RIESGOS DE LAS AERONAVES REMOTAMENTE TRIPULADAS BAJO EL ENFOQUE DE CIBERSEGURIDAD

Hurtado Cubillos, Alexander Eliecer
alexander-hurtado@upc.edu.co
Universidad Piloto de Colombia

***Resumen*— En el desarrollo de este artículo se realizará un estudio explicativo donde se abordarán temas relacionados con la gestión del riesgo (identificación de amenazas, establecer consecuencias por daños, asignar probabilidades de ocurrencias y determinar la severidad en caso de que ocurran) y como se puede mitigar las amenazas por medio del diseño de Objetivos de Seguridad Operacionales (OSO) a través de la metodología SORA (Specific Operations Risk Assessment) en un Avión Remotamente Tripulado, enfocado en la arquitectura técnica, las políticas y procedimientos regulatorios para Colombia establecidos por la Unidad Administrativa Especial de Aeronáutica Civil . Por otro lado se presenta un método gráfico de semaforización para la evaluación y un marco cuantitativo de gestión del riesgo cibernético, su probabilidad e impacto, y contramedida, adaptado al dominio de la ART, teniendo en cuenta las operaciones previas al vuelo, durante el vuelo y posteriores al vuelo, considerando varias amenazas, como ataques al hardware comprometido por diseño, software comprometido intencionalmente o debido a un diseño deficiente, computadora portátil de misión, comunicaciones inalámbricas, redes e instalaciones de almacenamiento de dato.**

***Abstract*— In the development of this article, an explanatory study will be carried out where issues related to risk management will be addressed (identification of threats, establishing consequences for damage, assigning probabilities of occurrences and determining the severity in case they occur) and how it can be mitigated. threats through the design of Operational Security Objectives (OSO) through the SORA methodology (Specific Operations Risk Assessment) in a Remotely Manned Aircraft, focused on the technical architecture, policies and regulatory procedures for Colombia established by the Administrative Unit Civil Aeronautics Special. On the other hand, a graphic traffic light method is presented for the evaluation and a quantitative framework for cyber risk management, its probability and impact, and countermeasure, adapted to the domain of ART, taking into account pre-flight and during-flight operations. and post-flight, considering various threats, such as attacks on hardware compromised by design, software compromised intentionally or due to poor design, mission laptop, wireless communications, networks and data storage facilities.**

Índice de Términos*— *Aeronave remotamente tripulada, Análisis de riesgos, Enlace de mando y control, SORA, riesgo, valoración del riesgo, vulnerabilidad.

I. INTRODUCCIÓN

De acuerdo con los últimos estudios realizados por empresas de consultoría e investigación de mercado, entre ellas Emergen Research, hace referencia al crecimiento del mercado de los vehículos aéreos no tripulados (UAV) a nivel mundial, el cual se valoró en 19,22 Billones de dólares en el año 2020 y se prevé que alcance los 56,18 Billones de dólares para el año 2027. El mercado de vehículos aéreos no tripulados actualmente cuenta con una alta demanda atribuida a su creciente aplicación en la inteligencia, vigilancia y reconocimiento (ISR), apoyo de combate, búsqueda y rescate, transporte, topografía y cartografía, extinción de incendios, gestión del tráfico, almacenamiento y procesamiento de datos [1].

Los aviones remotamente tripulados (ART) han aumentado exponencialmente en los últimos años, ocupando el espacio aéreo colombiano en cantidades cada vez mayores para proporcionar una gama de servicios de monitoreo, medición, detección, seguridad, vigilancia de infraestructuras. Esta tecnología y los riesgos asociados están en constante cambio, debido a este crecimiento de uso de los ART, tanto en el sector público como privado, ha aumentado los incentivos para los piratas informáticos, que se quieran apropiar de estos activos para obtener ganancias financieras, causar daños y / o crear inestabilidad, por lo tanto, el proceso de minimizar las vulnerabilidades sobre este tipo de activo se convierte en una carrera sin fin contra los ciberdelincuentes.

Los riesgos físicos (Colisiones contra aeronaves, contra estructuras terrestres, contra personas) de las ART han sido abordados de manera detallada por la Unidad Administrativa Especial de Aeronáutica Civil de Colombia a través de la resolución 04201 del 27 de diciembre del 2018 [2], sin embargo, en la actualidad los riesgos cibernéticos para los ART han recibido poca atención por parte de las entidades regulatorias colombianas.

II. MARCO TEÓRICO

Un vehículo aéreo no tripulado (VANT), del inglés UAV (Unmanned Aerial Vehicle), mas más apropiadamente RPAS (del inglés Remotely Piloted Aircraft System) o ART (Aviones Remotamente Tripulados, comúnmente conocido como dron hace referencia de acuerdo al diccionario de la real

española, a una aeronave que vuela sin tripulación, la cual ejerce su función de forma remota.

Un ART puede poseer varios tipos de tecnología de piloto automático, pero, en todo momento, el piloto remoto puede intervenir en la gestión del vuelo. Las características de performance de las aeronaves pueden diferir considerablemente de las aeronaves tripuladas tradicionales. Independientemente, el piloto remoto operará la aeronave con arreglo al reglamento del aire del Estado y del espacio aéreo en el cual opera la ART. Esto comprenderá el cumplimiento de las directivas e instrucciones proporcionadas por la dependencia de servicios de tránsito aéreo [3].

Estos vehículos aéreos cuentan con un componente de conducción mediante radio control, pero no se limitan solo a las instrucciones que reciben, pueden ejecutar actividades o tareas de forma autónoma, gracias a los sensores de nivel, altura, giroscopio y al Sistema de Posicionamiento Global (GPS) que se le incorpora su plataforma en función a los trabajos requeridos. Estos componentes les permiten a ART, tomar decisiones sin la intervención de un ser humano, convirtiéndolos en aparatos con cierto nivel de autonomía.

Esta definición proporciona una buena comprensión fundamental de qué es un ART y cómo se controla, sin embargo, para que el ART funcione, se requiere la interacción entre varios componentes. En términos generales, un ART se construye en términos generales con las partes que se muestran en Fig. 1.

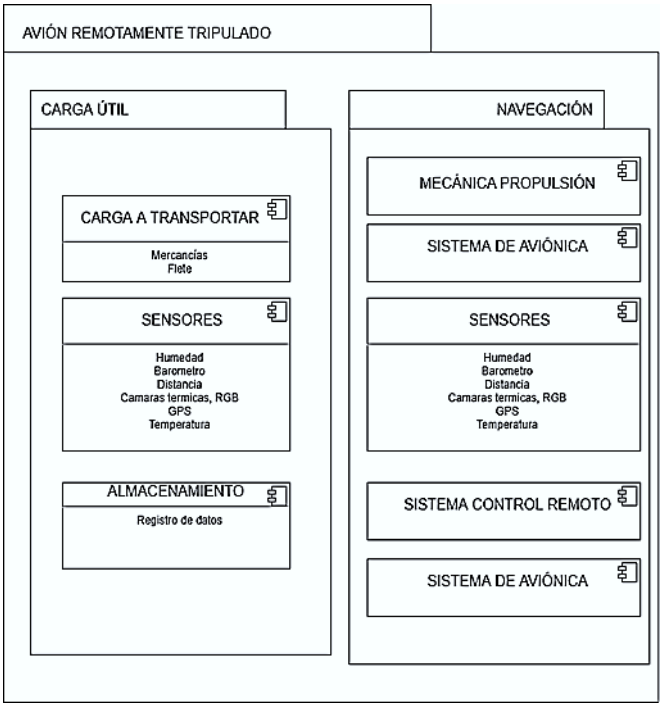

Fig. 1 Modelo General ART. Fuente: Construcción de los Autores

A. *Arquitectura de Comunicación*

La aeronave debe estar bajo el control de pilotaje de sólo una estación de piloto remoto a la vez. El sistema debería ser capaz de apoyar la transferencia automática de la autoridad de enlace de datos C2 entre estaciones de piloto remoto designadas utilizando un intercambio de datos digitales. Todos los canales de comunicación utilizados en ART son inalámbricos. Esto hace que el canal de comunicación sea vulnerable.

B. *Comando y Control Enlaces C2.*

El enlace de comando y control (C2) es el enlace de datos entre la aeronave pilotada a distancia y la estación de piloto remoto con el fin de gestionar el vuelo. Hay una variedad de posibles arquitecturas y consideraciones, por ejemplo el diseño, la seguridad y la gestión del C2 Link.

Radio línea de visión - RLOS (Radio Line Of Sight)

- El ART y el radio de tierra tiene comunicación directa entre sí.
- Una radio de tierra se puede separar del circuito integrado programable del ART con el piloto, con los limites línea de visión ya que el retardo adicional de la señal es pequeño

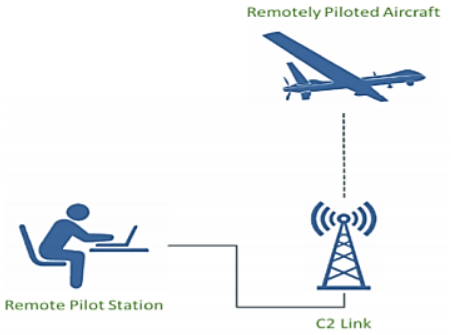

Fig. 2. Radio Line Of Sight – RLOS Fuente: Organización de Aviación Civil Internacional https://www.icao.int/

Radio Más allá de la línea de visión – BRLOS (Beyond Radio Line Of Sight).

- ART y el piloto no pueden comunicarse directamente porque la distancia entre ellos es muy grande en comparación con la curvatura de la tierra
- El retardo de la señal es significativamente más largo que para RLOS
- Los satélites se pueden utilizar para admitir el enlace C2

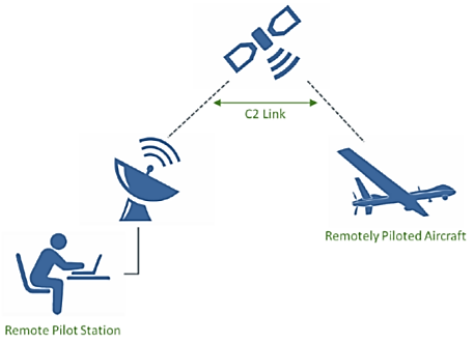

Fig. 3 Beyond Radio Line Of Sight – BRLOS. Fuente: Organización de Aviación Civil Internacional https://www.icao.int/

C. *Control.*

Proporciona funciones para que el circuito integrado programable modifique el comportamiento de ART por medio

de órdenes automáticas o manuales a través del piloto de la aeronave.

- Control de vuelo de ART: aerodinámica, propulsión, tren de aterrizaje, etc.
- Control del sistema de detección y evitación ART: transpondedor, ADS-B, etc.
- Permite la grabación de datos del vuelo, etc.

D. Comunicación

Proporciona funciones para que el circuito integrado programable modifique el comportamiento de ART por medio de órdenes automáticas o manuales a través del piloto de la aeronave.

III. Metodología Sora (Specific Operations Risk Assessment).

La Evaluación de Riesgos de Operaciones Específicas (SORA) es una metodología holística, centrada en las operaciones [4], propuesta por un grupo de expertos de las Autoridades de Aviación, JARUS (Joint Authorities for Rulemaking on Unmanned Systems) aceptada a nivel internacional. desarrollado para ayudar a la evaluación de los riesgos en la operación de un ART, presentando un marco genérico e integral para identificar los peligros, las amenazas, las mitigaciones y los objetivos de seguridad asociados a cualquier operación de un ART.

A. Modelo de riesgo SORA

La metodología SORA utiliza el modelo de Bowtie (corbatín) para ilustrar los escenarios de riesgo considerados. Los elementos principales de este modelo incluyen: (1) Peligro, (2) amenazas, (3) daños y (4) barreras.

Fig. 4 Amenazas-Peligros-Daños-Mitigaciones en la Metodología SORA. Fuente: Guía para operadores de RPAS (https://www.seguridadaerea.gob.es).

Identificación del daño: teniendo en cuenta el riesgo existente, se deben identificar los daños potenciales. Los principales daños a tener en cuenta son los siguientes:

- Lesiones fatales a terceros en tierra.
- Lesiones fatales a terceros en aire
- Daño a una infraestructura crítica

Identificación del peligro: se deben evaluar los peligros relacionados con la operación de un ART que pueden conducir a un daño. Se establece que el único riesgo relacionado con la operación de un ART que puede conducir a cualquiera de las tres categorías de daños identificados anteriormente es la operación del ART fuera de control.

Identificación de amenazas genéricas: se trata de la identificación de los hechos que pueden causar que ocurra un peligro si no se mantiene bajo control. Las principales amenazas potencialmente aplicables a cualquier operación de ART. Los daños se ubican en el lado derecho del peligro y representan las posibles consecuencias del peligro o el resultado final de los escenarios. En este momento, la metodología SORA considera solo dos tipos de Daños relacionados con la vida de la persona: “lesiones fatales a terceros en tierra”, “lesiones fatales a terceros en el aire”. Para mitigar el escenario de riesgo, se podrían aplicar varias Barreras (o medios de mitigación) [5]:

- Mitigaciones a los daños a personas en tierra.
- Mitigaciones estratégicas y tácticas para el riesgo de colisión con aeronaves tripuladas.
- Mitigaciones a las amenazas a través de los objetivos de seguridad operacional (OSOs).

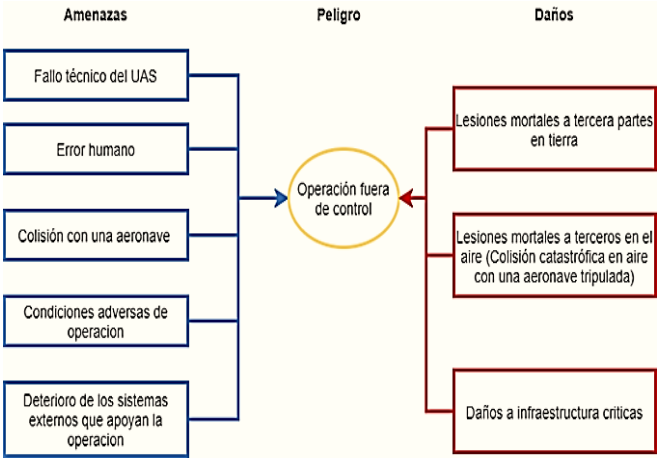

Fig. 5 Amenazas, peligros y daños ART según metodología SORA. Construcción de los autores en base Guía SMM de OACI

B. Extensión de la metodología SORA hacia la ciberseguridad

Las Autoridades Conjuntas para la Reglamentación de Sistemas No Tripulados (JARUS) han emitido la Evaluación de Riesgos de Operaciones Específicas (SORA) Anexo E (Cyber) el 4 de junio de 2021, como un documento de consulta externa. Este material ha sido desarrollado para proporcionar una guía sobre cómo mitigar las amenazas cibernéticas a la seguridad de las operaciones de UAS dentro del contexto de SORA y, como tal, está destinado a apoyar a todos los usuarios potenciales, desde operadores muy pequeños hasta organizaciones grandes y complejas. JARUS adoptó un lenguaje para comunicar mejor las ideas que quiere compartir con la comunidad de operadores.

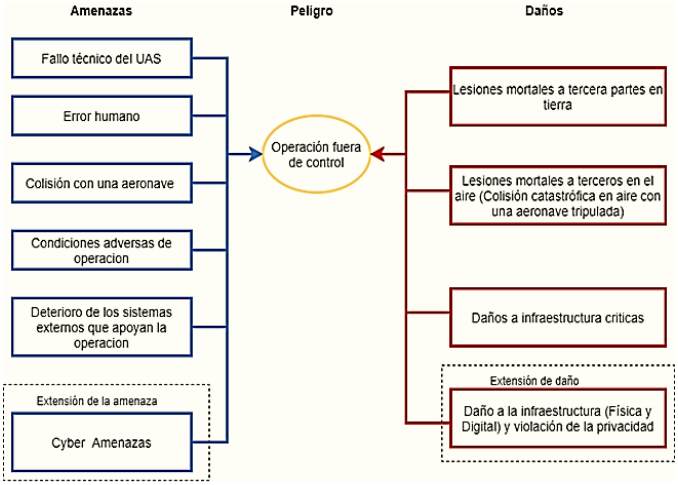

Fig. 6 Modelo de riesgo SORA extendido. Fuente: Construcción de los autores en base Guía SMM de OACI.

Según la metodología SORA Hay tres categorías amplias de requisitos de seguridad en la aviación:

- Seguridad de la aviación: los requisitos, distintos del cibernético, prescritos por los reguladores de la aviación para garantizar la seguridad.
- Ciberseguridad: Aquellos requisitos de ciberseguridad necesarios para proteger el core del negocio, la garantía de que la seguridad no se ve afectada por eventos cibernéticos o amenazas.
- Seguridad cibernética: Aquellos requisitos de ciberseguridad que han sido desarrollados por el gobierno en algunos casos, pueden ser prescritos por los entes reguladores de la aviación para Evitar que los eventos o amenazas cibernéticos tengan un impacto negativo en la Seguridad Nacional. Se aplica a menudo a sistemas de control de aeronaves (ACD), servicios de información de aerolíneas (AISD) y sistemas de control de tierra (GCD) es decir es decir, Gestión del tráfico aéreo (ATM) / Control de tráfico aéreo (ATC).

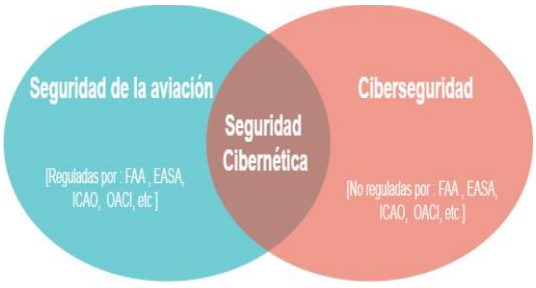

Fig. 7 Tres categorías de requisitos de seguridad en la aviación (SORA). Construcción de los autores en base SORA Anexo E.

IV. Análisis Preliminar De Amenazas

El análisis de Amenazas implica identificar, cuantificar y abordar riesgos asociados con los Aviones Remotamente tripulados bajos los tres principios de la seguridad de la información (Confidencialidad, Integridad, Disponibilidad), con el propósito que el grupo diseñador y Operador del sistema comprenda el perfil de las amenazas, tipos y riesgos de seguridad que puede comprometer el ART Quimbaya, con el fin de tener el conocimiento suficiente para definir los diferentes Objetivos de Seguridad Operacional (OSO) con un enfoque a la ciberseguridad.

A. Ataques a la Confidencialidad

Esta propiedad se ocupa principalmente del acceso no autorizado a la información y la forma más común de comprometer esta propiedad es la interceptación de información. Los componentes principales del modelo ART, son vulnerables a esta clase de ataque, por ejemplo, la Estación de Control, Enlace de comunicación y seres humanos (Grupo Diseñador y Operador). Las Amenazas relacionadas con la estación de control se basan principalmente en software mal intencionado (virus, malware, troyanos, Keylogers, etc.)

Por otro lado, la seguridad de los enlaces de comunicación entre varios componentes del sistema puede verse comprometida, a través de ataques a la red como: escuchas ilegales, suplantación de identidad, ataques entre capas [6] y ataques multiprotocolo. Para el Factor humano, la tendencia creciente de las redes sociales ha dado lugar a un aumento de nuevos tipos de amenazas. Algunos de estos incluyen ingeniería social.

B. Ataques a la Integridad

La integridad del Avión Remotamente Tripulado Quimbaya, podría verse fácilmente comprometida mediante dos operaciones básicas, es decir, mediante la modificación de datos existente o la fabricación de nuevos datos. La modificación tiene como objetivo alterar los datos durante el tránsito o el almacenamiento, mientras que la fabricación implica la creación de nuevas señales y su transmisión como si fueran las señales originales.

Por otro lado, los eventos naturales tales como rayos, lluvia, viento, etc., pueden causar cierta pérdida de integridad y agregar ruido no deseado a una señal de comunicación del ART. Sin embargo, estos eventos naturales son ocasionales, y la mayoría de los protocolos y equipos de comunicación intentan solucionar los problemas causados por ellos mediante un mecanismo de detección y corrección de errores [6].

C. Ataquesa a la Disponibilidad

Los ataques que comprometen la disponibilidad de los datos en los ART se pueden lograr de dos maneras; mediante el control del ART o la interrupción de la comunicación.

En el primer método de ataque, el atacante compromete el ART o la estación de Control, el atacante puede hacerse con el control del ART y modificar la funcionalidad de sus componentes. En el caso de los sensores por ejemplo la cámara, después de obtener el control del sistema, el atacante podría apagar la cámara. En el segundo método de ataque que compromete la disponibilidad del sistema, los atacantes interrumpen el enlace de comunicación entre el ART y el Estación de Control. Esto se puede hacer en diferentes formas, principalmente a través de interferencias y suplantación de señales.

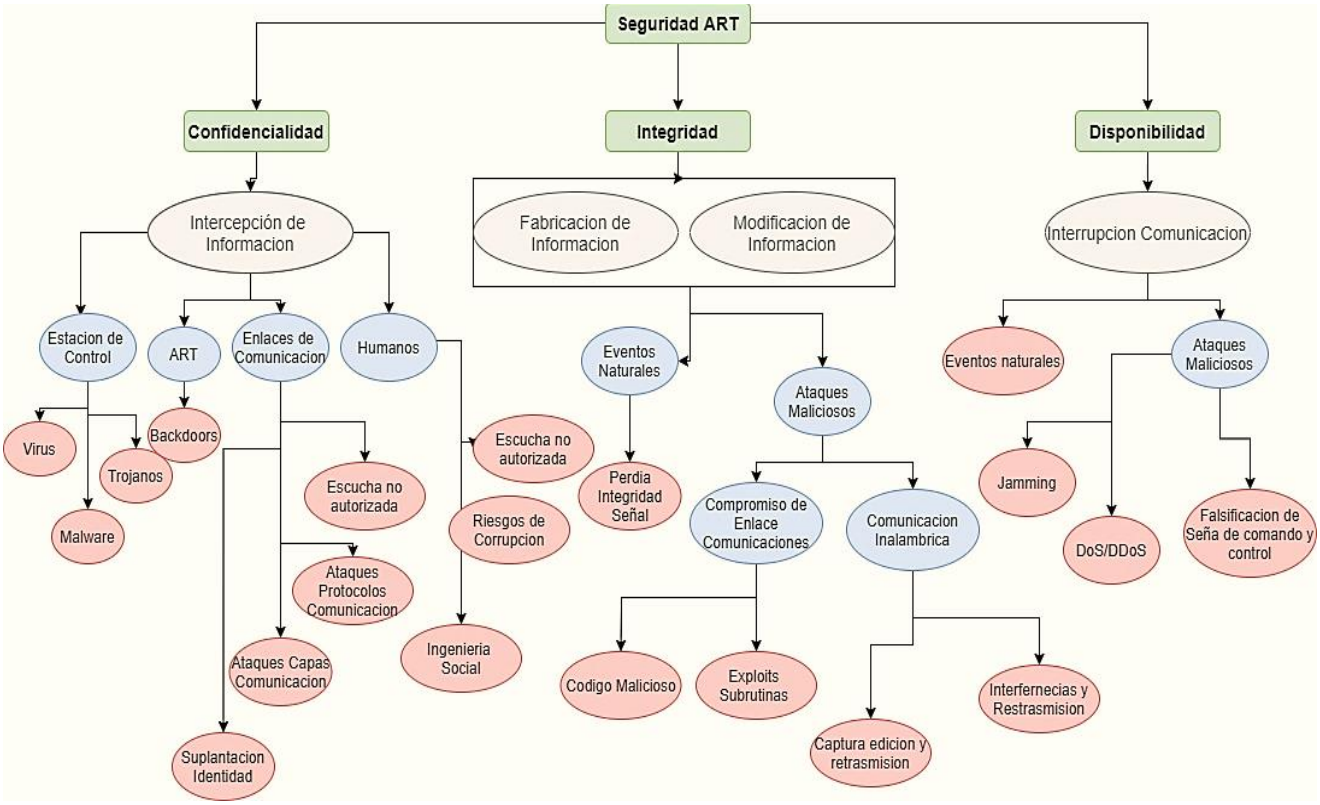

Fig. 8 Modelo de Amenazas para el ART (Confidencialidad, Integridad y Disponibilidad). Fuente: Cyber Security Threat Analysis and Attack Simulation for Unmanned Aerial Vehicle Network by Ahmad Y. Javaid.

V. Análisis De Riesgo Mediante El Método De Simulación

Atreves del software FreeCAD podemos crea el modelo del ART en tres dimensiones (ingeniería asistida por computadora, para la asistencia en ingeniería mecánica y el diseño de elementos mecánicos).

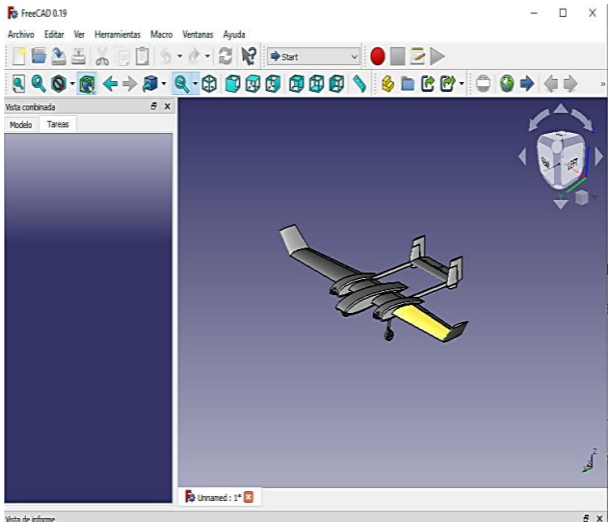

Fig. 9 Pantallazo Modelo ART Software FreeCAD. Fuente: Propia del Autor.

Podemos enfocamos en la simulación visual del ARP para poder evaluar los impactos de un ataque a través del software FlightGear.

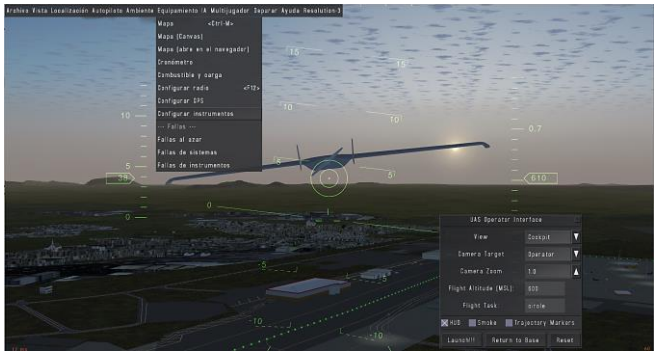

Fig. 10 Entorno de simulación de FlightGear que muestra los tipos de ataques aplicados. Fuente: Pantallazo Sistema FlightGear.

Para simular ataques en este entorno, indujimos fallas en varios sistemas para verificar las alertas generadas y la respuesta del sistema a esas fallas. Finalmente, medimos el nivel de daño causado por la falla al ART. Cabe señalar que la aeronave en estas simulaciones dependía por completo de los modelos existentes diseñados con el software FreeCAD. Por lo tanto, cualquier alerta generada debería formar parte del diseño del modelo ART. Se introdujeron tres tipos de ataques en este sistema, causando Falla de instrumentos, Falla de sistemas y Fallas al azar.

Podemos implementar módulos especializados e intégralos a FlightGear como UAVSim, el cual cuenta con un banco de pruebas de simulación bajo el código abierto OMNeT ++ y uno de sus módulos de código abierto desarrollados independientemente llamado INET, El diseño de red y los módulos de nivel superior están codificados en

NED, un lenguaje diseñado específicamente en OMNeT ++, mientras que el funcionamiento de nivel inferior se codifica mediante C + [8]. La interfaz gráfica interactiva cuenta con un banco de pruebas que permite cambiar varios parámetros. El banco de pruebas admite comunicación inalámbrica, capacidad de simulación componente ART y análisis de red detallado en niveles de protocolos. Además, cuenta con un banco de ataques dirigidos a diferentes componentes. La figura XX muestra la arquitectura de pruebas bajo tecnología OMNeT ++.

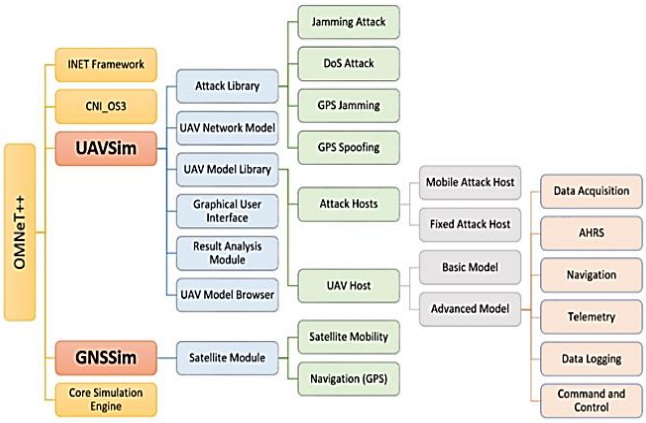

Fig. 11 UAVSim Módulos. Fuente: A. Y. Javaid, W. Sun, M. Alam, UAVSim: A simulation testbed for unmanned aerial vehicle network cyber security análisis.

La interfaz gráfica es uno de los submódulos más importantes de UAVSim, la cual facilita el uso para la simulación y reduce la experiencia técnica necesaria para comprender la arquitectura subyacente y la disposición del módulo.

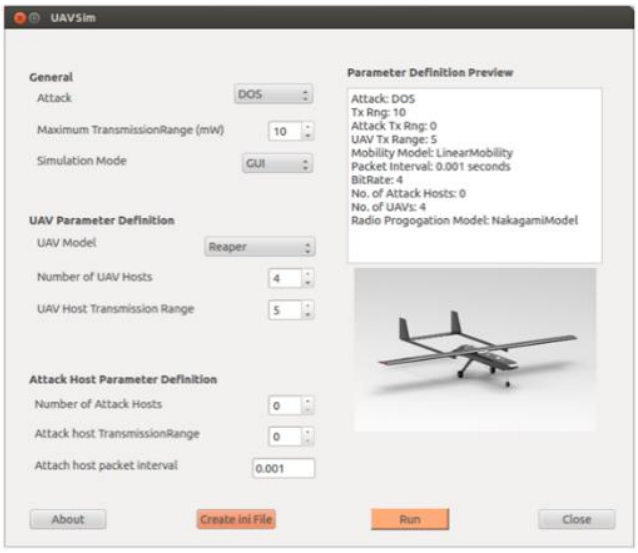

Fig. 12 GUI UAVsim. Fuente: https://github.com/kamikaze/uavsim.

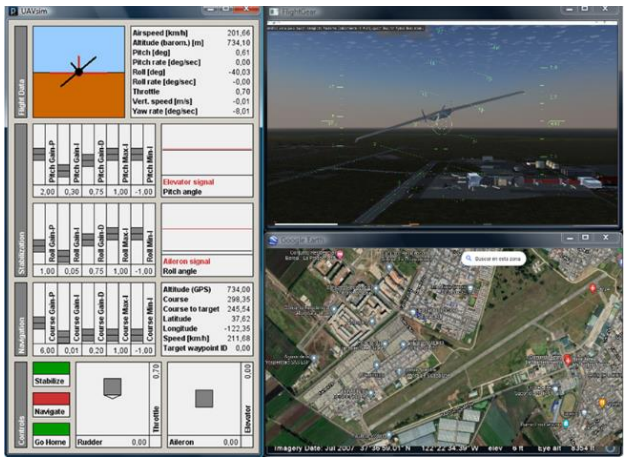

Fig. 13 Integracion UAVsim , FlightGear , Google Earth. Fuente: Pantallazo simulación

Uno de los usos más importantes de esta simulación fue en la siguiente fase de Evaluación de Riesgo e Impacto, donde el impacto y la probabilidad de diversas amenazas se definieron como varios niveles. Por último, también se calculó el riesgo que suponen esas amenazas.

VI. Riesgos por fase de operación (Antes del Vuelos y Durante el vuelo)

Se identifica los ataques asociados con los riesgos de realizar una operación de vuelo durante sus fases antes del vuelo y durante el vuelo. Los tipos de ataque se clasifican de acuerdo con el CAPEC (Common Attack Pattern Enumerations and Classifications).

El ART está compuesto por varios componentes o sub-sistemas los cuales pueden tener vulnerabilidades, en el entorno operativo se puede dar varios escenarios de ataques, Estos ataques tienen una probabilidad de éxito específica. Hay una relación la relación directa entre el impacto, probabilidad y el entorno operativo con el riesgo.

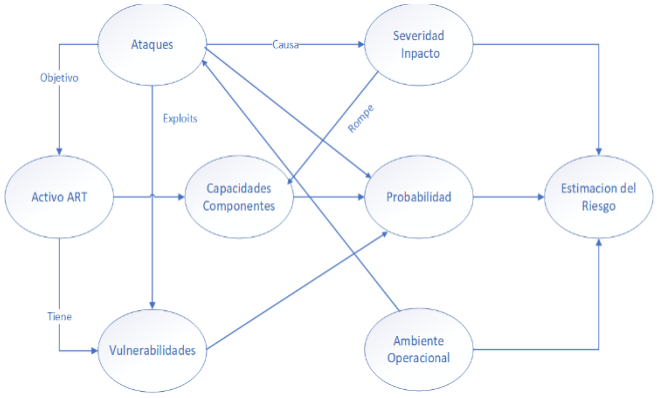

Fig. 14 Modelo Conceptual del Riesgo Propuesto para el ART. Fuente: propia

Se identifica los ataques asociados con el riesgo asociados a realizar una operación de cuelo durante sus fases antes del vuelo y durante el vuelo. Los tipos de ataque se clasifican de acuerdo con el CAPEC (Common Attack Pattern Enumerations and Classifications). La evaluación de riesgos

especifica la probabilidad y el impacto de los ataques. También se identifican las acciones actuales y recomendadas para mitigar el riesgo.

TABLA I RIESGO - MANIPULACIÓN ENLACES C2 COMANDO Y CONTROL

Identificación del ataque	
Tipo de Ataque (CAPEC) 216 Manipulación de canales de comunicación; 272 manipulación de protocolos; https://capec.mitre.org/data/definitions/216.html https://capec.mitre.org/data/definitions/272.html	
Dominios del ataque Comunicaciones, Software	
Fase de la Operación Previa al vuelo, Durante el Vuelo	
ºMecanismos de ataque 1.1 Ataque hombre en el medio 1.2 Abuso Funcionalidad existente 1.3 Intercepción del mensaje 1.4 Ataque de reflexión en el protocolo de autenticación 1.5 Manipulación de protocolos entre componentes 1.6 Suplantación de Sensores (Sensor Spoofing)	
Componentes y Ataques	Hardware: Sensores GPS (1.1, 1.2, 1.3, 1.5) Sensores Cámaras (1.2, 1.3, 1.5). Sensores de detección y evasión de obstáculos (1.2, 1.3)
	Funcionalidades de los componentes (Protocolos, Software, Algoritmos): • Enlace de transmisión de datos de la misión (1.1,1.4) • Enlace de trasmisión datos GPS (1.2, 1.3, 1.6)
Nivel de Riesgo	Región Tolerable

TABLA II RIESGO - INTERFERENCIAS SEÑALES C2 COMANDO Y CONTROL

Identificación del ataque	
Tipo de Ataque (CAPEC) 601 Interferencias 607 Obstrucción https://capec.mitre.org/data/definitions/607.html https://capec.mitre.org/data/definitions/601.html	
Fases de Operación: Durante el Vuelo	
Dominios del ataque Comunicaciones, Software, hardware	
Mecanismos de ataque 1.1 Interferencia enlace de comunicación 1.2 Interferencia GPS (GPS jamming) 1.3 Interferencia Sensores	
Componentes y Ataques	Hardware: Sensores GPS (1.2,1.3) Sensores Cámaras (1.1,1.3). Sensores de detección y evasión de obstáculos (1.3)
	Funcionalidades de los componentes (Protocolos, Software, Algoritmos): Enlace de transmisión de datos de la misión (1.1) Enlace de trasmisión datos GPS (1.2)
Nivel de Riesgo	Región Tolerable

TABLA III RIESGO - PÉRDIDA GPS

Identificación del ataque	
Tipo de Ataque (CAPEC) 607: Obstrucción 272: Manipulación de protocolo 117: Intercepción https://capec.mitre.org/data/definitions/607.html https://capec.mitre.org/data/definitions/272.htm https://capec.mitre.org/data/definitions/117.html	
Fases de Operación: Durante el Vuelo	
Dominios del ataque Comunicaciones, Software, hardware	
Mecanismos de ataque 3.1 Suplantación de GPS (manipulación de protocolo) 3.2 Interferencia de GPS (obstrucción) 3.3 Sniffing sensores (interceptación)	
Componentes y Ataques	Hardware: Sensores GPS (3.1, 3.3) Sensores Cámaras (3.1,3.3). Sensores de detección y evasión de obstáculos (3.1, 3.3) Magnetómetro(3.1,3.3)
	Funcionalidades de los componentes (Protocolos, Software, Algoritmos): Trasmisión de datos GPS (3.1, 3.3)
Nivel de Riesgo	Región Tolerable

TABLA IV RIESGO - PÉRDIDA DE ENLACE DE DATOS

Identificación del ataque
Tipo de Ataque (CAPEC) 607: Obstrucción 216 Manipulación del canal de comunicación 117: Intercepción https://capec.mitre.org/data/definitions/607.html https://capec.mitre.org/data/definitions/216.html https://capec.mitre.org/data/definitions/117.html
Fases de Operación: Durante el Vuelo
Dominios del ataque Comunicaciones, Software, hardware
Mecanismos de ataque

4.1 Interferencia del enlace de comunicación (obstrucción) 4.2 Ataque Hombre en el medio (Manipulación del canal de comunicación) 4.3 Interferencia de GPS (obstrucción)	
Componentes y Ataques	Funcionalidades de los componentes (Protocolos, Software, Algoritmos): Enlace de datos de la misión (ID 3.1, 3.2) Transmisión de datos GPS (ID 3.3)
Nivel de Riesgo	Región Tolerable

TABLA V RIESGO - COLISIÓN ART

Identificación del ataque	
Fases de Operación: Previa al vuelo y Durante el Vuelo	
Dominios del ataque Comunicaciones, Software, hardware	
Mecanismos de ataque 5.1 Ataque de integridad de hardware 5.2 Punto muerto forzado 5.3 Inserción de malware 5.4 Inyección 5.5 Explotación confianza-cliente 5.6 Omisión de autenticación 5.7 Interferencia enlace de comunicación 5.8 Intercepción datos GPS 5.9 Ataque Replay 5.10 Suplantación de sensores 5.11 Interferencias de sensores	
Componentes afectados	Hardware: Circuitos electrónicos de control de velocidad (5.1, 5.4) Motores (ID 5.1) •
	Funcionalidades de los componentes (Protocolos, Software, Algoritmos): • Controlador de vuelo (ID 5.1-5.5) • Percepción del ambiente (ID 5.2, 5.4, 5.6) • Piloto Automático (ID 5.2, 5.4, 5.6)
Consecuencias	Daños a personas Daños al dron Daños a infraestructura
Nivel de Riesgo	Región Intolerable

TABLA VI RIESGO - FALLA DEL SOFTWARE DEL PILOTO AUTOMÁTICO

Identificación del ataque	
Fases de Operación:	
Previa al vuelo y Durante el Vuelo	
Dominios del ataque Comunicaciones, Software, hardware	
Mecanismos de ataque 6.1 Integridad de la señal (inyección de comando) 6.2 Secuestro de sesión 6.3 Malwares (contaminar recurso) 6.4Inyección de código 6.5 Ataque a la integridad del hardware 6.6 Inyección de fallas de hardware 6.7 Inyección de comandos 6.8 Ataque hombre en el medio 6.9 Intercepción datos GPS 6.10 ataque Replay	
Componentes afectados	Hardware: Piloto Automático (6.3)
	Funcionalidades de los componentes (Protocolos, Software, Algoritmos): • Enlace de Misión (ID6.2, 6.8,-6.10) • Enlace de Comando y Control (ID 6.2, 6.7, 6.8, 6.10)
Nivel de Riesgo	Región Tolerable

TABLA VII RIESGO - FALLA EN LA ESTACIÓN DE PILOTO REMOTO

Identificación del ataque	
Fases de Operación: Previa al vuelo y Durante el Vuelo	
Dominios del ataque Comunicaciones, Software, hardware	
Mecanismos de ataque 7.1 Spyware 7.2 Malware 7.3 Omisión de autenticación 7.4 Explotación confianza Cliente 7.5 interceptación 7.8 Manipulación de infraestructura	
Componentes afectados	Hardware: Estacion de Control (ID 7.1, 7.2)
	Funcionalidades de los componentes (Protocolos, Software, Algoritmos): • Trasmisión de datos de GPS (ID 7.3 – 7.6) • Trasmisión de datos Comando y control (ID 7.3 – 7.6)
Nivel de Riesgo	Región Tolerable

VII. CATEGORIZACIÓN DE LOS POSIBLES ATAQUES

A. Ataques de software previa al vuelo

TABLA VIII TIPO DE ATAQUE CAPEC (624): INYECCIÓN

Nombre del ataque
Inyecciones de código
Componente (físico)
Firmware
Mecanismo de ataque (CAPEC)
https://capec.mitre.org/data/definitions/152.html
Inyección de parámetros
Inclusión de código
Inyección de recursos
Inyección de código
Inyección de comando
Ejecución local del código
Inyección de objetos
Inyección de tráfico
Inyección de fallas de hardware
Atributos de la seguridad afectados
Integridad
Riesgo
Falla del Software del piloto automático

TABLA IX TIPO DE ATAQUE CAPEC (115): OMISIÓN DE AUTENTICACIÓN

Nombre del ataque
Omisión de autenticación
Componente (físico)
Software, geographic information system software
Mecanismo de ataque (CAPEC)
https://capec.mitre.org/data/definitions/156.html
Suplantación del contenido
Suplantación de identidad
Suplantación de la ubicación del recurso
Spoofing
Manipulación del comportamiento humano
Atributos de la seguridad afectados
Autenticación, Confidencialidad
Riesgo
Perdida de Control del ART

B. Ataques de hardware previos al vuelo

TABLA X TIPO DE ATAQUE CAPEC (441): INSERCIÓN DE LÓGICA MALICIOSA

Nombre del ataque
Privación de descanso o sobrecarga de los sensores
Componente (físico)
Batería
Mecanismo de ataque (CAPEC)
https://capec.mitre.org/data/definitions/262.html
Manipulación de infraestructura
Manipulación de archivos
Configuración / manipulación del entorno
Ataque de integridad del software
Modificación durante la fabricación
Manipulación durante la distribución
Ataque de integridad de hardware
Inserción de lógica maliciosa
Contaminar recurso
Obstrucción
Atributos de la seguridad afectados
Integridad, disponibilidad
Riesgo
Pérdida de Control del ART por Agotamiento de la batería

TABLA XI TIPO DE ATAQUE CAPEC (638): MODIFICACIÓN DE FIRMWARE

Nombre del ataque
Ataque de integridad de hardware
Componente (físico)
GPS, Cámara, Sensores de Navegación
Mecanismo de ataque (CAPEC)
https://capec.mitre.org/data/definitions/262.html
Manipulación de infraestructura
Manipulación de archivos
Configuración / manipulación del entorno
Ataque de integridad del software
Modificación durante la fabricación
Manipulación durante la distribución
Ataque de integridad de hardware
Inserción de lógica maliciosa
Contaminar recurso
Obstrucción
Atributos de la seguridad afectados
Integridad
Riesgo
Choque ART, Fallo del piloto automático

TABLA XII TIPO DE ATAQUE CAPEC (624): INYECCIÓN DE FALLAS DE HARDWARE

Nombre del ataque
Pulso Electromagnetico
Componente (físico)
Barómetro, giroscopio, acelerómetro, antena
Mecanismo de ataque (CAPEC)
https://capec.mitre.org/data/definitions/152.html
Inyección de fallas de hardware
Atributos de la seguridad afectados
Integridad, disponibilidad
Riesgo
Choque ART, Fallo del piloto automático

C. Ataques de hardware durante vuelo

TABLA XIII TIPO DE ATAQUE CAPEC (272): MANIPULACIÓN DE PROTOCOLO

Nombre del ataque Suplantación de Sensores
Componente (físico) Sensor GPS, sensores para evitar obstáculos, sensor de cámara, sensor de infrarrojos, magnetómetro, barómetro
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/156.html Suplantación de contenido Suplantación de identidad Suplantación de la ubicación del recurso Spoofing Manipulacion comportamiento humano https://capec.mitre.org/data/definitions/148.html Suplantación de suma de comprobación Señales GPS falsificadas Suplantación de mensajes UDDI / ebXML
Atributos de la seguridad afectados Integridad
Riesgo Perdida GPS, Choque ART, Perdida Situación Operacional

TABLA XIV TIPO DE ATAQUE CAPEC (607): OBSTRUCCIÓN

Nombre del ataque Jamming Sensores
Componente (físico) Sensor GPS, sensores para evitar obstáculos, sensor de cámara, sensor de infrarrojos, magnetómetro, barómetro
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/262.html Interferencia Bloqueo
Atributos de la seguridad afectados Integridad, disponibilidad
Riesgo Perdida GPS, Choque ART, Perdida Situación Operacional

TABLA XV TIPO DE ATAQUE CAPEC (117): INTERCEPCIÓN

Nombre del ataque sniffing sensores.
Componente (físico) Sensor GPS, sensores para evitar obstáculos, sensor de cámara, sensor de infrarrojos, magnetómetro, barómetro
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/118.html Excavación Interceptación Ingeniería inversa Análisis de protocolo Obtención de información
Atributos de la seguridad afectados Confidencialidad
Riesgo Fuga de Información

D. Ataques de software durante vuelo

TABLA XVI TIPO DE ATAQUE CAPEC (441): INSERCIÓN DE LÓGICA MALICIOSA

Nombre del ataque Spyware
Componente (físico) Estación de Control del ART
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/152.html Inyección de parámetros Inclusión de código Inyección de recursos Inyección de código Inyección de comando Ejecución local del código Inyección de objetos Inyección de tráfico
Atributos de la seguridad afectados Integridad, Confidencialidad
Riesgo Perdida GPS, Choque ART, Perdida Situación Operacional

Nombre del ataque Malwares (Virus/worms/Trojan/Rootkit/)
Componente (físico) Estación de Control del ART
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/152.html Inyección de parámetros Inclusión de código Inyección de recursos Inyección de código Inyección de comando Ejecución local del código Inyección de objetos Inyección de tráfico
Atributos de la seguridad afectados Integridad
Riesgo Choque ART Errores o fallas en el piloto automático

E. Ataques sistemas comunicaciones durante vuelo

TABLA XVII TIPO DE ATAQUE CAPEC (607): OBSTRUCCIÓN

Nombre del ataque Interferencias en los enlaces de comunicación
Componente (físico) Enlace de transmisión de datos.
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/262.html Manipular los recursos del sistema Obstrucción Contaminar recurso https://capec.mitre.org/data/definitions/607.html Bloqueo Interferencia
Atributos de la seguridad afectados Disponibilidad
Riesgo Pérdida de enlace de datos,

TABLA XVIII TIPO DE ATAQUE CAPEC (594): INYECCIÓN DE TRÁFICO

Nombre del ataque Inyección de Comando
Componente (físico) Enlace de transmisión de control
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/152.html Inyección de parámetros Inclusión de código Inyección de recursos Inyección de código Inyección de comando Ejecución local del código Inyección de objetos Inyección de tráfico
Atributos de la seguridad afectados Integridad
Riesgo Choque ART, Error piloto automatico

Nombre del ataque Inyección de datos falsos
Componente (físico) Enlace de transmisión de control
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/156.html Suplantación de contenido Suplantación de identidad Suplantación de la ubicación del recurso https://capec.mitre.org/data/definitions/148.html Señales GPS falsificadas Suplantación de suma de comprobación Suplantación de mensajes UDDI / ebXML
Atributos de la seguridad afectados Integridad
Riesgo Choque ART, Error piloto automatico

TABLA XIX TIPO DE ATAQUE CAPEC (22): EXPLOTACIÓN DE LA CONFIANZA EN EL CLIENTE

Nombre del ataque Fuzzing
Componente (físico) Enlace de transmisión de control
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/223.html Fuzzing Fuerza bruta https://capec.mitre.org/data/definitions/28.html Mapeo de la aplicación
Atributos de la seguridad afectados Autenticación
Riesgo Choque ART, Error piloto automatico
Contramedidas actuales Firewall Manual de Monitoreo del vuelo Lista de verificación para manejar condiciones de emergencia.

TABLA XX TIPO DE ATAQUE CAPEC (272): MANIPULACIÓN DE PROTOCOLO

Nombre del ataque Aislamiento a nivel de red
Componente (físico) Enlace de transmisión de control
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/262.html Obstrucción Contaminar recurso Manipulación de infraestructura https://capec.mitre.org/data/definitions/161.html Envenenamiento de caché Falsificación de solicitudes
Atributos de la seguridad afectados Disponibilidad
Riesgo Pérdida de enlace de datos (pérdida de comunicación)

TABLA XXI TIPO DE ATAQUE CAPEC (607): OBSTRUCCIÓN

Nombre del ataque Interferencias señales GPS
Componente (físico) GPS
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/262.html Obstrucción Contaminar recurso

inserción de lógica maliciosa Manipulación durante la distribución Manipulación de archivos https://capec.mitre.org/data/definitions/607.html Interferencia Bloqueo
Atributos de la seguridad afectados Disponibilidad
Riesgo Perdida señal GPS, Choque ART, Error Piloto Automático

TABLA XXII TIPO DE ATAQUE CAPEC (272): MANIPULACIÓN DE PROTOCOLO

Nombre del ataque Aislamiento a nivel de red
Componente (físico) Enlace de transmisión de control
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/262.html Obstrucción Contaminar recurso Manipulación de infraestructura https://capec.mitre.org/data/definitions/161.html Envenenamiento de caché Falsificación de solicitudes
Atributos de la seguridad afectados Disponibilidad
Riesgo Pérdida de enlace de datos (pérdida de comunicación)

TABLA XXIII TIPO DE ATAQUE CAPEC (115): OMISIÓN DE AUTENTICACIÓN

Nombre del ataque Ataque de desautenticación
Componente (físico) Enlace C2 comando y control
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/262.html Obstrucción Contaminar recurso Inserción de lógica maliciosa https://capec.mitre.org/data/definitions/115.html Falsificación de solicitudes Contrabando de respuesta
Atributos de la seguridad afectados Disponibilidad
Riesgo Pérdida de enlace de datos

F. Ataques a la seguridad física durante el vuelo

TABLA XXIV TIPO DE ATAQUE CAPEC (507): ROBO FÍSICO

Nombre del ataque Robo y vandalismo
Componente (físico) ART
Mecanismo de ataque (CAPEC) https://capec.mitre.org/data/definitions/225.html Robo físico Evitando la seguridad física Abuso de privilegios
Atributos de la seguridad afectados Disponibilidad, confidencialidad
Riesgo Perdida del ART o componentes
Contramedidas actuales Protocolos de seguridad fisica **Recomendaciones** Implementar sistema de alarmas y de seguimiento GPS alterno al enlace de comando y control.

VIII. CONCLUSIONES

- Se realizo una investigación de diferentes metodologías para el análisis de riesgos bajo el contexto operacional de un avión remotamente tripulado, encontrado que la metodología que más se adapta a los estándares internacionales interpuestos por la OACI (Organización de Aviación Civil Internacional) es la metodología SORA (Evaluación de riesgos de operaciones específicas),elaborada por JARUS(Autoridades conjuntas para la elaboración de normas sobre sistemas no tripulados) , la cual ofrece una guía tanto al operador como a la autoridad competente para establecer si una operación con un ART puede llevarse a cabo de manera segura.
- A través de la metodología SORA se realizó el análisis de riesgos partiendo del diseño del ART, atreves de un análisis amenaza lo cual implico cuantificar y abordar riesgos asociados con los Aviones Remotamente tripulados bajos los tres principios de la seguridad de la información (Confidencialidad, Integridad, Disponibilidad).
- La concientización y la capacitación en ciberseguridad son fundamentales para garantizar que las partes interesadas dentro de las organizaciones comprendan claramente las metodologías y normatividad aplicable para el análisis de riesgos enfocados en la operación del ART.

REFERENCIAS

[1] Emergen Research, «Unmanned Aerial Vehicle Market,» Emergenresearch, New York, 2020.

[2] Aeronáutica Civil de Colombia, «Reglamentos Aeronáuticos,» aerocivil, Bogota, 2021.

[3] ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, «Circular 328, Sistemas de aeronaves no tripuladas (UAS),» icao, España, 2022.

[4] European Union Aviation Safety Agency, «Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation,» EASA, New York, 2019.

[5] Organización de Aviación Civil Internacional, «Manual de gestión de la seguridad operacional (SMM).,» OACI, España, 2021.

[6] W. Wang, Y. Sun, H. Li, and Z. Han,, Cross-layer attack and defense in cognitive radio networks, EEUU: IEEE, 2010.

[7] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, «Denial of service attacks in wireless networks: The case of jammers,» *IEEE Communications Surveys & Tutorials,* vol. 13, nº 2, p. 445, 2011.

[8] IEEE Globecom Workshops, UAVSim: A simulation testbed for unmanned aerial vehicle network cyber security analysis, EEUU: GC Wkshps, 2015.