Ciberseguridad Satelital: Machine Learning para preservar integridad de señales GPS en aeronaves de la FAC

Mayor (FAC) Sergio Baudin Cruz

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) Sergio Baudin Cruz
Identificación	**:**	1030531767
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Dr. Jairo Andrés Becerra Ortiz
Tutor temático	**:**	Dr. Giovanni Gómez Rodríguez
Fecha de entrega	**:**	15 de julio de 2025
Extensión	**:**	9294 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.

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

Ciberseguridad Satelital: Machine Learning para preservar integridad de señales GPS en aeronaves de la FAC

Satellite Cybersecurity: Machine Learning to preserve GPS integrity signals of Colombian Air Space Force aircrafts

Sergio Baudin Cruz[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: el estudio aborda temas de ciberseguridad satelital en el uso del GPS por parte de la Fuerza Aeroespacial Colombiana, enfocándose en el segmento de usuario del sistema satelital, mediante la aplicación de metodologías observacional y experimental para identificar vulnerabilidades, amenazas y posibles ataques, destacándose el *spoofing* como un ataque crítico a la integridad de los datos GPS.

Como respuesta, se diseñó un modelo de aprendizaje automático basado en Random Forest, entrenado con datos reales y simulados, que permite detectar señales anómalas en tiempo real a bordo de aeronaves. El modelo fue implementado en una Raspberry Pi, validado en simulaciones y pruebas de campo, con la finalidad de mejorar la resiliencia y seguridad operacional frente a ciberataques al sistema satelital GPS.

[1] Mayor de la Fuerza Aeroespacial Colombiana. Candidato a magíster en ciberseguridad y ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Ingeniero Informático, Escuela Militar de Aviación y Magister en Seguridad de la Información, Universidad de los Andes, Colombia. https://orcid.org/0009-0005-6931-1063 - Contacto: sergio.cruz@esdeg.edu.co.

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

Palabras clave: Ciberseguridad satelital, GPS, Machine Learning, Navigation Warfare, *Spoofing*, SPARTA

Abstract: The target of this study is satellite cybersecurity in the GPS uses by the Colombian Aerospace Force, focusing on the user segment of the satellite system. It applies observational and experimental methodologies to identify vulnerabilities, threats, and potential attacks, highlighting *spoofing* as a critical threat to the integrity of GPS data.

As a response, a machine learning model based on Random Forest was designed, trained with real and simulated data, enabling real-time detection of anomalous signals aboard aircraft. The model was implemented on a Raspberry Pi, validated through simulations and field tests, with the aim of enhancing resilience and operational safety against cyberattacks targeting the Global Positioning System.

Keywords: Satellite Cybersecurity, GPS, Machine Learning, Navigation Warfare, *Spoofing*, SPARTA.

Introducción

En la era digital actual, la creciente dependencia de tecnologías basadas en infraestructura satelital ha incrementado la necesidad de proteger estos sistemas, un ejemplo de dichas infraestructuras es el Sistema Global de Navegación por Satélite (GNSS), compuesto principalmente por las constelaciones Global Positioning System (GPS) de Estados Unidos, GLONASS de Rusia, Galileo de la Unión Europea, BeiDou de China, Quasi-Zenith Satellite System (QZSS) de Japón y Navigation with Indian Constellation (NavIC/IRNSS) de India. Las frecuencias de operación pueden observarse en la figura 1 (Kaplan & Hegarty, 2017, p. 2).

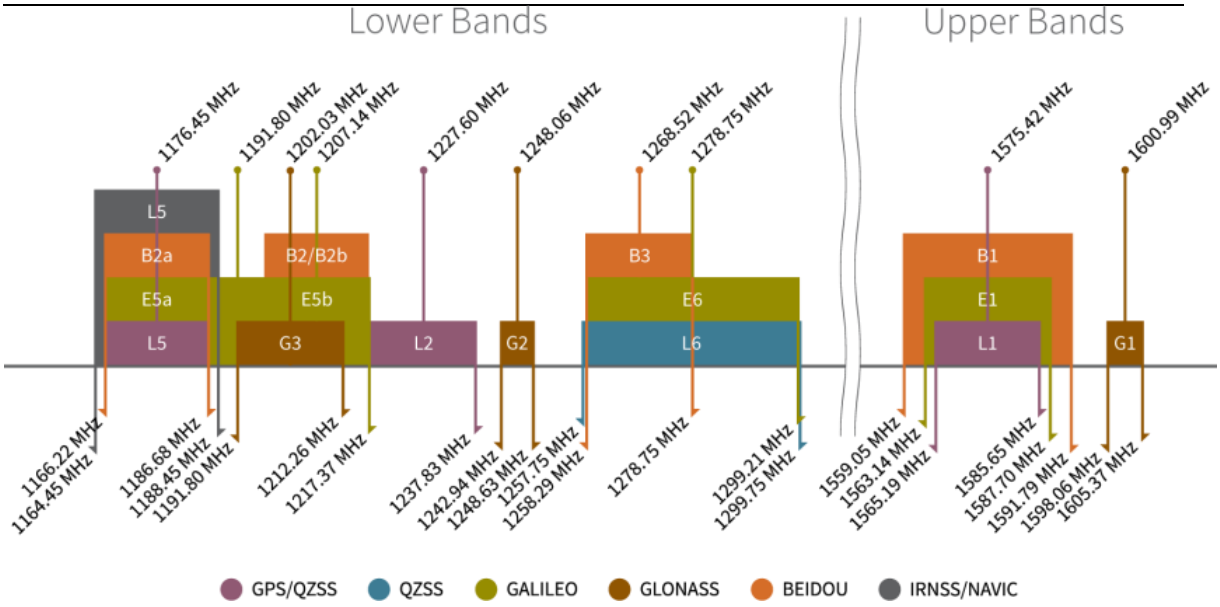
El papel fundamental del GNSS es proporcionar a los usuarios la capacidad de determinar su posición, mediante la recepción y el procesamiento de datos satelitales, lo que permite establecer su localización, navegación y el tiempo (PNT) (Bernhard Hofmann-Wellenhof et al., 2008, p. 3).

En el presente caso de estudio se analiza el GPS, el cual se ha consolidado como una herramienta esencial para el desarrollo de operaciones aéreas en la Fuerza Aeroespacial Colombiana (FAC), no obstante, cada uno de los segmentos que componen este sistema presenta desafíos relevantes que deben abordarse. Por esta razón, se plantea esta investigación desde el enfoque de la ciberseguridad, considerando el conjunto de medidas, estrategias y prácticas diseñadas para salvaguardar la integridad de los datos satelitales del GPS (Wright, 2023, p. 1).

A partir de este punto, se desarrollará una investigación que tenga en cuenta las particularidades del hardware, el software y las formas de operación de los tres segmentos

del sistema satelital propuestos por Ear et al. (2023, p. 5): el espacial, el terrestre y el de usuario.

Figura 1 Uso de frecuencias de cada constelación GNSS

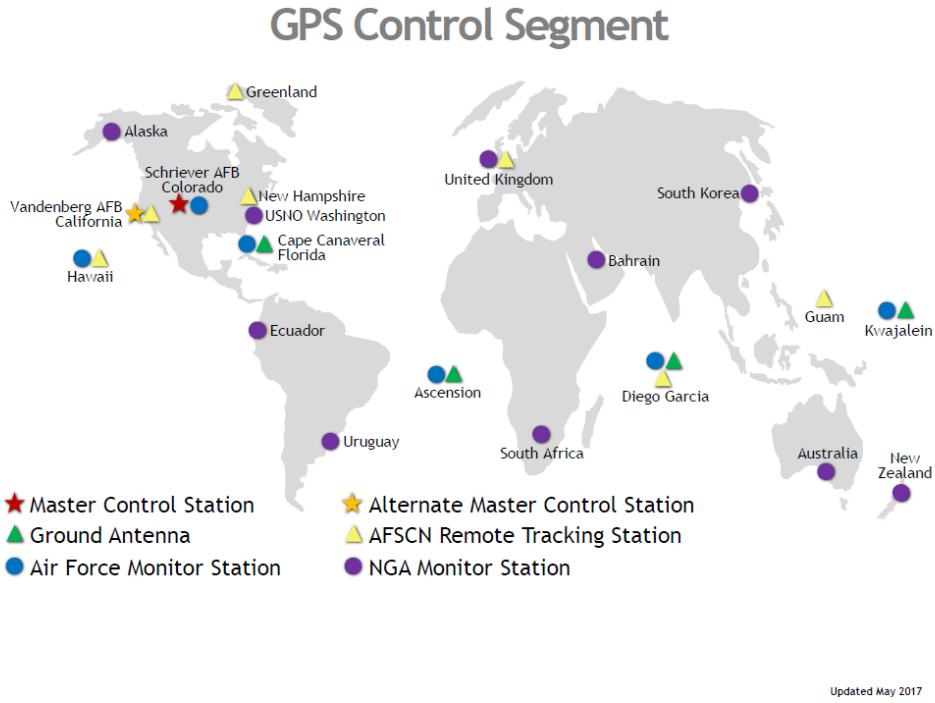


Fuente: imagen tomada de (Calian Group, 2025).

La presente investigación se enfoca en el sistema de usuario, teniendo en cuenta que Colombia no tiene control directo sobre los satélites de esta constelación y, dentro del segmento de control, no hay estaciones en territorio nacional, como se puede observar en la figura 2. Sin embargo, de acuerdo con lo propuesto por Bailey (2021, p. 17), se explorarán las vulnerabilidades –debilidades inherentes al diseño, implementación, operación o gestión del sistema satelital–, amenazas –circunstancia, evento o actor con el potencial de causar daño al sistema satelital, aprovechando las vulnerabilidades–, riesgos –valoración del evento potencial en el sistema satelital, de la explotación de una vulnerabilidad por una amenaza– y los ataques en los que se puede ver inmerso el sistema –acto intencional en el que un actor

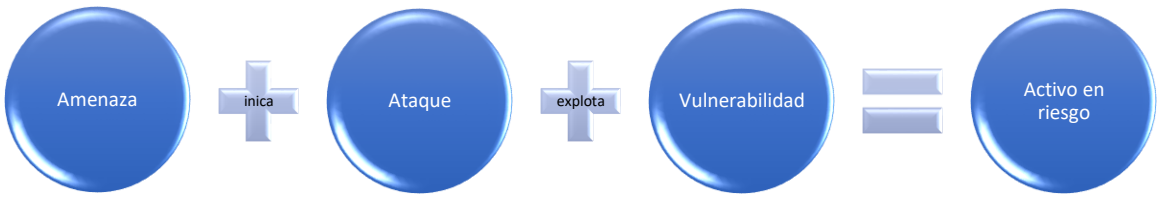
evade la seguridad del sistema satelital con la finalidad de causar daño–. Esta relación se puede ver en la figura 3.

Figura 2 Estaciones del segmento de control GPS a nivel mundial



Fuente: imagen tomada de (Garcia, 2017).

Figura 3 Relación entre amenaza, ataque, vulnerabilidad y riesgo en ciberdefensa



Fuente: elaboración propia adaptado de la relación entre términos de Bailey (2021, p. 18).

Teniendo en cuenta la anterior relación, se pueden observar amenazas y ataques provenientes de varios dominios, entendiendo el ciberespacio y el espectro electromagnético como espacios donde confluyen los segmentos de control y de usuario con el segmento

espacial. Se entiende por espectro electromagnético el espacio intangible donde confluye la información del sistema espacial y la guerra electrónica como una acción militar dirigida para controlar el espectro electromagnético (Wade, 2019). Pese a esta confluencia con la guerra electrónica, el alcance del presente trabajo se limita a las acciones en ciberseguridad para proteger la integridad de los datos GPS.

Una aproximación de protección y entendimiento del sistema se puede encontrar mediante la aplicación del framework SPARTA, el cual brinda una visión completa (desde la visión estadounidense) del sistema espacial con las tácticas y técnicas desde el punto de vista cibernético, y cómo se pueden aplicar medidas de protección en profundidad a estos sistemas espaciales (Aerospace Corporation, 2022b), logrando llegar a una alternativa de diseño para la protección mediante el monitoreo de datos GPS usando inteligencia artificial. Se finaliza con el diseño de un modelo de machine learning (ML), ajustado a las necesidades de operación de las aeronaves de la FAC. Posterior al entrenamiento con datos legítimos de vuelos de aeronaves de la FAC, se usará el modelo resultante para recibir señales GPS y mostrar si la señal es legítima o de *spoofing*.

Metodología

Con la finalidad de enfocar la investigación del presente trabajo en el campo de ciberseguridad, se exploró lo propuesto por Thomas W. Edgar y David O. Manz, quienes, mediante métodos científicos, pudieron conducir investigaciones en ciberseguridad. De acuerdo con el ajuste de la investigación propuesta, se tomaron dos métodos principales.

El primero es la investigación observacional, considerada para obtener conocimiento y comprender un sistema cibernético real, adaptada para dar respuesta a preguntas de investigación abiertas, mediante un proceso de recopilación de información, análisis y reporte (Edgar & Manz, 2017, pp. 100–108). El segundo método de investigación explorado es el experimental, que busca entender el comportamiento de un sistema mediante un proceso controlado. La categoría a explorar en este tipo de investigación es la cuasiexperimental; este tipo de investigación se utiliza cuando se desea probar una hipótesis en un entorno de laboratorio, pero todas las variables del entorno no son controlables, y se tendrá en cuenta el diseño de cohorte, donde se cuenta con un grupo de datos que se pueden controlar y otro grupo que el investigador no puede controlar (Edgar & Manz, 2017, pp. 251–264).

De acuerdo con la descripción de la investigación observacional y experimental y teniendo en cuenta la **pregunta de investigación: ¿Cómo diseñar un modelo de machine learning (ML) que permita verificar la integridad de los datos recibidos en la banda L de sistemas GNSS que utilicen las aeronaves de la Fuerza Aeroespacial Colombiana (FAC), con el fin de mitigar las principales ciberamenazas a sus activos espaciales y garantizar la continuidad de las operaciones militares?**, se estructuró el presente trabajo. En primer lugar, se realizó un estudio exploratorio de literatura enfocada al funcionamiento de sistemas satelitales, amenazas, vulnerabilidades y riesgos cibernéticos asociados a estos sistemas, para moldear la respuesta de la pregunta de investigación, verificando cuáles son los principales fallos en ciberseguridad en sistemas espaciales, y finalmente llegar a la aplicación de machine learning (ML). En segundo lugar, se realizaron pruebas de laboratorio, con la finalidad de diseñar y probar un modelo de ML en condiciones cercanas a la operación

real del sistema y descartando las variables externas del entorno real (teniendo en cuenta que no se pueden controlar variables como clima, ruido, radiación solar, polución, entre otros), llegando de esta forma a la respuesta de la pregunta de investigación.

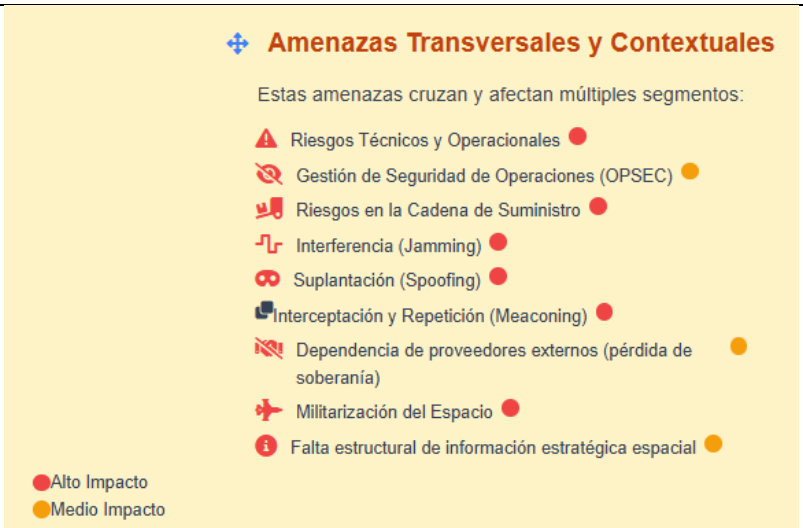
Amenazas invisibles: vulnerabilidades y ciber-riesgos en la Infraestructura Satelital

Cada segmento del GPS representa retos importantes en ciberseguridad, con puntos vulnerables que podrían llevar a la materialización de un ataque contra la integridad, disponibilidad o confidencialidad de la información que maneja el sistema satelital. Por tal razón, es necesario realizar una segmentación de las vulnerabilidades que pueden encontrarse en el sistema y, con la finalidad de seguir el enfoque que tiene esta investigación, se describirán solamente vulnerabilidades conocidas en los segmentos terrestres y de usuario.

Las vulnerabilidades en estos segmentos pueden tener consecuencias graves y de gran alcance, afectando no solo a los operadores y usuarios directos de los servicios satelitales, sino también a sectores críticos que dependen de ellos (Hamill-Stewart & Rashid, 2024, p. 1).

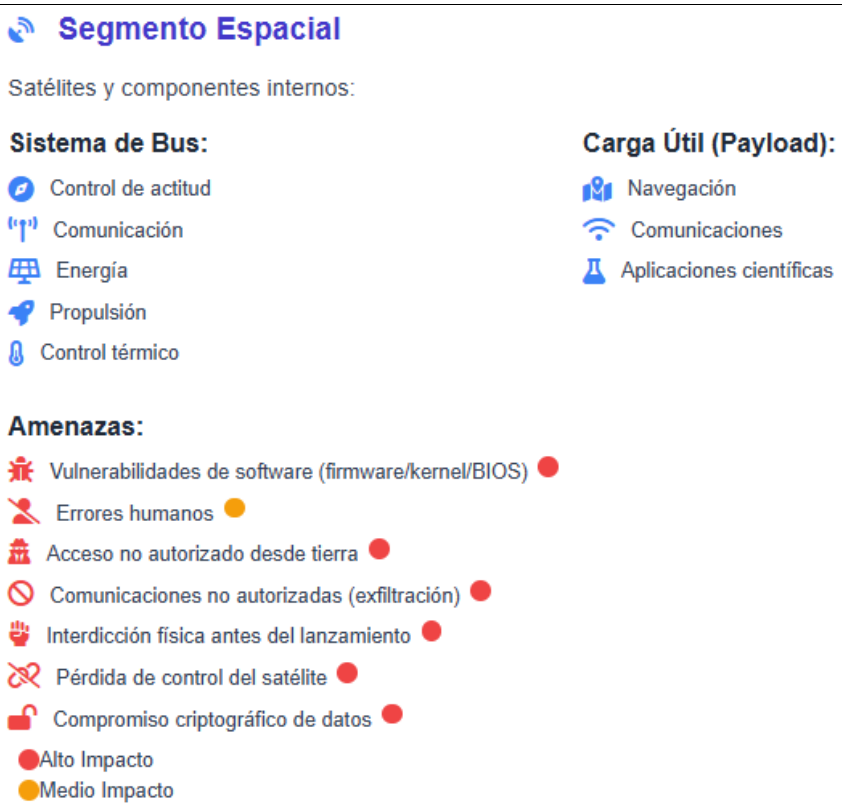
Se puede observar en las figuras 4 a 8 las amenazas más comunes asociadas a los segmentos del sistema espacial.

Figura 4 Amenazas trasversales a todo el sistema espacial



Fuente: elaboración propia construida con conceptos de amenazas de (Tang, 2021), (Kavallieratos & Katsikas, 2023), (Ear et al., 2023), (Wade, 2019), (Scholl & Suloway, 2023), (Hamill-Stewart & Rashid, 2024).

Figura 5 Amenazas del segmento espacial

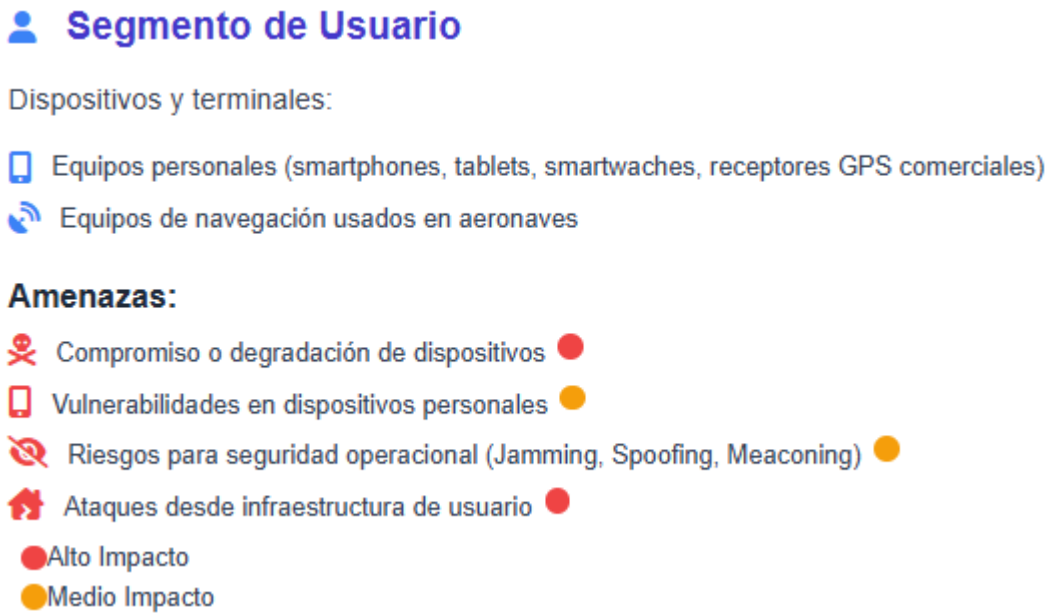


Fuente: elaboración propia construida con conceptos de amenazas de (Tang, 2021), (Kavallieratos & Katsikas, 2023), (Ear et al., 2023), (Wade, 2019), (Scholl & Suloway, 2023), (Hamill-Stewart & Rashid, 2024).

Figura 6 Amenazas del segmento de control

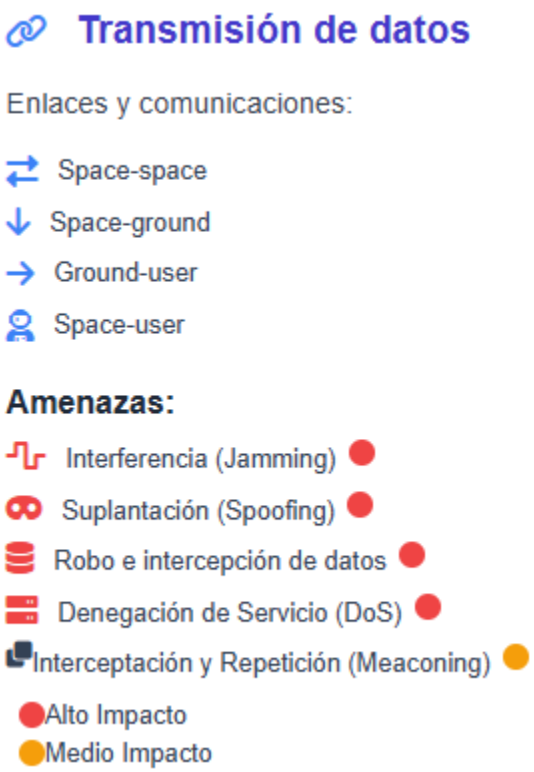
Fuente: elaboración propia construida con conceptos de amenazas de (Tang, 2021), (Kavallieratos & Katsikas, 2023), (Ear et al., 2023), (Wade, 2019), (Scholl & Suloway, 2023), (Hamill-Stewart & Rashid, 2024)

Figura 7 Amenazas del segmento de usuario



Fuente: Figura construida con conceptos de amenazas de (Tang, 2021), (Kavallieratos & Katsikas, 2023), (Ear et al., 2023), (Wade, 2019), (Scholl & Suloway, 2023), (Hamill-Stewart & Rashid, 2024), (Periyasami et al., 2024)

Figura 8 Amenazas en la transmisión de datos



Fuente: elaboración propia construida con conceptos de amenazas de (Tang, 2021), (Kavallieratos & Katsikas, 2023), (Ear et al., 2023), (Wade, 2019), (Scholl & Suloway, 2023), (Hamill-Stewart & Rashid, 2024), (Periyasami et al., 2024)

Puntos críticos en el sistema satelital: vulnerabilidades conocidas en hardware, software y transmisión

A continuación, se profundizará en las vulnerabilidades específicas relacionadas con el hardware, el software y la transmisión en los sistemas satelitales.

Vulnerabilidades en hardware

Los componentes físicos, como microchips, antenas, controladoras y otros elementos electrónicos que componen los segmentos terrestres y de usuario, son susceptibles a una variedad de amenazas y fallos que pueden comprometer su funcionamiento. Aunque no

representan grandes retos como los componentes de hardware del segmento satelital, existen situaciones de relevancia para la ciberseguridad. La vulnerabilidad común de estos equipos es el acceso físico por personas no autorizadas (Johanna Niecknig et al., 2023, p. 27).

Por otra parte, estas vulnerabilidades pueden ser tanto inherentes al diseño y fabricación como inducidas intencionalmente. A continuación, se presentan algunas de las más conocidas:

- **Manipulación y fallos intencionados:** existe la posibilidad de que los componentes sean manipulados durante la fabricación o el ensamblaje para incluir funcionalidades ocultas o puntos débiles que puedan ser explotados posteriormente (Joshi et al., 2022, p. 68). Esta manipulación podría afectar la confidencialidad al extraer información sensible, como claves de cifrado o credenciales de autenticación; la integridad, al alterar la información contenida; o la disponibilidad, al causar fallos en componentes esenciales.
- **Vulnerabilidades en las estaciones terrestres:** las estaciones terrestres son puntos críticos para el control y la comunicación con los satélites. Teniendo en cuenta su distribución en diferentes ubicaciones a nivel global, también presentan vulnerabilidades, ya que es posible tener acceso físico no autorizado a estas instalaciones, lo que podría permitir la manipulación directa de los equipos, la inserción de dispositivos maliciosos o la interrupción de las comunicaciones (Hamill-Stewart & Rashid, 2024, p. 2).
- **Falta de mecanismos de autenticación:** los receptores son vulnerables a ataques de suplantación, debido a la falta de autenticación en las señales que

> reciben de los satélites. Siempre que reciban señales dentro del rango de frecuencias establecido, es posible suplantar las señales emitidas por los satélites legítimos. Las consecuencias pueden ser graves en aplicaciones críticas como la navegación aérea y marítima, los sistemas de sincronización de tiempo y las operaciones militares (Hamill-Stewart & Rashid, 2024, p. 1).

Vulnerabilidades en software

El software es un componente crítico en los segmentos de control y de usuario, y presenta una amplia superficie de ataque para los atacantes. Estas vulnerabilidades pueden ser explotadas para comprometer la confidencialidad, integridad y disponibilidad del sistema espacial. Algunas de las vulnerabilidades en software pueden ser las siguientes:

- **Actualizaciones inseguras:** el proceso de actualización de software en los sistemas de control terrestres puede introducir vulnerabilidades si no se gestiona y autentica de forma segura, permitiendo a un atacante insertar software malicioso, haciéndolo pasar por una actualización legítima (Adamczyk, 2024).
- **Inyección de malware:** las estaciones, al estar conectadas a redes terrestres y potencialmente a internet, son vulnerables a la inyección de malware, que puede ingresar al sistema por diferentes vectores. Una vez dentro, podría realizar una variedad de acciones, como robar datos confidenciales, interrumpir las operaciones de control o proporcionar puertas de acceso traseras a sistemas críticos (Hamill-Stewart, 2024).

- **Vulnerabilidades de software de terceros:** los receptores GPS se integran con otras aplicaciones de terceros para proporcionar funcionalidades específicas. Las vulnerabilidades de estas aplicaciones podrían ser aprovechadas para comprometer la seguridad del receptor GPS o los datos de posición, navegación o tiempo (PNT) que maneja. Por ejemplo, una aplicación de mapas con una vulnerabilidad de seguridad podría ser utilizada como punto de entrada para acceder al sistema del receptor y alterar la información de ubicación (Adamczyk, 2024).

Vulnerabilidades en transmisión

La transmisión de datos desde el segmento satelital al segmento de control y de usuario se convierte en uno de los mayores retos de seguridad para mantener la integridad y confidencialidad de los datos, teniendo en cuenta que el vector de ataque es muy extenso y no se puede controlar de forma eficiente. A continuación, se presentan algunas amenazas, asociadas a vulnerabilidades comunes en la transmisión de datos:

- **Autenticación débil:** la falta de autenticación robusta en los terminales ubicados en las estaciones terrestres puede aumentar los riesgos asociados con los enlaces de comunicación inseguros. En caso de que un atacante logre acceder a un terminal, podría potencialmente interceptar o manipular las comunicaciones con el satélite, incluso si están parcialmente cifradas. La combinación de enlaces no cifrados y una autenticación deficiente crea una superficie de ataque significativa. Por consiguiente, la protección del

segmento de control y de usuario requiere un enfoque integral que aborde tanto el cifrado de las comunicaciones como la seguridad física y lógica de las estaciones terrestres y sus terminales (Kavallieratos & Katsikas, 2023, p. 5).

- **Jamming:** los receptores de señales satelitales son susceptibles a interferencias intencionales. El jamming se produce cuando una fuente externa emite señales de radiofrecuencia en la misma banda que las señales del satélite, con suficiente potencia para saturar el receptor (Wade, 2019, p. 3.2), causando una denegación de servicio (DoS) para el usuario. Esto sería crítico para los sistemas de navegación satelital, donde la precisión y la disponibilidad de la señal deben ser constantes. Estos ataques pueden ser llevados a cabo por diversos actores, incluso individuos con equipos relativamente sencillos (Kavallieratos & Katsikas, 2023, p. 8).
- ***Spoofing*:** la suplantación de señales satelitales implica la transmisión de señales falsificadas que imitan las señales genuinas del satélite, con la intención de engañar al receptor para que calcule el PNT incorrectamente. Un ataque exitoso podría tener consecuencias significativas, especialmente en aplicaciones críticas como la navegación aérea, donde la información de posicionamiento errónea podría llevar a accidentes o a la toma de decisiones equivocadas. La evolución de estos ataques ha aumentado con la disponibilidad de suplantaciones definidas por software, que permiten generar señales falsas, complejas y convincentes (Kavallieratos & Katsikas, 2023, pp. 4–5)

Consecuencias críticas: ciber-riesgos asociados a la integridad de datos satelitales

La integridad de los datos satelitales es fundamental para la correcta operación de los segmentos de control y de usuario, en especial para aplicaciones que dependen de la precisión de dichos datos. Las vulnerabilidades descritas anteriormente comprometen la integridad de los datos recibidos y pueden tener consecuencias graves, afectando diferentes campos que utilizan receptores GPS para su funcionamiento (Bailey, 2021, pp. 2–3; Oakley, 2020, p. 78).

El *spoofing* se puede considerar como la amenaza más crítica a la integridad de los datos de navegación. Un ataque de suplantación exitoso podría desviar aeronaves de su curso, causar colisiones marítimas o terrestres y afectar la sincronización que proporcionan los GNSS a infraestructuras críticas como las redes de energía y comunicaciones digitales (Poirier, 2024).

Vectores de ataque en la constelación GPS: ciberamenazas del sistema

Partiendo de las vulnerabilidades en los dos segmentos de interés y las consecuencias críticas, se tiene una aproximación a algunos vectores de ataque, entendiendo en forma preliminar la materialización de un ciberataque desde la Cyber Kill Chain propuesta por Geetha et. al. (2024b, pp. 83–88).

Segmento terrestre

Su importancia como vector de ataque radica en el acceso directo a los sistemas de control satelital y en la interconexión con toda la infraestructura. Una característica fundamental es que incorpora tecnologías de la información y operación (Periyasami et al., 2024, p. 25).

Marcos de análisis de ciberamenazas como MITRE ATT&CK brindan herramientas valiosas para identificar vulnerabilidades y caracterizar las técnicas, tácticas y procedimientos (TTPs) empleados contra los sistemas terrestres. Estos marcos de referencia muestran cómo las ciberamenazas dedican esfuerzos a observar, recolectar datos y comprender los sistemas, para la obtención de acceso inicial mediante ataques (Hamill-Stewart, 2024).

Segmento de usuario

De acuerdo con las vulnerabilidades del sistema, se busca entender los fallos en la integridad del PNT causados por una ciberamenaza, la cual podría implementar *spoofers* (suplantadores de identidad o señal) definidos por software, capaces de generar una señal falsa similar a la genuina, pero con información diferente, aumentando gradualmente su potencia hasta que el receptor la siga. La construcción de estos sistemas definidos por radio (SDR) oscila entre 1000 y 2000 USD para sistemas como el demostrado por el profesor Todd Humphreys (Periyasami et al., 2024, pp. 47–48).

De igual forma, se puede encontrar un ataque como el meaconing, vector de ataque común para las señales GPS militares cifradas, el cual consiste en capturar la trama completa de señal GPS emitida de forma legítima por el satélite y retransmitirla con un leve retardo en el tiempo, sin ser necesario descifrar la señal. Esta réplica con retardo puede engañar a sistemas de piloto automático dependientes del GPS, cambiando su trayectoria de vuelo (Periyasami et al., 2024, pp. 34–35).).

Actores y ataques materializados relevantes

La capacidad de ejecutar ciberataques contra sistemas espaciales como el GPS varía entre diferentes actores, desde individuos con habilidades básicas (script kiddies) hasta actores tipo Estado-Nación o grupos de hackers con capacidades y recursos sofisticados (ver tabla 2), sin descartar a los insiders, que representan una vulnerabilidad clara para la infraestructura GPS. Teniendo en cuenta lo anterior, se han materializado ataques que muestran la naturaleza e impacto de las amenazas a estos segmentos (ver tabla 1).

Tabla 1. Ataques relevantes efectuados al sistema GPS

Año	Actor	Sistema afectado	Ataque efectuado	Fuente
2000	Agencia de Seguridad Francesa	Señales de navegación GPS en tanques militares británicos y estadounidenses	*Jamming*	(Fritz, 2013, p. 15)
1998-2008	Corea del Norte	Posicionamiento GPS de 553 aeronaves	*Jamming*	(Ear et al., 2023, p. 8)
2011	Irán	Secuestro de UAV estadounidense RQ-170, con señales de control satelital	*Jamming* y *spoofing*	(Tang, 2021, p. 6)
2017	Rusia	Sistemas de navegación marítima de embarcaciones en el Mar Negro con posición errónea	*Spoofing*	(Periyasami et al., 2024, pp. 47–48)
2024	Rusia	Posicionamiento GPS de misiles, con *spoofers* en torres de antenas celulares	*Jamming* y *spoofing*	(Periyasami et al., 2024, p. 47)
2024	No determinado	Señales de navegación GPS en aeronave de la FAC con desfase de 128 NM	*Spoofing*	Autor

Fuente: elaboración propia con base en las fuentes citadas

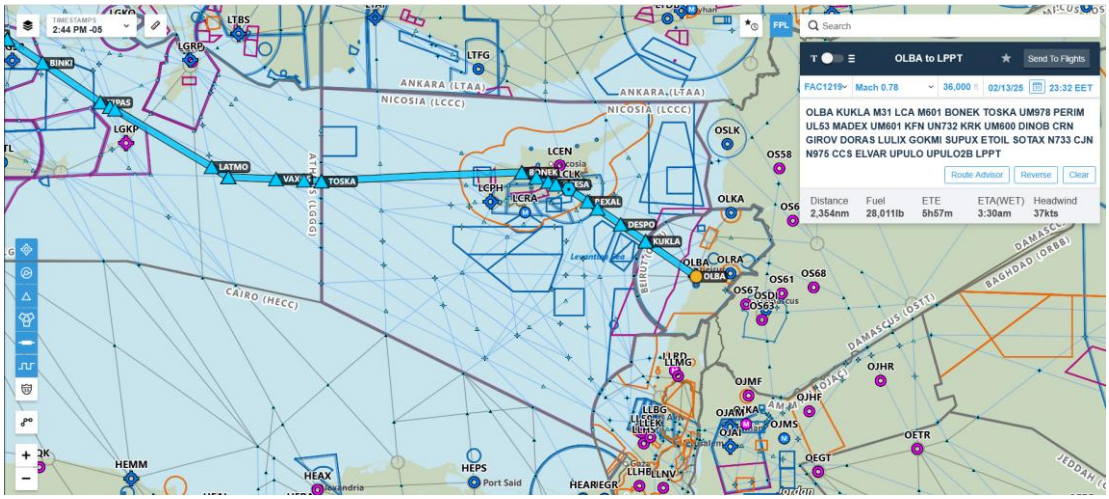
Tabla 2. Actores relevantes con capacidad de afectación a sistemas espaciales

Actor	País	Capacidad	Fuente
Thrip	China	Ciberataques a satélites operativos en el 2018	(Feldman & Taylor, 2025, p. 46)
Fancy bear (APT28)	Rusia	Hacking a satélites de comunicaciones	(Hamill-Stewart & Rashid, 2024, p. 3)
Volt Typhoon	China	Hacking sistemas satelitales de información geográfica	(Hamill-Stewart & Rashid, 2024, p. 3)
Peach Sandstorm (APT28)	Irán	Acceso a datos de descarga, mediante ataques a la autenticación	(Hamill-Stewart & Rashid, 2024, p. 3)
Turla	Rusia	Hacking a satélites de comunicaciones	(Periyasami et al., 2024, p. 46)
Killnet	Rusia	Hacking a interfaz de usuario satélites de comunicaciones	(Poirier, 2024)

Fuente: elaboración propia con base en las fuentes citadas

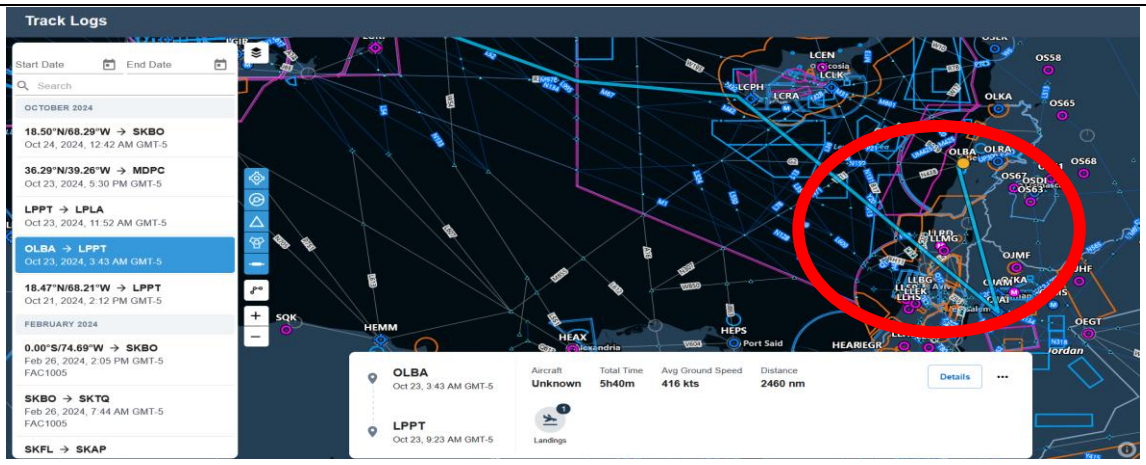
Uno de los ataques mencionados en la tabla 1, se presentó en el vuelo efectuado por el FAC 1219 el día 23/10/2024, en la ruta OLBA – LPPT (figura 9) donde se observó una diferencia de 128 NM, entre la posición real de la aeronave y lo observado en una aplicación de navegación por GPS (figura 10).

Figura 9 Trayectoria planeada del FAC1219



Fuente: imagen tomada de aplicación ForeFlight usada por un tripulante del vuelo.

Figura 10 Log del seguimiento del vuelo con datos satelitales

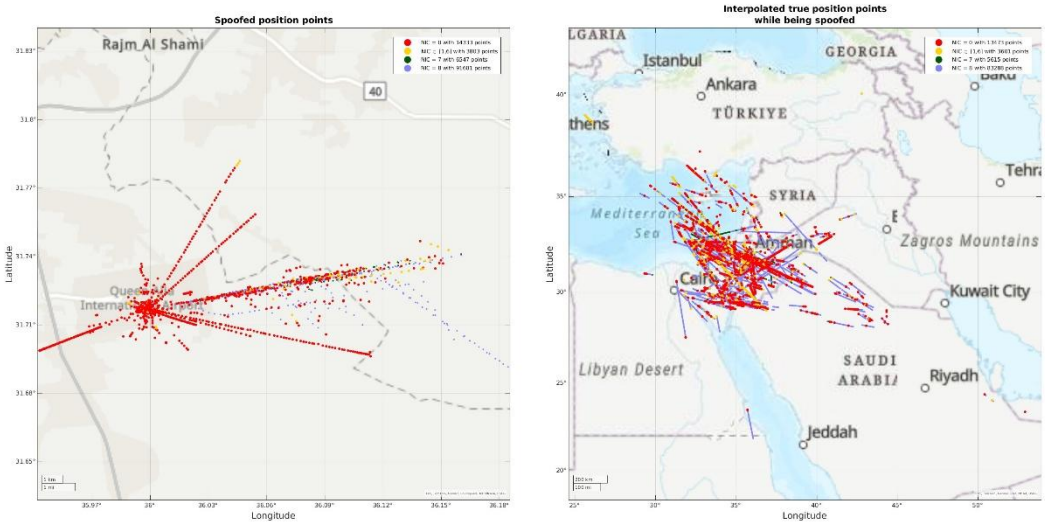


Fuente: imagen tomada de aplicación ForeFlight usada por un tripulante del vuelo.

De igual forma, se realizó una verificación de anomalías detectadas y reportadas por otros usuarios en la zona, encontrando un ataque de *spoofing* que enviaba coordenadas en un

área cercana a Madaba – Jordania, como se observa en la figura 11 (Stanford University, 2023), las cuales coinciden con las coordenadas erróneas recibidas por los sistemas de navegación del FAC 1219.

Figura 11 Región afectada por *spoofing* el día 23/10/2024



Fuente: imagen tomada de (Stanford University, 2023).

Defensas cibernéticas en el espacio: estrategias de mitigación para la ciberseguridad satelital

Las defensas cibernéticas son indispensables para salvaguardar la confidencialidad, integridad y disponibilidad de los sistemas satelitales. Por tal razón, se deben construir estrategias de mitigación, desde el endurecimiento de sistemas hasta la verificación de la integridad de los datos, para fortalecer la resiliencia de la infraestructura satelital y cubrir, de esta manera, los vacíos que deja la falta de políticas asociadas a la ciberseguridad satelital o la mala interpretación de las políticas existentes. Este campo es fundamental para anticipar,

resistir y recuperarse de las ciberamenazas, contribuyendo a la continuidad y fiabilidad de los servicios espaciales frente a un panorama de riesgos dinámico y persistente (Shahzad et al., 2024, p. 3).

Modelos de ciberseguridad para integridad de datos: arquitecturas y frameworks de protección en sistemas satelitales

La ciberseguridad aplicada a sistemas espaciales requiere modelos útiles y aplicables de acuerdo con el ambiente operacional. En el caso del GPS, no es la excepción; este requiere un enfoque de ciberseguridad especializado, capaz de entender el contexto complejo del sistema en los tres segmentos y de tener un panorama completo en la gestión de riesgos cibernéticos. Este enfoque lo brinda Scholl y Suloway (2023, pp. 11–12), quienes, en la NIST IR 8270, dan a conocer unos pasos requeridos para el desarrollo de un framework para el manejo de riesgos en sistemas espaciales. Estos pasos son:

- Establecer un alcance y prioridades
- Orientar
- Crear un perfil actual
- Realizar evaluación de riesgos
- Crear un perfil objetivo
- Determinar, analizar y priorizar brechas
- Implementar un plan de acción

Para el presente caso de estudio, se puede tomar otro reporte interagencial enfocado en PNT, siendo el documento NIST IR 8323r1 el que contiene un framework específico para

el sistema GNSS, aplicado específicamente al segmento de usuario. Este establece cinco puntos de referencia dentro del contexto de eventos de ciberseguridad en el PNT, de la siguiente forma:

- Identificar
- Proteger
- Detectar
- Responder
- Recuperar

Estas funciones le dan a la organización un modelado de riesgos de ciberseguridad adecuado en PNT (McCarthy et al., 2023, p. 7).

A partir de estos reportes interagenciales, se pueden tomar ciertas recomendaciones para ajustar marcos formales de ciberseguridad en sistemas espaciales, tal como lo hizo la corporación estadounidense Aerospace, que, de acuerdo con Bailey (2025, p. 2), lideró el desarrollo de un framework llamado "Space Attack Research and Tactic Analysis" (SPARTA), el cual modela las técnicas, tácticas y procedimientos de los posibles ciberataques a los sistemas espaciales, brindando herramientas para entender los ataques, amenazas y las posibles contramedidas que se pueden aplicar para contrarrestarlos.

Tácticas, técnicas y contramedidas del framework SPARTA para integridad de datos

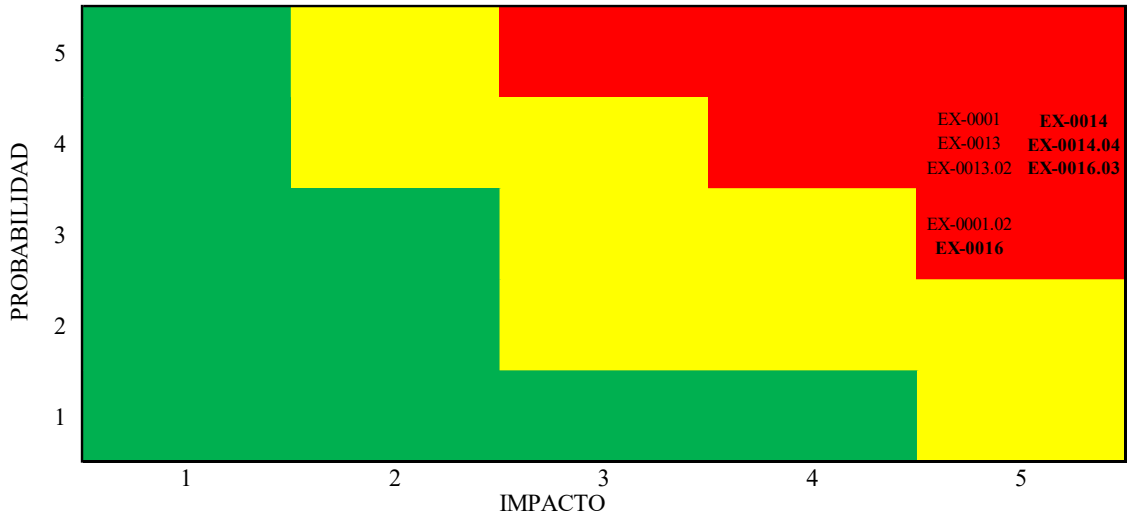
Teniendo en cuenta el framework propuesto por la Corporación Aerospace, se modelarán las técnicas, tácticas y contramedidas propuestas para los ataques en contra de la integridad de la señal del GPS, con enfoque en las aeronaves de la FAC.

- **Tácticas:** dentro de la matriz de tácticas, se pudo ubicar los vectores de ataque al GPS dentro de la ejecución, la cual tiene el código ST0004. Esta consiste en que la amenaza o actor ejecuta código malicioso en el sistema espacial (Aerospace Corporation, 2022d), siendo esta la táctica utilizada para ejecutar *spoofing*, *jamming* y *meaconing*.
- **Técnicas:** para la táctica específica ST0004, se encuentran diferentes técnicas que pueden estar asociadas:
    - Repetición (EX-0001), específicamente repetición de tráfico (EX-0001.02), donde se puede ubicar el meaconing.
    - Inundación de comunicaciones (EX-0013), específicamente datos erróneos (EX-0013.02) que es la introducción de datos, ruido o señales en un canal objetivo para impedir el procesamiento normal de datos del sistema (Aerospace Corporation, 2022c).
    - Spoofing (EX-0014), específicamente spoofing de PNT (EX-0014.04) donde se realiza el envío ilegítimo de señales PNT, alterando el funcionamiento normal de los GNSS (Aerospace Corporation, 2022f).
    - Jamming (EX-0016), específicamente jamming de PNT (EX-0016.03) donde se inhibe la recepción legítima de señales PNT, impidiendo el funcionamiento normal del GPS (Aerospace Corporation, 2022e).

Ubicando las técnicas específicas para los ataques descritos anteriormente, se puede obtener una puntuación de riesgo para el GPS. De acuerdo con lo observado en la misión de la FAC a Beirut en 2024, se evidencia que el impacto y la probabilidad de

ocurrencia de este tipo de ataque es alta. Con la finalidad de modelar el riesgo, se tomó el modelo SPARTA, integrando las técnicas mencionadas previamente. El resultado se presenta en la figura 12, donde se observan todas las técnicas con un riesgo alto.

Figura 12 Riesgo teórico del modelo de riesgos de SPARTA



Fuente: elaboración propia adaptada de riegos asociados a técnicas de (Aerospace Corporation, 2022e).

- **Contramedidas**: teniendo en cuenta las técnicas EX-0001.02, EX-0013.02, EX-0014.04 y EX-0016.03, y de acuerdo con el mapa de control de contramedidas proporcionado por Aerospace Corporation (2022a), se proponen cinco contramedidas para mitigar dichas técnicas, según lo siguiente:
    - Autenticación (CM0031): esta contramedida se centra en mecanismos de autenticación para todas las sesiones de comunicación, tanto entre satélites como con las estaciones terrestres. Debe ser bidireccional y basada en

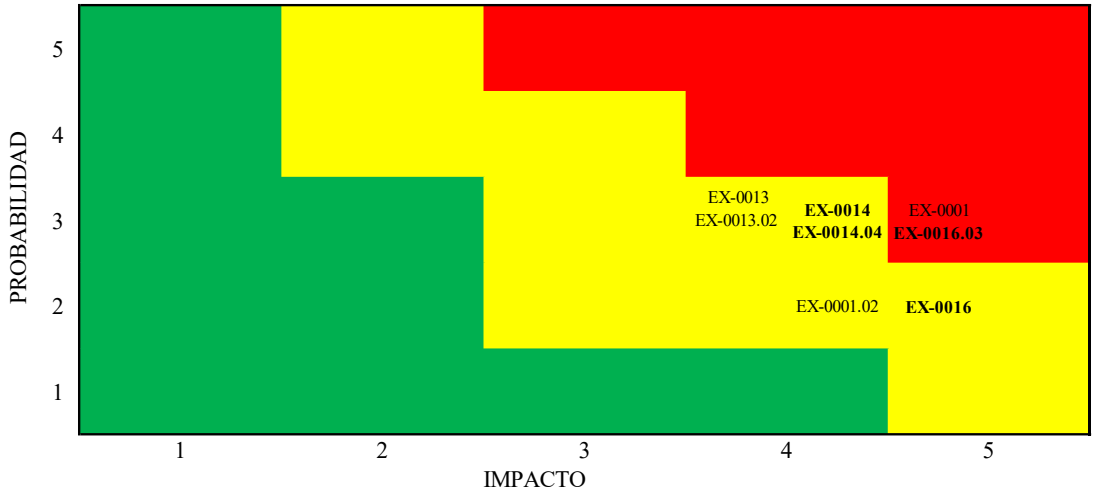
criptografía antes de permitir el establecimiento de cualquier conexión remota.

- Detección y prevención de intrusiones a bordo (CM0032): esta contramedida propone el uso de un sistema de detección/previsión de intrusiones (IDS/IPS), con la finalidad de monitorear los componentes o sistemas críticos de la misión, así como auditar y registrar las acciones que se realizan en ellos. Un aspecto crucial es la capacidad del IDS/IPS para responder activamente a las amenazas detectadas en diversas etapas del ataque.
- Gestión robusta de fallas (CM0042): esta contramedida se centra en asegurar que el sistema de gestión de fallas inherente al satélite no pueda ser explotado como un vector de ataque que permita la manipulación de maniobras de corrección orbital, afecte la integridad de la telemetría o el uso de operaciones de proximidad para forzar al satélite a entrar en modo seguro.
- PNT robusto (CM0048): esta contramedida aborda la protección de los sistemas vitales para la operación satelital. Recomienda utilizar un mecanismo de autenticación que permita a los receptores verificar la autenticidad tanto de la información recibida como de la entidad que la transmite, asegurando así que provenga de una fuente confiable.
- Anulación de antena y filtrado adaptativo (CM0083): esta contramedida se refiere a técnicas de mitigación de jamming en la recepción de señales. Teniendo en cuenta que los satélites pueden ser diseñados con antenas capaces de anular o minimizar las señales provenientes de una región geográfica

específica en la superficie terrestre o de ubicaciones en el espacio donde se detecta interferencia. La anulación es útil cuando la interferencia proviene de un número limitado de ubicaciones detectables; sin embargo, también puede bloquear las transmisiones de usuarios legítimos que se encuentren dentro del área anulada. Por otro lado, el filtrado adaptativo se utiliza para bloquear bandas de frecuencia específicas independientemente de dónde se originen estas transmisiones.

Teniendo en cuenta la aplicación de estas contramedidas, **y lo propuesto por Ear et al. (2024, p. 3) quienes usaron el concepto *Notional Risk Scores (NRS)* para evaluar cuantitativamente los riesgos cibernéticos asociados a sistemas espaciales, basándose en controles de ciberseguridad y control de riesgos de la *NIST* y la experiencia de algunos investigadores de ciberseguridad para desarrollar un algoritmo para seleccionar los controles adecuados para reducir los riesgos asociados a las amenazas cibernéticas expuestas con anterioridad, posterior la selección de las contramedidas correctas el nivel del riesgo residual se calcula con un análisis cualitativo de expertos y mapeando cada una de las técnicas asociadas a la amenaza y las contramedidas aplicadas, dando como resultado un riesgo residual o como se observa en la figura 13, la mitigación del riesgo de las técnicas descritas, obteniendo un riesgo residual medio-alto, es relevante tener presente que para que la contramedida aplicada pueda reducir el riesgo debe frustrar la técnica previniendo la ejecución, detectándola de forma oportuna o limitando sus consecuencias.**

Figura 13 Riesgo residual posterior aplicación de contramedidas

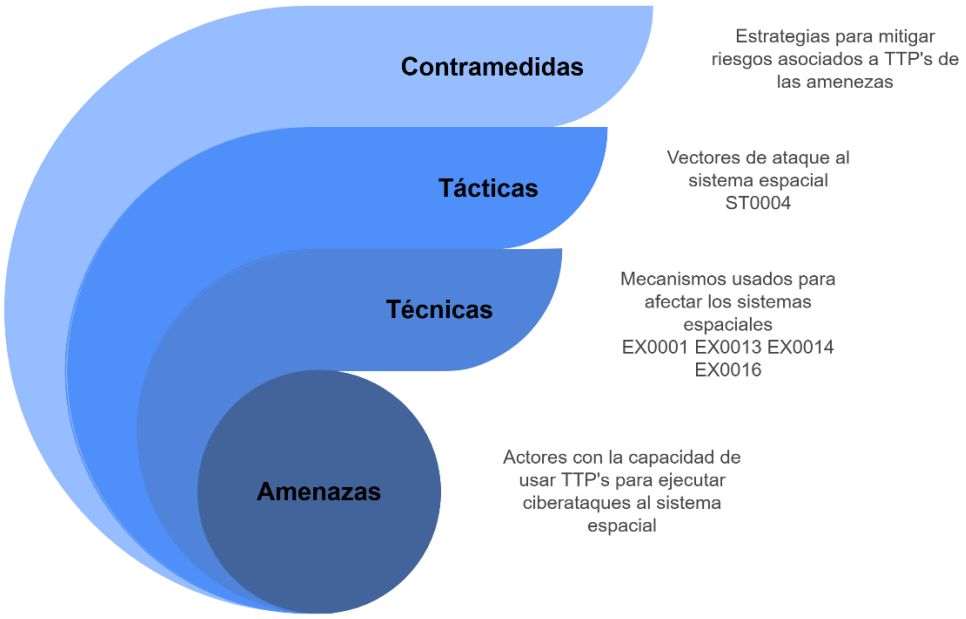


Fuente: elaboración propia con información herramienta contramedidas (Aerospace Corporation, 2022h).

De acuerdo con lo anterior es importante mencionar que la reclasificación del riesgo de alto a medio alto, se realiza de acuerdo a lo enunciado por Ear et al. (2024, p. 5), el riesgo residual se obtiene de forma subjetiva, al tener un componente cualitativo predominante, sin embargo, el estudio de las contramedidas a aplicar de acuerdo a cada técnica aplicada por la amenaza tiene el soporte adecuado para confiar en su aplicación, en la mitigación del impacto al materializarse algún riesgo en el sistema satelital, con base en esto se puede estudiar la aplicación de controles que prevengan la ejecución, la detecten de forma oportuna o limiten sus consecuencias.

Fortificando el segmento de usuario: contramedidas para salvaguardar la integridad de la señal GPS

Figura 14 Explicación gráfica del framework SPARTA



Fuente: elaboración propia con base en el Framework SPARTA explicado con anterioridad.

De acuerdo con las amenazas, las técnicas y tácticas que pueden usarse, y con base en el framework SPARTA, es necesario considerar las particularidades de todo el sistema espacial para fortificar el segmento de usuario. Partiendo de las contramedidas del framework, hay factores como las restricciones de tamaño, capacidad de procesamiento y potencia que limitan el diseño y la operación de contramedidas robustas, así como la aplicación de medidas de protección eficientes, teniendo en cuenta que, muchas veces, es más importante la funcionalidad del sistema que la protección del mismo (Shahzad et al., 2024, p. 13).

Una propuesta efectiva para la fortificación del segmento de usuario puede considerar lo siguiente:

- **Autenticación robusta del dispositivo de usuario**: es importante tener certeza sobre los dispositivos que reciben datos del segmento satelital o de control. Para esto, se pueden aplicar algunos métodos, como el uso de llaves inteligentes en los dispositivos, las cuales permiten la gestión de claves de cifrado o procesos de registro *Over-The-Air (OTA),* que permiten una autenticación continua después de un registro inicial (Delgado & Carmona Tapia, 2024). Estos métodos permiten la autenticación de los dispositivos finales dentro del sistema, posibilitando establecer comunicación segura entre el segmento satelital y el de usuario.
- **Implementación de mecanismos de cifrado ligero:** según Shahzad et al. (2024, p. 14), esta implementación es una opción válida para evitar la recepción de datos ilegítimos dentro del sistema, estableciendo un protocolo seguro de comunicación totalmente funcional en el segmento de usuario.
- **Infraestructura de llave pública:** según Rushanan y Gillis, el Gobierno de Estados Unidos utiliza una infraestructura de llave pública en el GPS, permitiendo firmar digitalmente las señales de los segmentos de control y de usuario, y estableciendo comunicaciones seguras dentro del sistema satelital. Esto lleva al establecimiento de algoritmos *antispoofing*, que rechazan por defecto las señales que no estén firmadas con la llave pública del sistema (2025, pp. 236–238). Esta alternativa es aplicable en la construcción de sistemas bajo este método y es ampliamente utilizada en sistemas críticos, como los implementados por las Fuerzas Militares.

- **Monitoreo, reconocimiento e inteligencia:** la alerta situacional es parte fundamental en la fortificación del segmento de usuario. La aplicación de monitoreo, vigilancia y reconocimiento al sistema espacial es esencial para implementar medidas de seguridad como la seguridad de la información (INFOSEC) y las operaciones de seguridad (OPSEC), endureciendo la postura de seguridad en este segmento (Periyasami et al., 2024, p. 18). Un método de monitoreo eficiente es el uso de análisis de datos en tiempo real en este segmento.

La aplicación coherente de estas medidas de endurecimiento representa una capa esencial de defensa en la estrategia de ciberseguridad para sistemas satelitales. Es importante tener en cuenta que algunas medidas deben ser adoptadas desde la fase de construcción del sistema, mientras que otras, como el monitoreo en el segmento, pueden ser implementadas en los equipos que actualmente posee la FAC.

Inteligencia artificial aplicada en ciberseguridad: modelo de ML para verificación de integridad de datos GPS

Dentro de las contramedidas propuestas en el framework SPARTA, se identificaron la detección y prevención de intrusiones a bordo, la gestión robusta de fallas y el PNT robusto, las cuales pueden ser abordadas desde la propuesta de monitoreo, reconocimiento e inteligencia. Para ello, se puede diseñar un modelo de machine learning (ML) que clasifique señales anómalas en datos GPS recibidos en las aeronaves de la FAC.

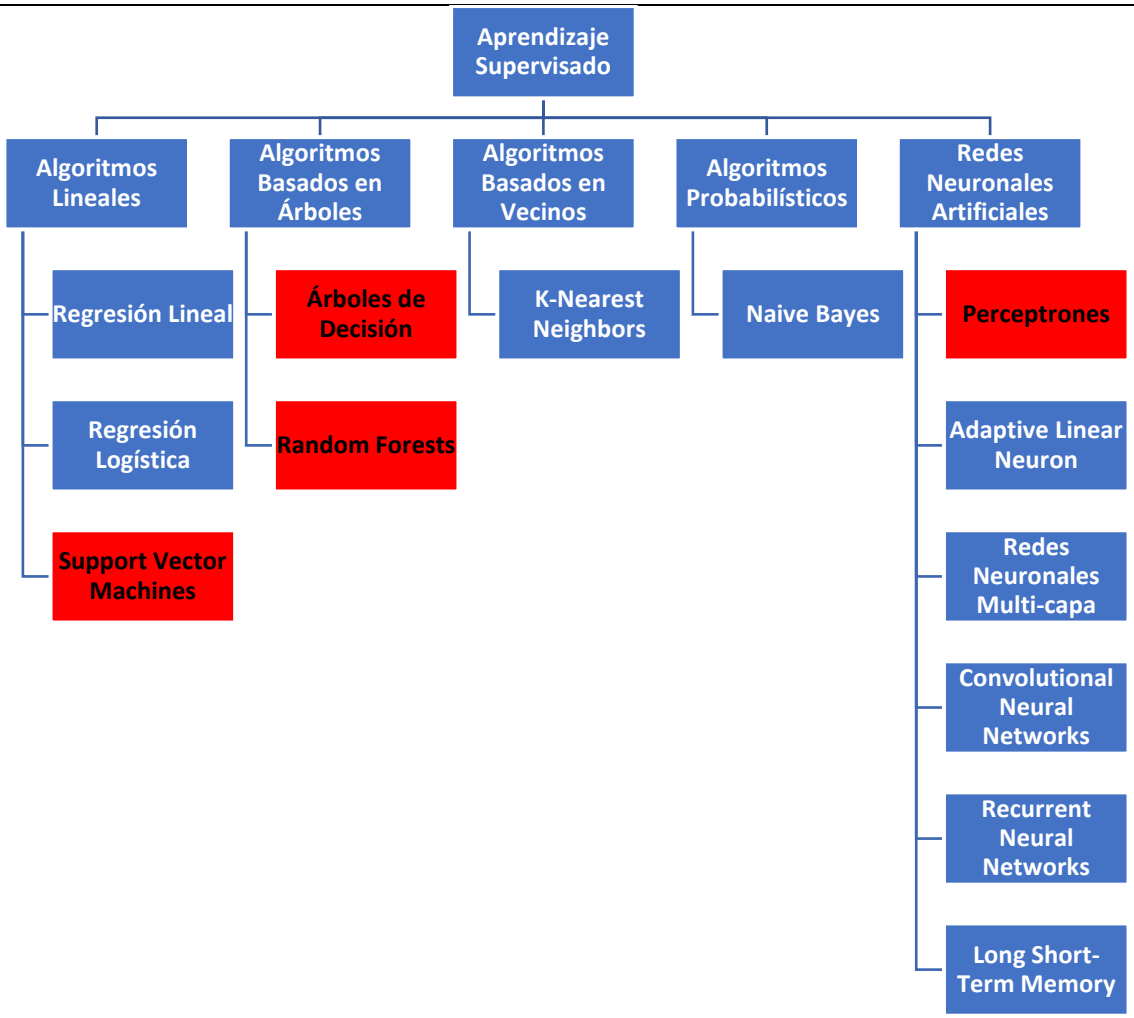
Para esto, es necesario realizar una verificación de los diferentes algoritmos de ML que se podrían utilizar. Inicialmente, se contemplan los algoritmos de aprendizaje

supervisado, los cuales requieren datos etiquetados —en este caso, como legítimos o como *spoofing*—. De esta forma, se entrena el modelo de clasificación indicando la etiqueta de cada dato en el conjunto de datos (dataset) (Sarang, 2023, p. 43). Algunos de los más relevantes se pueden observar en la figura 15.

Otra opción es considerar algoritmos de aprendizaje no supervisado, que utilizan datos no etiquetados. Estos algoritmos obtienen información de acuerdo con el comportamiento de variables independientes (Patel, 2019, p. 18). Algunos de los más destacados se presentan en la figura 16.

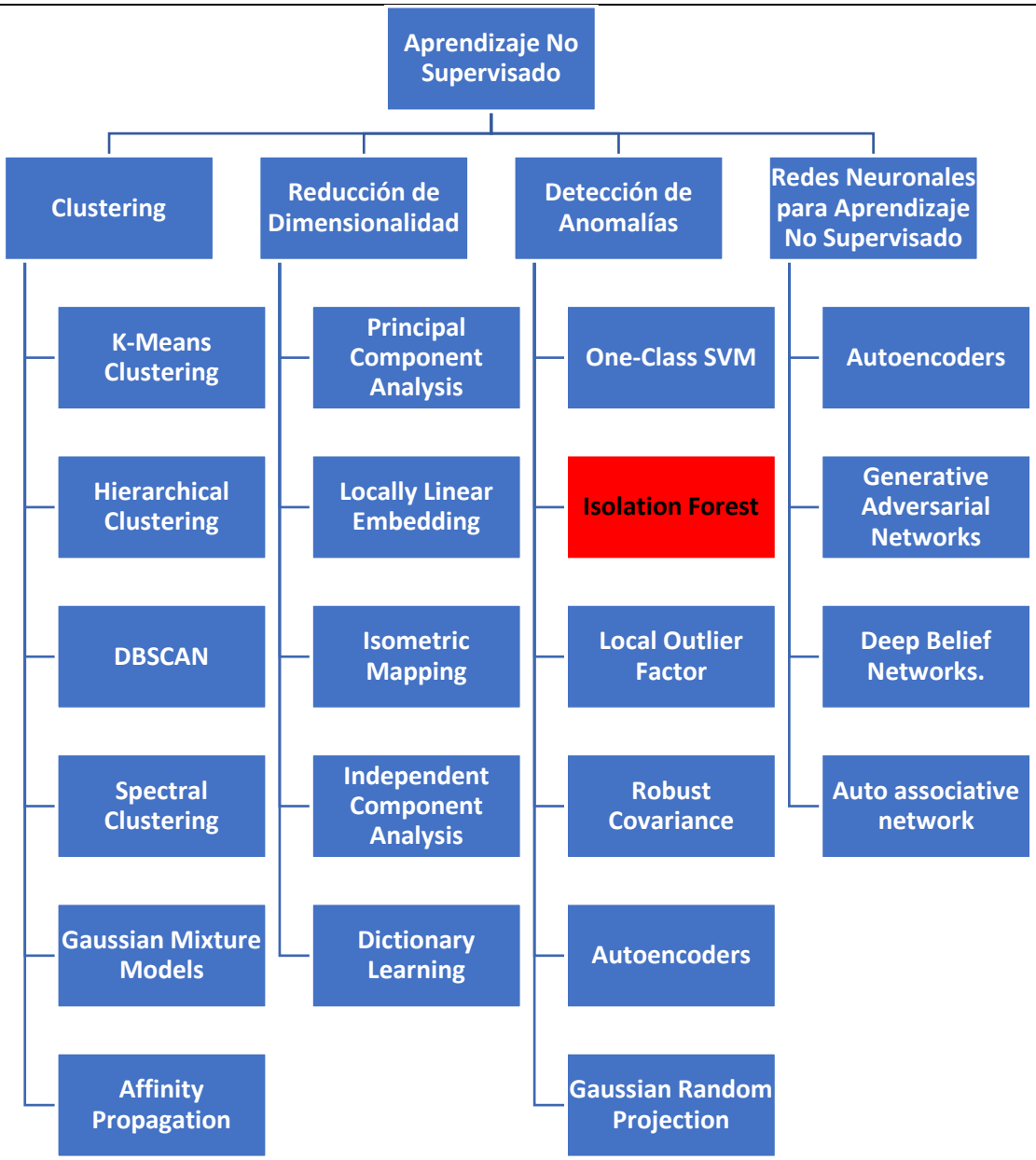
Con la finalidad de seleccionar el algoritmo más adecuado para el modelado de ML orientado a verificar la integridad de los datos GPS, y de acuerdo con el estudio realizado por Huang et al. (2025, pp. 3–5), se tuvo en cuenta la categorización del modelado deseado. Se identificaron cinco algoritmos de aprendizaje supervisado y un algoritmo de aprendizaje no supervisado que podrían desempeñar un rol importante en el entrenamiento del modelo de verificación. Esta selección se realizó teniendo en cuenta que el tipo de anomalía a detectar corresponde a anomalías contextuales, enfocando el modelo en variaciones repentinas en los datos recibidos.

Figura 15 Algoritmos de aprendizaje supervisado



Fuente: elaboración propia con base en los algoritmos propuestos por Barua et al. (2024), Amr (2020) y Winn y Bishop (2024).

Figura 16 Algoritmos de aprendizaje no supervisado



Fuente: elaboración propia con base en los algoritmos propuestos por Barua et al. (2024), Amr (2020), Winn y Bishop (2024), Patel (2019).

Fundamentos del modelo: algoritmos y técnicas conocidas de Machine Learning

De acuerdo con el acercamiento inicial, los algoritmos que se seleccionaron como posibles candidatos fueron:

- **Multi-Layer Perceptron (MLP):** es un algoritmo supervisado para clasificación o regresión. Es un tipo de red neuronal artificial compuesta por múltiples capas; utiliza retropropagación para entrenarse y es capaz de modelar relaciones complejas y no lineales (Amr, 2020, pp. 282–284).
- **Random Forest (RF):** es un algoritmo supervisado para clasificación o regresión. Combina múltiples árboles de decisión entrenados con subconjuntos del conjunto de datos y el concepto de vecinos cercanos, mejorando la precisión y reduciendo el sobreajuste (Amr, 2020, p. 319).
- **Light Gradient Boosting Machine (LightGBM):** es un algoritmo supervisado para clasificación o regresión, basado en boosting con árboles. Para optimizar la eficiencia y velocidad, utiliza histogramas y crecimiento de árbol por hoja, lo que lo hace ideal para grandes volúmenes de datos (Sarang, 2023, p. 174).
- **Extreme Gradient Boosting (XGB):** es un algoritmo supervisado para clasificación o regresión. Es una implementación avanzada de LightGBM, que incluye regularización y manejo eficiente de datos faltantes, lo que lo hace ideal para tareas exigentes (Sarang, 2023, p. 179).
- **Support Vector Machine (SVM):** es un algoritmo supervisado para clasificación o detección de anomalías. Encuentra el hiperplano óptimo que separa clases; funciona bien con espacios de alta dimensión y puede utilizar núcleos (kernels) para separar datos no lineales (Barua et al., 2024, pp. 239–240).

- **Isolation Forest (iForest):** es un algoritmo no supervisado para detección de anomalías. Aísla observaciones construyendo árboles aleatorios, y los valores atípicos requieren menos divisiones para aislarse (Agyemang, 2024, p. 6).

Con base en estos algoritmos, se diseñó un modelo de ML en Python con el fin de seleccionar el algoritmo con mayor precisión en la detección de anomalías en la señal GPS, obteniendo los resultados expuestos en la tabla 3. Se concluyó que el mejor algoritmo para el modelo de verificación de integridad, con datos de vuelos reales, fue el Random Forest, con una precisión de 98.72%.

Tabla 3. Comparación de resultados del entrenamiento de un data set de varios vuelos de aeronaves de la FAC con un total de 1800 entradas

	MLP	RF	LightGBM	XGB	SVM	iForest
f1-score en Datos íntegros	0.7219	**0.9617**	0.9508	0.9562	0.9477	0.8884
f1-score en Datos *spoofing*	0.9358	**0.9923**	0.9904	0.9914	0.9897	-
Precisión	0.8957	**0.9872**	0.9839	0.9856	0.9828	0.8325

Fuente: elaboración propia con base los resultados del entrenamiento de los diferentes algoritmos de ML

Random Forest mostró mejores resultados en la clasificación de señales anómalas, partiendo de los parámetros de navegación (latitud, longitud, velocidad y altitud). Teniendo en cuenta que este algoritmo realiza divisiones del dataset en subgrupos por categorías, se pueden evaluar fases diferentes como ascenso, vuelo crucero y descenso, así como distintos vuelos incluidos dentro del dataset. Esta división permite al modelo entrenar de forma dinámica y en paralelo varios árboles de decisión, lo que brinda una mayor precisión en datasets con grandes volúmenes de datos (Sarang, 2023, p. 155).

Entrenamiento y validación del modelo: uso de datos simulados y reales para la precisión

Para el entrenamiento del modelo de ML, se utilizaron datos de la plataforma FlightRadar24, donde se recopilaron 7500 registros de 13 vuelos diferentes de aeronaves de la FAC. Teniendo en cuenta que en la actualidad existen equipos capaces de simular con alta precisión los datos de la señal enviada desde el segmento satelital, se construyó el modelo de ML únicamente con el componente de navegación GPS. De esta forma, se realizó una clasificación en subgrupos como días de vuelo y fases de vuelo, con la finalidad de tener un panorama completo del comportamiento normal de la aeronave, considerando latitud, longitud, velocidad y altitud.

Con las bases para la construcción y entrenamiento del modelo, se siguieron los siguientes pasos:

1) Preparación de los datos
    a. **Recopilación y limpieza:** posterior a la adquisición de los datos, fue necesario realizar una limpieza, eliminando datos nulos, duplicados o no relevantes dentro del dataset. Una limpieza adecuada es vital para la calidad del modelo (Aceves-Fernández, 2023, p. 86). Como el modelo es supervisado, fue necesario crear un escenario con un dataset simulado de datos de *spoofing*, para obtener el etiquetado de datos íntegros y no íntegros.
    b. **Transformación y codificación:** se normalizaron los datos según el formato requerido por el algoritmo. Asimismo, se conservaron

únicamente los datos a utilizar en el modelo, considerando que solo se emplearán datos de navegación, tiempo y un identificador de la aeronave. Se aplicará la misma codificación para la recepción de datos en tiempo real (Barua et al., 2024, pp. 120–123).

2) División del Conjunto de Datos

   a. **Conjunto de entrenamiento:** este es el conjunto de datos utilizado para entrenar el modelo. Se tomó un porcentaje del total de datos descargados. Con estos datos se construyeron múltiples árboles de decisión basados en subconjuntos de datos y características específicas, para determinar la validez de los datos procesados, considerando los datos normalizados de FlightRadar24 y los datos generados que representan *spoofing* (Sarang, 2023, p. 43).

   b. **Conjunto de validación:** es el conjunto de datos usado para afinar los parámetros del modelo —aquellos que no se entrenan, sino que se configuran previamente—. También se emplea para evaluar el rendimiento del modelo durante el proceso de desarrollo y ajuste. Este conjunto fue creado con datos de vuelos del mismo tipo de aeronave en días diferentes, con el propósito de garantizar que fuera completamente diferente al conjunto de entrenamiento (Amr, 2020, p. 54).

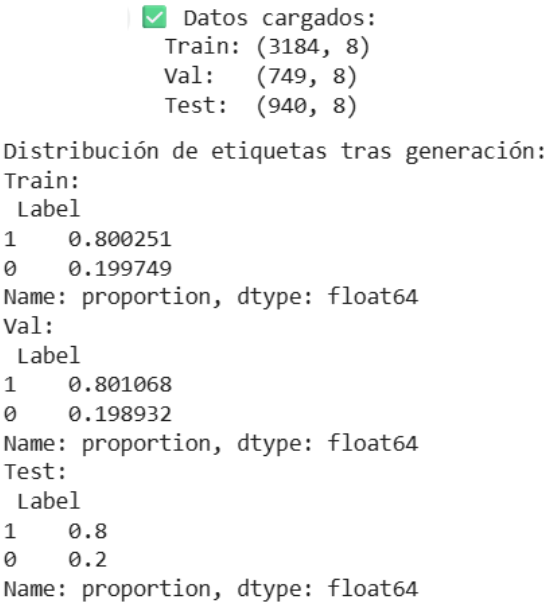
   c. **Conjunto de prueba:** este último conjunto es completamente independiente y se reserva exclusivamente para la evaluación final del

> rendimiento del modelo óptimo. Con este conjunto se simula el rendimiento frente a datos nuevos y no vistos. Para esta fase se emplearán datos en tiempo real (Amr, 2020, p. 54).

Teniendo en cuenta que los datos obtenidos en la plataforma FligthRadar 24, son datos en esencia íntegros y el algoritmo que resulto adecuarse más al modelado a diseñar es supervisado, eso quiere decir, que el algoritmo necesita datos etiquetados como íntegros y no íntegros, por tal razón se verificaron las variables del data set, seleccionando la posición y el rumbo de la aeronave como datos clave en la verificación de un ataque de *spoofing*, encontrando una relación directa con la función Harversine, la cual es fundamental en datos de navegación, que se emplea al calcular distancia y ángulo entre 2 puntos en una superficie esférica (De Luca, 2024), por tal razón se uso esta formula para generar puntos en el data set fuera de ruta, desplazando las coordenadas de la trayectoria real de la aeronave entre 3 y 25 millas náuticas, el algoritmo diseñado para la creación de un nuevo data set, se encuentra en el repositorio del proyecto (https://github.com/baudinuniandes/Satellite-Cybersecurity-ML-for-GPS-integrity/blob/main/scripts/generate_spoofing.py), se selecciona un rango entre 3 y 25 nm teniendo en cuenta que el avión no se va a desplazar a esa distancia en 1 segundo, considerando una posición

anómala dentro del data set, con el nuevo punto generado aleatoriamente se remplaza de forma aleatoria el punto seleccionado y se modifica el identificador de integro (1) por no integro (0), este proceso se repite hasta completar un 20% del total de datos almacenados en el data set original.

Figura 17 División del conjunto de datos completo



Fuente: elaboración propia, imagen tomada de ejecución del programa de entrenamiento del modelo

3) Entrenamiento del modelo: el algoritmo RF se entrena utilizando el conjunto de entrenamiento. En scikit-learn*, esto se realiza con el método fit() del

* De acuerdo con Amr, scikit-learn es una biblioteca que proporciona la infraestructura adecuada para el manejo de datos en Python, permitiendo a los científicos de datos realizar un sinfín de transformaciones de datos utilizando herramientas de manejo de datos para una interacción rápida entre diferentes algoritmos, manteniendo el control total sobre los parámetros y configuración de los mismos, en un entorno complejo como la inteligencia artificial.

objeto clasificador, el cual recibe las características y las etiquetas necesarias para el entrenamiento. Es en este proceso donde se construye el bosque de árboles de decisión (Amr, 2020, p. 82).

4) Afinación de hiperparámetros[†]: este es un paso importante para optimizar el rendimiento del modelo. Los hiperparámetros controlan la construcción del bosque y de los árboles individuales, de acuerdo con Sarang (2023, pp. 156–162).
5) Validación del modelo: la validación se realiza para estimar el rendimiento del modelo durante la fase de afinación de hiperparámetros. Para la construcción de este modelo se usó la validación cruzada, considerando que es la técnica más robusta, de acuerdo con lo expresado por Amr (2020, pp. 95–97). Esta técnica contempla el uso de conjuntos de datos diferentes para entrenamiento y validación, la limitación del crecimiento de los árboles, y el uso de técnicas de estimación de precisión de los clasificadores, aplicando estas buenas prácticas desde la librería scikit-learn.
6) Evaluación final del modelo: de acuerdo con lo expuesto por Aceves-Fernández (2023, pp. 124–128), una vez que se determinan los hiperparámetros óptimos, el modelo final se entrena con el conjunto de

[†] Según Amr los hiperparámetros son configuraciones externas a un modelo de *machine learning* que no se aprenden directamente de los datos durante el proceso de entrenamiento, sino que estos se establecen antes de que el entrenamiento comience. A diferencia de los parámetros del modelo, que son inferidos a partir de los datos, los hiperparámetros definen la arquitectura, la estructura y el comportamiento del algoritmo de aprendizaje.

entrenamiento completo, es decir, con los conjuntos de entrenamiento y validación. Posteriormente, el modelo se evalúa utilizando el conjunto de prueba independiente (no utilizado en ninguna etapa anterior), aplicando las siguientes métricas:

a. **Exactitud (Accuracy):** porcentaje de predicciones correctas.
b. **Precisión (Precision):** porcentaje de verdaderos positivos entre todas las predicciones positivas. Para este modelo es crucial detectar la integridad de señales GPS sin generar falsos positivos.
c. **Sensibilidad (Recall):** porcentaje de verdaderos positivos entre todos los casos positivos reales.
d. **Puntuación F1 (F1-score):** media armónica de precisión y sensibilidad.
e. **Matriz de confusión (Confusion matrix):** muestra el número de verdaderos positivos, verdaderos negativos, falsos positivos y falsos negativos.
f. **Curva ROC (Receiver Operating Characteristic) y AUC (Area Under the Curve):** se evalúa el rendimiento del clasificador a diferentes umbrales de decisión. Un AUC más alto indica una mejor capacidad de discriminación.

Figura 18 Métricas de evaluación final

```
=== Métricas Finales en Test ===
Accuracy:  0.8435
Precision: 0.9903
Recall:    0.8123
F1-score:  0.8925
AUC:       0.9106
Confusion Matrix:
 [[182   6]
 [141 610]]
```

Fuente: elaboración propia, imagen tomada de ejecución del programa de entrenamiento del modelo

Validación y evaluación: como se podría integrar el modelo en una operación de la FAC

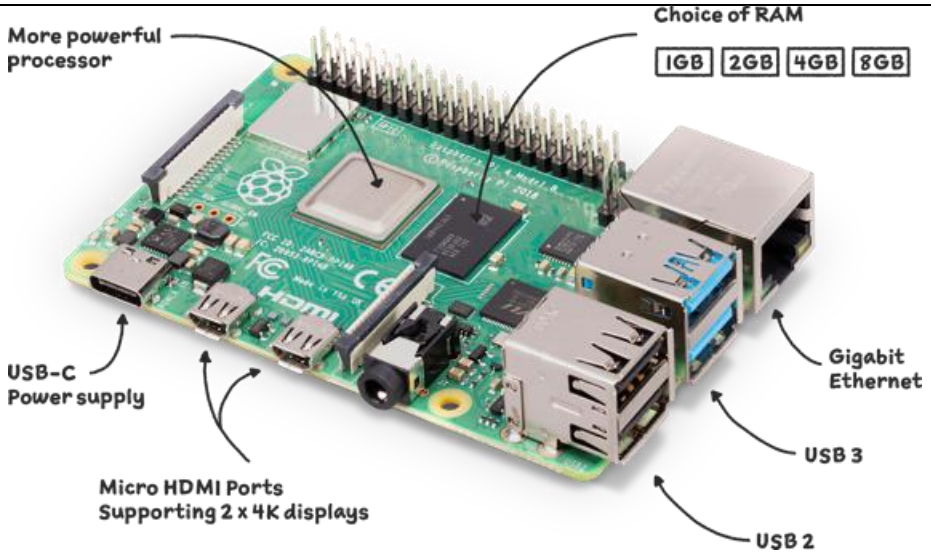
Con el diseño del modelo ya afinado y probado, es necesario desarrollar una propuesta para desplegar un modelo funcional al interior de una aeronave de la FAC, con la finalidad de verificar, en tiempo real, las señales GPS recibidas durante las operaciones que desarrolle dicha aeronave. Para esta propuesta se realizó una aproximación a dispositivos capaces de procesar un modelo de ML. De acuerdo con Salerno (2025, pp. 255–256), existen opciones como las placas Arduino Nano, Raspberry Pi, ESP32, entre otras.

Para este proyecto, se seleccionó una Raspberry Pi 4B, con capacidad de procesamiento y 4 GB de memoria RAM (ilustración en figura 19), la cual brinda una gran flexibilidad para ejecutar código y acciones desde dispositivos portátiles. Este dispositivo se encargaría de recibir las señales satelitales, procesarlas con el modelo entrenado y emitir una señal visual que indique si la señal es íntegra o no. Para ello, se propone lo siguiente:

1. Despliegue en la Raspberry Pi: este es el puente crítico entre el modelo diseñado y el hardware (en la recepción y respuesta). El modelo RF entrenado offline debe ser exportado en un formato que pueda ser cargado y ejecutado

de forma eficiente en la Raspberry Pi. Por esta razón, se seleccionaron las librerías scikit-learn, joblib, numpy y math para el procesamiento de datos; gpsd para la recepción e interpretación de los datos GPS; y RPi para interactuar con LEDs de colores (Amr, 2020, p. 490). Con las librerías cargadas y el modelo entrenado y refinado, se contaría con el software necesario para poner en producción el diseño de ML.

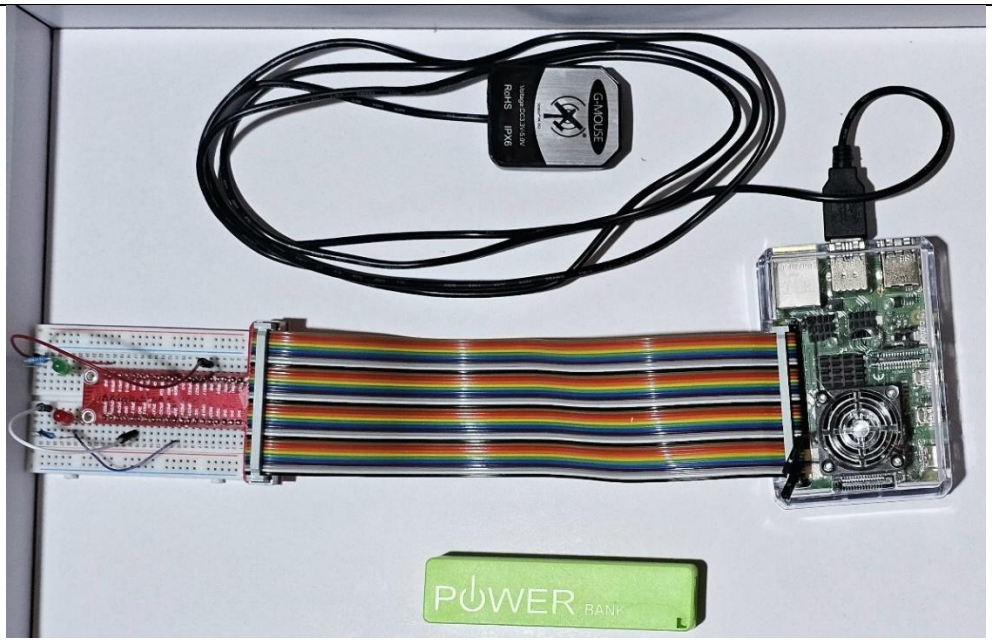
Figura 19 Estructura de la Raspberry Pi 4



Fuente: imagen tomada de (Raspberry Pi Ltd, 2020)

2. Entorno de ejecución en la Raspberry Pi: con los ajustes correctos en el software, ahora es necesario adecuar el hardware requerido para la ejecución del modelo. Para ello, se necesita la tarjeta Raspberry Pi completamente configurada, una antena receptora GPS (en este caso se utilizó una antena VK-162 USB GPS Dongle), una batería portátil de 5V 3A y un conjunto de conexiones para LEDs. Como ilustración, véase la figura 20.

Figura 20 Configuración de hardware para implementación del modelo de ML



Fuente: fotografía tomada por el autor.

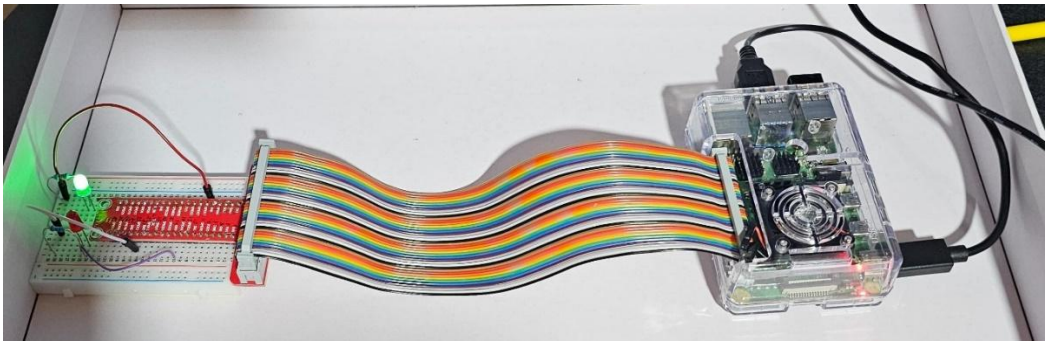
3. Pruebas en simulación: el modelo integrado debe probarse en un entorno de simulación de vuelo. Para ello, se utilizó un HackRF One (figura 21), que permite generar señales de *spoofing* mediante SDR, **un escenario similar al mencionado en la tabla 1, en donde los equipos de navegación de una aeronave de la FAC recibieron datos GPS erróneos,** y realizar la prueba de recepción de *spoofing* simulada en un entorno controlado. En este entorno, el modelo completo fue ejecutado desde la Raspberry Pi, de forma totalmente funcional. Al recibir la señal GPS, el LED verde permaneció encendido (ver imagen 22), indicando que la señal era íntegra. Posteriormente, al generarse una señal con coordenadas erróneas (ver figura 24), el LED verde se

apagó y se iluminó el LED rojo (ver imagen 23), indicando que la señal no era íntegra.

Figura 21 Dispositivo HackRF One

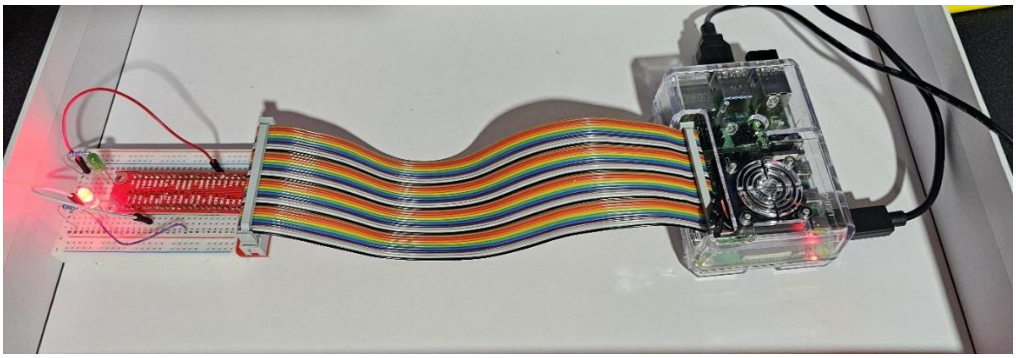
Fuente: fotografía tomada por el autor.

Figura 22 Ejecución del modelo con recepción integra



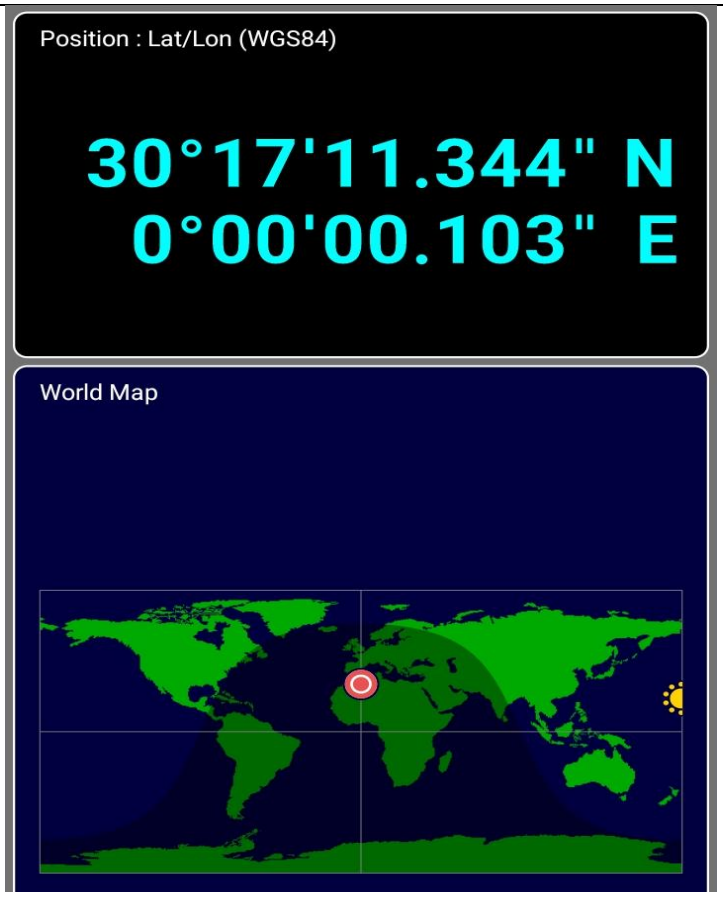
Fuente: fotografía tomada por el autor.

Figura 23 Ejecución del modelo con recepción de *spoofing* simulado



Fuente: fotografía tomada por el autor.

Figura 24 Recepción de coordenadas *spoofing*



Fuente: imagen tomada de la aplicación GPS Test.

4. Pruebas del hardware: una vez superadas las simulaciones, se realizaron pruebas con el hardware real, inicialmente en tierra, con datos de sensores reales o emulados, y posteriormente en vuelo, lo cual permitió probar la eficiencia de la Raspberry Pi para asegurar su funcionalidad y verificar que cumpliera con los requisitos de latencia necesarios, sin encontrarse ninguna desviación con respecto a lo planteado en la fase de simulación. En la fase de vuelo no se ejecutó la simulación de *spoofing* por razones de seguridad operacional, sin embargo, el modelo funciono de acuerdo a lo entrenado, en las diferentes fases del vuelo.

De esta forma, se logró comprobar la viabilidad del uso de un modelo de ML para la detección de señales anómalas en un vuelo real. La adaptación del hardware puede realizarse de acuerdo con las necesidades específicas de la aeronave de la FAC, teniendo presente la importancia de garantizar las condiciones de operación del sistema de procesamiento en borde. Acompañado del uso de este dispositivo, también puede incluirse, dentro del planeamiento de la misión, el análisis propuesto por la Universidad de Stanford (2023), que permite identificar las áreas con posible afectación por *spoofing* y definir con antelación los procedimientos a ejecutar en caso de ingresar en dicha condición.

Con la intención de facilitar el acceso a la implementación del modelo propuesto, se creó un repositorio en GitHub: https://github.com/baudinuniandes/Satellite-Cybersecurity-ML-for-GPS-integrity, donde reposa toda la información referente al diseño y estructuración del modelo.

Conclusiones

La necesidad de la FAC de utilizar sistemas como el GPS subraya la importancia de implementar medidas de seguridad en el uso del sistema satelital, este estudio aborda una problemática crítica y emergente en el ámbito de la ciberseguridad aeroespacial, específicamente en la salvaguarda de la integridad de los datos de navegación GNSS, con un enfoque particular en el segmento de usuario para las operaciones de la FAC. Los hallazgos principales se articulan de la siguiente manera:

- **Identificación de riesgos críticos: la investigación logra identificar y caracterizar de manera efectiva las vulnerabilidades y ciberamenazas inherentes al uso del GPS en el contexto operacional de la FAC, destacando el *spoofing* como una de las amenazas más críticas para la integridad de los datos de navegación, como lo presentado en el caso de estudio del vuelo del FAC 1219, proporcionando una validación empírica fundamental de la urgencia y relevancia de esta amenaza.**
- **Propuesta de solución basada en Machine Learning: el trabajo culmina con el diseño e implementación de un modelo de ML basado en el algoritmo Random Forest, para la detección en tiempo real de señales GPS anómalas que puedan asociarse con un ciberataque de *spoofing*, utilizando parámetros de navegación clave como latitud, longitud, velocidad y altitud.**
- **Validación práctica: un hallazgo relevante es la validación del modelo a través de entrenamiento con datos reales de vuelos de la FAC y datos**

de *spoofing* simulados, de igual forma la implementación en una plataforma de computación de borde, como la Raspberry Pi 4B, demuestra la viabilidad técnica de una solución práctica y desplegable en entornos aeronáuticos.

Teniendo en cuenta la pregunta de investigación planteada "¿Cómo diseñar un modelo de machine learning (ML) que permita verificar la integridad de los datos recibidos en la banda L de sistemas GNSS que utilicen las aeronaves de la Fuerza Aeroespacial Colombiana (FAC), con el fin de mitigar las principales ciberamenazas a sus activos espaciales y garantizar la continuidad de las operaciones militares?", el trabajo de grado la aborda con un diseño metodológico que combina la investigación observacional y cuasiexperimental, logrando lo siguiente:

1. **Identificación y caracterización de amenazas: la base del diseño se inició con un estudio de la literatura actual para identificar los principales riesgos, vulnerabilidades y ciberamenazas en sistemas satelitales, en los segmentos terrestre y de usuario, se tuvo un eje central en la aplicación del framework SPARTA para modelar tácticas, técnicas y contramedidas, logrando de esta forma un marco estructurado para entender la superficie de ataque y las necesidades de mitigación.**
2. **Selección del algoritmo de ML: se identificó una base para el modelo en ciertas características de algunos algoritmos y se realizó una evaluación comparativa de estos algoritmos, seleccionando finalmente Random Forest por su rendimiento superior, con parámetros de navegación como latitud, longitud, velocidad y altitud.**

3. **Preparación y entrenamiento del modelo: para el diseño del modelo era importante tener una buena preparación de datos, por lo que se usaron datos de registros de vuelos reales de aeronaves de la FAC desde FlightRadar24 y se generó un conjunto de datos simulados de *spoofing* para el etiquetado necesario en el aprendizaje supervisado, posterior se realizó la validación y prueba, junto con la afinación de hiperparámetros y la validación cruzada, brindando una metodología robusta para asegurar la precisión del modelo.**

4. **Implementación en entorno de borde: era necesario poder ejecutar el modelo en un vuelo real, por lo tanto, para su ejecución se seleccionó una Raspberry Pi 4B, por su capacidad de procesamiento y flexibilidad para *edge computing*, donde se reciben y procesan señales en tiempo real, indicando la integridad de la señal mediante indicadores visuales (LEDs).**

El presente trabajo realiza un aporte significativo y concreto al campo de la ciberseguridad satelital aplicada, teniendo en cuenta los siguientes aspectos:

- **Solución practica para la verificación de la integridad en el segmento de usuario, mediante el prototipo funcional de un sistema de detección de anomalías de GNSS en tiempo real.**
- **Integración de ML en operaciones críticas, mostrando la viabilidad de incorporar técnicas avanzadas de inteligencia artificial en el entorno operativo de una aeronave, mediante el uso de computación de borde.**

- **Mitigación específica de una amenaza crítica, mediante la detección temprana de anomalías en la integridad de datos, previniendo la toma de decisiones erróneas por parte de la tripulación, fortaleciendo la seguridad operacional.**
- **Aplicación estructurada de marcos de Ciberseguridad, usando metodologías reconocidas como SPARTA y NIST.**

Para maximizar el impacto de este trabajo, se plantean las siguientes líneas futuras de investigación, para abordar temas relevantes en la ciberseguridad satelital:

1. **Ampliación del alcance de detección del modelo y su robustez:**
   - **Detección multi-amenaza: expandir las capacidades del modelo para detectar no ataques de *spoofing*, sino también otras ciberamenazas críticas a los sistemas GNSS, incluso poder ubicar una posible ubicación del emisor de la amenaza. Esto podría requerir el análisis de diferentes características de la señal o la integración de múltiples sensores.**
   - **Adaptación dinámica del modelo: investigar mecanismos que permitan al modelo de ML adaptarse a la evolución de las capacidades de ataque y defensa, así como a cambios en el entorno operativo.**
   - **Resistencia a la manipulación del modelo: explorar la robustez del modelo de ML frente a ataques de evasión o envenenamiento**

de datos, que podrían ser diseñados por adversarios para engañar al sistema de detección.

2. Integración con contramedidas activas y estrategias de recuperación:

- **Respuesta automatizada: ir más allá de la detección para diseñar e implementar mecanismos de respuesta automática o semiautomática ante la identificación de un ataque de *spoofing*. Esto podría incluir la activación de sistemas de navegación alternativos, la recalibración del PNT, o la emisión de alertas críticas a la tripulación o a los sistemas de control.**

3. Desarrollo de herramientas automatizadas para la gestión de riesgos:

- **Visualización y notificación interoperable: desarrollar interfaces y sistemas de notificación que integren las alertas de detección del modelo con los sistemas de aviónica de la aeronave y con los centros de comando y control en tierra, asegurando una conciencia situacional unificada y en tiempo real.**

4. Establecer directrices de aplicación de ciberseguridad y ciberdefensa en el dominio espacial:

- **Framework SPARTA: usar el framework para generar un estándar en la identificación de amenazas y posibles acciones de mitigación en los entornos que tengan conexión con el sistema espacial.**

- **Crear políticas a nivel nacional referentes a ciberseguridad satelital: es relevante establecer una ruta clara frente a las políticas a implementar para salvaguardar la operación espacial desde la ciberseguridad.**

Estas líneas de investigación e implementación permitirán que el trabajo actual evolucione hacia una solución más integral, adaptable y robusta frente al dinámico panorama de amenazas en los sistemas satelitales desde la perspectiva de ciberseguridad.

Referencias

Aceves-Fernandez, M. A. (Ed.). (2023). *Machine Learning and Data Minin*g. IntechOpen.

Adamczyk, M. (2024, mayo 7). *Current state of cybersecurity threat landscape in space sector* [Video]. YouTube. https://www.youtube.com/watch?v=dysNoQ4ACAg

Aerospace Corporation. (2022a). *Countermeasures | SPARTA*. https://sparta.aerospace.org/countermeasures/SPARTA

Aerospace Corporation. (2022b). *Defense-in-Depth for Space Systems*. https://sparta.aerospace.org/related-work/did-space

Aerospace Corporation. (2022c). *Erroneous Input, Technique EX-0013.02 | SPARTA.* https://sparta.aerospace.org/technique/EX-0013/02/

Aerospace Corporation. (2022d). *Execution, Tactic ST0004 | SPARTA.* https://sparta.aerospace.org/tactic/ST0004

Aerospace Corporation. (2022e). *Position, Navigation, and Timing (PNT) Jamming, Technique EX-0016.03 | SPARTA.* https://sparta.aerospace.org/technique/EX-0016/03/

Aerospace Corporation. (2022f). *Position, Navigation, and Timing (PNT) Spoofing, Technique EX-0014.04 | SPARTA.* https://sparta.aerospace.org/technique/EX-0014/04/

Agyemang, E. F. (2024). *Anomaly detection using unsupervised machine learning algorithms: A simulation study*. Scientific African, 26, e02386. https://doi.org/10.1016/j.sciaf.2024.e02386

Amr, T. (2020). *Hands-on machine learning with scikit-learn and scientific Python toolkits: A practical guide to implementing supervised and unsupervised machine learning algorithms in Python*. Packt.

Bailey, B. (2021). *Cybersecurity Protections for Spacecraft: A Threat Based Approach*. AEROSPACE REPORT NO. TOR-2021-01333-REV A.

Bailey, B. (2025, mayo). *Needed advancement for research and development in space cybersecurity*. The Aerospace Corporation. https://aerospace.org/sites/default/files/2025-05/AdvancementInSpaceCybersecurity_Bailey_20250506.pdf

Barua, T., Hiran, K. K., Jain, R. K., & Doshi, R. (2024). *Machine Learning with Python*. De Gruyter. https://doi.org/10.1515/9783110697186

Calian Group. (2025). *GNSS Constellations, Radio Frequencies and Signals—AT | Calian.* Advanced Technologies. https://www.calian.com/advanced-technologies/gnss/information-support/gnss-constellations-radio-frequencies-and-signals/

Delgado, T., & Carmona Tapia, C. (2024, mayo 7). *The security-by-design approach when building a new LEO constellation*. [Video]. YouTube. https://www.youtube.com/watch?v=YIL1V2WAzf0

De Luca, G. (2024, marzo 18). *Haversine Formula | Baeldung on Computer Science*. https://www.baeldung.com/cs/haversine-formula

Ear, E., Remy, J. L. C., Feffer, A., & Xu, S. (2023). *Characterizing Cyber Attacks against Space Systems with Missing Data: Framework and Case Study (No. arXiv:2309.04878)*. arXiv. https://doi.org/10.48550/arXiv.2309.04878

Edgar, T. W., & Manz, D. O. (2017). *Research methods for cyber security*. Syngress, an imprint of Elsevier.

Feldman, M., & Taylor, H. (2025). *Space Piracy: Preparing for a Criminal Crisis in Orbit. John Wiley and Sons.*

Garcia, D. (2017). *AFSCN Remote Tracking Station.* https://www.gps.gov/multimedia/images/GPS-control-segment-map.pdf

Hamill-Stewart, J. (2024, mayo 7). *Threats against satellite ground infrastructure: Retrospective analysis of attacks*. [Video]. YouTube. https://www.youtube.com/watch?v=ATFlNgy-XoA

Hamill-Stewart, J., & Rashid, A. (2024). *Threats Against Satellite Ground Infrastructure: A retrospective analysis of sophisticated attacks. Proceedings 2024 Workshop on Security of Space and Satellite Systems.* Workshop on Security of Space and Satellite Systems, San Diego, CA, USA. https://doi.org/10.14722/spacesec.2024.23087

Huang, H., Wang, P., Pei, J., Wang, J., Alexanian, S., & Niyato, D. (2025). *Deep Learning Advancements in Anomaly Detection: A Comprehensive Survey (No. arXiv:2503.13195)*. arXiv. https://doi.org/10.48550/arXiv.2503.13195

Johanna Niecknig, Wendel Lohmer, Max Gebhardt, Stefanie Grundner, Manuel Hoffmann, André Penzien, Steffen Kuntz, Miriam Goellner, Tarsicio López Delgado, Frank

Keck, Matthias Berger, & Sascha Fankhänel. (2023). *Technical Guideline BSI TR-03184 Information Security for Space Systems—Part 1: Space segment. 1.0.*

Joshi, S., Bairwa, A. K., Nandal, A., Radenkovic, M., & Avsar, C. (Eds.). (2022). *Cyber Warfare, Security and Space Research: First International Conference, SpacSec 2021, Jaipur, India, December 9–10, 2021, Revised Selected Papers (Vol. 1599).* Springer International Publishing. https://doi.org/10.1007/978-3-031-15784-4

Kavallieratos, G., & Katsikas, S. (2023). *An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space*. International Journal of Critical Infrastructure Protection, 43, 100640. https://doi.org/10.1016/j.ijcip.2023.100640

McCarthy, J., Li-Baboud, Y.-S., Brule, J., & Meldorf, K. (2023). *Foundational PNT profile: Applying the cybersecurity framework for the responsible use of positioning, navigation, and timing (PNT) services (No. NIST IR 8323r1; p. NIST IR 8323r1).* National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8323r1

Oakley, J. G. (2020). *Cybersecurity for Space: Protecting the Final Frontier.* Apress. https://doi.org/10.1007/978-1-4842-5732-6

Patel, A. A. (2019). *Hands-On unsupervised learning using Python: How to build applied machine learning solutions from unlabeled data (First edition, second release).* O'Reilly.

Periyasami, K., Katina, P. F., & Ramasamy, R. (Eds.). (2024). *Cyber space and outer space security. River Publishers.* https://doi.org/10.1201/9781003558118

Poirier, C. (2024, mayo 7). *The dynamics of cyber conflicts on space systems in the war in Ukraine*. [Video]. YouTube. https://www.youtube.com/watch?v=RS_WYP-MuNo

Raspberry Pi Ltd. (2020). *Raspberry Pi 4 Model B. Raspberry Pi.* https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

Rushanan, J. J., & Gillis, J. T. (2025). *Cryptography and satellite navigation. Artech House.*

Salerno, S. (2025). Tiny Machine Learning Quickstart: Machine Learning for Arduino Microcontrollers. Apress. https://doi.org/10.1007/979-8-8688-1294-1

Sarang, P. (2023*). Thinking Data Science: A Data Science Practitioner's Guide.* Springer International Publishing. https://doi.org/10.1007/978-3-031-02363-7

Scholl, M., & Suloway, T. (2023). *Introduction to cybersecurity for commercial satellite operations (No. NIST IR 8270; p. NIST IR 8270).* National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8270

Shahzad, S., Deane, F., Joiner, K. F., Qiao, L., & Suprun, E. (2024). *Cyber Resilience in Space Infrastructure: Strategies for Protecting Critical Space Assets*. SSRN. https://doi.org/10.2139/ssrn.5076427

Stanford University. (2023, octubre). *GNSS Interference Detection using ADS-B.* Stanford GPS Lab. https://waas-nas.stanford.edu/#/heatmapSpof/2024_10_23/

Tang, A. C. B. (2021). *A Review on Cybersecurity Vulnerabilities for Urban Air Mobility*. https://doi.org/10.2514/6.2021-0773

Wade, N. M. (2019). *Cyber 1: The cyberspace operations & electronic warfare SMARTbook : multi-domain guide to offensive/defensive CEMA and CO (First edition).* Lightning Press.

Winn, J. M., & Diethe, T. (with Bishop, C. M., Guiver, J., & Zaykov, Y.). (2024). *Model-based machine learning (First edition). CRC Press.*