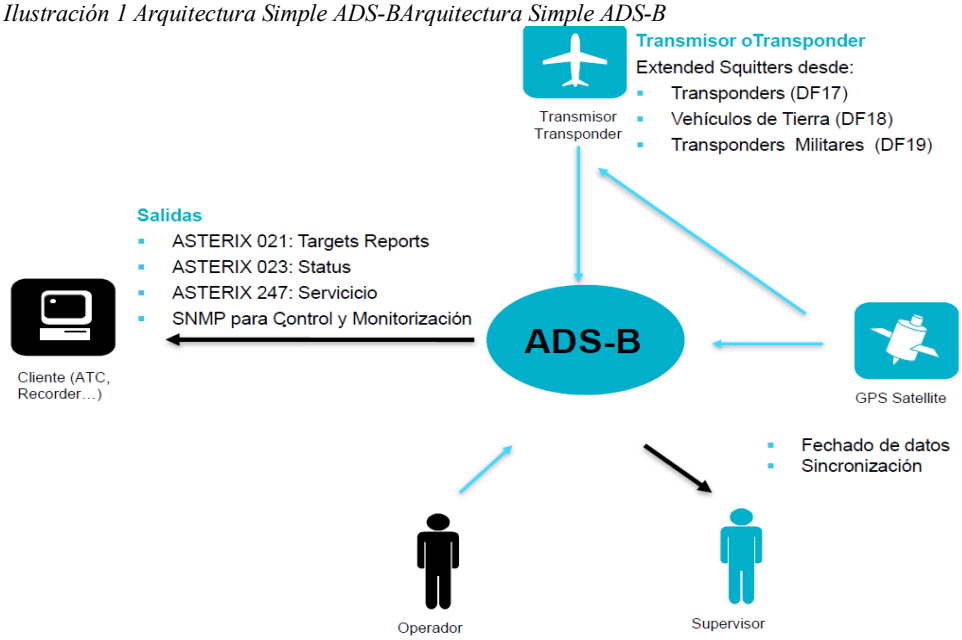
El Automatic Dependent Surveillance-Broadcast, en adelante ADS-B, es una tecnología de vigilancia que permite la transmisión automática de información como la posición, identificación, velocidad y altitud de una aeronave, lo que contribuye a la seguridad y eficiencia del tráfico aéreo.

El desarrollo del ADS-B tiene raíces en las iniciativas de vigilancia aérea de los años 90, como parte del programa de modernización CNS/ATM (Communications, Navigation, Surveillance / Air Traffic Management) impulsado por la OACI (Agbeyibor, 2014). Su despliegue inicial en Estados Unidos a través del programa Capstone en Alaska mostró

beneficios en reducción de accidentes, pero también reveló su fragilidad al no considerar amenazas cibernéticas emergentes (Secure ADS-B, 2014). A partir de la década del 2010, casos como el "ghost aircraft injection" presentado en DefCon 20 por investigadores de seguridad (Haines & Foster, 2012), y el aumento exponencial de incidentes de GPS spoofing en zonas de conflicto como Siria y el Mar Negro (Ronen & Ben-Moshe, 2021), han forzado a replantear su arquitectura técnica desde una perspectiva de seguridad. Así, el fenómeno de las amenazas al ADS-B debe entenderse no solo como un riesgo técnico, sino como una consecuencia histórica de un diseño concebido en un entorno tecnológicamente menos hostil (Strohmeier et al., 2014).

La siguiente ilustración muestra la estructura y los componentes importantes del sistema ADS-B, a través de transmisores, se emiten señales conocidas como "Extended Squitters", que abarcan información proveniente de transpondedores comerciales (DF17), vehículos de tierra (DF18) y transpondedores militares (DF19). Estos datos se sincronizan mediante señales de satélite GPS, permitiendo la integridad temporal de la información transmitida. El sistema ADS-B proporciona múltiples salidas de datos, incluyendo ASTERIX 021 (informes de objetivos), ASTERIX 023 (estado) y ASTERIX 247 (servicio), además del protocolo SNMP para control y monitorización:

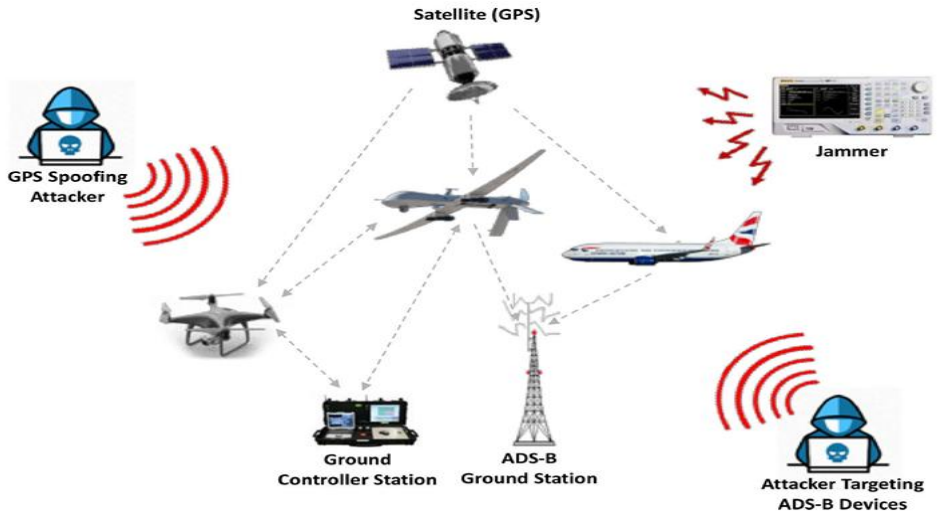
Ilustración 1 Arquitectura Simple ADS-BArquitectura Simple ADS-B



Fuente: Indra (Indra, 2020, p. 6)

A continuación, la imagen representa una arquitectura del sistema de vigilancia aérea basada en el sistema ADS-B, y muestra los posibles vectores de ataque que comprometen su seguridad, donde se observa cómo diferentes dispositivos aeronáuticos (aviones tripulados, drones y estaciones terrestres) interactúan con satélites GPS, estaciones de control y estaciones receptoras ADS-B. Sin embargo, estos están expuestos a amenazas cibernéticas como el *GPS spoofing* (engaño de la señal GPS), *jamming* (interferencia de señales de radiofrecuencia), y ataques dirigidos directamente a dispositivos ADS-B, lo cual puede comprometer la integridad, disponibilidad y autenticidad de los datos transmitidos. Estas vulnerabilidades serán descritas y analizadas, poniendo en riesgo la seguridad del tráfico aéreo (Ahmed et al., 2024, p. 11).

Ilustración 2 Conceptualización Ciberataques al Sistema ADS-



Fuente: (Ahmed et al., 2024, p. 11).

En Colombia, el sistema ADS-B ha sido implementado como parte de la vigilancia aeronáutica, para fortalecer y mejorar la seguridad operacional del espacio aéreo, facilitando la detección temprana de conflictos y emergencias en la gestión de este (Benavides Moncayo, 2016, p. 1; Gómez, 2015, p. 22). Así mismo, la Aeronáutica Civil de Colombia ha establecido directrices específicas para la instalación y operación del sistema ADS-B, en conformidad con los estándares internacionales y las políticas de seguridad nacional, promoviendo además la implementación del ADS-B Out como requisito obligatorio para las aeronaves que operan en el espacio aéreo colombiano desde el 1º de enero de 2025. Así mismo, en el presente artículo se establece como contexto de análisis, las vulnerabilidades entre las comunicaciones avión-avión y avión con la infraestructura en tierra principalmente.

A continuación, se relacionarán las principales vulnerabilidades del sistema ADS-B, junto con algunos tipos de ataques asociados:

1.1.Falta de Autenticación y Amenazas Asociados

El sistema ADS-B transmite información sin mecanismos que verifiquen la autenticidad de los mensajes, permitiendo que cualquier individuo con un receptor adecuado pueda interceptar mensajes del sistema (Pennapareddy, Srinivasan & Natarajan, 2024, p. 996). Esto abre la posibilidad a riesgos de suplantación de la identidad de aeronaves, compromiso de la integridad de los datos y la exposición de información confidencial, afectando incluso vuelos militares o de seguridad nacional (Strand, 2017, p. 22; Pennapareddy et al., 2024, p. 997).

1.2. Ataques de Inyección de Mensajes (Message Injection) y Amenazas Asociados

Debido a que el sistema ADS-B no verifica la autenticidad de los mensajes transmitidos, es posible que un atacante emita señales falsas que simulen aeronaves inexistentes, alteren rutas o modifiquen datos de vuelo, generando confusión en el control del tráfico aéreo, lo que puede llegar a provocar caos en el control de tráfico aéreo (Abu Al-Haija & Al-Tamimi, 2024, p. 10-11). Entre los ataques asociados son:

- **Inyección de Aviones Fantasma:** Creación de aeronaves inexistentes en los sistemas de vigilancia, forzando modificaciones innecesarias en rutas y aumentando el riesgo de colisiones (Shang et al., 2019, p. 5).
- **Modificación de Trayectorias Virtuales:** Alteración de posiciones de aeronaves legítimas, induciendo errores críticos en navegación (Wang et al., 2020, p. 7).
- **Denegación de Servicio (DoS):** Saturación de sistemas de tráfico aéreo mediante el envío masivo de mensajes falsos, afectando la toma de decisiones en tiempo real (Ahmed, 2024, p. 6).

- **Compromiso del Sistema de Prevención de Colisiones (TCAS):** Manipulación de datos que puede forzar maniobras evasivas innecesarias por parte de las aeronaves, incrementando el riesgo de accidentes (Al-Haija & Al-Tamimi, 2024, p. 12).

1.3. Eliminación de Mensajes (Message Deletion) y Amenazas Asociados

Aunque es poco probable, a menos se utilicen recursos de uso Militar, se pueden eliminar mensajes del sistema ADS-B antes de que lleguen a los sistemas de control mediante técnicas de interferencia destructiva (Holemans, 2016, p. 14-15). Este tipo de ataque puede hacer que una aeronave desaparezca del radar, aumentando la probabilidad de colisiones y complicando la gestión del tráfico aéreo (O'Donnell, 2020, p. 96). Algunos de los riesgos y ataques asociados son:

- **Desaparición de aeronaves:** Aumento del riesgo de colisión en espacios congestionados (Strand, 2017, p. 25).
- **Pérdida de control situacional:** Decisiones erróneas basadas en información incompleta o errónea (Manesh, 2019, p. 23).
- **Ataques combinados:** Eliminación de mensajes combinada con la inyección de datos falsos, generando caos operacional (O'Donnell, 2020, p. 102).

Aunque este tipo de ataque está presente dentro de las vulnerabilidades del sistema ADS-B, emplearlo en el contexto colombiano, sería poco probable, a menos que se realizara en pruebas de laboratorio o con tecnologías militares (aviones de guerra electrónica, inhibidor de señales, etc.).

1.4. Ataques de Suplantación de GPS (GPS Spoofing) y Amenazas Asociados

Dado que el ADS-B depende de las señales GPS para determinar la ubicación de las aeronaves, es vulnerable a los ataques de suplantación de señales, lo que puede desviar aeronaves de sus rutas originales y provocar confusión en el tráfico aéreo (Strand, 2017, p. 32). Se ha observado un incremento alarmante del 500% en incidentes de spoofing en 2024, afectando hasta 1.500 vuelos diarios (OPSGROUP, 2024, p. 5). Algunos de las consecuencias son:

- **Impacto en sistemas de aeronaves:** Afectación de sistemas de navegación, aumento de alertas falsas en el GPWS y pérdida de vigilancia en ADS-B y CPDLC (OPSGROUP, 2024, p. 39-42).
- **Impacto en el control de tráfico aéreo (ATC):** Incremento de la carga de trabajo, pérdida de separación entre aeronaves y posibles incursiones en espacios aéreos restringidos (OPSGROUP, 2024, p. 47).

1.5. Denegación de Servicio (Jamming & DoS) y Amenazas Asociados

Los transmisores ADS-B, pueden ser bloqueados mediante interferencias, impidiendo la recepción de datos por parte de estaciones terrestres y aeronaves (Kacem, 2016, p. 41). Algunas técnicas incluyen el **ground station flood denial,** mediante la inundación de mensajes ADS-B en estaciones terrestres. El **aircraft flood denial** con la inundación de mensajes dirigidos a aeronaves. Por ejemplo, un grupo de atacantes podría llegar a generar interferencias en el canal ADS-B en un área específica, bloqueando las comunicaciones y dejando a los controladores aéreos sin datos en tiempo real, lo que generaría un caos (Kacem, 2016, p. 41).

1.6. Normatividad

Se deben tener en cuenta los estándares normativos internacionales como el AC 90-114B de la FAA, el DOC 9985 de la OACI y el reglamento EASA 1207/2011, los cuales orientan técnicamente la implementación segura del ADS-B y respaldan las medidas de autenticación y mitigación propuestas en este estudio, así mismo se relacionan a continuación las principales normativas del sistema ADS-B a nivel internacional y nacional:

- **ICAO DOC 9985 – Guidance for ADS-B Implementation:** establece recomendaciones sobre seguridad y autenticación para transmisiones ADS-B a nivel global.
- **EUROCONTROL Specification for ADS-B Surveillance:** provee lineamientos técnicos sobre integridad, disponibilidad y autenticación.
- **FAA Advisory Circular AC 90-114B (2022):** guía de operación y requisitos técnicos en EE. UU. sobre ADS-B Out, incluyendo aspectos de seguridad.
- **Reglamentos EASA sobre comunicación aeronáutica (EU No. 1207/2011 y sus enmiendas):** exigen seguridad e interoperabilidad para transmisores ADS-B.

La profundización relacionada con las normatividades, serán ampliadas dentro del Anexo I del presente artículo.

2. Resultados

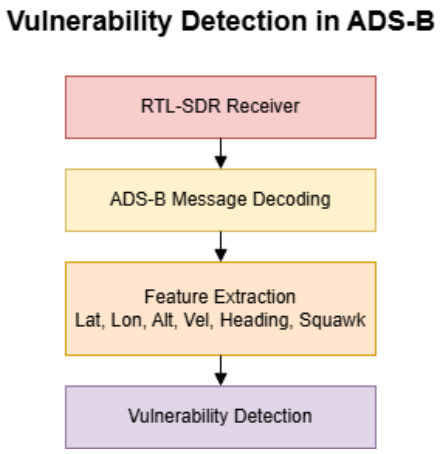
A continuación, se llevarán algunas pruebas simuladas y reales en la validación de la existencia de la vulnerabilidad de Message Injection tanto en entorno simulado como real.

2.1. Validación de la Vulnerabilidad Message Injection de forma Simulada y Real

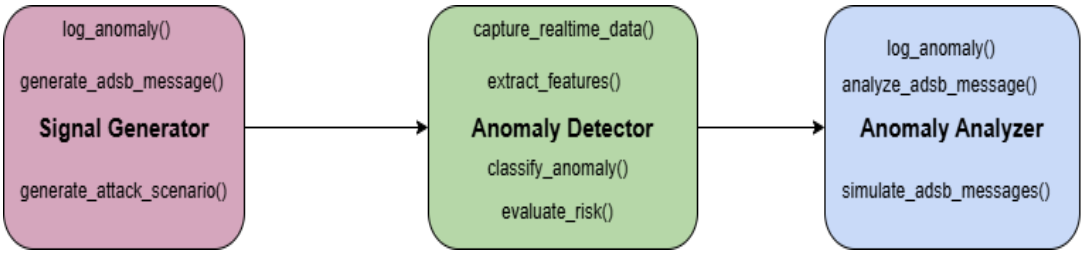
La presente iniciativa tiene como objetivo el desarrollar e implementar un sistema que permita la detección de la vulnerabilidad Message Injection en el sistema ADS-B, mediante simulación y pruebas controladas en entornos reales con HackRF.

Para simular escenarios controlados de ciberataques al sistema ADS-B, se emplea el módulo adsb_signal_generator.py, que genera señales con vulnerabilidades previamente definidas. Esto permite evaluar el sistema en condiciones específicas antes de su implementación en un entorno real. El generador utiliza la librería pyModeS para construir mensajes ADS-B en formato hexadecimal, siguiendo el estándar ICAO. Los mensajes son transmitidos a una frecuencia de 1090 MHz, emulando su respectiva radiodifusión. Así mismo, a continuación, se mostrarán las ilustraciones de los diagramas de programación (bloques y funciones) y las pruebas realizadas:

Ilustración 3 Diagrama de la Detección de Amenazas



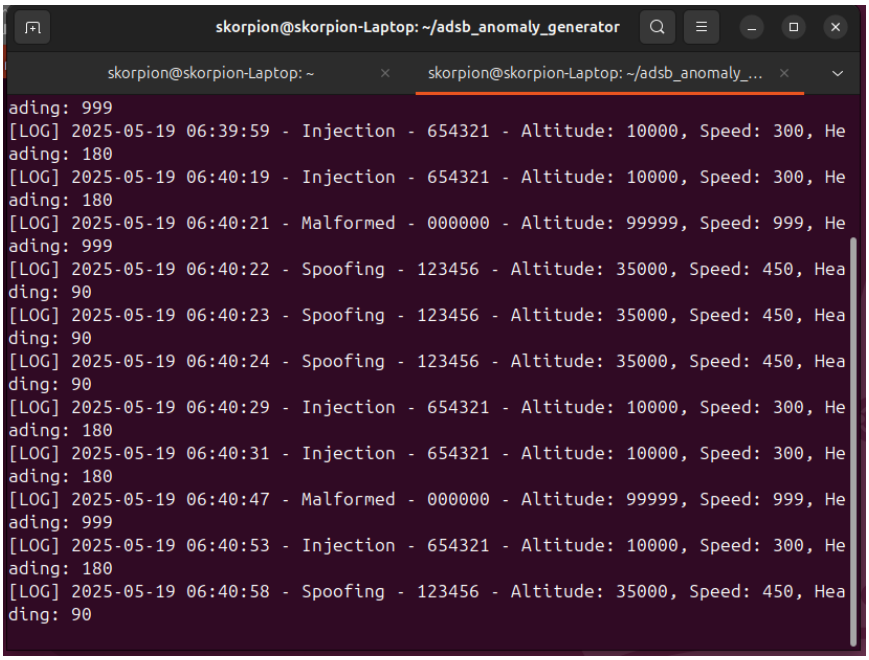
Fuente: Elaboración propia
Ilustración 4 Diagrama de Clases Escenario Simulado



Fuente: Elaboración propia

En el contexto del proyecto de detección de vulnerabilidades ADS-B, se llevaron a cabo pruebas controladas, con la finalidad de evaluar la capacidad del sistema en la identificación de ataques cibernéticos simulados, tal como Message Injection. Las pruebas se realizaron utilizando un generador de señales que simula estos comportamientos, para la verificación del correcto funcionamiento del módulo de detección en un entorno controlado:

Ilustración 5 Pruebas Simuladas Vulnerabilidades

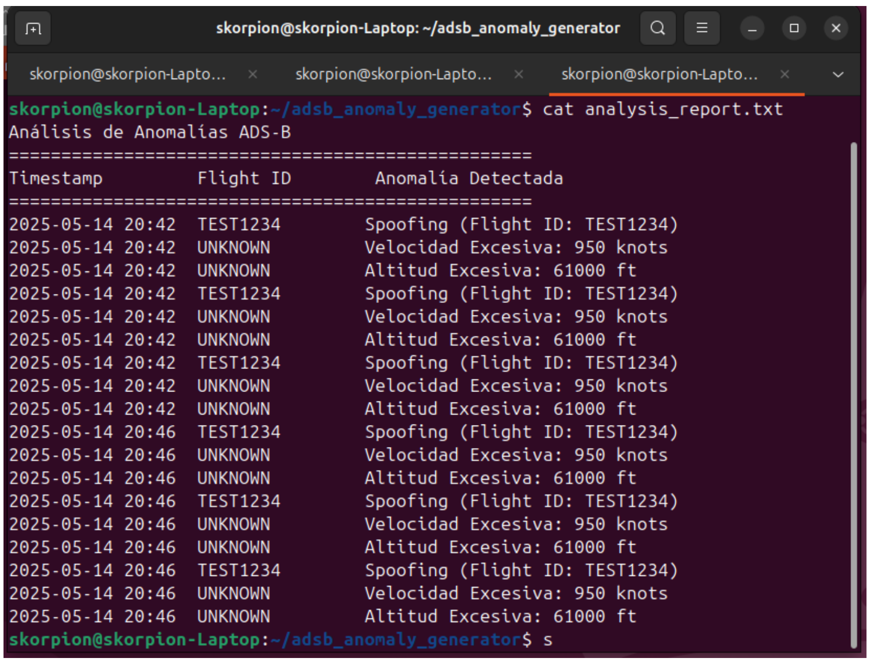


Fuente: Elaboración propia

La siguiente ilustración presenta el contenido del archivo analysis_report.txt, donde se registran de forma estructurada las vulnerabilidades detectadas. El reporte organiza la

información en columnas que indican la marca de tiempo (timestamp), el identificador de vuelo (Flight ID) y la descripción de la anomalía, incluyendo la naturaleza del ataque y los parámetros anómalos identificados. Esta estructura facilita el análisis posterior y la generación de informes detallados sobre los incidentes detectados:

Ilustración 6 Registro de las Vulnerabilidades Detectadas

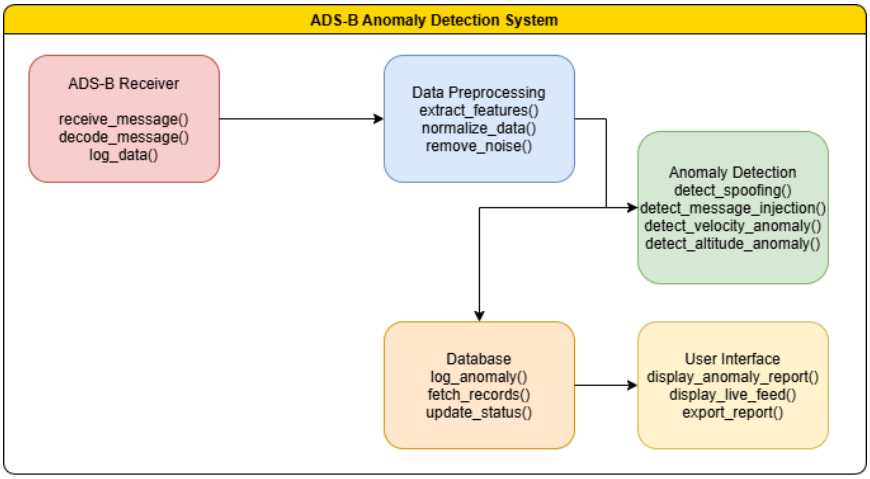


```
skorpion@skorpion-Laptop:~/adsb_anomaly_generator$ cat analysis_report.txt
Análisis de Anomalías ADS-B
==================================================
Timestamp          Flight ID         Anomalía Detectada
==================================================
2025-05-14 20:42  TEST1234        Spoofing (Flight ID: TEST1234)
2025-05-14 20:42  UNKNOWN         Velocidad Excesiva: 950 knots
2025-05-14 20:42  UNKNOWN         Altitud Excesiva: 61000 ft
2025-05-14 20:42  TEST1234        Spoofing (Flight ID: TEST1234)
2025-05-14 20:42  UNKNOWN         Velocidad Excesiva: 950 knots
2025-05-14 20:42  UNKNOWN         Altitud Excesiva: 61000 ft
2025-05-14 20:42  TEST1234        Spoofing (Flight ID: TEST1234)
2025-05-14 20:42  UNKNOWN         Velocidad Excesiva: 950 knots
2025-05-14 20:42  UNKNOWN         Altitud Excesiva: 61000 ft
2025-05-14 20:46  TEST1234        Spoofing (Flight ID: TEST1234)
2025-05-14 20:46  UNKNOWN         Velocidad Excesiva: 950 knots
2025-05-14 20:46  UNKNOWN         Altitud Excesiva: 61000 ft
2025-05-14 20:46  TEST1234        Spoofing (Flight ID: TEST1234)
2025-05-14 20:46  UNKNOWN         Velocidad Excesiva: 950 knots
2025-05-14 20:46  UNKNOWN         Altitud Excesiva: 61000 ft
2025-05-14 20:46  TEST1234        Spoofing (Flight ID: TEST1234)
2025-05-14 20:46  UNKNOWN         Velocidad Excesiva: 950 knots
2025-05-14 20:46  UNKNOWN         Altitud Excesiva: 61000 ft
skorpion@skorpion-Laptop:~/adsb_anomaly_generator$ s
```

Fuente: Elaboración propia

A continuación, se muestra el flujo general del sistema de detección de vulnerabilidades ADS-B en un entorno real. El flujo de datos comienza con la recepción de mensajes ADS-B, pasando por el preprocesamiento y la extracción de características, hasta llegar al módulo de detección de vulnerabilidades. Los resultados se registran en la base de datos y se visualizan en la interfaz del usuario:

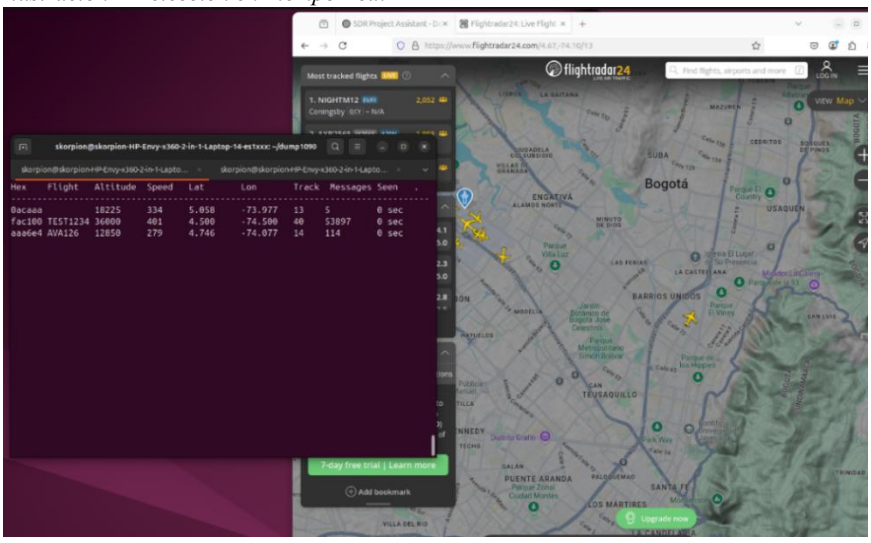
Ilustración 7 Diagrama de Clases Escenario Real



Fuente: Elaboración propia

La siguiente ilustración presenta la salida del receptor ADS-B, también se observan las aeronaves detectadas, incluida la aeronave fantasma inyectada mediante HackRF. Se puede observar la aeronave con el identificador "TEST1234", que corresponde a un mensaje inyectado para simular el ataque asociado:

Ilustración 2 Detección en Tiempo Real

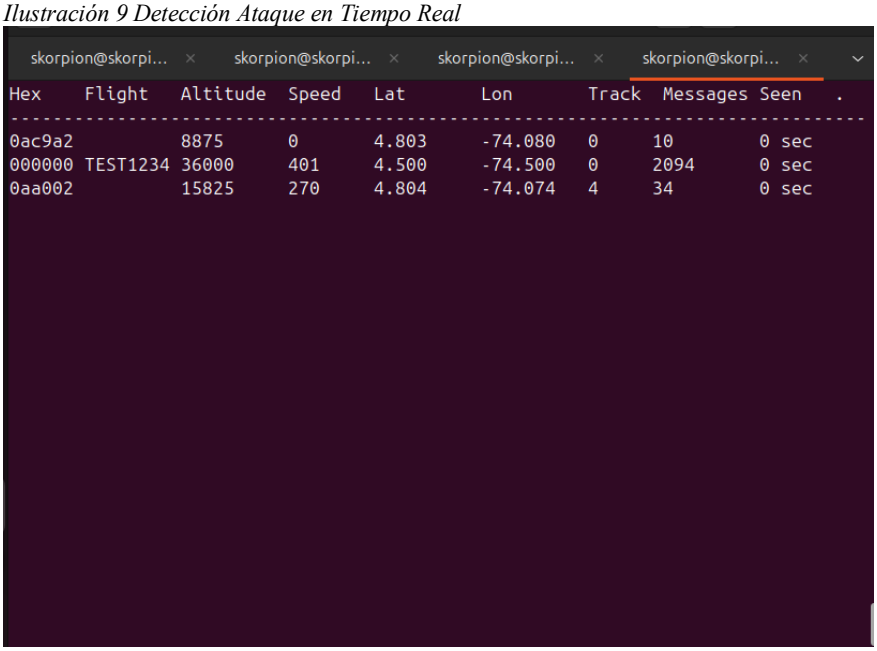


Fuente: Elaboración propia

A continuación, se muestra la ejecución del proyecto a través del script start_adsb_project.sh. Se inicia el receptor ADS-B utilizando dump1090 y se activa el script

de detección de vulnerabilidades, que procesa los mensajes ADS-B en tiempo real y busca identificar patrones de ataque:

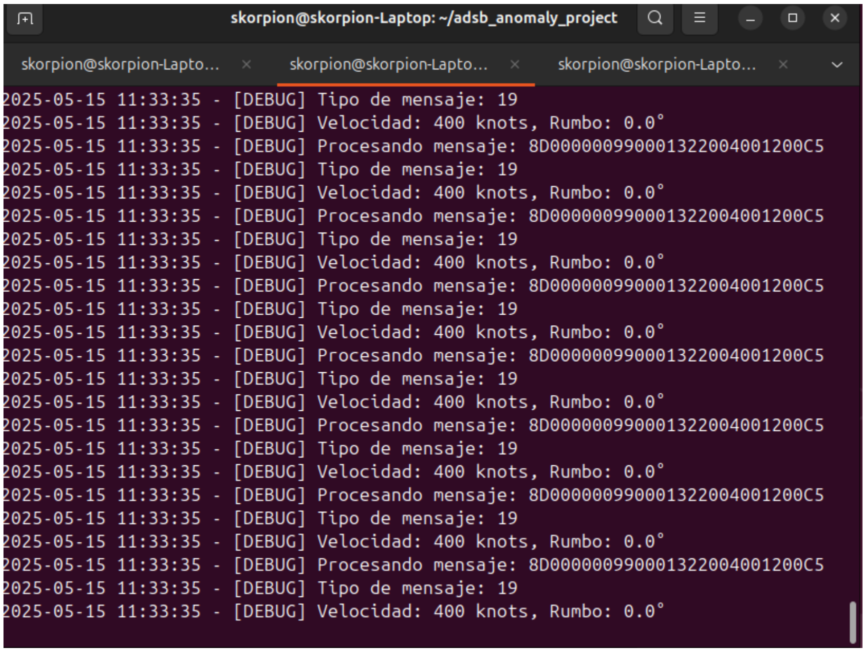
Ilustración 9 Detección Ataque en Tiempo Real



Fuente: Elaboración propia

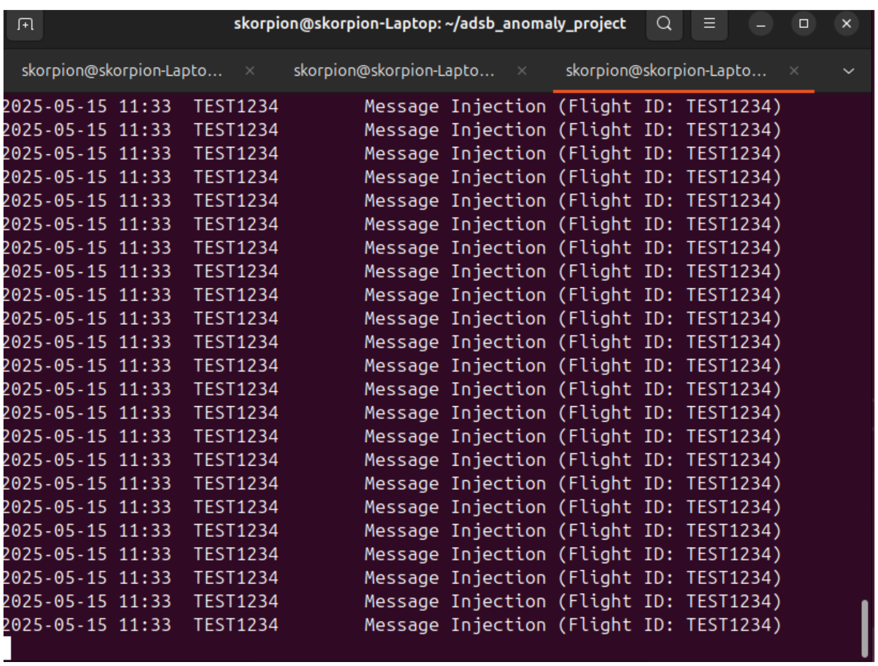
Finalmente, en la siguiente ilustración se detalla el registro de mensajes capturados y procesados en tiempo real. Los mensajes procesados se analizan en busca de inconsistencias en velocidad, rumbo y altitud, permitiendo detectar potenciales ataques como Message Injection, en los parámetros de vuelo:

Ilustración 10 Registro de Detección Message Injection



Fuente: Elaboración propia.

Ilustración 11 Registro de Detección Message Injection II

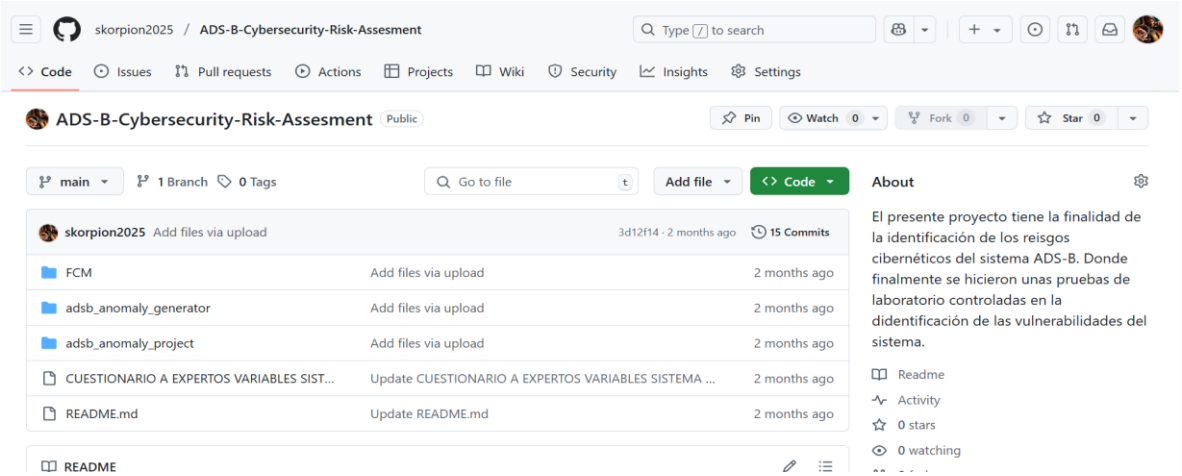


Fuente: Elaboración propia.

Con el fin de facilitar el acceso a los desarrollos realizados durante la investigación, se ha dispuesto un repositorio público en la plataforma GitHub. Este repositorio reúne todos los scripts, configuraciones y documentación asociados para la detección de vulnerabilidades cibernéticas en el sistema ADS-B, desarrollado como parte de esta propuesta de investigación aplicada en entornos simulados y reales:

https://github.com/skorpion2025/ADS-B-Cybersecurity-Risk-Assesment

Ilustración 11B Imagen Repositorio



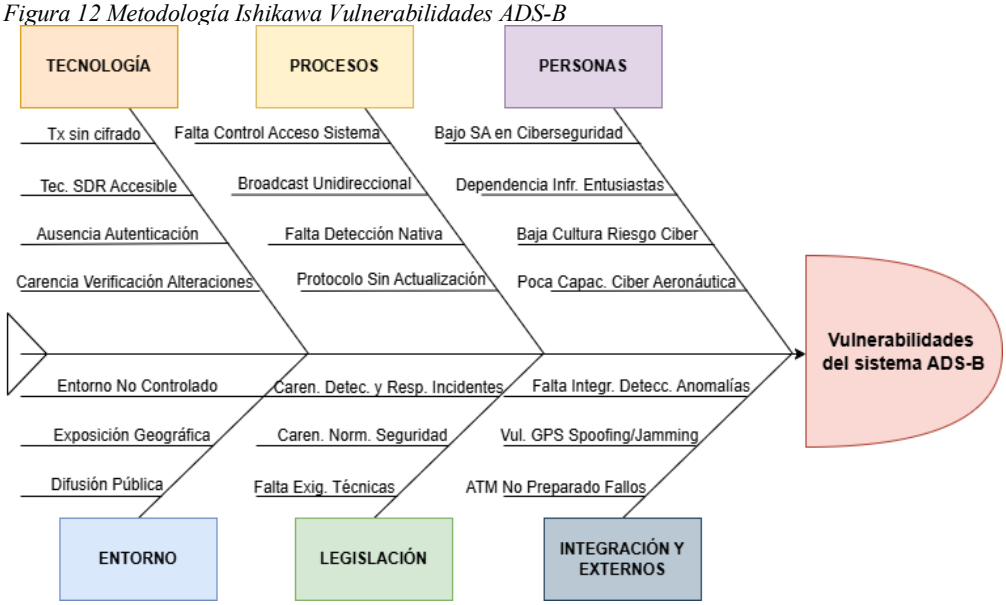
Fuente: Elaboración propia.

El repositorio titulado "ADS-B Cybersecurity Risk Assessment" contiene la arquitectura completa del desarrollo, incluyendo módulos de generación de señales sintéticas, mecanismos de detección en tiempo real, así como scripts de automatización e integración con receptores SDR (Software Defined Radio) y dump1090. Asimismo, se incorporan archivos de documentación técnica y reportes de ejecución que respaldan los resultados obtenidos durante las pruebas experimentales. Así mismo, se implementó como iniciativa la creación de un dispositivo real para mencionada detección llamado como "CyberSkyGuard".

Por lo tanto, vistas las anteriores pruebas, el sistema ADS-B, se expone a riesgos críticos debido a su arquitectura abierta. Para identificar la problemática, se aplicó el modelo

Ishikawa (diagrama de espina de pescado), con la finalidad de visualizar de forma estructurada los factores técnicos, humanos, procesales, regulatorios, ambientales y sistémicos que originan vulnerabilidades, para facilitar la priorización de intervenciones en la ciberseguridad del espacio aéreo moderno.

Figura 12 Metodología Ishikawa Vulnerabilidades ADS-B



Fuente: Elaboración Propia

Teniendo en cuenta lo anterior, se brinda un mejor entendimiento de la problemática en materia de ciberseguridad del sistema ADS-B, la cual deriva de los elementos tratados mediante el esquema de espina de pescado anterior, visualizando múltiples factores, desde el nivel tecnológico hasta el humano y regulatorio, contribuyen a un sistema de vigilancia aérea funcional pero vulnerable.

2.2. Clasificación de los principales riesgos de acuerdo con el tipo de amenaza con el uso del sistema ADS-B

Las vulnerabilidades del sistema ADS-B, inherentes al diseño del protocolo, han sido ampliamente documentadas y categorizadas, evidenciando la necesidad de desarrollar

modelos de clasificación que no solo permitan identificarlas, sino también evaluar su severidad y probabilidad de ocurrencia para obtener el nivel de riesgo. En este contexto, Strohmeier, Lenders y Martinovic (2015) proponen un esquema de clasificación basado en la complejidad del ataque y su impacto potencial en la integridad y disponibilidad de los datos transmitidos. Por su parte, Haass, Craiger y Kessler (2018) sugieren un modelo de clasificación que incluye tanto amenazas intencionales (ataques cibernéticos) como riesgos operacionales (fallos técnicos o interferencias naturales). Basado en los anteriores planteamientos y a la revisión bibliográfica anterior, se hace un resumen de ésta, para plasmar a continuación una tabla con distintos tipos de ataques que pueden ser realizados al sistema ADS-B en función de su severidad y probabilidad:

Ilustración 13 Evaluación de Amenazas, obteniendo Riesgos ADS-B

ATACK	METHOD	SEVERITY	PROBABILITY
Aircraft reconnaissance	Eavesdropping	low	lowest
Ground Station Flood Denial	Signal Jamming	medium	lower
Aircraft Flood Denial	Signal Jamming	medium	low-medium
Aircraft Disappearance	Message Deletion	high	low
Ground Station Ghost Injection	Message Injection	high	low
Aircraft Ghost Injection	Message Injection	medium	low-medium
Virtual Aircraft Hijacking	Message Modification	high	medium
Virtual Trajectory Modification	Message Modification	high	medium
Aircraft Spoofing	Message Modification	high	low

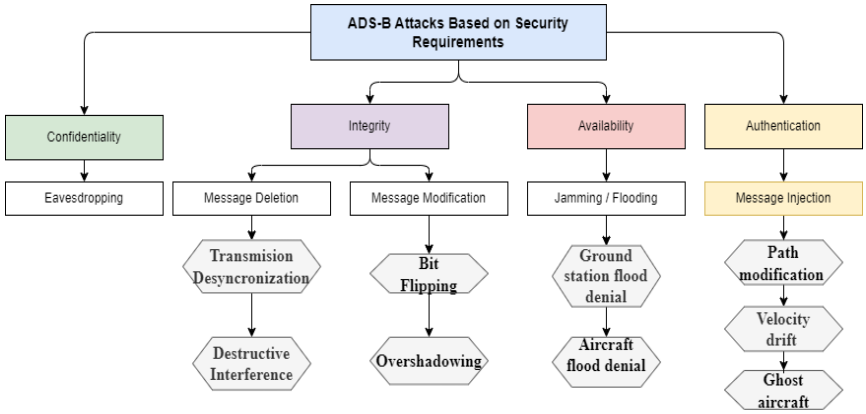
Fuente: Elaboración propia as partir de la bibliografía anterior

La clasificación de las amenazas en el sistema ADS-B se fundamenta en dos criterios principales: severidad y probabilidad de ocurrencia con la finalidad de obtener los riesgos. La severidad se define como el grado de impacto que una amenaza puede tener sobre la integridad del sistema, variando desde baja (como en el caso de la interceptación pasiva o eavesdropping), hasta alta (como en la modificación de mensajes o spoofing, donde un atacante podría manipular información crítica de la aeronave). Por otro lado, la probabilidad de ocurrencia se basa en la facilidad técnica de llevar a cabo el ataque y la frecuencia con la que dicho ataque podría presentarse en un entorno operativo real (Strohmeier, Lenders & Martinovic, 2015; Haass, Craiger & Kessler, 2018).

En este contexto, se observa que las amenazas clasificadas con alta severidad, como la modificación o eliminación de mensajes, presentan un riesgo crítico para la integridad de los datos ADS-B, ya que podrían inducir a errores en la interpretación de la posición y trayectoria de las aeronaves. En contraste, las amenazas con alta probabilidad, como la interceptación de mensajes (eavesdropping), aunque no comprometen directamente la integridad de los datos, pueden proporcionar información valiosa a los atacantes para planificar acciones más sofisticadas. Esta evaluación permite, por tanto, establecer prioridades en los esfuerzos de mitigación y definir políticas de defensa adaptadas a cada tipo de amenaza identificado en el sistema ADS-B.

A continuación, se muestra una categorización de los ataques al sistema ADS-B basada en los requisitos fundamentales de seguridad: confidencialidad, integridad, disponibilidad y autenticación.

Ilustración 14 Categorización de los Ataques al Sistema ADS-B



Fuente: Elaboración propia

En cuanto a la confidencialidad, se identifican ataques de espionaje (*eavesdropping*) al no haber cifrado en las transmisiones. Bajo la integridad, los ataques incluyen la eliminación (*message deletion*) y modificación de mensajes, los cuales pueden derivar en técnicas como la desincronización de transmisión, interferencias destructivas, *bit flipping* y *overshadowing*. La disponibilidad se ve comprometida mediante interferencias tipo *jamming* o *flooding*, como ataques de denegación de servicio a estaciones terrestres o saturación por múltiples aeronaves.

Una vez identificadas las principales vulnerabilidades y amenazas, además de haber realizado una evaluación de éstas, a continuación, se realizará la gestión de los riesgos identificados del sistema ADS-B.

2.3. Gestión de los Riesgos Identificados con el Uso del Sistema ADS-B

Para la gestión de riesgos del sistema ADS-B, primero se realizó una revisión entre distintos métodos, por lo tanto, se muestra a continuación una tabla comparativa entre distintas metodologías para el análisis de riesgos, plasmando ventajas y limitaciones, así

mismo, se incluye una columna que resalta las ventajas específicas de la metodología FAST frente a cada una de las metodologías comparadas:

Tabla 3. Comparativa Metodologías

Met.	Enfoque	Ventajas	Limitaciones	Ventaja de FAST
FAST	Análisis funcional para identificar funciones críticas y sus interacciones	Proporciona una visión integral del sistema mediante el análisis de funciones críticas	Requiere experiencia en análisis funcional y puede ser complejo para sistemas grandes	N/A
STRIDE	Identificación de amenazas basadas en seis categorías: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	Cubre múltiples tipos de amenazas de forma estructurada y sistemática	No considera directamente el impacto financiero ni la probabilidad del riesgo	FAST proporciona una visión integral basada en funciones, mientras que STRIDE se enfoca solo en amenazas específicas
OCTAVE	Evaluación de riesgos organizacionales mediante activos, amenazas y vulnerabilidades	Fomenta la conciencia situacional a nivel organizacional	Enfocado en activos organizacionales, no en amenazas técnicas específicas	FAST permite un análisis funcional que abarca tanto activos organizacionales como funciones técnicas críticas
NIST SP 800-30	Proceso estructurado para la evaluación de riesgos en sistemas de información	Metodología probada y ampliamente adoptada	Requiere recursos significativos para una implementación completa	FAST proporciona un análisis funcional más detallado que permite identificar funciones críticas específicas
MITRE ATT&CK	Marco basado en tácticas, técnicas y procedimientos (TTPs) de ataques cibernéticos	Actualización continúa basada en nuevas amenazas y técnicas de ataque	Enfocado en amenazas conocidas; no aborda amenazas emergentes	FAST facilita la identificación de funciones vulnerables más allá de las técnicas conocidas en ATT&CK
ISO 27001	Gestión de seguridad de la información basada en	Amplia adopción global y enfoque en controles	Requiere implementación rigurosa y	FAST se centra en funciones operativas críticas, mientras que

	estándares internacionales	específicos de seguridad	mantenimiento constante	ISO 27001 se enfoca en controles estandarizados
ISO 31000	Gestión del riesgo mediante principios, marcos y procesos	Amplio alcance para gestión integral de riesgos	No está específicamente orientada a ciberseguridad, sino a riesgos generales	FAST permite un enfoque más detallado y técnico al analizar funciones operativas

Fuente: Elaboración previa.

La siguiente matriz, representa los riesgos iniciales elaborada con base en la metodología de análisis cualitativo, en la cual se ubican las principales amenazas que afectan la seguridad del sistema ADS-B antes de aplicar cualquier medida de mitigación. Cada riesgo ha sido clasificado de acuerdo con su probabilidad de ocurrencia (eje vertical) y su nivel de severidad en caso de materializarse (eje horizontal). Se resaltan amenazas críticas con la inyección de mensajes, la suplantación mediante GPS spoofing y la modificación de mensajes, que aparecen en zonas de riesgo alto o catastrófico (rojo). Esta representación sirve para priorizar acciones de respuesta y fortalecer los mecanismos de ciberseguridad del sistema aeronáutico:

Matriz 1. Clasificación Inicial riesgos

	Minimal (5)	Minor (4)	Major (3)	Hazardous (2)	Catastrophic (1)
Frequent (A)					Inyección de mensajes
Probable (B)			Falta de autenticación		GPS Spoofing
Remote (C)					Modificación de mensajes
Extremely Remote (D)					Eliminación de mensajes
Extremely Improbable (E)					

Fuente: Elaboración propia

La metodología FAST resalta como una herramienta para el análisis de riesgos en sistemas complejos y automáticos, ya que permite estructurar de manera jerárquica las funciones del sistema, facilitando la identificación de áreas críticas y la evaluación de riesgos desde una perspectiva funcional (Bartolomei & Miller, 2001, p. 4; Aslan et al., 2023, p. 6; Paja et al., 2024, p. 12). A diferencia de otras metodologías centradas en actividades o procesos específicos, FAST se enfoca en cómo las funciones interactúan para cumplir los objetivos del sistema, permitiendo una visión integral que considera tanto los elementos técnicos como los organizacionales y operativos, lo que la convierte en una opción para abordar las complejidades del entorno ADS-B, especialmente en contextos de ciberseguridad donde la identificación de funciones críticas es esencial para la mitigación de amenazas (Bartolomei & Miller, 2001, p. 5; Aslan et al., 2023, p. 10; Paja et al., 2024, p. 15).

2.3.1. Aplicación Método FAST (Functional Security in Automation)

El enfoque FAST, es un modelo de seguridad funcional aplicado a la automatización, cuyo objetivo es abordar las amenazas de ciberseguridad en sistemas industriales interconectados, mediante la identificación de funciones del sistema, activos, amenazas de seguridad y técnicas de mitigación (Kuhlenkamp & Kletti, 2023, p. 12).

Consecuentemente, a continuación, se muestran diagramas como resultado sobre la gestión del riesgo elaborados con base en el modelo FAST para las principales vulnerabilidades del sistema ADS-B, complementando los resultados mediante matrices usando elementos de la normativa NIST 800-30:

2.3.2. Falta de Autenticación

El siguiente diagrama describe cómo la ausencia de mecanismos de autenticación en el sistema ADS-B permite la suplantación de aeronaves mediante transmisiones no verificadas. Desde la función de "transmitir datos ADS-B", se identifica cómo un activo principal la identidad y trayectoria de la aeronave, que puede ser explotada por una amenaza (un actor no autorizado que transmite información falsa, por ejemplo). Así mismo, el flujo de riesgo se detiene mediante el tratamiento con autenticación tipo MAC (Media Acces Control), listas blancas de emisores conocidos y validación cruzada de trayectorias, proporcionando una respuesta estructurada para evitar que se comprometan la conciencia situacional y la seguridad aérea.

Para abordar de manera sistemática la vulnerabilidad asociada a la falta de autenticación en las transmisiones ADS-B, se desarrollaron matrices de análisis de riesgos mediante la metodología NIST SP 800-30. Estas matrices permiten identificar amenazas,

vulnerabilidades, impactos y controles asociados a la ausencia de mecanismos de verificación de origen de los mensajes emitidos:

Identificación del Escenario

Función afectada: Transmisión de datos ADS-B

Activo crítico: Identidad y trayectoria de aeronaves

Amenaza: Suplantación de aeronave no autorizada

Vulnerabilidad: Ausencia de autenticación

Impacto potencial: Alteración de rutas, colisiones, carga cognitiva excesiva

Controles actuales: Validación cruzada, MAC/whitelist, alertas

Matriz 2. Identificación de Activos, Amenazas y Vulnerabilidades

ID	Activo Crítico	Amenaza	Vulnerabilidad	Fuente de Amenaza
A1	Datos ADS-B	Spoofing de aeronave	Falta de autenticación	Atacante con SDR
A2	Trajectoria	Inyección de trayectorias	Validación limitada de rutas	Insider / Cibercriminal
A3	Sistema de Log	Borrado de logs o manipulación	Ausencia de integridad en bitácoras	Actor malicioso avanzado

Fuente: Elaboración propia

Matriz 3 – Estimación de Probabilidad e Impacto

ID	Probabilidad	Impacto	Nivel de Riesgo
A1	Alta	Alto	**Alto**
A2	Media	Alto	**Alto**
A3	Baja	Medio	**Medio**

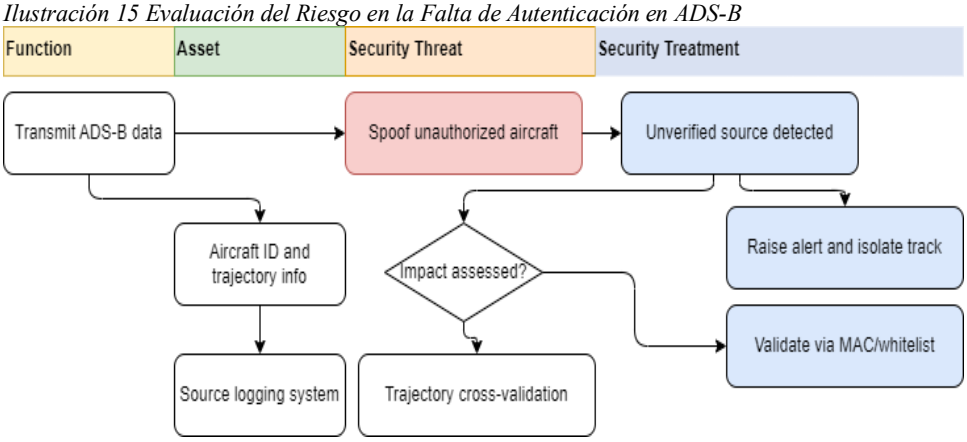
Fuente: Elaboración propia

Matriz 4 – Evaluación de Riesgos Cualitativa (Impacto x Probabilidad)

	Impacto Bajo	Impacto Medio	Impacto Alto
Probabilidad Alta	Medio	Alto	Alto
Probabilidad Media	Bajo	Medio	Alto
Probabilidad Baja	Bajo	Medio	Medio

Fuente: Elaboración propia

Ilustración 15 Evaluación del Riesgo en la Falta de Autenticación en ADS-B



Fuente: Elaboración propia

A continuación, se exponen las matrices obtenidas mediante NIST 800-30 partiendo de los elementos analizados en la gráfica anterior:

Matriz 5 – Controles de Seguridad y Tratamiento

ID	Riesgo	Control Existente	Control Propuesto	Tipo de Tratamiento
A1	**Spoofing**	Alerta y aislamiento, MAC whitelist	Autenticación digital + Validación de origen	Mitigar
A2	**Inyección de rutas**	Validación cruzada	Correlación radar + AI detección de anomalías	Mitigar
A3	**Manipulación de logs**	Registro básico local	Bitácora cifrada con hash y firma digital	Mitigar

Fuente: Elaboración propia

Matriz 6 – Evaluación de Controles (NIST)

ID	Control Evaluado	Efectividad	Brechas Identificadas
C1	Validación por MAC	Media	No evita spoofing sofisticado
C2	Validación cruzada	Alta	Funcional, pero dependiente de cobertura
C3	Alerta + Aislamiento	Media	Reacción efectiva, pero no preventiva
C4	Logs locales	Baja	Riesgo de manipulación

Fuente: Elaboración propia

Matriz 7 – Tratamientos y Plan de Acción

Riesgo	Acción Correctiva	Responsable	Tiempo Estimado	Prioridad
Spoofing (A1)	Integrar autenticación digital en ADS-B	CCO CyberSec	3 meses	Alta
Rutas falsas (A2)	Implementar IA de detección de anomalías	DevSecOps	4 meses	Alta
Logs (A3)	Incorporar bitácoras cifradas y firmadas	InfraSec	2 meses	Media

Fuente: Elaboración propia

El uso de estas matrices ayuda a categorizar el riesgo de suplantación de aeronaves como crítico, priorizando la implementación de autenticación digital, validación cruzada por multilateración y segmentación lógica de emisores confiables. De esta manera, se fortalece el enfoque preventivo frente a una debilidad estructural del protocolo ADS-B.

2.3.3. Inyección de Mensajes (Message Injection)

A continuación, el diagrama representa cómo un atacante puede aprovechar la falta de autenticación y cifrado para introducir mensajes falsos en el canal ADS-B, creando aeronaves fantasmas (*ghost aircraft*) o trayectorias erróneas. Se sigue el modelo FAST desde la función de captura del estado de aeronaves, pasando por la amenaza directa (inyección de paquetes) hasta las técnicas de mitigación, como detección de datos falsificados, alertas operacionales y filtrado de tráfico. La gestión de este riesgo se apoya en validaciones cruzadas con radar secundario o multilateración y análisis de integridad del mensaje.

La inyección de mensajes constituye una de las amenazas de mayor documentación del sistema ADS-B. Para evaluar su impacto y formular estrategias de mitigación, se complementa con la metodología NIST 800-30, generando matrices de riesgo que relacionan causas, activos afectados, controles de seguridad y niveles de probabilidad e impacto:

Identificación del Escenario

Función afectada: Captura del estado de la aeronave

Activo crítico: Datos de sensores, estado de vuelo

Amenaza: Inyección de mensajes

Vulnerabilidad: Falta de autenticación/validación de origen

Impacto potencial: Comandos falsos, decisiones erróneas, congestión del tráfico

Controles actuales: Monitoreo, escaneo, alertas, filtrado de paquetes

Matriz 8 – Identificación de Activos, Amenazas y Vulnerabilidades

ID	Activo Crítico	Amenaza	Vulnerabilidad	Fuente de Amenaza
B1	Datos de sensores	Inyección de mensajes	Falta de verificación de contenido	Atacante con SDR
B2	Estado de aeronave	Comandos falsos	Falta de autenticación de señales externas	Cibercriminal
B3	Escaneo del sistema	Saturación de canal	Escaso filtrado automático	Insider / sabotaje

Fuente: Elaboración propia

Matriz 9 – Estimación de Probabilidad e Impacto

ID	Probabilidad	Impacto	Nivel de Riesgo
B1	Alta	Alto	**Alto**
B2	Alta	Alto	**Alto**
B3	Media	Medio	**Medio**

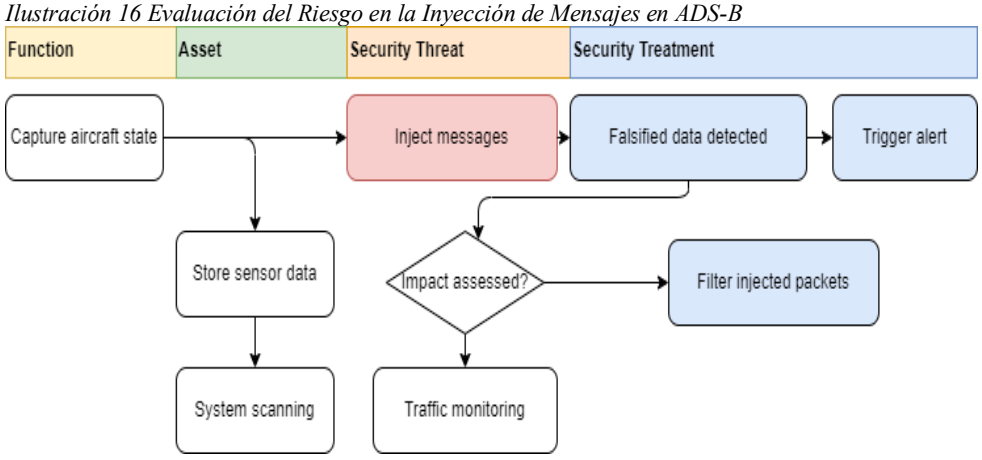
Fuente: Elaboración propia

Matriz 10 – Evaluación de Riesgos Cualitativa (Impacto x Probabilidad)

	Impacto Bajo	Impacto Medio	Impacto Alto
Probabilidad Alta	Medio	Alto	**Alto**
Probabilidad Media	Bajo	Medio	Alto
Probabilidad Baja	Bajo	Bajo	Medio

Fuente: Elaboración propia

Ilustración 16 Evaluación del Riesgo en la Inyección de Mensajes en ADS-B



Fuente: Elaboración propia

A continuación, se exponen las matrices obtenidas mediante NIST 800-30 partiendo de los elementos analizados en la gráfica anterior:

Matriz 11 – Controles de Seguridad y Tratamiento

ID	Riesgo	Control Existente	Control Propuesto	Tipo de Tratamiento
B1	Inyección de mensajes	Alerta por datos falsos	Filtrado basado en huella digital	Mitigar
B2	Comando falso	Monitoreo de tráfico	Validación multi-origen + correlación de sensores	Mitigar
B3	Saturación del canal	Escaneo reactivo	Sistema de detección de patrones anómalos	Mitigar

Fuente: Elaboración propia

Matriz 12 – Evaluación de Controles (NIST)

ID	Control Evaluado	Efectividad	Brechas Identificadas
C1	Alerta por falsificación	Media	Tiempo de respuesta elevado
C2	Monitoreo	Alta	Dependiente del operador
C3	Escaneo reactivo	Baja	Limitado para ataques masivos

Fuente: Elaboración propia

Matriz 13 – Tratamientos y Plan de Acción

Riesgo	Acción Correctiva	Responsable	Tiempo Estimado	Prioridad
Inyección (B1)	Implementar filtrado con AI/ML	DevSecOps	4 meses	Alta
Comando falso (B2)	Desarrollar validación multi-sensorial	CCO CyberSec	3 meses	Alta
Saturación (B3)	Activar correladores de tráfico adaptativo	InfraSec	2 meses	Media

Fuente: Elaboración propia

Las matrices evidencian que este tipo de ataque presenta alta probabilidad y consecuencias críticas, exigiendo un enfoque técnico y operativo integral. Las contramedidas priorizadas incluyen filtros de paquetes falsos, validación de trayectorias mediante sensores complementarios y sistemas de alerta temprana para el personal ATC.

2.3.4. Modificación de Mensajes (Message Modification)

El flujo identifica el riesgo de que un atacante altere en tránsito mensajes válidos del sistema ADS-B, cambiando parámetros críticos como la altitud, velocidad o ID de la aeronave. Desde la función de transmisión de mensajes, el activo comprometido es el

contenido legítimo de datos de vuelo. El modelo FAST permite conectar esta amenaza con tratamientos como sistemas de detección de vulnerabilidades, supervisión de integridad del mensaje y validación mediante inteligencia artificial. El flujo incorpora decisiones de impacto para permitir la reacción del sistema y la activación de contramedidas.

Para analizar la amenaza relacionada, se construyeron matrices de evaluación basadas en NIST SP 800-30. Estas permiten mapear el flujo de datos vulnerables, identificar puntos de manipulación y proponer mecanismos de integridad y monitoreo durante la transmisión:

Identificación del Escenario

Función afectada: Transmisión de mensajes ADS-B

Activo crítico: Identidad de aeronave, datos de vuelo

Amenaza: Modificación de mensajes en tránsito

Vulnerabilidad: Falta de protección de integridad en el canal

Impacto potencial: Rutas alteradas, colisiones virtuales, decisiones erradas del ATC

Controles actuales: Monitoreo de integridad, verificación cruzada con ML, detección de anomalías.

Matriz 14 – Identificación de Activos, Amenazas y Vulnerabilidades

ID	Activo Crítico	Amenaza	Vulnerabilidad	Fuente de Amenaza
C1	Mensajes ADS-B	Modificación en tránsito	Falta de integridad y autenticación	Atacante con SDR
C2	Datos de vuelo	Corrupción de identidad	Ausencia de firma digital	Cibercriminal
C3	Algoritmo de verificación	Engaño por mensajes modificados	Falsos positivos por ruido	Ruido de red o interferencia

Fuente: Elaboración propia

Matriz 15 – Estimación de Probabilidad e Impacto

ID	Probabilidad	Impacto	Nivel de Riesgo
C1	Alta	Alto	**Alto**
C2	Media	Alto	**Alto**

C3	Media	Medio	**Medio**

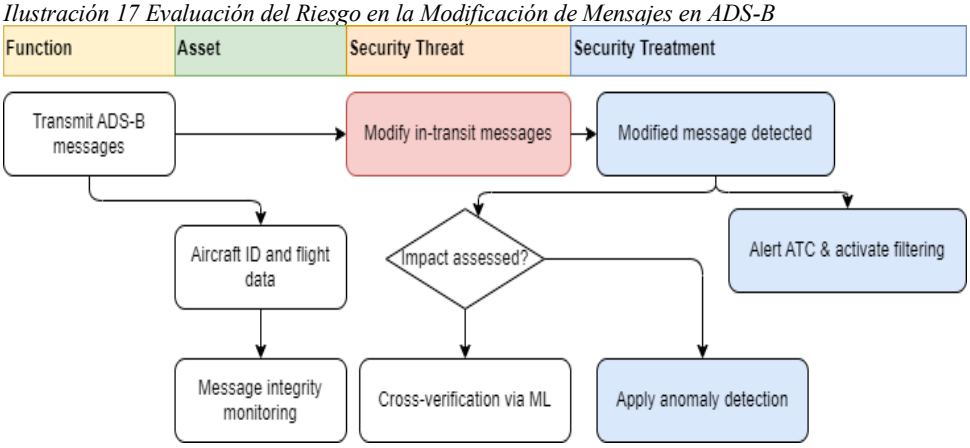
Fuente: Elaboración propia

Matriz 16 – Evaluación de Riesgos Cualitativa (Impacto x Probabilidad)

	Impacto Bajo	**Impacto Medio**	**Impacto Alto**
Probabilidad Alta	Medio	Alto	**Alto**
Probabilidad Media	Bajo	Medio	**Alto**
Probabilidad Baja	Bajo	Bajo	Medio

Fuente: Elaboración propia

Ilustración 17 Evaluación del Riesgo en la Modificación de Mensajes en ADS-B



Fuente: Elaboración propia

A continuación, se exponen las matrices obtenidas mediante NIST 800-30 partiendo de los elementos analizados en la gráfica anterior:

Matriz 17 – Controles de Seguridad y Tratamiento

ID	**Riesgo**	**Control Existente**	**Control Propuesto**	**Tipo de Tratamiento**
C1	Modificación en tránsito	Detección de integridad de mensaje	Firma digital + HMAC	Mitigar
C2	Corrupción de datos de vuelo	Verificación cruzada con ML	Confirmación con datos redundantes (radar secundario)	Mitigar
C3	Ruido y falsos positivos	Algoritmo de detección de anomalías	Mejora del umbral y entrenamiento continuo	Mitigar

Fuente: Elaboración propia

Matriz 18 – Evaluación de Controles (NIST)

ID	**Control Evaluado**	**Efectividad**	**Brechas Identificadas**
C1	Detección de modificación	Alta	No detiene la modificación, solo alerta

C2	ML para verificación	Media	Posibles errores por falsos positivos
C3	Detección de anomalías	Media	Sensible al ruido no malicioso

Fuente: Elaboración propia

Matriz 19 – Tratamientos y Plan de Acción

Riesgo	Acción Correctiva	Responsable	Tiempo Estimado	Prioridad
Modificación (C1)	Integrar firma digital en cada mensaje ADS-B	DevSecOps	4 meses	Alta
Corrupción (C2)	Correlación con múltiples fuentes (ADS-C, radar)	CCO CyberSec	3 meses	Alta
Ruido (C3)	Optimizar umbral y entrenamiento del algoritmo	InfraSec	2 meses	Media

Fuente: Elaboración propia

El uso de las matrices evidencia que los sistemas carecen de controles suficientes para detectar alteraciones en tiempo real. Se concluye la necesidad de implementar mecanismos de detección de anomalías mediante inteligencia artificial, verificación de mensajes por hash o HMAC, y validaciones cruzadas de datos críticos.

2.3.5. Eliminación de Mensajes (Message Deletion)

El riesgo evaluado es la interferencia activa que impide la transmisión o recepción de mensajes ADS-B (por ejemplo, por ataques selectivos), haciendo que la aeronave desaparezca del radar. Desde la función de captura de estado y sincronización de datos, se compromete el activo de la continuidad en el flujo de mensajes. El modelo FAST permite identificar esta vulnerabilidad como una amenaza crítica, aunque sea poco probable la materialización a menos que se usen recursos Militares, responder con detección de paquetes ausentes, alertas a operadores y escaneo del sistema. Se propone como mitigación el uso de sistemas redundantes (TCAS, radar primario, etc.).

La evaluación del riesgo asociado a la eliminación de mensajes ADS-B se realizó mediante matrices que ayudan a identificar el impacto operativo de esta amenaza, las vulnerabilidades que la facilitan, y los controles tecnológicos o procedimentales que pueden ser aplicados para mitigarla:

Identificación del Escenario

Función afectada: Captura del estado de la aeronave

Activo crítico: Datos de sensores, integridad del canal de comunicación

Amenaza: Eliminación de mensajes

Vulnerabilidad: Ausencia de verificación de continuidad y redundancia de datos

Impacto potencial: Pérdida de visibilidad, decisiones de control aéreo equivocadas

Controles actuales: Detección de mensajes perdidos, alertas, monitoreo de tráfico.

Matriz 20 – Identificación de Activos, Amenazas y Vulnerabilidades

ID	Activo Crítico	Amenaza	Vulnerabilidad	Fuente de Amenaza
D1	Datos de sensores	Eliminación de mensajes	Falta de redundancia y monitoreo de continuidad	Atacante con jammer
D2	Estado de aeronave	Ocultamiento de trayectoria	No detección de silencios en la señal	Interferencias externas
D3	Sistema de monitoreo	Falsa percepción de normalidad	Falta de validación temporal	Fallas técnicas o sabotaje

Fuente: Elaboración propia

Matriz 21 – Estimación de Probabilidad e Impacto

ID	Probabilidad	Impacto	Nivel de Riesgo
D1	Alta	Alto	**Alto**
D2	Media	Alto	**Alto**

D3	Media	Medio	**Medio**

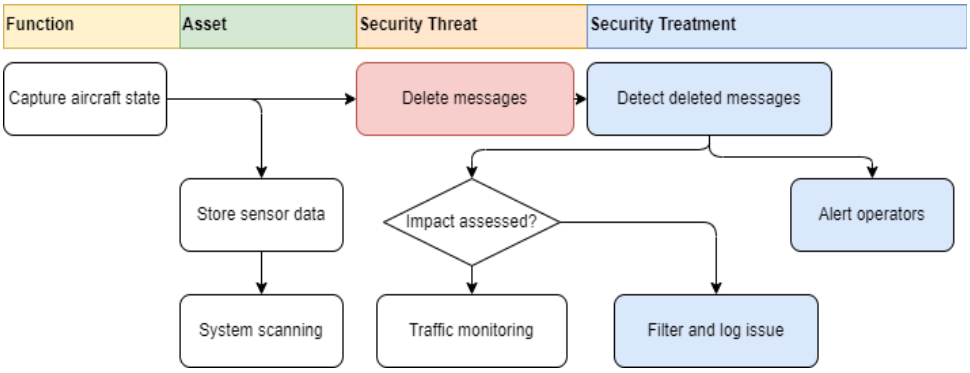
Fuente: Elaboración propia

Matriz 22 – Evaluación de Riesgos Cualitativa (Impacto x Probabilidad)

	Impacto Bajo	**Impacto Medio**	**Impacto Alto**
Probabilidad Alta	Medio	Alto	**Alto**
Probabilidad Media	Bajo	Medio	**Alto**
Probabilidad Baja	Bajo	Bajo	Medio

Fuente: Elaboración propia

Ilustración 18 Evaluación del Riesgo en la Eliminación de Mensajes en ADS-B



Fuente: Elaboración propia

Matriz 23 – Controles de Seguridad y Tratamiento

ID	**Riesgo**	**Control Existente**	**Control Propuesto**	**Tipo de Tratamiento**
D1	Eliminación de mensajes	Detección de silencios	Canal redundante + heartbeat	Mitigar
D2	Ocultamiento de ruta	Alerta a operadores	Correlación de sensores y temporización	Mitigar
D3	Falsa normalidad	Registro de eventos	Validación temporal de consistencia	Mitigar

Fuente: Elaboración propia

Matriz 24 – Evaluación de Controles (NIST)

ID	**Control Evaluado**	**Efectividad**	**Brechas Identificadas**
C1	Detección de mensajes perdidos	Media	No detecta eventos aislados o intermitentes

C2	Alertas a operadores	Alta	Requiere capacitación y respuesta rápida
C3	Registro y monitoreo	Media	Necesita validación temporal

Fuente: Elaboración propia

Matriz 25 – Tratamientos y Plan de Acción

Riesgo	Acción Correctiva	Responsable	Tiempo Estimado	Prioridad
Eliminación (D1)	Incorporar sistema de heartbeat con temporizador	DevSecOps	3 meses	Alta
Ocultamiento (D2)	Activar alertas por ventana de silencio superior a 2s	CCO CyberSec	2 meses	Alta
Falsa normalidad (D3)	Validar eventos con time stamps y frecuencia esperada	InfraSec	1 mes	Media

Fuente: Elaboración propia

Las matrices desarrolladas muestran que la eliminación de mensajes representa un riesgo significativo en situaciones operacionales complejas. Se destaca la necesidad de incorporar redundancia de canales, reintentos automáticos de transmisión y registro continuo de pérdidas para mejorar la resiliencia del sistema frente a esta amenaza.

2.3.6. Suplantación de GPS (GPS Spoofing)

Se aborda la manipulación de señales GPS para alterar la ubicación percibida por la aeronave. La función principal es localizar la posición del vuelo, y el activo comprometido es la señal GPS y las coordenadas derivadas. El atacante suplanta estas señales, generando errores de navegación o desvíos potencialmente peligrosos. El modelo FAST muestra una respuesta escalonada: detección de señales falsas, activación de validación cruzada con sensores y verificación con fuentes múltiples como Multi-GNSS. Como refuerzo, se plantea la validación visual o por radar y la consulta de trayectorias con ATC.

Se aplicó la metodología NIST SP 800-30 para construir matrices que caracterizan esta amenaza, sus causas, consecuencias y medidas de tratamiento. Esta aproximación permite evaluar de forma estructurada el impacto sobre el posicionamiento de aeronaves:

Identificación del Escenario

Función afectada: Ubicación de aeronave

Activo crítico: Señal GNSS / coordenadas de vuelo

Amenaza: Suplantación (spoofing) de señal GPS

Vulnerabilidad: Falta de validación cruzada y uso de una única fuente GNSS

Impacto potencial: Desviación de trayectoria, errores en la ubicación, incidentes operacionales

Controles actuales: Detección de señales falsas, verificación ATC, validación Multi-GNSS

Matriz 26 – Identificación de Activos, Amenazas y Vulnerabilidades

ID	Activo Crítico	Amenaza	Vulnerabilidad	Fuente de Amenaza
E1	Señal GNSS	Spoofing GPS	Receptores sin validación múltiple	Atacante con equipo GNSS
E2	Coordenadas de vuelo	Falsificación de posición	Ausencia de verificación cruzada	Cibercriminal / interferencia
E3	Validación ATC	Confirmación errónea	Error humano o dependencia del mismo sistema	Fallo en redundancia

Fuente: Elaboración propia

Matriz 27 – Estimación de Probabilidad e Impacto

ID	Probabilidad	Impacto	Nivel de Riesgo
E1	Alta	Alto	**Alto**
E2	Alta	Medio	**Alto**
E3	Media	Medio	**Medio**

Fuente: Elaboración propia

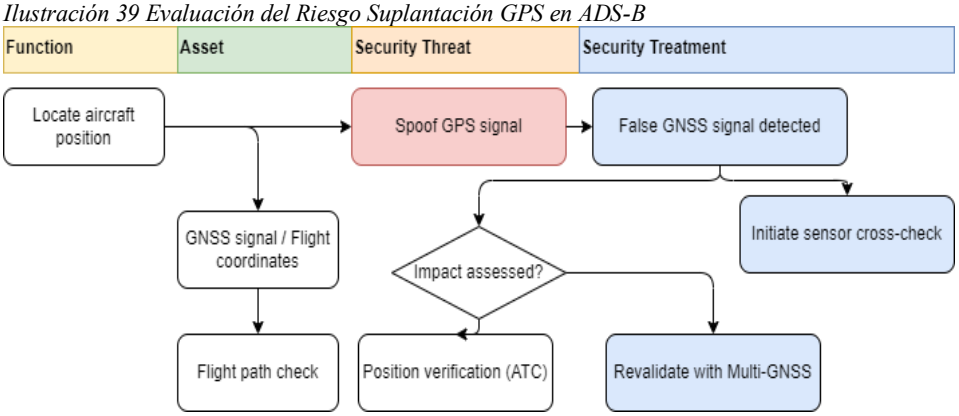
Matriz 28 – Evaluación de Riesgos Cualitativa (Impacto x Probabilidad)

	Impacto Bajo	Impacto Medio	Impacto Alto
Probabilidad Alta	Medio	Alto	**Alto**

Probabilidad Media	Bajo	Medio	Alto
Probabilidad Baja	Bajo	Bajo	Medio

Fuente: Elaboración propia

Ilustración 39 Evaluación del Riesgo Suplantación GPS en ADS-B



Fuente: Elaboración propia

Matriz 29 – Controles de Seguridad y Tratamiento

ID	Riesgo	Control Existente	Control Propuesto	Tipo de Tratamiento
E1	Spoofing de GPS	Alerta por GNSS falso	Validación multi-GNSS + detección espectral	Mitigar
E2	Coordenadas incorrectas	Verificación visual y con trayectoria	Comparación con sensores inerciales (INS)	Mitigar
E3	Validación por ATC	Coordinación operativa	Redundancia externa con base en radar secundario	Mitigar

Fuente: Elaboración propia

Matriz 30 – Evaluación de Controles (NIST)

ID	Control Evaluado	Efectividad	Brechas Identificadas
C1	Alerta de señal falsa GNSS	Alta	No siempre precisa en zonas saturadas
C2	Verificación cruzada visual	Media	Subjetiva y depende del entorno operacional
C3	Coordinación ATC	Media	Lenta ante suplantaciones rápidas

Fuente: Elaboración propia

Matriz 31– Tratamientos y Plan de Acción

Riesgo	Acción Correctiva	Responsable	Tiempo Estimado	Prioridad
Spoofing GNSS (E1)	Incorporar validación Multi-GNSS con señales mixtas	DevSecOps	4 meses	Alta
Coordenadas falsas (E2)	Validación con INS y correlación temporal	CCO CyberSec	3 meses	Alta

Validación ATC (E3)	Redundancia con radar + validación independiente	InfraSec	2 meses	Media

Fuente: Elaboración propia

La integración de FAST en conjunto con las matrices resultantes de la aplicación de la metodología NIST 800-30 aplicado al sistema ADS-B ofrece una solución para proteger el control del tráfico aéreo contra amenazas cibernéticas. La combinación de autenticación digital, IA para detección de vulnerabilidades y segmentación de redes, son importantes para mejorar la resiliencia del sistema ADS-B ante los diferentes ataques cibernéticos.

El análisis a continuación muestra los resultados tras la aplicación de medidas de mitigación frente a ataques cibernéticos sobre el sistema ADS-B. Donde todos los ataques evaluados han sido contenidos dentro de niveles de severidad (baja o media) y con una probabilidad (baja o muy baja) de ocurrencia, lo que indica una mejora del perfil de riesgo general. Esto refleja que las estrategias de seguridad implementadas (como la autenticación de mensajes, validación cruzada, segmentación de redes y algoritmos de detección basados en IA) han logrado reducir la exposición a amenazas críticas. La mitigación ha desplazado los riesgos desde zonas de alta criticidad hacia un escenario residual controlado, mejorando la resiliencia del sistema ante vectores de ataque conocidos:

Matriz 32– Matriz Resultante Riesgos Posterior Medidas Mitigación

ATACK	METHOD	SEVERITY	PROBABILITY
Aircraft reconnaissance	Eavesdropping	low	lowest
Ground Station Flood Denial	Signal Jamming	low	low
Aircraft Flood Denial	Signal Jamming	low	low
Aircraft Disappearance	Message Deletion	medium	low
Ground Station Ghost Injection	Message Injection	medium	low
Aircraft Ghost Injection	Message Injection	low	low
Virtual Aircraft Hijacking	Message Modification	medium	low
Virtual Trajectory Modification	Message Modification	medium	low
Aircraft Spoofing	Message Modification	medium	low

Fuente: Elaboración propia

Como resultado de la aplicación de medidas de mitigación sobre las amenazas identificadas en el sistema ADS-B, se observan reducciones del nivel de riesgo. Amenazas que previamente eran clasificadas como catastróficas o peligrosas (como la modificación e inyección de mensajes) han sido movidas hacia niveles con menor probabilidad o severidad, como resultado de la implementación de controles como validación cruzada, detección por inteligencia artificial, listas blancas y verificación de integridad de mensajes. Del mismo modo, riesgos como el *spoofing GPS* y la eliminación de mensajes, aunque persisten en la matriz, se ubican ahora en niveles moderados o controlados. Este resultado demuestra la

ayuda de las estrategias adoptadas, alineadas con los principios del NIST SP 800-30 y el modelo FAST.

A continuación, se mostrará la matriz resultante, donde los criterios de la severidad y la probabilidad se especifican a continuación de acuerdo con el *Risk Management Handbook* (FAA-H-8083-2):

Categorías Severidad

Categoría	Descripción
Catastrophic (1)	Fallecimientos, pérdida total del avión o sistema, impacto catastrófico en la misión o servicio.
Hazardous (2)	Heridas graves o múltiples, reducción significativa del margen de seguridad, pérdida funcional crítica.
Major (3)	Heridas menores a los ocupantes, degradación significativa del rendimiento o funcionalidad.
Minor (4)	Disminución leve de la seguridad, molestias operativas sin impacto grave.
Minimal (5)	Sin consecuencias apreciables en la operación ni en la seguridad.

Fuente: Elaboración propia de acuerdo al Risk Management Handbook (FAA-H-8083-2).

Categorías Probabilidad

Categoría	Descripción
Frequent (A)	Es probable que ocurra frecuentemente (ocurre varias veces durante el ciclo operativo).
Probable (B)	Es razonable esperar que ocurra en algún momento durante la vida del sistema.
Remote (C)	Es poco probable que ocurra, pero ha sido reportado en sistemas similares.
Extremely Remote (D)	Es muy poco probable, aunque concebible (tal vez una vez en la vida útil del sistema).
Extremely Improbable (E)	Virtualmente imposible que ocurra (requiere múltiples fallos simultáneos y altamente improbables).

Fuente: Elaboración propia de acuerdo al Risk Management Handbook (FAA-H-8083-2)

En la siguiente matriz y con base a la clasificación de acuerdo con la FAA, se ubican las cinco principales de amenazas: la falta de autenticación, la eliminación, modificación e inyección de mensajes, así como el spoofing GPS. Las zonas en color rojo indican riesgos altos o críticos que requieren atención inmediata, mientras que las zonas amarillas y verdes

representan riesgos moderados o bajos, respectivamente, una vez se han aplicado las estrategias de mitigación como se observaron en los apartados anteriores del documento:

Matriz Resultante – Tratamientos y Plan de Acción

	Minimal (5)	Minor (4)	Major (3)	Hazardous (2)	Catastrophic (1)
Frequent (A)					
Probable (B)		Falta de autenticación			
Remote (C)					
Extremely Remote (D)				Eliminación de mensajes	Modificación de mensajes
Extremely Improbable (E)			GPS Spoofing		Inyección de mensajes

Fuente: Elaboración propia a partir de los resultados de análisis previo

Teniendo en cuenta que en la realidad se pueden llegar a efectuar ataques al sistema ADS-B como se pudo observar anteriormente. A continuación, se muestra una tabla, la cual presenta una clasificación del impacto operacional de las vulnerabilidades del sistema ADS-B, organizada según cinco niveles de severidad (Extremo, Alto, Medio, Bajo, Muy Bajo) y estructurada en torno a cinco dimensiones clave: el efecto en la operación, la tripulación, el servicio de tránsito aéreo y ejemplos específicos del impacto en entornos operacionales. Esta clasificación permite visualizar cómo distintas amenazas, como la suplantación de identidad, la inyección o eliminación de mensajes y la suplantación de señales GPS, pueden escalar en cuanto al impacto operacional en sus diferentes niveles, con la finalidad de aplicar medidas de detección y mitigación eficaces a los riesgos. Por lo tanto, el análisis proporciona una

herramienta crítica para priorizar acciones de ciberseguridad, coordinar respuestas entre tripulaciones y servicios de control, y orientar la inversión en sistemas redundantes y algoritmos de detección que permitan reducir la probabilidad de incidentes en el entorno aeronáutico:

Tabla 3 Clasificación del Impacto Operacional de las Vulnerabilidades del ADS-B

CLASE PELIGRO	EXTREMO	ALTO	MEDIO	BAJO	MUY BAJO
Efecto en la operación	Pérdida conciencia situacional del controlador y pilotos por múltiples señales contradictorias.	Reducción significativa en la funcionalidad del sistema ADS-B en entornos congestionados.	Impacto moderado en separación o pérdida temporal de exactitud posicional.	Reducción leve de confiabilidad situacional sin alterar operaciones.	No afecta la operación si se detecta o mitiga a tiempo.
Efecto sobre la tripulación	Saturación cognitiva severa que impide gestionar adecuadamente la carga de trabajo, provocando pérdida de control procedimental de la aeronave.	Fatiga del piloto al validar señales dudosas o enfrentarse a falsa separación.	Incremento de carga cognitiva para discriminar tráfico real de ficticio.	Atención dividida por señales sin impacto funcional.	Sin impacto en la ejecución de funciones de la tripulación.
Efecto sobre el servicio de tránsito aéreo	Saturación del sistema de control aéreo, imposibilidad de mantener coordinación intersectorial, y activación de protocolos de contingencia nacional.	Reducción de la capacidad ATC por sobrecarga en verificación de múltiples trayectorias.	Aumento del workload ATC en sector local por mensajes incorrecto.	Supervisión reforzada por parte de ATC sin cambio en capacidad.	Sin impacto en la separación ni gestión del tráfico.
Ejemplo de efectos operacionales del ADS-B	Saturación de pantallas radar con múltiples aeronaves falsas (flooding), imposibilidad de	Activación de medidas evasivas, desvío de aeronaves o retrasos	Manejo de falsas trayectorias temporales, pérdida de	Tráfico duplicado sin impacto, descartado	Mensaje inyectado detectado y descartado

	validar ATC.	trayectorias	coordinados por ATC.	redundancia momentánea.	visual o por TCAS.	automáticamente por el sistema.

Fuente: Elaboración propia

Con la finalidad de fortalecer la mitigación de riesgos cibernéticos en el sistema ADS-B, y partiendo del resultado de gestión de los riesgos mediante el modelo FAST. A continuación, se plantea un plan con acciones específicas para abordar vulnerabilidades críticas como la falta de autenticación, la modificación e inyección de mensajes, la suplantación de GPS y la eliminación de datos, para mitigar la materialización de los riesgos asociados:

Tabla 4 Plan de Mitigación Riegos Ciberseguridad ADS-B.

Vulnerabilidad	Acción Específica	Actividad Sugerida
Falta de Autenticación	Implementar MAC y listas blancas de emisores válidos.	Proponer a la UAEAC la implementación de la tecnología propuesta mediante un tercero que tenga el servicio y certificación de instalación.
Modificación de Mensajes	Desplegar sistemas de monitoreo para la verificación de la calidad del mensaje, mediante los campos CRC (Cyclic Redundancy Check) en los modos DF17-DF18 y del campo Payload (ME –Message, Extended) para constatar la integridad.	Proponer la implementación específicamente al Centro de Control de Tráfico Aéreo (ATC) a través de la UAEAC.
Inyección de Mensajes	Generar sistemas de correlación de datos antes diferentes fases de vuelo de las aeronaves.	Sugerir la implantación de modelos existentes de correlación de datos de las aeronaves en vuelo a la UAEAC.
Suplantación de GPS	Uso de sensores redundantes al GNSS (ejemplo, uso de sistemas GLONASS, Galileo o BeiDou), además de sistemas Inerciales, MLAT basándose en el tiempo de llegada (TDOA).	Analizar la viabilidad de utilización de sensores y sistemas para buscar la redundancia de información de posicionamiento global.
Eliminación de Mensajes	Desarrollar sistemas de análisis predictivos, para suplir mensajes faltantes, mediante el uso de la predicción bitácoras, retransmisiones desde fuentes redundantes y tolerancia a fallos.	(la materialización de un evento de este tipo es poco probable de materializarse, a menos que se hagan con equipos muy avanzados, principalmente Militares).

Todas (formación)	Formar al personal inmerso en las operaciones con ADS-B sobre el entendimiento de los datagramas y los riesgos de ciberseguridad asociados al sistema.	Recomendar la formación del personal inmerso en las operaciones del ADS-B a nivel nacional por parte de la UAEAC.

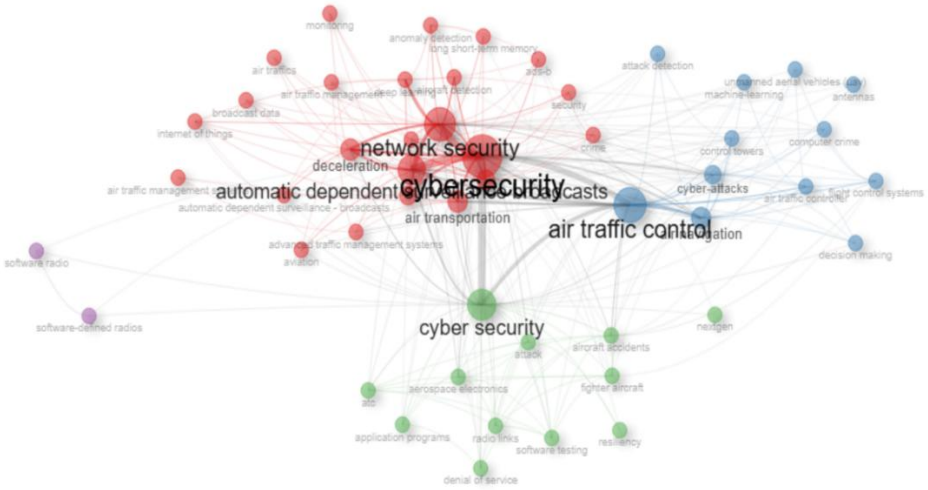
Fuente: Elaboración propia.

Una vez realizado la gestión de los riesgos mediante la metodología FAST y generar la clasificación del impacto operacional y proponer un plan de mitigación, a continuación, se propone un modelo híbrido para la valoración de los efectos generados dentro del sistema ADS-B.

2.4. Propuesta de un modelo híbrido para la valoración de los efectos de las vulnerabilidades del sistema ADS-B.

Como parte del análisis bibliográfico preliminar, se utilizó la herramienta Bibliometrix a través de su módulo Biblioshiny, con el fin de identificar los principales conceptos y las relaciones temáticas presentes en la literatura científica relacionada con la ciberseguridad en el sistema ADS-B. Mediante la generación de una red de co-ocurrencias de palabras clave (co-occurrence network), se evidenció la conexión entre distintos términos según como se muestra la imagen a continuación, denotando la importancia de desarrollar modelos de evaluación de amenazas que integren elementos tanto técnicos como operacionales:

Ilustración 20 Red de Co_Ocurrencias del Sistema ADS-B



Fuente: Elaboración propia

Los clústeres temáticos identificados permiten ser tenidos en cuenta para la elaboración de una metodología híbrida que combina el enfoque FAST con la lógica de los Mapas Cognitivos Difusos (Fuzzy Cognitive Maps). Este enfoque busca modelar, de manera estructurada y dinámica, la interacción de factores de riesgo en contextos aeronáuticos, lo que busca fortalecer así la toma de decisiones frente a amenazas emergentes en entornos de navegación aérea digitalizados y abiertos.

Para plasmar la idea descrita, se usará la herramienta para la modelación y se llama Mental Modeler, donde es necesario primero identificar variables o elementos clave que permitan modelar los riesgos cibernéticos en ADS-B y su mitigación de manera estructurada y adaptable a la incertidumbre de los ataques cibernéticos.

2.4.1. Identificación de Variables Clave en la Gestión de Riesgos con FAST y Mapas Cognitivos Difusos

Para la implementación mediante Mental Modeler, se extrajeron las variables más recurrentes del resultado de la metodología Delphi aplicada a personal expertos (08 personas)

en conocimientos como ADS-B, ciberseguridad, navegación aérea y aviación (los resultados de las encuestas reposan en el repositorio de GitHub). También son usados datos obtenidos de la red de co_ocurrencias descritas previamente, siendo interrelacionadas con los resultados obtenidos mediante los modelos FAST y STRIDE, donde estas deben representar los elementos esenciales de seguridad, riesgos, amenazas y mitigaciones dentro del sistema ADS-B, integrando la capacidad de modelar la incertidumbre inherente a los ataques cibernéticos mediante mapas cognitivos difusos:

Tabla 4 Elementos de la Modelación

CATEGORÍA	ÍTEM	FRECUENCIA
Activos Claves	Señal GNSS (GPS)	5
	Transmisor ADS-B aéreo	4
	Servidor de vigilancia aérea (ATC)	4
	Receptor terrestre ADS-B	3
	Infraestructura de red de control aéreo	3
Amenazas Cibernéticas	Interferencia RF (Jamming)	5
	Spoofing GPS (Suplantación de GPS)	5
	Acceso no autorizado a red ADS-B	3
	Inyección de mensajes (Message Injection)	3
	Desincronización de transmisiones	2
Medidas de Mitigación	Sistemas redundantes (Radar primario)	4
	Multilateración (MLAT)	4
	Autenticación Digital (MAC, listas blancas)	4
	Segmentación de redes críticas	3
	Cifrado de datos (AES-256)	2
Variables de Decisión FCM	Tiempo de reacción ante incidentes	4
	Capacidad de Coordinación Interinstitucional	4
	Nivel de Detección	4
	Precisión del sistema de detección	3
	Cobertura de fusión de sensores	2

Fuente: Elaboración propia

En la tabla Elementos y Criterios Elaboración Gráfico Mental Modeler, se presentan algunas (5 de 100, el resto se comparten en el repositorio) de las relaciones causales explicadas (criterios y elementos), basada en los modelos previamente explicados, para descomponer de manera estructurada las interacciones entre amenazas cibernéticas, activos críticos, funciones operacionales y medidas de mitigación en el sistema ADS-B. Cada relación fue cuantificada (valor entre 0 y 1) e interpretada como positiva o negativa, dependiendo del efecto que una variable causa sobre otra. Este enfoque facilita la modelación en herramientas como *Mental Modeler*, permitiendo representar visualmente cómo cambios en una parte del sistema (por ejemplo, la autenticación de mensajes) pueden afectar el comportamiento general, la capacidad de detección, y la reducción del impacto operacional de un ataque.

Tabla 6 Algunos Elementos y Criterios Elaboración Gráfico Mental Modeler

Desde	Nodo Afectado	Relación	Dirección
Interferencia RF (Jamming)	Receptor terrestre ADS-B	0.8	Negativa
Spoofing GPS (Suplantación de GPS)	Receptor terrestre ADS-B	0.8	Negativa
Acceso no autorizado a red ADS-B	Receptor terrestre ADS-B	0.8	Negativa
Inyección de mensajes (Message Injection)	Receptor terrestre ADS-B	0.8	Negativa
Desincronización de transmisiones	Receptor terrestre ADS-B	0.8	Negativa
…..	…..	….	……

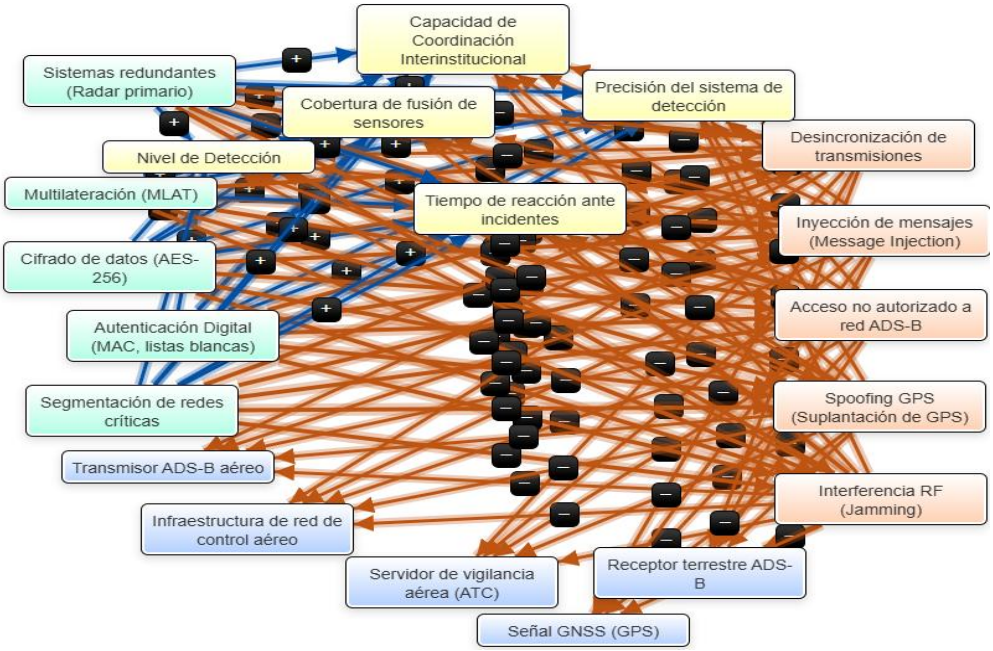
Fuente: Elaboración propia

Realizar este tipo de análisis causal, aporta con múltiples beneficios para el fortalecimiento de la ciberseguridad en entornos aeronáuticos. Primero, promueve una comprensión sistémica del riesgo, permitiendo a los responsables de seguridad anticiparse a las posibles consecuencias de ataques específicos. Segundo, facilita la toma de decisiones

estratégicas, ya que permite identificar qué componentes o medidas tienen mayor efecto mitigador.

Por lo tanto, el siguiente gráfico muestra un modelo conceptual de relaciones causales aplicadas al sistema ADS-B, elaborado bajo la metodología FAST y representado mediante el software *Mental Modeler*. Cada nodo representa un componente crítico del sistema, clasificado por función (amenazas, activos, técnicas de mitigación y variables de decisión), mientras que las flechas indican la dirección e intensidad del efecto que una variable ejerce sobre otra. Las conexiones azules con el símbolo "+" representan relaciones positivas (por ejemplo, la mejora en detección gracias al uso de MLAT), mientras que las flechas anaranjadas con el símbolo "–" representan relaciones negativas (por ejemplo, el impacto que la inyección de mensajes tiene sobre los receptores terrestres). Este tipo de visualización facilita entender la dinámica del sistema ante ciberamenazas, y cómo la implementación de medidas como autenticación, cifrado o segmentación de red puede mitigar ataques como spoofing, eliminación o modificación de mensajes, contribuyendo a una mayor resiliencia del entorno aeronáutico.

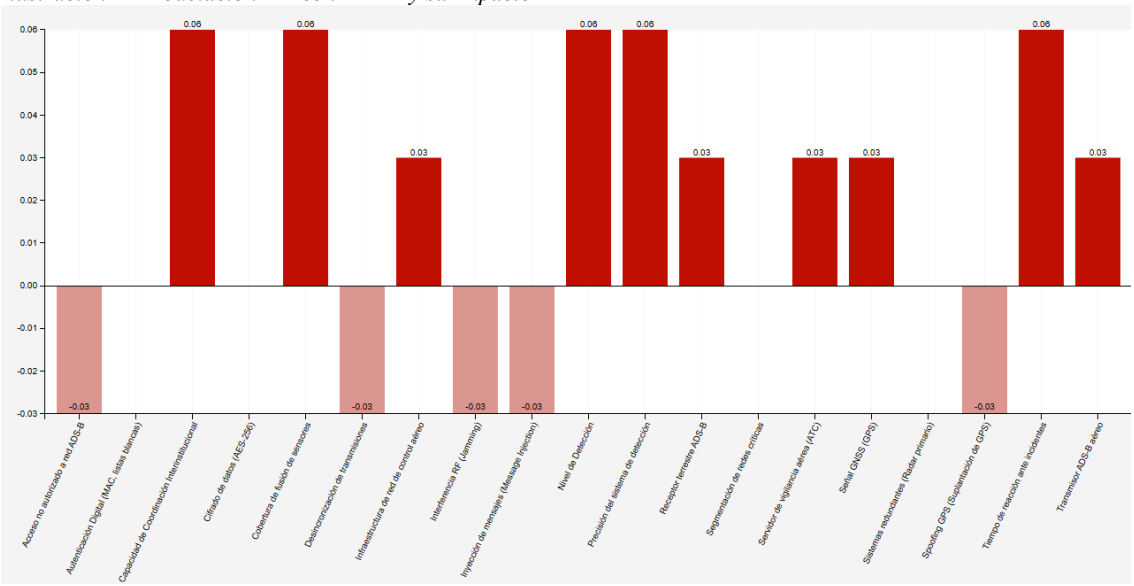
Ilustración 21 Diseño Gráfico del Modelo Propuesto



Fuente: Elaboración propia.

Teniendo en cuenta lo anterior, se obtiene una relación matricial, la cual representa cuantitativamente el resultado del análisis de relaciones causales aplicado al sistema ADS-B mediante la herramienta *Mental Modeler*. Cada celda contiene un valor entre -1 y 1 que refleja el impacto de un componente (columna) sobre otro (fila), donde los valores negativos indican una relación inhibitoria (mitigación o reducción de riesgo) y los positivos una relación de fortalecimiento o agravamiento. El siguiente escenario, fue generado a partir del modelo de relaciones difusas elaborado en Mental Modeler, utilizando como insumo los elementos más relevantes del sistema ADS-B, de acuerdo con los datos obtenidos y descritos previamente, para visualizar la influencia acumulada de cada componente dentro del sistema, con el fin de priorizar acciones estratégicas en ciberseguridad del sistema ADS-B:

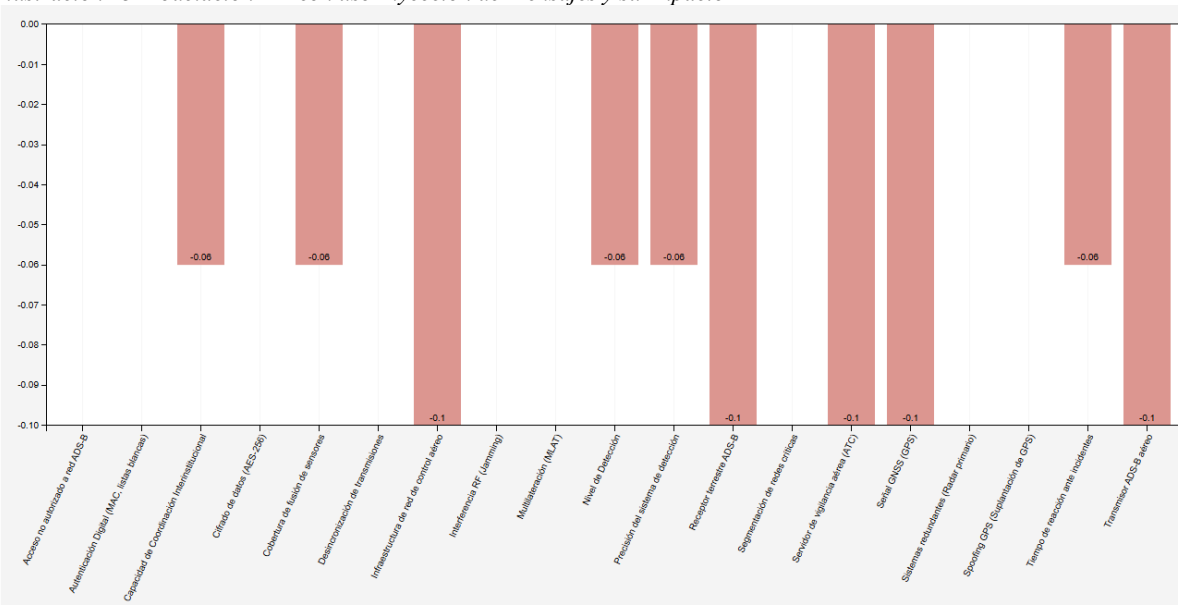
Ilustración 22 Modelación "1" con MLAT y su Impacto



Fuente: Elaboración propia

En gráfico anterior, se muestra la influencia neta de cada variable dentro del sistema ADS-B, evidenciando cuáles elementos aportan positivamente a la seguridad operacional y cuáles representan un riesgo. Destacan con impacto positivo variables como la coordinación interinstitucional, la multilateración (MLAT), el cifrado de datos y el nivel de detección, lo cual sugiere que fortalecer estas capacidades puede mejorar significativamente la resiliencia del sistema. Por el contrario, ataques como la interferencia por Radiofrecuencia (jamming), el spoofing GPS y la inyección de mensajes tienen una influencia negativa, subrayando su rol crítico como riesgos a mitigar:

Ilustración 23 Modelación "2" con uso Inyección de Mensajes y su Impacto



Fuente: Elaboración propia

La anterior muestra un escenario simulado en el que se analizan los efectos acumulativos negativos dentro del sistema ADS-B. Todos los elementos representados tienen un valor negativo, indicando que, en este contexto, las interacciones entre variables resultan en un impacto desfavorable sobre el sistema, en los componentes como: Infraestructura de red de control aéreo, Receptor terrestre ADS-B y el Servicio de vigilancia aérea (ATC), cada uno con un peso de -0.10, lo que refleja un alto grado de riesgo e interferencia en el sistema de vigilancia.

Este resultado sugiere que, ante un escenario adverso (por ejemplo, con múltiples amenazas activas y medidas de mitigación insuficientes), incluso los activos críticos y las variables diseñadas para reforzar la ciberseguridad (como las medidas de detección). Por tanto, el análisis destaca la necesidad de una revisión profunda de las interacciones del sistema, el refuerzo de capacidades preventivas y reactivas, y la implementación de acciones coordinadas e integrales para revertir este escenario desfavorable.

El uso de mapas cognitivos difusos en Mental Modeler permite desarrollar una metodología avanzada y dinámica para la gestión de riesgos cibernéticos en ADS-B. Esta propuesta contribuye a una protección más efectiva y adaptativa, mejorando la resiliencia del sistema ante ataques.

A continuación, se propone como iniciativa un procedimiento operativo con la finalidad de fortalecer los protocolos ante la atención a los ataques cibernéticos al sistema ADS-B en el contexto colombiano que permitan fortalecer las medidas de tipo procedimental y mitigar los riesgos generados en la operación aeronáutica.

2.5. Estructura del Procedimiento C.A.R.E.

Actualmente en Colombia, dentro de la Aeronáutica Civil, se está trabajando en procedimientos para atender momentos de crisis generados por ataques cibernéticos en el ambiente aeronáutico, por lo tanto, en complemento se propone el Procedimiento C.A.R.E. (Coordinación, Autenticación, Respuesta y Evaluación) siendo una iniciativa, diseñada con la finalidad de fortalecer la ciberseguridad del sistema ADS-B, como resultado del análisis de todos los elementos analizados en el presente artículo, para fortalecer la seguridad operacional:

- **Coordinación Multinivel e Interinstitucional**, mediante la activación inmediata de un Centro de Gestión de Incidentes de Ciberseguridad Aeronáutica (CGICA) dentro del ATC ante detección de una anomalía ADS-B. Este centro deberá tener interconexión con Equipos CERT/CIRT aeronáuticos nacionales, personal de seguridad de la aviación (pilotos, operadores, técnicos) y con la FAC (para la defensa aérea, en casos de aeronaves sospechosas), a través del uso de canales seguros de

comunicación redundantes (VHF, HF, red privada IP cifrada). La detección de una anomalía en el sistema ADS-B puede llegar a originarse por la recepción de mensajes inconsistentes, duplicados o con trayectorias no previstas. Los controladores aéreos (ATC), mediante sus sistemas de vigilancia y experiencia operativa, identificarían estos comportamientos atípicos como posibles amenazas cibernéticas o fallos técnicos.

- **Autenticación y Validación Dinámica**, a través de la implementación en tiempo real de una doble validación de tráfico sospechoso, mediante la validación automatizada apoyada de otros sistemas (motor de IA entrenado en detección, uso de LSTM, predicción de trayectorias, etc.), además de la verificación visual (cuando sea posible), y confrontación con el plan de vuelo, código transponder y ruta prevista. Una vez coordinada la respuesta, se activa una doble validación del tráfico sospechoso. La primera en automatizada se basa en la verificación se apoya en sistemas inteligentes que reconocen patrones de vuelo anormales y ayudan a confirmar si una aeronave reportada es real o una simulación falsa. La segunda es manual, realizada por el personal de control de tránsito aéreo, quienes contrastan la información con planes de vuelo, registros visuales y comunicación directa por radio.
- **Respuesta Operacional Estratificada** con la activación inmediata del protocolo de tráfico:

  - Clasificación del espacio aéreo en zonas seguras, sospechosas y críticas.
  - Vectorización de tráfico hacia patrones de espera.

- Aplicación de protocolos ABD (Air Bridge Denial) si la amenaza compromete soberanía nacional.

Dependiendo del nivel de amenaza validado, se ejecuta una respuesta operacional diferenciada. El espacio aéreo se divide en zonas seguras, sospechosas y críticas, y las aeronaves pueden ser vectorizadas a patrones de espera seguros. En casos extremos, se puede aplicar el protocolo de negación de acceso aéreo (ABD), especialmente si se presume un uso hostil o criminal del canal ADS-B.

- **Evaluación y Aprendizaje Continuo,** mediante la generación automática de un registro forense aeronáutico digital (bitácora digital) por cada incidente. Revisión de cada evento bajo un esquema After Action Review (AAR) estandarizado posterior al incidente. Actualización del sistema de detección y respuesta mediante aprendizaje supervisado continuo y retroalimentación del personal operativo.

Con base en los aprendizajes del incidente, se actualizan los algoritmos de detección, los procedimientos operativos y las directrices institucionales. La idea es que el sistema ADS-B y sus protocolos asociados evolucionen de forma resiliente ante nuevas amenazas, manteniendo altos estándares de seguridad operacional.

2.5.1. Diagramas de Flujo del Procedimiento C.A.R.E.

A. Flujo General de Activación del Procedimiento C.A.R.E.

- Detección de anomalías en el sistema ADS-B.
- Activación CGICA.
- Implementación de medidas de respuesta (vectorización, patrón de espera, ABD)

- Emisión de Cyber-NOTAM y comunicación interinstitucional.

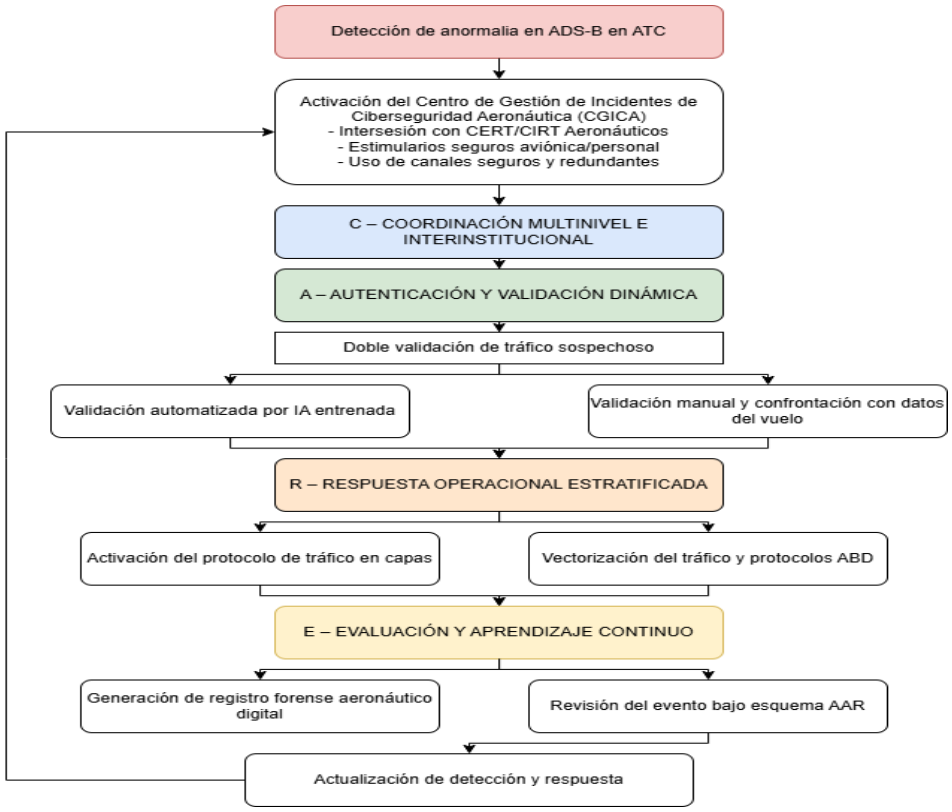
B. Flujo de Verificación de Aeronave Sospechosa

- Identificación de mensaje ADS-B inconsistente.
- Correlación con plan de vuelo / transponder / historial.
- Intento de contacto por radio.
- Verificación visual (si aplica) o MLAT/radar.
- Activación del protocolo correspondiente (respuesta/negación/acercamiento militar)

C. Métricas de Evaluación del Procedimiento

- Tiempo medio de reacción ante una amenaza detectada.
- Grado de cobertura de fusión multisensor (MLAT + PSR + ADS-B).
- Porcentaje de tripulaciones entrenadas en procedimiento CARE.
- Número de simulacros y ejercicios realizados.

Ilustración 24 Diagrama Procedimiento C.A.R.E.



Fuente: Elaboración propia.

La siguiente tabla presenta algunos actores involucrados en la implementación del Procedimiento C.A.R.E., describiendo su rol fundamental dentro del esquema de respuesta ante incidentes de ciberseguridad en el sistema ADS-B, así como las respectivas responsabilidades clave para garantizar una actuación coordinada, eficiente y oportuna en escenarios de amenaza:

Tabla 7 Roles y Responsabilidades en el Procedimiento C.A.R.E.

Actor	Rol Principal	Responsabilidades Clave
Centro de Gestión de Incidentes de Ciberseguridad Aeronáutica (CGICA)	Coordinar la respuesta ante incidentes de ciberseguridad en ADS-B.	Activar alertas; coordinar con ATC, FAC, CERT; mantener comunicación segura y constante.
Controladores Aéreos (ATC)	Detectar vulnerabilidades iniciales y activar protocolos de respuesta.	Registrar vulnerabilidades ADS-B; seguir el procedimiento de validación; emitir alerta a CGICA.

Fuerza Aérea Colombiana (FAC)	Apoyar con recursos de vigilancia, interceptación y negación aérea si es necesario.	Asignar recursos aéreos; evaluar riesgo de aeronaves no identificadas; coordinar con ATC.

Fuente: Elaboración propia

Resultado Esperado

- Reducción del tiempo de reacción ante incidentes cibernéticos en el sistema ADS-B.
- Incremento de la conciencia situacional tripulada y no tripulada.
- Salvaguarda de la vida humana mediante decisiones oportunas en cabina y en ATC.
- Fortalecimiento de la seguridad operacional conforme a los principios del Anexo 19 de la OACI.

Conclusiones

De acuerdo con lo revisado en el artículo científico, se concluye que, aunque el sistema ADS-B ha contribuido en la gestión del tráfico aéreo, la arquitectura abierta del sistema y la carencia de mecanismos de autenticación y cifrado, lo hacen vulnerables antes ciberataques, tanto pasivos como activos, afectando los principios de confidencialidad, integridad, disponibilidad y autenticidad (CIDA), comprometiendo la seguridad de las operaciones aéreas. A través de un enfoque híbrido basado en los modelos FAST, STRIDE, NIST 800-30 y mapas cognitivos difusos, se caracterizaron de manera dinámica los riesgos.

La investigación permitió validar, mediante pruebas en entornos simulados y reales, la existencia de dichas vulnerabilidades, en particular el ataque de Message Injection, evidenciando su viabilidad técnica incluso con herramientas de bajo costo como HackRF y

RTL-SDR. Esto resalta la urgencia de adoptar medidas de detección y mitigación adaptables a la realidad operativa. Por lo que se propone el uso de la iniciativa CyberSkyGuard.

Como respuesta a esta problemática, se propuso un modelo híbrido de gestión de riesgos que combina la metodología FAST con Mapas Cognitivos Difusos, permitiendo una caracterización dinámica y estructurada de los factores críticos y sus interacciones dentro del sistema. Este modelo facilita la priorización de acciones estratégicas y la toma de decisiones informadas en entornos de incertidumbre cibernética.

Además, se diseñó el Procedimiento C.A.R.E. (Coordinación, Autenticación, Respuesta y Evaluación), con el objetivo de articular la respuesta institucional ante incidentes cibernéticos en el sistema ADS-B colombiano. Este procedimiento ofrece una guía operativa escalable que fortalece la resiliencia del sistema, incorporando coordinación interinstitucional, validación dinámica de tráfico, respuesta estratificada y mecanismos de aprendizaje continuo.

En síntesis, el presente estudio no solo evidencia las brechas críticas del sistema ADS-B frente a amenazas cibernéticas, sino que también ofrece herramientas prácticas y metodológicas para su mitigación. Estas propuestas buscan ser un aporte significativo para la formulación de políticas de seguridad operacional y ciberdefensa en la aviación colombiana, alineadas con las mejores prácticas internacionales y los marcos normativos vigentes.

Referencias

Abu Al-Haija, M., & Al-Tamimi, F. (2024). ADS-B security vulnerabilities and attack mitigations. Journal of Aerospace Cybersecurity, 12(1), 10-11.

Abu Al-Haija, Q., & Al-Tamimi, A. (2024). Secure aviation control through a streamlined ADS-B perception system. Applied System Innovation, 7(2), 27.

Aerocivil. (2023). Reporte de ciberseguridad en la aviación colombiana. Unidad Administrativa Especial de Aeronáutica Civil, p. 18.

Agbeyibor, R. C. (2014). *Secure ADS-B: Towards Airborne Communications Security in the Federal Aviation Administration's Next Generation Air Transportation System* (Tesis de maestría, Air Force Institute of Technology). https://scholar.afit.edu/etd/584

Ahmed, W. (2024). ADS-B Communication in Modern Air Traffic Management: Threats, Risks and Security Solutions.

Ahmed, W., Bhatti, N. A., Masood, A., Alharbi, A. A. K., & Alotaibi, S. (2024). Advancements in ADS-B security: A comprehensive survey of vulnerabilities, mitigation strategies, system requirements, and emerging research trends (p. 11). Preprints.org. https://doi.org/10.20944/preprints202405.0586.v2

Amin, S., Clark, T., & Offutt, R. (2014). Design of a cyber security framework for ADS-B based surveillance systems.

Benavides Moncayo, O. L. (2016). Consideraciones para la implementación del sistema de Vigilancia Dependiente Automática – Radiodifusión (ADS-B) en Colombia. Revista Visión Electrónica. Universidad Distrital Francisco José de Caldas.

Bria, O., & Giacomantone, J. (2020). Colaboración ADS-B en la Predicción SSR.

Brown, R., Lee, H., & Smith, A. (2023). Deep learning for anomaly detection in GPS navigation systems. IEEE Transactions on Aerospace and Electronic Systems, 59(2), 154–169.

Cadena, E. L. (2019). Requerimientos de ADS-B en Colombia: optimizar procedimientos de instalación. Foro Regulatorio Informativo, Bogotá - Colombia. Aeronáutica Civil de Colombia.

Caparroso, J. (2023). Incremento del ransomware en el sector aeronáutico en Colombia durante 2022. Lumu Advisory Report, 30.

CASA. (2016). Questions and Answers for Owners of Australian General Aviation Aircraft.

Costigan, S., & Hennessy, M. (2023). Cybersecurity education frameworks for critical infrastructure sectors. Cybersecurity Policy and Practice Review, 7(4), 50–64.

Cretin, A., Vernotte, A., Chevrot, A., Peureux, F., & Legeard, B. (2020). Test data generation for false data injection attack testing in air traffic surveillance. IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 143-152.

Elmarady, A.A.W., & Rahouma, K. (2021). Actual TDoA-based augmentation system for enhancing cybersecurity in ADS-B.

Federal Aviation Administration (FAA). (2022). ADS-B Operations Manual.

Federal Aviation Administration (FAA). (2022). Automatic Dependent Surveillance-Broadcast Operations (AC 90-114B). FAA. Disponible en: https://www.faa.gov/regulations_policies/advisory_circulars.

Florez, J. A., Avendaño Hurtado, J. L. E., Barragán, C. U., & Díaz, L. A. (2023). Estrategia de resiliencia para los servicios de vigilancia aeronáutica en Colombia. Congreso de Desarrollo Aeroespacial Colombiano, 19-20 de octubre de 2023. Aeronáutica Civil de Colombia.

Gómez, L. (2015). Vigilancia Dependiente Automática (ADS-B) en Colombia. Ciencia y Poder Aéreo, 10(1), 21-32. Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.18667/cienciaypoderaereo.215.

Haass, J. C., Craiger, J. P., & Kessler, G. C. (2018). A Framework for Aviation Cybersecurity. IEEE Aerospace Conference. Embry-Riddle Aeronautical University, USA. doi: 10.1109/AERO.2018.1234567.

Habler, E., & Shabtai, A. (2018). Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. Computers & Security, 78, 155-173.

Haines, B., & Foster, N. (2012). *Exploiting the Automatic Dependent Surveillance-Broadcast System via False Target Injection*. Presentado en DefCon 20

Hassan, M., Rahman, M., Ahmed, K., & Ali, A. (2024). Performance Analysis of Machine Learning Algorithms in Detecting Cyber Attacks Targeting ADS-B.

Holemans, L. (2016). Securing automatic dependent surveillance broadcast (ADS-B) transmissions against spoofing. Utica College.

Holemans, T. (2016). Cybersecurity risks in air traffic management. International Journal of Critical Infrastructure Protection, 8(3), 14-15.

Indra. (2020). Sistema ADS-B en la Gestión del Tráfico Aéreo. Disponible en: https://www.indracompany.com.

Kacem, T. (2016). Secure ADS-B (Doctoral dissertation). George Mason University, Fairfax, VA.

Kacem, T., Wijesekera, D., & Costa, P. (2015). Integrity and Authenticity of ADS-B Broadcasts. IEEE Aerospace Conference, Big Sky, MT.

Kacem, T., Wijesekera, D., Costa, P., Monteiro, M., & Barreto, A. (2015). Secure ADS-B Design & Evaluation. IEEE International Conference on Vehicular Electronics and Safety (ICVES), Yokohama, Japan.

Klir, G. J., & Yuan, B. (1995). Fuzzy Sets and Fuzzy Logic: Theory and Applications. Prentice Hall.

Lubbe, H., Serfontein, R., & Coetzee, M. (2024). Assessing the effectiveness of ADS-B mitigations. ICCWS 2024.

Manesh, M. R. (2019). Investigating ADS-B spoofing threats. IEEE Aerospace Conference, 80.

Manesh, M. R., & Kaabouch, N. (2017). Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. International Journal of Critical Infrastructure Protection, 19, 16–31. https://doi.org/10.1016/j.ijcip.2017.10.002.

MinTIC. (2023). Plan de Ciberseguridad y Ciberdefensa Nacional 2023–2026. Ministerio de Tecnologías de la Información y las Comunicaciones, p. 33.

Monteiro, M., Barreto, A., Kacem, T., Carvalho, J., & Wijesekera, D. (2015). Detecting Malicious ADS-B Broadcasts Using Wide Area Multilateration. Digital Avionics Systems Conference (DASC), IEEE/AIAA 34th.

Organización de Aviación Civil Internacional (OACI). (2014). ADS-B Implementation and Operations Guidance Document.

Organización de Aviación Civil Internacional (OACI). (2019). Estrategia de ciberseguridad de la aviación. OACI. https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx.

Ray, G., & Ray, J. (2023). Detecting ADS-B Replay Cyberattacks in the National Airspace System. Issues in Information Systems, 24(1), 170-185.

Ronen, E., & Ben-Moshe, T. (2021). GPS spoofing detection using deep learning for aviation applications. *Sensors*, 21(4), 1451. https://doi.org/10.3390/s21041451

Strohmeier, M., Lenders, V., & Martinovic, I. (2014). Realities and challenges of NextGen air traffic management: The case of ADS-B. *IEEE Communications Magazine*, 52(5), 111–118. https://doi.org/10.1109/MCOM.2014.6815901.

Strohmeier, M., Lenders, V., & Martinovic, I. (2015). On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. IEEE Communications Surveys & Tutorials, 17(2), 1066-1087. doi: 10.1109/COMST.2014.2365951.

Universal Avionics. (2016). Comprendiendo el cumplimiento del ADS-B Out. Disponible en: https://www.universalavionics.com.

Zadeh, L. (1965). Fuzzy Sets. Information and Control, 8(3), 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X.

Anexo I.

Normatividad

El sistema ADS-B, se ha convertido en un estándar global, con distintas fechas de implementación en cada región, como, por ejemplo:

Estados Unidos

Desde el 1 de enero de 2020, todas las aeronaves que operen en espacio aéreo controlado deberán contar con ADS-B OUT (FAA, 2022, p. 5).

Europa

Desde diciembre de 2017, todas las aeronaves que vuelen en el espacio aéreo europeo, deberán estar equipadas con ADS-B, con excepciones limitadas para aeronaves antiguas (OACI, 2014, p. 30).

Australia

Desde el año 2013, las aeronaves que vuelan por sobre el nivel de vuelo FL290, deberán contar con ADS-B. En 2017, el requisito se extendió a todas las aeronaves en vuelos IFR (CASA, 2016, p. 20).

Marco Regulatorio en Colombia

Colombia ha adoptado un enfoque progresivo en la implementación del ADS-B dentro del marco del **Plan Nacional de Navegación Aérea (PNA)**, estando alineados con las regulaciones de la **OACI** y los estándares internacionales de vigilancia aérea (Gómez, 2015, p. 28). Las principales regulaciones y normativas aplicadas en Colombia para el uso del ADS-B incluyen:

- **Resolución 5197 de 2010 (Aerocivil)**, la cual define los requerimientos técnicos para la implementación del ADS-B en Colombia.
- **Regulación de la OACI (Doc 9871 y Anexo 10, Volumen IV)**, donde se establece los parámetros para la transmisión de datos de vigilancia y seguridad operacional.
- **Plan Nacional de Navegación Aérea (PNA)**, es un documento base para la transición hacia tecnologías basadas en datos satelitales como ADS-B (Gómez, 2015, p. 30).
- **Circular Reglamentaria 002 de 2014**, la cual regula la instalación y operación de equipos ADS-B en aeronaves dentro del espacio aéreo colombiano.
- **Resolución No. 02217 del 26 de octubre de 2023**, Aerocivil, establece la obligatoriedad del uso del sistema ADS-B en aeronaves civiles, **a partir del 1 de enero de 2025**. Esta disposición aplica a todas las aeronaves que operen en el espacio aéreo colombiano, dentro de zonas que serán determinadas por la autoridad aeronáutica. La resolución modifica el numeral 91.1711 del Reglamento Aeronáutico de Colombia (RAC 91), incluyendo los requisitos técnicos mínimos que deben cumplir las aeronaves, como contar con transmisores ADS-B. Esta regulación responde a la necesidad de modernizar el sistema de vigilancia aérea, mejorar la eficiencia del control del tránsito aéreo y alinearse con los compromisos internacionales en materia de seguridad operacional y gestión del espacio aéreo (Unidad Administrativa Especial de Aeronáutica Civil, 2023).

Anexo II.

1. Implementación Operativa del Procedimiento C.A.R.E. y Modelo Híbrido

Para implementar el procedimiento C.A.R.E. y el modelo híbrido de gestión de riesgos (FAST + Mapas Cognitivos Difusos), se propone un plan en cuatro fases escalables:

Fase I - Diagnóstico y capacitación inicial: implica un diagnóstico de capacidades actuales de vigilancia y respuesta ante incidentes cibernéticos del sistema ADS-B en Colombia. Se deben identificar brechas tecnológicas, humanas y procedimentales. Paralelamente, se ejecutará un plan de formación a operadores ATC, técnicos de la UAEAC y miembros de la FAC en identificación de tráfico sospechoso, uso de protocolos CARE y empleo básico de IA aplicada a detección.

Excelente	70 100
Regular	50 69
Malo	49 o menos

No.	Paso	Cómo se realizará	Tiempo estimado	Medición del avance	Nota	Estado
1	Conformar el equipo de trabajo interinstitucional	Convocatoria formal mediante	Semana 1	Acta de constitución y lista oficial de	80	80%
2	Definir objetivos operativos y técnicos de la fase	Sesión de planificación	Semana 1	Documento oficial con alcance, metas y	49	49%
3	Identificar los puntos críticos de vigilancia aérea en Colombia	Análisis geoespacial y	Semana 2	Mapa con zonas priorizadas y criterios	80	80%
4	Levantamiento del estado actual del sistema ADS-B	Revisión técnica en campo y	Semana 2	Informe de estado actualizado por región y	93	93%
5	Auditoría de ciberseguridad a la infraestructura ADS-B	Aplicación de herramientas de	Semanas 3-4	Reporte de auditoría con hallazgos y	66	66%
6	Análisis de vulnerabilidades en estaciones terrestres y receptores	Pruebas técnicas controladas en	Semana 4	Informe técnico de vulnerabilidades con	50	50%
7	Inventariar capacidades actuales de detección de anomalías	Entrevistas técnicas y revisión	Semana 4	Inventario consolidado y graficado de	58	58%
8	Evaluar protocolos actuales de respuesta ante incidentes ADS-B	Revisión documental y	Semana 5	Matriz de evaluación de protocolos con brechas	95	95%
9	Aplicar encuestas tipo Delphi a personal clave	Diseño, aplicación digital y análisis	Semana 5	Resumen analítico y matriz de respuestas.	79	79%
10	Determinar brechas en la formación del talento humano	Cruce entre perfiles actuales y	Semana 6	Informe diagnóstico con plan de	97	97%
11	Analizar la existencia de canales seguros de coordinación institucional	Revisión de infraestructura de	Semana 6	Lista de canales seguros activos y mapa	17	17%
12	Elaborar matriz de riesgos basada en diagnóstico inicial	Cruce de hallazgos técnicos, humanos	Semana 7	Matriz de riesgos estructurada y	33	33%
13	Identificar posibles indicadores de desempeño (KPI)	Definición consensuada con	Semana 7	Listado de KPI priorizados con	34	34%
14	Diseñar plan de capacitación modular	Diseño curricular con enfoque por	Semana 8	Plan curricular completo aprobado.	10	10%
15	Definir contenidos básicos de formación en ciberseguridad ADS-B	Diseño de módulos temáticos con	Semana 8	Contenidos organizados en formato	1	1%
16	Seleccionar instructores o entidades capacitadoras	Convenios, contratación o	Semana 9	Listado con instructores	5	5%
17	Diseñar sesiones prácticas con SDR (HackRF / RTL-SDR)	Creación de guías y escenarios de	Semana 9	Documentación de sesiones prácticas	0	0%
18	Implementar plan piloto de capacitación inicial	Ejecución con grupo focal	Semana 10	Registro de asistencia, desempeño y encuesta	0	0%
19	Recopilar retroalimentación y ajustar plan de capacitación	Focus group, análisis y rediseño	Semana 11	Informe de retroalimentación y	0	0%
20	Emitir informe de cierre de la Fase I	Síntesis final con anexos técnicos y	Semana 12	Documento entregado, validado y archivado	0	0%

Fuente: Elaboración propia

Fase II - Integración tecnológica mínima viable (MVP)

Instalación de módulos de detección basados en IA entrenada con datos del sistema ADS-B y simulaciones previas. Debe incluir validadores de mensajes ADS-B con técnicas LSTM, verificación cruzada con radar secundario y MLAT, e integración con receptores SDR:

				Excelente	70 100	
				Regular	50 69	
				Malo	49 o menos	

No.	Paso	Cómo se realizará	Tiempo estimado	Medición del avance	Nota	Estado
1	Definir requerimientos técnicos funcionales del MVP	Sesión técnica con expertos en	Semana 1	Documento de requisitos firmado por	80	80%
2	Diseñar la arquitectura técnica del sistema de detección	Diseño de diagramas de flujo	Semana 2	Diagrama validado e integrado al documento	49	49%
3	Seleccionar los algoritmos de IA adecuados (LSTM / RNN)	Evaluación comparativa de	Semana 2	Informe técnico con modelo seleccionado y	80	80%
4	Recolectar y preparar datasets de entrenamiento	Extraer y limpiar datos ADS-B	Semana 3	Dataset estructurado y anotado con ataques	93	93%
5	Entrenar modelos LSTM con datos etiquetados	Uso de frameworks como TensorFlow	Semana 4	Modelo entrenado con log de métricas y	66	66%
6	Validar y evaluar el rendimiento de los modelos IA	Aplicar métricas de desempeño	Semana 4	Tabla de resultados comparativos y	50	50%
7	Desarrollar módulo de preprocesamiento de datos ADS-B	Codificación en Python para	Semana 5	Script funcional validado con múltiples	58	58%
8	Implementar motor de correlación de datos	Desarrollo de lógica de	Semana 5	Motor integrado y probado con datos	95	95%
9	Integrar receptores SDR (HackRF / RTL-SDR) al sistema	Configuración de drivers, dump1090	Semana 6	Captura exitosa de mensajes y	79	79%
10	Configurar bases de datos para registro de eventos	Implementación de base MySQL o	Semana 6	Base operativa con eventos registrados en	97	97%
11	Diseñar interfaz gráfica para visualización en tiempo real	Desarrollo de GUI con herramientas	Semana 7	GUI funcional conectada al backend	17	17%
12	Integrar fuentes externas de verificación (MLAT y radar	Conexión mediante APIs o	Semana 7	Pruebas exitosas de validación cruzada con	33	33%
13	Simular diferentes ataques en laboratorio con SDR	Uso de scripts de simulación de	Semana 8	Log de simulaciones ejecutadas y respuesta	34	34%
14	Ajustar el sistema con base en los resultados de las pruebas	Optimización de parámetros y	Semana 8	Sistema ajustado con reporte técnico de	10	10%
15	Probar la latencia del sistema y su capacidad en tiempo real	Benchmark de tiempo de	Semana 9	Informe de latencia validado por	1	1%
16	Establecer protocolos de alerta y respuesta dentro del MVP	Diseño de flujos y reglas de negocio	Semana 9	Documento de protocolos aprobado	5	5%
17	Ejecutar un piloto del MVP en una instalación real (ATC o torre de	Instalación supervisada y	Semana 10	Bitácora de funcionamiento piloto y	0	0%
18	Recopilar retroalimentación de los operadores	Encuestas estructuradas y	Semana 11	Matriz de retroalimentación	0	0%
19	Documentar todo el sistema y publicar en repositorio controlado	Redacción de manuales,	Semana 11	Repositorio actualizado y revisado	0	0%
20	Emitir informe técnico de evaluación del MVP	Elaboración de informe	Semana 12	Documento entregado y validado por comité	0	0%

Fuente: Elaboración propia

Fase III - Implementación del Centro de Gestión de Incidentes de Ciberseguridad Aeronáutica (CGICA): El CGICA se debe constituir como una célula operativa dentro del ATC con conectividad segura a CERT/CIRT, Fuerza Aérea y autoridades civiles. Este centro activa y coordina el procedimiento CARE ante eventos. Los canales redundantes y protocolos de escalamiento deben definirse con anticipación.

				Excelente	70 100	
				Regular	50 69	
				Malo	49 o menos	

No.	Paso	Cómo se realizará	Tiempo estimado	Medición del avance	Nota	Estado
1	Emitir acto administrativo de creación del CGICA	Redacción y aprobación por	Semana 1	Publicación oficial del acto administrativo.	80	80%
2	Diseñar la estructura organizacional del CGICA	Definición de organigrama y	Semana 2	Documento de estructura validado	49	49%
3	Definir los escenarios operacionales que activan el CGICA	Análisis de riesgos y definición de	Semana 2	Lista de escenarios de activación	80	80%
4	Establecer el protocolo de escalamiento de incidentes	Diseño de flujos jerárquicos de	Semana 3	Protocolo aprobado por mando conjunto	93	93%
5	Diseñar los flujos operativos internos del CGICA	Modelado BPMN o diagramas UML	Semana 3	Diagramas operativos validados y difundidos.	66	66%
6	Seleccionar la sede física o virtual del CGICA	Visitas técnicas, análisis de	Semana 4	Acta de selección de sede con justificación	50	50%
7	Asegurar conectividad con CERT, CIRT y FAC	Pruebas de conectividad	Semana 4	Informe de pruebas de enlace exitosas.	58	58%
8	Dotar al CGICA de infraestructura técnica básica	Adquisición, instalación y	Semana 5	Inventario instalado y checklist técnico	95	95%
9	Integrar el CGICA con el MVP desarrollado en la Fase II	Interconexión API y pruebas de alerta	Semana 5	Alertas recibidas correctamente y	79	79%
10	Implementar herramientas de gestión de incidentes (SIEM/CIRP)	Despliegue de plataforma SIEM y	Semana 6	Plataforma operativa con eventos	97	97%
11	Diseñar protocolo de emisión de "Cyber-NOTAM"	Diseño del formato, flujo y	Semana 6	Protocolo formalizado y piloto emitido.	17	17%
12	Definir procedimientos de coordinación con la FAC	Acuerdo interinstitucional	Semana 7	Procedimientos firmados y personal	33	33%
13	Formar al personal del CGICA	Capacitación técnica, jurídica y	Semana 7	Certificados de formación emitidos y	34	34%
14	Diseñar bitácora digital forense estandarizada	Creación de plantilla digital	Semana 8	Bitácora implementada en el sistema del	10	10%
15	Desarrollar panel de control e interfaz de operación del CGICA	Desarrollo o integración de	Semana 8	Panel funcional accesible al equipo	1	1%
16	Simular escenarios de activación del CGICA	Ejercicios con ATC, FAC y UAEAC	Semana 9	Informe de simulacro con hallazgos y	5	5%
17	Evaluar interoperabilidad legal e institucional	Análisis normativo y entrevistas con	Semana 9	Informe jurídico-operativo con	0	0%
18	Generar documentación y manuales operativos	Redacción colaborativa y	Semana 10	Manuales publicados y entregados al personal.	0	0%
19	Establecer indicadores de desempeño del CGICA	Definición de KPI con base en	Semana 10	Lista de indicadores con línea base inicial.	0	0%
20	Iniciar operaciones en fase de alistamiento (Soft Launch)	Activación con monitoreo 24/7 y	Semana 11-12	Bitácora operativa y acta de transición a	0	0%

Fuente: Elaboración propia

Fase IV - Evaluación y mejora continua: mediante métricas como el tiempo de detección de anomalías, reducción de falsos positivos, participación en simulacros y retroalimentación operativa, se evalúa el desempeño del procedimiento. La retroalimentación se emplea para reentrenar modelos y ajustar reglas de decisión en Mental Modeler:

				Excelente	70 100	
				Regular	50 69	
				Malo	49 o menos	
No.	**Paso**	**Cómo se realizará**	**Tiempo estimado**	**Medición del avance**	**Nota**	**Estado**
1	Establecer un comité técnico de evaluación continua	Designación formal de	Semana 1	Acta de conformación del comité y	80	80%
2	Definir métricas clave de desempeño (KPI)	Sesión técnica con expertos para	Semana 2	Listado de KPIs aprobados y	49	49%
3	Diseñar una bitácora estandarizada de incidentes	Diseño digital con campos	Semana 2	Formato implementado en sistema CGICA.	80	80%
4	Monitorear el desempeño del modelo IA en tiempo real	Registro y análisis mensual de	Mensual	Dashboard de rendimiento	93	93%
5	Recolectar datos operativos del CGICA en cada activación	Automatización del registro en la	Continuo	Histórico de incidentes con trazabilidad	66	66%
6	Ejecutar simulacros trimestrales de incidentes ADS-B	Diseño y ejecución de ejercicios con	Cada 3 meses	Informes post-simulacro y actas de	50	50%
7	Aplicar encuestas de retroalimentación a operadores y	Encuestas digitales anónimas	Trimestral	Tasa de participación y análisis de	58	58%
8	Analizar causas raíz de incidentes mal gestionados	Uso de diagramas de Ishikawa y	Tras cada incidente	Informe técnico con acciones correctivas	95	95%
9	Ajustar hiperparámetros del modelo LSTM	Reentrenamiento mensual con	Mensual	Registro de versiones y mejoras de desempeño.	79	79%
10	Actualizar las reglas de inferencia del FCM en Mental Modeler	Revisión semestral de pesos y	Cada 6 meses	Archivo actualizado con validación experta.	97	97%
11	Validar si las variables críticas del FCM siguen siendo relevantes	Evaluación participativa entre	Cada 6 meses	Matriz de validación con ajustes	17	17%
12	Desarrollar versión 2.0 del procedimiento C.A.R.E.	Incorporar mejoras	Anual	Procedimiento actualizado con	33	33%
13	Establecer un sistema automatizado de reportes mensuales	Configuración de scripts o	Mensual	Informe mensual enviado y archivado	34	34%
14	Crear un repositorio institucional de aprendizaje continuo	Uso de plataforma GitLab o interna	Semana 4	Repositorio activo con actualizaciones	10	10%
15	Actualizar los manuales operativos y guías de usuario	Revisión semestral con	Cada 6 meses	Versión actualizada con control de	1	1%
16	Incluir a la academia y centros de investigación en la mejora del	Firma de convenios y	Trimestral	Número de proyectos y papers en conjunto.	5	5%
17	Realizar auditorías externas de ciberseguridad anualizadas	Contratación o asignación de	Anual	Informe de auditoría con plan de acción	0	0%
18	Ampliar el modelo a otros sistemas aeronáuticos (ej. radar primario,	Estudio técnico y plan piloto de	Anual	Informe de viabilidad y hoja de ruta.	0	0%
19	Difundir resultados a nivel nacional e internacional	Publicaciones, ponencias,	Semestral	Número de publicaciones y	0	0%
20	Planificar una reestructuración mayor cada 2 años	Evaluación estratégica del	Cada 2 años	Documento estratégico de actualización	0	0%

Fuente: Elaboración propia

Las cuatro fases del procedimiento C.A.R.E. enfrentan desafíos estructurales y operativos que deben ser gestionados estratégicamente para lograr su implementación

exitosa. Entre los principales retos se encuentra la interoperabilidad limitada entre plataformas ATC heredadas y tecnologías emergentes, lo cual puede dificultar la integración fluida de los módulos IA, validadores de mensajes y sistemas de alerta del MVP.

Además, existe una resistencia institucional al cambio, especialmente en entornos donde los protocolos operativos tradicionales han prevalecido por décadas. A esto se suma la escasez de personal capacitado en ciberseguridad aeronáutica, lo cual impacta directamente la sostenibilidad del CGICA y la correcta aplicación del modelo híbrido FAST-FCM. Por tanto, el avance dependerá de una gestión efectiva del cambio, inversión en formación y una arquitectura abierta que permita integración progresiva.

En cuanto a los requisitos de recursos, se requiere una combinación de talento humano altamente especializado (ingenieros, ATC, modeladores cognitivos, oficiales FAC), infraestructura tecnológica (receptores SDR, servidores, SIEM, enlaces seguros), y respaldo normativo institucional. Para medir la efectividad del procedimiento, se deben aplicar métricas de éxito como: tiempo promedio de detección de anomalías, tasa de falsos positivos/negativos, tiempo de respuesta ante ciberincidentes, cobertura de simulacros, número de actualizaciones del procedimiento CARE y reentrenamientos IA exitosos. Estas métricas permiten evaluar la madurez técnica y operativa del sistema, así como su capacidad de adaptación frente a amenazas emergentes, brindando una guía práctica y continua para su mejora.

2. Costo-Beneficio de la Implementación del Procedimiento C.A.R.E. y Modelo Híbrido

A pesar de que la inversión inicial puede ser considerable, se plantea el siguiente análisis cualitativo de costo-beneficio:

Elemento	Costos Asociados	Beneficios Esperados
Implementación de autenticación	Software especializado, validadores LSTM, sensores redundantes	Prevención de spoofing, suplantación e inyección de mensajes.
Entrenamiento del personal	Cursos técnicos, simulacros, tiempo de inactividad	Mejora de la conciencia situacional y respuesta oportuna ante anomalías.
CGICA y red de comunicación	Infraestructura física y digital segura	Coordinación efectiva y respuesta integral ante ciberincidentes.
Simuladores y sensores redundantes	Adquisición de MLAT, PSR, sensores GNSS	Validación cruzada y reducción de falsos positivos y negativos.
Uso de Mental Modeler y FCM	Tiempo de modelado, entrenamiento de expertos	Capacidad predictiva ante ciberamenazas complejas e interacciones múltiples.

Fuente: Elaboración propia

Relación costo-beneficio estimada:

- Los costos estimados de implementación oscilan entre 250.000 y 800.000 USD, según el nivel de cobertura e integración deseada. Sin embargo, estos costos no son significativos si se tiene en cuenta el fortalecimiento en materia de Seguridad Operacional el prevenir accidentes aéreos y salvar vidas.
- Las pérdidas potenciales por un solo incidente grave (como spoofing no detectado en espacio aéreo controlado) pueden superar los 3 millones USD en daños, interrupciones y responsabilidad legal.

Incluso desde un enfoque cualitativo, los beneficios operacionales, reputacionales y de seguridad superan ampliamente los costos iniciales, justificando la implementación progresiva del procedimiento y modelo.

3. Limitaciones del Estudio y Líneas Futuras de Investigación

Limitaciones:

- Las pruebas de simulación de ataques como el **Message Injection** se realizaron en escenarios controlados, por lo que no representan toda la complejidad de un entorno aeronáutico real.
- La implementación del modelo FCM mediante Mental Modeler aún no ha sido desplegada operacionalmente en el entorno ATC nacional.
- La herramienta de IA para validación dinámica aún se encuentra en una etapa de madurez técnica media (modelos LSTM sin entrenamiento masivo en datos reales de tráfico aéreo).
- No se exploraron a profundidad ataques de cadena de suministro ni vulnerabilidades en redes de comunicación satelital.

Líneas de investigación futuras:

A. **Desarrollo de sensores virtuales con IA** que puedan estimar trayectorias plausibles ante pérdida de señal, aplicando redes neuronales recurrentes (RNN) en combinación con GPS multi-constelación.
B. **Simulación de ataques combinados (spoofing + jamming)** en tiempo real mediante escenarios controlados en centros ATC universitarios.
C. **Exploración del uso de blockchain** para la autenticación de transmisiones aeronáuticas y trazabilidad de registros ADS-B.
D. **Estudios comparativos de resiliencia operativa** en escenarios con y sin implementación del protocolo CARE, mediante juegos de guerra cibernéticos (cyber wargaming).

E. **Desarrollo de una normativa nacional** para respuesta ante ciberincidentes en vigilancia aérea, integrando el procedimiento CARE como estándar.