Diseño de un Sistema C-UAS para la neutralización de UAS No identificados. Caso de estudio Aeropuerto El Dorado, Bogotá, Colombia

Peña Herrea, Thomas Felipe.
tfpenah@udistrital.edu.co
Universidad Distrital Francisco José de Caldas

Resumen La creciente amenaza de los Sistemas Aéreos no Tripulados (UAS), comúnmente conocidos como drones, a la seguridad y operatividad aeroportuaria es un desafío de gran importancia en Colombia. El vuelo de UAS cerca de aeropuertos exige la adopción de soluciones de defensa robustas para prevenir colisiones, la interrupción de operaciones aéreas y el riesgo de vigilancia no autorizada.

Para abordar esta problemática, se el diseño de un sistema C-UAS (Counter Unmanned Aircraft System) aplicado al Aeropuerto Internacional El Dorado de Bogotá, con enfoque en la neutralización de drones hostiles mediante interferencia (jamming). Se empleó el software HTZ Warfare, utilizando insumos de alta precisión como modelos digitales del terreno (DTM), bases de edificios (BGL), capas de clutter y modelos de propagación ITU-R P.452-18. A través de la simulación de cobertura de 13 jammers estratégicamente ubicados, se determinó un área efectiva de neutralización dentro del entorno aeroportuario. El sistema de detección por direction finding (DF) fue descrito a nivel teórico, aunque no implementado en la fase práctica. La validación por parte de un experto en telecomunicaciones resaltó una fiabilidad del 98% del diseño bloqueando señales de control a 2.4GHz dese los 2 a 120m de altura en toda el área del aeropuerto, sujeta a condiciones de campo y viabilidad operativa. Además, se aplicó una encuesta que evidenció una percepción favorable hacia la implementación de estos sistemas en aeropuertos civiles. Se concluye que la integración de herramientas de simulación de alta precisión permite evaluar soluciones viables y efectivas para la mitigación de amenazas UAS en infraestructuras críticas.

Índice de Términos C-UAS (Sistema antiaéreo no tripulado), Guerra electrónica, Espectro electromagnético, Jamming, Radiolocalización.

I. INTRODUCCIÓN

El rápido crecimiento y la constante evolución tecnológica de los sistemas aéreos no tripulados (UAS) han transformado diversas áreas civiles, comerciales y de entretenimiento, desde la entrega de paquetes hasta la vigilancia agrícola y el control de incendios. Sin embargo, la proliferación masiva de esta tecnología, que ya no es exclusiva de las autoridades militares o policiales, ha generado serios desafíos en términos de seguridad, protección y privacidad para la sociedad. Un fenómeno cada vez más alarmante es la serie de incidentes relacionados con drones que ocurren en las proximidades de instalaciones aeroportuarias [1]. Estos incidentes, que van desde simples avistamientos hasta colisiones y cierres de aeropuertos, demuestran que el uso indebido de los UAS constituye una amenaza real y en aumento.

Ejemplos concretos de esta amenaza son los cierres del aeropuerto de Gatwick en Londres en 2018, que afectaron a 140.000 pasajeros y costaron a las aerolíneas millones de libras, o el cierre del aeropuerto de Newark en 2019, que se estima causó 90 millones de dólares en pérdidas económicas. Estos sucesos subrayan que la interrupción de las operaciones aéreas no solo conlleva un riesgo de colisión, sino también costos innecesarios, retrasos y un impacto negativo en la reputación de las autoridades de aviación. El número de reportes de avistamientos de UAS no autorizados en el espacio aéreo controlado de EE. UU., documentados por la FAA, ha mostrado un aumento gradual y constante en los últimos años [4].

Ante este panorama, ha surgido una nueva área de investigación y desarrollo conocida como Counter-UAS (C-UAS), cuyo propósito es detectar y neutralizar estos drones ilegales o maliciosos. Un sistema C-UAS completo se define como un conjunto de tecnologías y metodologías que interactúan para llevar a cabo un proceso de defensa estructurado. Este ciclo de defensa consta de cuatro fases clave: prevención, detección, identificación/clasificación, decisión y neutralización [1]. Sin embargo, la defensa contra los UAS no es una tarea sencilla debido a las características únicas de estos dispositivos, especialmente los de categoría mini y micro (también conocidos como UAS LSS o "Low, Slow, Small"). Su pequeño tamaño, baja velocidad y reducida sección transversal de radar (RCS) los hacen difíciles de detectar para los sistemas de radar convencionales, que están diseñados para aeronaves más grandes y veloces. Además, la amenaza se agrava cuando estos drones operan en formaciones coordinadas, creando enjambres que buscan saturar la capacidad de respuesta de los sistemas de defensa.

La complejidad del problema requiere un enfoque multifacético, ya que la adopción de una única tecnología de detección o neutralización no es suficiente para la protección integral de un aeropuerto. Los sistemas C-UAS disponibles en

el mercado utilizan una combinación de sensores de detección, que incluyen radares, escáneres de radiofrecuencia (RF), sensores acústicos y cámaras visuales (tanto electro-ópticas como infrarrojas). De manera similar, las contramedidas para la neutralización se dividen en dos categorías principales: electrónicas (soft kill) y cinéticas (hard kill)[2].

A pesar de la existencia de estas tecnologías, su aplicación en entornos civiles como los aeropuertos presenta importantes desafíos. Las medidas de interferencia electrónica (jamming), por ejemplo, que son muy efectivas, pueden ser ilegales en muchos países y representan un riesgo de interferencia con señales de comunicación esenciales para la aviación, como los sistemas de aterrizaje instrumental (ILS). Además, algunas de las contramedidas soft kill, que se basan en la interrupción de las señales de control y GNSS, se vuelven inútiles cuando la amenaza proviene de drones que operan de manera autónoma, con una ruta de vuelo preprogramada y sin emisión de señales [4].

Ante la falta de estándares internacionales y la ambigüedad legal que rodea a estas tecnologías, es imperativo que los operadores aeroportuarios desarrollen planes de resiliencia y contingencia para proteger sus activos críticos. Este trabajo, en línea con los objetivos planteados en la literatura [1,3], busca proporcionar una visión integral de los riesgos que plantean los UAS y ofrecer recomendaciones para el diseño de sistemas C-UAS eficaces en instalaciones aeroportuarias. El objetivo es analizar los beneficios y las limitaciones de las tecnologías disponibles, y proponer un plan de acción de resiliencia para que los gestores aeroportuarios puedan aumentar la robustez de sus infraestructuras críticas contra estas amenazas aéreas.

Para lograrlo, el presente estudio se centrará en el diseño de un sistema C-UAS utilizando el software especializado HTZ Warfare, una herramienta avanzada para la planificación y optimización de sistemas antidrones. El diseño se enfocará en aeropuertos de Colombia, tomando en cuenta la geografía y las obstrucciones (clutter) de las ciudades locales para garantizar la precisión de la simulación. Este enfoque permitirá la simulación detallada de escenarios de amenaza y la evaluación del rendimiento de las contramedidas de guerra electrónica en un entorno real [5]. El trabajo se estructura en varias secciones. Tras esta introducción, se presenta un estudio de los incidentes de drones a nivel mundial. A continuación, se examinan las tecnologías de detección y neutralización de C-UAS. Posteriormente, se analizan escenarios de ataque contra la infraestructura aeroportuaria, se propone un plan de protección C-UAS para cada caso y se discuten las limitaciones de aplicabilidad de estos sistemas en el contexto de la aviación. Como cierre del estudio, el trabajo concluye con los hallazgos y las recomendaciones para mejorar la seguridad y la resiliencia en los aeropuertos.

II. TECNOLOGÍA UAS Y C-UAS

A. Definición, clasificación y amenazas de los UAS

Los Sistemas de Aeronaves No Tripuladas (UAS) comprenden la aeronave no tripulada y los elementos necesarios para su operación: estación de control en tierra (GCS), enlaces de comunicación (C2 y video), sensores embarcados y subsistemas de navegación y telemetría [1]. El incremento en disponibilidad tecnológica (baterías de alta densidad, sensores miniaturizados y módulos de comunicaciones) ha permitido que los UAS pasen de aplicaciones recreativas a usos comerciales y tácticos, con implicaciones directas para la seguridad de infraestructuras críticas como los aeropuertos [2], [3].

La literatura clasifica los UAS en categorías por peso, altitud operativa y alcance. Para efectos de planificación C-UAS, una tipología práctica es la siguiente:

TABLA I
CLASIFICACIÓN DE LOS DRONES [3]

Categoría	Peso (kg)	Altitud típica (m AGL)	Alcance	Ejemplos
Micro	< 2	< 140	< 5 km	DJI Spark, Mavic
Mini	2 25	< 1000	< 25 km	Inspire, Matrice
Small	25 150	< 1700	< 50 km	Shadow 200
Medium	150 600	< 3300	200 500 km	Griff 300
Large	> 600	> 3300	>1000 km	Boeing X-45

En aeropuertos, los UAS de categoría micro y mini son los de mayor incidencia por su disponibilidad comercial y baja huella logística. Los incidentes más relevantes a nivel global demuestran impactos operativos significativos: el cierre temporario del aeropuerto de Gatwick (Reino Unido) en 2018 y otras interrupciones ilustran la sensibilidad del entorno aeroportuario a incursiones UAS [3].

Las amenazas asociadas se agrupan en tres ejes: (i) seguridad aérea (riesgo de colisión y pérdida de integridad de aproximaciones y salidas), (ii) seguridad pública (transporte de cargas peligrosas, espionaje) y (iii) ciberseguridad/denegación de servicio (interferencia con sistemas remotos o captación de información). Estos vectores definen los requisitos de detección precoz, identificación fiable y mitigación selectiva que deben perseguir los sistemas C-UAS [1], [2].

B. Tecnologías C-UAS: detección, identificación y neutralización

La arquitectura típica de un C-UAS integra tres subsistemas: detección, identificación/seguimiento y mitigación. La tendencia actual es implementar soluciones híbridas que combinan sensores RF, radar, cámaras EO/IR y acústica con motores de fusión y clasificación.

1) Detección por radar

Los radares diseñados para misión C-UAS usan técnicas de alta resolución y micro-Doppler para diferenciar firmas de rotors y estructuras. Desafíos técnicos incluyen la baja RCS (Radar Cross Section) de plataformas pequeñas, ángulos de incidencia bajos y clutter cercano al suelo. Soluciones actuales incorporan procesamiento adaptativo y

redes de radares de corto/mediano alcance para obtener cobertura 360° y redundancia [4].

2) Detección RF y Direction Finding (DF)
La detección pasiva RF se basa en la monitorización del espectro en bandas asociadas a enlaces C2 (2.4 GHz, 5.8 GHz y frecuencias propietarios). El DF (direction finding) ofrece ángulos de llegada que, combinados con múltiples estaciones, permiten la intersección y geolocalización del transmisor (piloto o UAS). Herramientas de planificación (p. ej. HTZ Warfare, ATDI) permiten modelar cobertura, precisión y mínimos jammables para diseño de despliegue [5], [6].

3) EO/IR y sensores acústicos
Cámaras visibles e infrarrojas permiten la validación visual y la identificación por huella, complementando radar y RF. Los sensores acústicos detectan patrones de ruido de hélices, útiles en entornos poco ruidosos; su integración mejora la detección a corto alcance.

4) Identificación y fusión multisensor
La fusión multisensor (data fusion) estabiliza la toma de decisiones: algoritmos de machine learning integran series temporales RF, señales radar y correlación visual para clasificar objetos y reducir falsas alarmas. Sistemas con niveles de confianza permiten políticas de actuación escalonadas (alerta, seguimiento, mitigación) evitando medidas agresivas sin evidencia suficiente [1], [4].

5) Neutralización (soft-kill / hard-kill)
Las contramedidas se dividen en soft-kill (no cinéticas) y hard-kill (cinéticas). Las medidas *soft*, como el jamming de enlaces C2, GNSS spoofing y comandos de takeover, presentan la ventaja de no generar residuos físicos, lo cual resulta crucial en entornos civiles como aeropuertos. Sin embargo, existe el riesgo de interferencia colateral. Por otro lado, las medidas *hard*, como redes capturadoras o sistemas láser, implican riesgos físicos y logísticos que las hacen menos viables en zonas con alta densidad de operaciones aéreas. [7], [8].



Figura 1. Arquitectura conceptual de un sistema C-UAS (detección, identificación y neutralización).

C. Jamming: fundamentos, simulación y riesgos

El jamming es una técnica de denegación deliberada de enlaces radioeléctricos. Su efectividad depende de la potencia del jammer, la sensibilidad y ganancia del receptor objetivo, la distancia y la técnica de modulación empleada por el enlace legítimo.

1. Bandas y objetivos típicos
En UAS comerciales, las bandas más empleadas son 900 MHz (en ciertos mercados), 2.4 GHz y 5.8 GHz para control y video; GNSS L1 (1575.42 MHz) para navegación y posicionamiento. La identificación de las bandas críticas permite diseñar estrategias selectivas de jamming que reduzcan daño colateral [2], [5].

2. Modelos y fórmulas
Para estimar la potencia recibida se utiliza la ecuación de Friis (expresada en dB):

$$Pr(dBm) = Pt(dBm) + Gt(dBi) + Gr(dBi) - 20\cdot\log10(4\cdot\pi\cdot R/\lambda) \quad (1)$$

La métrica J/S (Jammer-to-Signal) se calcula como: J/S(dB) = Pj(dBm) - Ps(dBm). Valores de J/S entre +5 dB y +10 dB suelen ser suficientes para degradar enlaces de control convencionales, aunque sistemas con salto de frecuencia (FH) o spread-spectrum exigen mayores J/S o técnicas de bloqueo continuado [5].

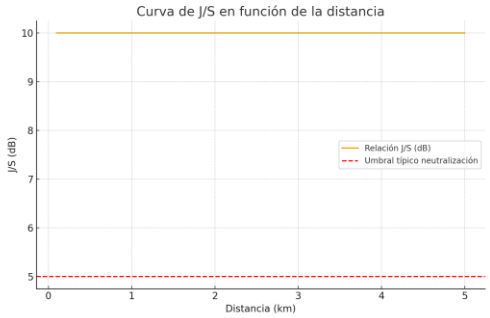


Figura 2. Relación Jammer-to-Signal (J/S) en función de la distancia, con umbral típico de neutralización.

3. Simulación y planificación
La fase de **simulación y planificación** conecta la teoría de propagación, jamming y geolocalización con el diseño práctico del despliegue C-UAS. Su propósito es obtener predicciones cuantitativas de cobertura y riesgo, optimizar emplazamientos y validar estrategias antes de ensayos en campo.
Herramientas profesionales (p. ej. HTZ Warfare, ATDI) permiten modelar terreno, edificaciones, mapas de clutter y realizar predicciones de cobertura para distintos tipos de antena (omnidireccional vs direccional) y potencias. Funciones útiles incluyen batch predictions (barridos de altura), mapas de mínimo jammable elevation y análisis sitio-a-sitio para evitar interferencias entre sensores y jammers [5], [6].

La predicción de cobertura radioeléctrica se basa en modelos que integran el modelo digital del terreno (DTM), clutter y geometría 3D de edificaciones, lo que determina pérdidas por difracción y zonas LOS/NLOS [4], [13]. La eficacia del jamming se expresa mediante la relación Señal/Interferencia (S/J), condicionada por la EIRP, el patrón de antena y el ancho de banda del emisor [5], [13]. En radar, la detección depende de potencia transmitida, RCS del objetivo y elevación de observación; además, la planificación debe considerar la posible degradación por interferencias radar↔jammer [15].

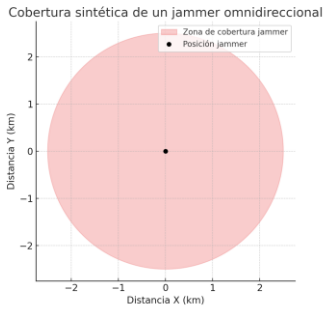


Figura 3. Cobertura sintética estimada de un jammer omnidireccional de alcance 2.5 km.

3.1) Propagación y cobertura radioeléctrica

La predicción de cobertura radioeléctrica integra el Modelo Digital del Terreno (DTM), los mapas de uso del suelo (clutter) y la geometría 3-D de edificios para estimar atenuación, difracción y zonas LOS/NLOS. Estos factores condicionan la detectabilidad de UAS por radar/RF y la eficacia del jamming a distintas alturas. Las herramientas de planificación permiten seleccionar modelos de propagación y definir grillas para obtener mapas de Field Strength (FS) por altura de objetivo [4], [13].

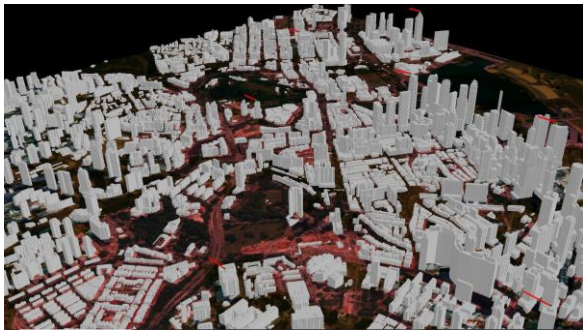


Figura 4. Geometría 3D de los edificios. [13]

3.2) Teoría del jamming (S/J y modos de interferencia

La eficacia de una contramedida RF se expresa en términos de la relación Señal/Interferencia (S/J o J/S). Un receptor deja de funcionar cuando la interferencia reduce la relación por debajo del umbral de protección específico del enlace. Los jammers se caracterizan por EIRP, patrón de antena, ancho de banda y modo operativo (fixed, wide-band diffusion, wide-band adaptive este último para enlaces FH). Las rutinas de planificación calculan mapas donde J/S supera umbrales definidos por el usuario. [13],.

3.3) Localización por DF y técnicas híbridas

La geolocalización por Direction Finding (DF) combina ángulos de llegada (AoA) y magnitudes (RSSI). La precisión depende de la geometría de la red DF, el error angular RMS de cada estación y el entorno (multipath). La fusión híbrida (mediciones reales + simulación) produce Localization accuracy maps probabilísticos, útiles para validar despliegues y priorizar pruebas en campo. [13], [14].

3.4) Modelado y análisis de radares

El rendimiento radar se modela con potencia transmitida, patrón de antena, RCS del objetivo y altura de observación. Es imprescindible evaluar cobertura por elevación, detección mínima por altura y la posible degradación debida a interferencias (jammer↔radar, radar↔radar). Las herramientas permiten además modelado bistático/multistático para diseños complejos. [13], [15].

3.5) Conceptos operativos y métricas

- **Field Strength (FS) / Coverage map:** mapa del nivel de campo en cada píxel; base para estimar detección y jamabilidad. [5], [13].



Figura. 4A. Ejemplo de mapa de Field Strength (FS). [13]

- **Minimum jammable elevation:** altura mínima en la que un jammer mantiene J/S ≥ umbral, función de topografía y clutter. [13].
- **Jammer-to-DF interference (site-to-site):** métrica que evalúa probabilidad de degradación de estaciones DF o radares por jammers util para mitigación de emplazamientos. [13], [15].
- **Localization accuracy map:** error de localización esperado (m) según geometría DF y propagación; usado para dimensionar número y posición de DF [14].
- **OTM (On-The-Move) path performance:** estimación de interceptación/jamming por waypoint; herramienta operativa para rutas móviles. [13].

3.6) Herramientas de HTZ Warfare / ATDI

3.6.1) Jamming (C.E.W.)

- **Jammer coverage:** genera mapas de áreas jammeadas para frecuencia/alturas

específicas, usando grid step y modelo de propagación conecta J/S teórica con representaciones espaciales [13].

- **Modos de jamming:** Fixed frequency; Wide band diffusion; Wide band adaptive (necesario para enlaces FH). Los parámetros temporales (channel scanning, time slot tolerance) condicionan el rendimiento ante FH [13].
- **Jammer power optimization:** calcula la potencia mínima por sitio para alcanzar un J/S objetivo, permitiendo balancear eficacia vs. impacto colateral. [13].

3.6.2) Localización y DF

- **DF coverage & Localization accuracy map:** evalúa cobertura angular y error de triangulación asociado a una red DF, soportando decisiones de redundancia y geometría [14].
- Hybrid localization from measurements: fusiona mediciones (RSSI/AoA) reales con simulación para construir distribuciones de probabilidad de la ubicación del transmisor; metodología reproducible para validar modelos [14].

3.6.3) Ruta móvil (OTM) y waypoint jamming

OTM / Waypoint jamming coverage calcula mapas jammeados por waypoint y evalúa la capacidad de neutralización a lo largo de una ruta móvil, permitiendo diseñar perfiles de potencia/antenado por waypoint [13].

3.6.4) Optimización de emplazamientos

Site search / Location optimization: analiza múltiples emplazamientos candidatos considerando cobertura objetivo y restricciones (LOS, interferencias). El sistema marca ubicaciones con riesgo (brown) que requieren mitigación adicional. [4], [13].

3.6.5) Radar toolbox

Funciones para radar coverage by elevation, análisis de radar interference, y modelado bistático/multistático, que permiten evaluar interacción radar↔jammer y coordinar frecuencias. [15].

3.6.6) Monitoreo y reporting

Bearing DB / Monitoring y WebView para almacenar bearings/mediciones y publicar mapas/reportes a Stakeholders; vital para debriefing y coordinación operativa. [13], [14].

3.7) Generación de capas vectoriales mediante SIG (QGIS)

Los Sistemas de Información Geográfica (SIG) permiten la creación, edición y análisis de datos espaciales georreferenciados. En el contexto de simulaciones radioeléctricas, estos datos son fundamentales para delimitar áreas de interés como pistas de aterrizaje, terminales o zonas perimetrales de infraestructura crítica. QGIS, un software SIG de código abierto, facilita la creación de capas vectoriales en formatos estándar como Shapefile (.shp), compatibles con herramientas de simulación como HTZ Warfare [20].

Para la generación de polígonos, se utiliza la funcionalidad "Crear nueva capa de archivo vectorial", donde se define el tipo de geometría (punto, línea o polígono), el sistema de referencia espacial (por ejemplo, EPSG:32618 - WGS 84 / UTM zona 18N para Colombia), y los atributos asociados. Luego, mediante la herramienta "Editar" y la opción "Añadir polígono", el usuario puede digitalizar manualmente zonas de interés basándose en imágenes satelitales o planos aeroportuarios [20].

Una vez generada y validada la geometría, la capa puede ser exportada y cargada en herramientas de simulación para superponerla al Modelo Digital del Terreno (DTM), datos de clutter o cobertura, y así acotar el área objetivo de análisis. Esta técnica mejora la precisión espacial en los cálculos de cobertura, localización de transmisores o evaluación de interferencias [20].

3.8) Supuestos, limitaciones y consideraciones metodológicas

- **Supuestos de RCS y perfiles UAS:** en ausencia de mediciones empíricas se emplean valores típicos de RCS y potencias TX; deben declararse porque condicionan alcances y detección radar. [15].
- **Modelos de propagación y resolución espacial:** la elección del modelo y del grid step (p. ej. 10 25 m en urbano) condicionan la fidelidad; justificar la elección en el estudio. [13].
- **Efectos dinámicos y FH:** la eficacia frente a FH depende de tiempos de escaneo y tolerancias temporales (ToA, launch delay, time-slot tolerance); simular estos parámetros evita sobreestimar el rendimiento del jammer. [13].
- **Interferencias colaterales y regulación:** el análisis debe incluir site-to-site para identificar vulnerabilidades (p. ej. ILS, VHF ATC);

cualquier emisión intencional exige permisos regulatorios y planes de coexistencia. [10], [11], [13].

3.9) Propuesta de estructura metodológica

- Definir supuestos: perfiles UAS (RCS, TX), bandas (p. ej. 900 MHz, 2.4 GHz, 5.8 GHz, GNSS L1), umbral J/S objetivo y grid step. [13], [15].
- Importar capas geoespaciales: DTM, edificios 3-D, clutter, vectores (KMZ/SHP). [13].
- Generar mapas base: Field Strength, radar coverage, DF coverage para alturas y rutas de interés. [13], [15].
- Analizar jamming: calcular minimum jammable elevation, batch predictions sobre rangos de altura y realizar jammer power optimization por sitio. [13].
- Simular OTM / waypoints: evaluar cobertura y J/S por waypoint para rutas móviles (OTM). [13].
- Evaluar site-to-site: verificar que jammers no degraden estaciones DF, radares o radioayudas; coordinar frecuencias y ajustar emplazamientos. [13], [15].
- Validación híbrida: integrar mediciones de campo (bearings, RSSI, observaciones EO/IR) en Hybrid localization from measurements y documentar desviaciones entre simulación y medición. [14].

3.10) Parámetros de simulación (HTZ/ATDI)

TABLA 2
RANGOS DE PARÁMETROS DE SIMULACIÓN

Parámetro	Valor típico / rango	Justificación
Grid step	10 25 m (urbano), 50 100 m (rural)	Determina resolución espacial de mapas FS y jamming.
Modelos de propagación	ITU-R P.452, Deygout/Delta-Bullington	Modelos recomendados para clutter y difracción.
Alturas de objetivo	30 m, 60 m, 120 m, 300 m	Cobertura típica de UAS en proximidad a aeropuertos.
Bandas simuladas	900 MHz, 2.4 GHz, 5.8 GHz, GNSS L1	Bandas usadas por UAS comerciales.
RCS asumido (radar)	0.01 0.05 m² (micro), 0.1 0.5 m² (small)	Valores típicos para simulaciones.
Umbral J/S	+5 dB (mín), +10 dB (robusto)	Umbrales para degradar enlaces C2 o GNSS.
Potencia jammer (EIRP)	30-45 dBm (1-30 W)	Valores típicos en simulaciones controladas.
Modo jammer	Fixed, Wide-band diffusion, Wide-band adaptive	Selección según tipo de señal objetivo (FH, DSSS).
Tiempo de escaneo FH	10-50 ms	Parámetro crítico para neutralizar enlaces con salto de frecuencia.
Validación híbrida	Bearings, RSSI, EO/IR	Combinar medición real con simulación para validar modelos.

4. Riesgos y mitigación del impacto colateral

El principal riesgo operacional de jamming es la interferencia no deseada sobre servicios críticos (VHF ATC, ILS, radar primario/secundario y redes públicas). Por ello, las actividades de jamming en entorno civil requieren permisos, planes de coexistencia y mecanismos de apagado de emergencia. Estudios muestran que la optimización de ubicación y potencia de jammers puede reducir significativamente la probabilidad de afectar radio ayudas [5], [7].

D. Marco legal y tendencias en Colombia

En Colombia la operación de UAS y el uso del espectro están regulados por la Aeronáutica Civil (Aerocivil) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), vía la Agencia Nacional del Espectro (ANE). La normativa vigente exige registro, certificación de operadores y prohíbe vuelos en zonas restringidas alrededor de aeropuertos salvo autorización expresa [10], [11].

3. Regulación Aerocivil (operación de UAS)

La Aerocivil ha emitido resoluciones y guías (p. ej. Resolución 04201/2018 y material incluido en el RAC) que especifican requisitos de operación, zonas prohibidas y procedimientos de autorización para actividades especiales. Las operaciones en el entorno de aeródromos requieren coordinación con la autoridad aeronáutica y, en general, la imposición de radio de seguridad alrededor de pistas limita severamente la posibilidad de vuelos no autorizados [10].

4. Reglamentos Aeronáuticos de Colombia (RAC 100)

En Colombia, la regulación de los sistemas de aeronaves no tripuladas (UAS) está definida por los Reglamentos Aeronáuticos de Colombia (RAC 100), expedidos por la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC). Este marco establece categorías de operación,

requisitos de idoneidad, autorizaciones y limitaciones de vuelo, con especial atención a la seguridad operacional y a la protección del espacio aéreo cercano a infraestructuras críticas.

Uno de los puntos más estrictos del RAC 100 son las restricciones de vuelo en torno a aeropuertos. El artículo 100.315 prohíbe la operación de UAS dentro de un radio de 9 km medidos desde el punto de referencia del aeródromo (ARP). No obstante, se contempla una excepción: entre los 6 y 9 km del ARP, los vuelos en categoría abierta pueden realizarse, siempre que no se exceda una altura de 200 pies (61 metros) AGL respecto al umbral más bajo de la pista [16]. Esta medida busca reducir riesgos de colisión con aeronaves tripuladas en fases críticas de despegue y aterrizaje.

Además, se establecen restricciones complementarias como:

- Prohibición de vuelos en un radio de **3 km de helipuertos**.
- Limitaciones para vuelos sobre **zonas de no vuelo (ZNVD)**, áreas de entrenamiento y zonas peligrosas.
- Necesidad de **coordinación previa con ATS (Air Traffic Services)** en operaciones específicas que se desarrollen dentro del área de influencia de aeródromos, bajo esquemas de *Collaborative Decision Making (CDM)*

En cuanto a las **tendencias regulatorias**, la Aerocivil ha venido armonizando la normativa con las recomendaciones de la **OACI**, especialmente en lo relativo a operaciones **BVLOS** (Beyond Visual Line of Sight) y vuelos con fines comerciales. Se prevé una expansión hacia el concepto de **"dronpuertos"** y corredores aéreos designados para logística, aunque siempre bajo autorizaciones específicas [16] De forma complementaria, fuentes internacionales de asesoría a operadores recreativos y comerciales destacan que en Colombia es obligatorio:

- Mantener siempre el dron dentro de línea de vista (VLOS).
- No superar los **400 pies AGL** salvo autorización especial.
- Obtener capacitación aprobada por Aerocivil antes de volar drones de uso comercial.
- Evitar vuelos en áreas urbanas densamente pobladas, eventos públicos y zonas militares [16], [17].

Para concluir, la regulación colombiana establece un **marco restrictivo en torno a aeropuertos y helipuertos**, buscando proteger la seguridad operacional del tráfico aéreo civil. Al mismo tiempo, se observa una **apertura progresiva hacia usos comerciales y logísticos**, pero siempre bajo condiciones estrictas de certificación, coordinación con ATS y cumplimiento de limitaciones técnicas y geográficas.

5. Gestión del espectro: MinTIC / ANE

El MinTIC regula el uso del espectro y establece que equipos emisores e inhibidores deben cumplir requisitos técnicos y solo pueden emplearse con autorizaciones explícitas. La ANE gestiona asignaciones y permisos temporales; el uso de bloqueadores comerciales está sujeto a prohibición o a excepciones bajo protocolos de seguridad y defensa [11].

6. Procedimiento para ensayos y despliegues controlados

Para realizar ensayos que involucren jamming en Colombia se recomienda el siguiente procedimiento: (i) simulación previa detallada (HTZ/ATDI) para acotar potencia y zonas afectadas; (ii) solicitud formal de permiso de uso temporal del espectro ante MinTIC/ANE; (iii) coordinación y autorización operativa con Aerocivil; (iv) implementación de plan de coexistencia electromagnética y protocolos de apagado de emergencia [5], [10], [11].

7. Uso de inhibidores, bloqueadores y amplificadores (jammers)

El espectro radioeléctrico es un bien público y su uso está regulado por el MinTIC y la Agencia Nacional del Espectro (ANE). En Colombia la Resolución 2774 de 2013 (y sus modificaciones) regula explícitamente la instalación y uso de inhibidores y bloqueadores de señales radioeléctricas (IBSR) y de amplificadores de señal (ASR). Su regulación es particularmente relevante para cualquier solución C-UAS que emplee jamming (soft-kill) porque estas tecnologías emiten energía radioeléctrica que puede afectar servicios aeronáuticos y de telecomunicaciones [17].

7.1) Puntos Importantes de la Resolución MinTIC 2774/2013

- **Prohibición general:** se prohíbe la instalación y uso de inhibidores/bloqueadores salvo en los casos y bajo las autorizaciones que la resolución establece; el uso no autorizado se considera clandestino y acarrea decomiso y sanciones administrativas o penales [17].
- **Autorización para ubicaciones fijas confinadas:** el MinTIC puede autorizar (temporal o permanente) el uso de IBSR en ubicaciones fijas confinadas para entidades públicas o del sector financiero que justifiquen la necesidad; la solicitud debe presentarse con antelación mínima y acompañarse de un expediente técnico detallado. Entre los requisitos técnicos exigidos están: diseño RF avalado por ingeniero profesional, especificaciones de EIRP, bandas y patrones de antena, mapas de cobertura de intensidad de señal (mínimo 500 m alrededor del sitio), contornos de propagación y cálculos que demuestren que no habrá afectación fuera del sitio autorizado [17].
- **Autorizaciones especiales para organismos de seguridad del Estado:** organismos de seguridad

pueden usar IBSR (fijos o móviles) en el ejercicio de sus funciones; la ANE y las autoridades competentes reglamentan procedimientos y protocolos para su uso y control [17].

- **Vigilancia y decomiso:** la ANE es la encargada de vigilar y controlar el espectro; el uso no autorizado da lugar a decomiso de equipos y sanciones según la Ley 1341 de 2009 [17].

7.2) Implicaciones para sistemas C-UAS con jamming en aeropuertos

- **Necesidad de permisos y diseño técnico riguroso:** cualquier despliegue incluso de ensayo de jammers en entorno aeroportuario requiere autorización previa del MinTIC/ANE (por el uso del espectro) y coordinación/permiso de la Aerocivil/UAEAC (por seguridad operacional). La documentación típicamente debe incluir mapas de cobertura, cálculos de EIRP, contornos de intensidad, y medidas de mitigación para evitar impacto en ILS, VHF, radar secundario/primario y comunicaciones ATC [16], [17].
- **Confinamiento y contingencias:** si se permite el uso, los permisos suelen exigir operación en ubicaciones confinadas, límites de potencia, filtros y directividad de antenas, monitoreo de emisiones y protocolos de apagado de emergencia (kill-switch) que permitan cesar la emisión inmediatamente ante evidencia de afectación. El solicitante debe presentar mediciones de verificación post-puesta en marcha [18].
- Riesgo de afectación a radioayudas y telecomunicaciones: los jammers pueden degradar GNSS L1, enlaces C2 (2.4/5.8 GHz), y servicios públicos (Wi-Fi, LTE), por lo que el análisis site-to-site y la modelación de contornos de intensidad con herramientas de planificación es obligatoria para evaluar riesgos y demostrar que la operación es compatible con la seguridad aérea [16], [18].
- Diferenciación legal entre actores: organismos de seguridad del Estado y la ANE tienen facultades específicas para usar IBSR en ciertos contextos; operadores privados solo pueden hacerlo con permisos explícitos y sujetos a condiciones estrictas. La normativa prevé sanciones, decomiso y responsabilidades en caso de afectación de servicios [18].

7.3) Recomendaciones operativas y regulatorias

- Diseñar pruebas en ambiente controlado: realizar simulaciones (HTZ/ATDI) y pruebas en ubicaciones confinadas autorizadas, con mapas de cobertura y umbrales J/S claramente definidos antes de solicitar permiso de emisión [16], [17].
- Coordinar con Aerocivil y ANE/MinTIC: presentar el plan operativo completo a ambas autoridades (impacto sobre radioayudas, contornos, mitigaciones, planes de apagado de emergencia) [17].
- Medición y verificación post-despliegue: incluir mediciones en tiempo real y reportes posteriores al inicio de funcionamiento para acreditar que las emisiones no afectan servicios adyacentes [17].

8. Aeropuerto Internacional El Dorado

El Aeropuerto Internacional El Dorado (códigos IATA: BOG, ICAO: SKBO) es el principal aeropuerto de Colombia y uno de los más transitados de América Latina [19],[20]. Ubicado en Bogotá, en las localidades de Fontibón y Engativá y ligeramente extendido al municipio de Funza, se encuentra aproximadamente a **12-13 km al occidente del centro urbano** [19]. Su elevación es de **2 548 metros sobre el nivel del mar**, lo que introduce consideraciones particulares en propagación y densidad atmosférica para análisis radioeléctricos [19]. El aeropuerto dispone de **dos pistas de 3 800 metros** de longitud con pavimento asfáltico, además de modernas terminales de pasajeros y una terminal de carga que lo posicionan como un HUB estratégico de conexiones nacionales e internacionales [19]. Durante el año 2024, movilizó más de **45 millones de pasajeros** y cerca de **809.000 toneladas de carga**, lo que subraya su importancia logística tanto para Colombia como para la región [19]. Dada su localización urbana y su gran tránsito aéreo, constituye un escenario realista y exigente para el diseño de sistemas C-UAS con interferencia radioeléctrica.



Figura 5. Plano esquemático del Aeropuerto Internacional "El Dorado", con disposición de las pistas Norte (13L/31R) y Sur (13R/31L), incluyendo sus dimensiones y separación entre ejes centrales [19].

III. DISEÑO Y SIMULACIÓN

A. Cálculo de Link Budget

Para validar cuantitativamente el desempeño del sistema de neutralización por jamming diseñado en el Aeropuerto Internacional El Dorado, se realizó un análisis de presupuesto de enlace (*Link Budget*). Este cálculo permite estimar el nivel de señal recibida (**Pr**) en distintos rangos, tomando como base la potencia transmitida y las características del sistema.

Se tienen los siguientes parámetros del sistema:

TABLA 3
PARÁMETROS DEL SISTEMA

Parámetro	**Valor**
Potencia transmitida (Pt)	50 W = 47 dBm
Ganancia antena transmisora (Gt)	6 dBi
Ganancia antena receptora (Gr)	0 dBi
Frecuencia de operación	2.4GHz

- Pérdida por espacio libre (FSPL)

$$L_{fs} = 32.44 + 20log_{10}(f_{MHz}) + 20log_{10}(d_{km}) \quad (2)$$

Aplicamos esta fórmula para 2 distancias diferentes basados en la distancia que va a subir cada Jammer, que es de 0.5km a 1km.

TABLA 4
RESULTADOS LINK BUDGET

Distancia	**FSPL (dB)**	**Pr(dBm)**
0.5 km	87.46	-34.46
1 km	93.52	-40.52

Con base en la documentación técnica y pruebas previas, se definieron tres niveles de confianza de interferencia según el valor de Pr (nivel recibido en el receptor del dron).

TABLA 5
RANGOS DE NIVELES DE RECEPCIÓN

Nivel (dBm)	**Confianza de jamming**
>= -120	Zona segura (sin jamming)
>= -40	95% Jamming Confidence
>= -35	99% Jamming Confidence

B. Delimitación espacial en QGIS

Para delimitar correctamente el área del Aeropuerto Internacional El Dorado y definir las zonas de exclusión y posibles emplazamientos para jammers, se utilizó QGIS como herramienta de preprocesamiento cartográfico. En QGIS se creó un polígono georreferenciado para representar la zona total del aeropuerto (Figura 6) y otro para delimitar la pista de aterrizaje, donde se excluye toda instalación de transmisores por seguridad operativa (Figura 7).

Ambos polígonos fueron generados utilizando la función "Crear nueva capa de archivo vectorial" en formato Shapefile (.shp), con el sistema de referencia espacial EPSG:32618 (WGS 84 / UTM zona 18N), tal como se recomienda para la región de Bogotá. Posteriormente, se usó la herramienta de edición para digitalizar manualmente las áreas de interés sobre imágenes satelitales de alta resolución disponibles en QGIS.

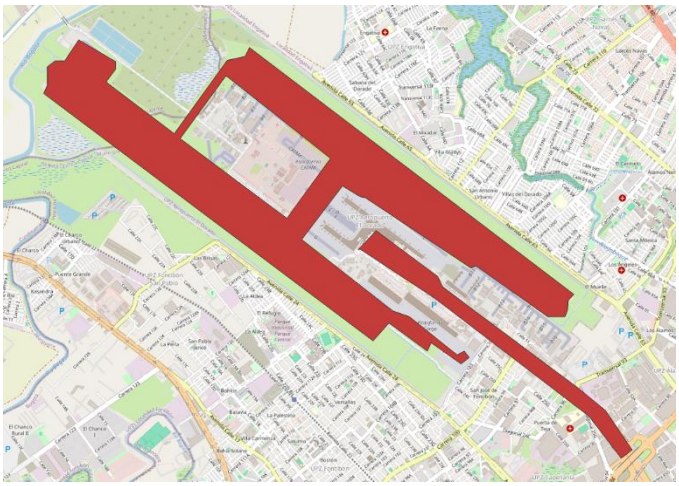


Figura 6. Polígono de delimitación del aeropuerto en QGIS.

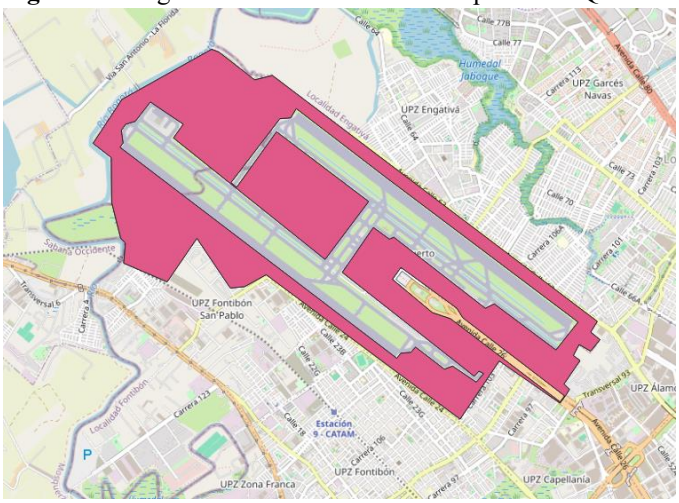


Figura 7. Polígono de zona de exclusión (pista) en QGIS

C. Configuración del Proyecto en HTZ Warfare

Para la simulación radioeléctrica del sistema C-UAS en el entorno aeroportuario de El Dorado, se utilizó el software **HTZ Warfare** debido a sus capacidades avanzadas de modelado electromagnético, integración de múltiples capas geoespaciales y personalización de parámetros de propagación.

Insumos del Proyecto

La configuración del entorno en HTZ incluyó la carga de los siguientes insumos geoespaciales:

- **Modelo Digital del Terreno (DTM):** Base de elevación utilizada para calcular la propagación en función del relieve.
- **Mapa Clutter (CLC):** Categorización del uso del suelo, incluyendo clases como zonas urbanas, aeropuertos, áreas verdes y cuerpos de agua.
- **Edificaciones (.BGL):** Modelo vectorial con alturas de edificaciones, lo cual permite calcular las pérdidas por difracción y obstrucción con mayor precisión.
- **Capas vectoriales (VCT):** Incluyen polígonos digitalizados en QGIS que delimitan las pistas de aterrizaje y zonas críticas del aeropuerto.
- **Configuración general del proyecto (.PRO):** Archivo principal que agrupa todas las capas e información de simulación.

La figura 8 muestra la pantalla de carga de estos elementos en el Project Manager de HTZ Warfare, evidenciando la correcta integración de todos los datos necesarios.

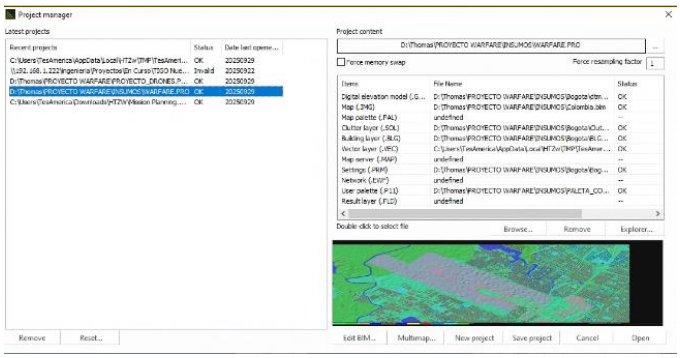


Figura 8. Carga de capas geoespaciales e insumos en HTZ Warfare.

Para modelar la cobertura de los sistemas de interferencia (jammers) sobre el espacio aéreo del aeropuerto, se seleccionó el modelo de propagación **ITU-R P.452-18**, el cual es adecuado para frecuencias comprendidas entre 1 GHz y 50 GHz, y toma en cuenta fenómenos como:

- Difracción por el terreno y edificios.
- Reflexión y absorción por obstáculos.

La figura 7 muestra la configuración del modelo de propagación en HTZ, con las opciones de pérdidas activadas para representar con precisión el entorno urbano del aeropuerto.

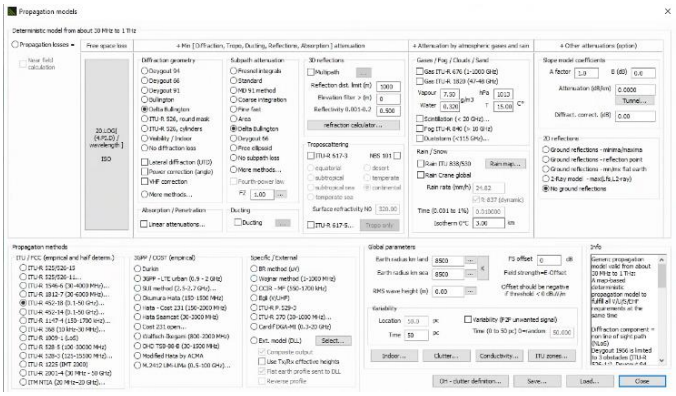


Figura 9. Parámetros del modelo ITU-R P.452-18 seleccionados para la simulación.

D. Importación de Polígonos en HTZ Warfare

Una vez creados, los polígonos fueron exportados y cargados en HTZ Warfare como capas vectoriales de tipo "área", empleando el visor de capas de usuario. En el entorno de HTZ, el polígono que representa la pista fue asignado como zona de restricción, mientras que el que representa el resto del aeropuerto fue considerado como zona disponible para el despliegue de jammers. En la **Figura 10 y 11** se visualiza la correcta importación de estos polígonos.

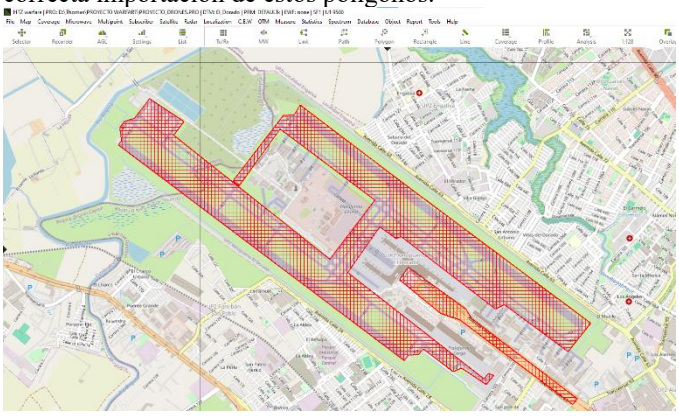


Figura 10. Polígono importado de la pista en HTZ Warfare.

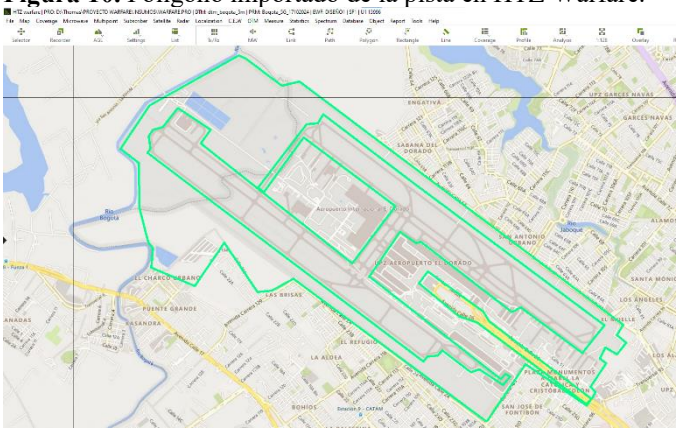


Figura 11. Polígono importado de la zona de delimitación en HTZ Warfare.

E. Análisis del entorno mediante capas de clutter

En paralelo, se cargó la base de datos de clutter del área del aeropuerto, la cual incluye una capa en formato .BGL con alturas de edificaciones integradas (Figura 12). La clasificación del clutter se basó en las propiedades de uso del suelo, como áreas urbanas, zonas verdes y estructuras aeroportuarias, cada una con su respectiva atenuación por tipo de terreno (Figura 13).

Este análisis es clave para la simulación de propagación, ya que incluso los drones en vuelo pueden verse parcialmente afectados por pérdidas de propagación debidas a vegetación o construcciones adyacentes.

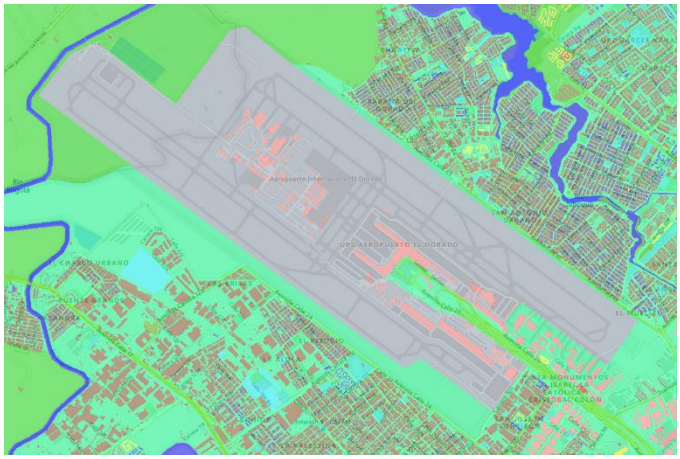


Figura 12. Clutter del aeropuerto cargado en HTZ Warfare.

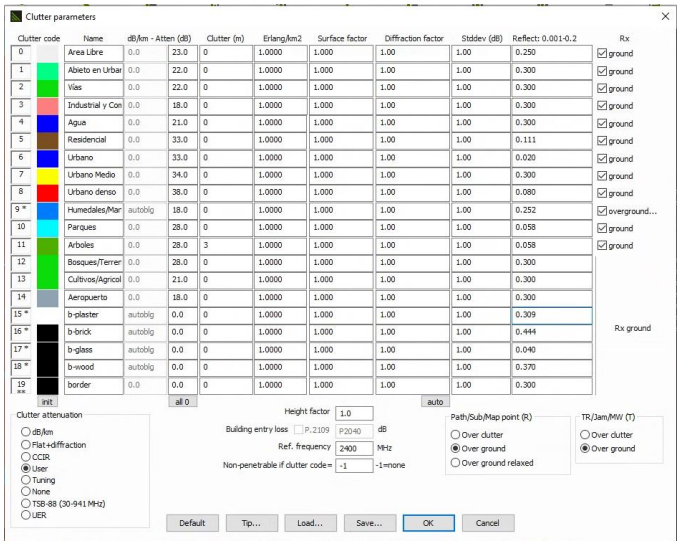


Figura 13. Clasificación del clutter por tipo de superficie y atenuación asociada.

F. Uso de la herramienta Site Search

Con las zonas delimitadas y el entorno caracterizado, se utilizó la función Site Search de HTZ Warfare para determinar los emplazamientos óptimos de jammers dentro del polígono permitido. Se ejecutó una búsqueda por porcentaje de cobertura esperada en diferentes escenarios, comparando resultados al incluir o excluir la zona de la pista (Figuras 14 y 15).

Esta herramienta evalúa cada celda de la cuadrícula definida por el usuario y marca los sitios óptimos con coloraciones según su rendimiento. Gracias a esta técnica, se garantizó que las ubicaciones seleccionadas no interfieran con la infraestructura crítica y ofrezcan un nivel adecuado de cobertura de jamming, respetando las restricciones impuestas por el entorno y las regulaciones aeroportuarias.



Figura 14. Resultados del site search dentro del polígono permitido para jammers.

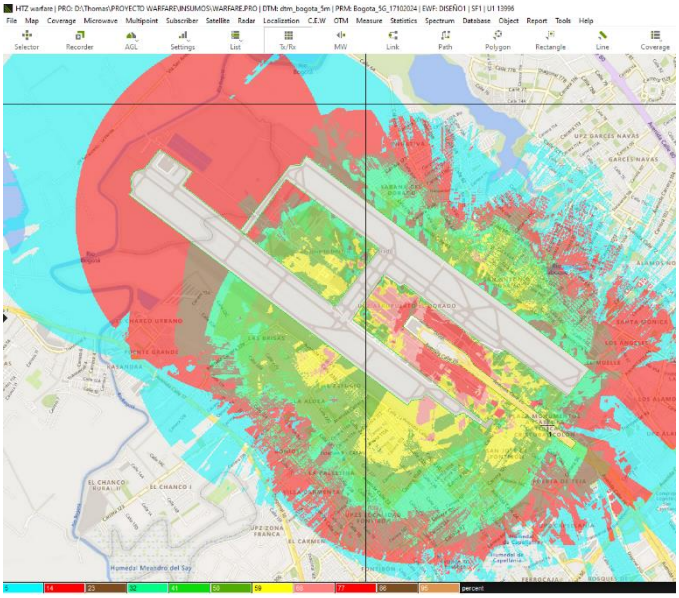


Figura 15. Resultados del site search excluyendo la pista de aterrizaje.

En la parte inferior se observan los porcentajes donde se obtendrá un área de mayor cobertura, que corresponden a cada color, de la mancha de cobertura sobre el aeropuerto. A continuación, en la Tabla 3 se muestran los porcentajes con mayor claridad.

TABLA 3
PORCENTAJE DE COBERTURA

Color	Porcentaje (%)
	5
	12
	19
	26
	33
	40
	47
	54
	61
	68
	75

De acuerdo a la mancha de cobertura obtenida, se observan las áreas con mayor porcentaje de cobertura donde un jammer tendrá mayor área de bloqueo. En base a esto, se colocan los jammers estratégicamente dentro del área del aeropuerto donde tendrán mayor área de bloqueo, teniendo en cuenta que no se pueden colocar dentro de la pista, sino en ubicaciones adyacentes a esta.

G. Parámetros de Simulación

TABLA 4
PARÁMETROS DE JAMMERS

Parámetro	Unidad	Valor típico / rango
EIRP / Potencia radiada	dBm / W	47 dBm (50 W)
Ganancia antena	dBi	6
Altura antena site	m	20
Bandas	MHz	2400
Umbral J/S	dB	+5 dB

De acuerdo a los parámetros de la tabla anterior, se definen los siguientes parámetros para los Jammers, que se encuentran en la figura 16.

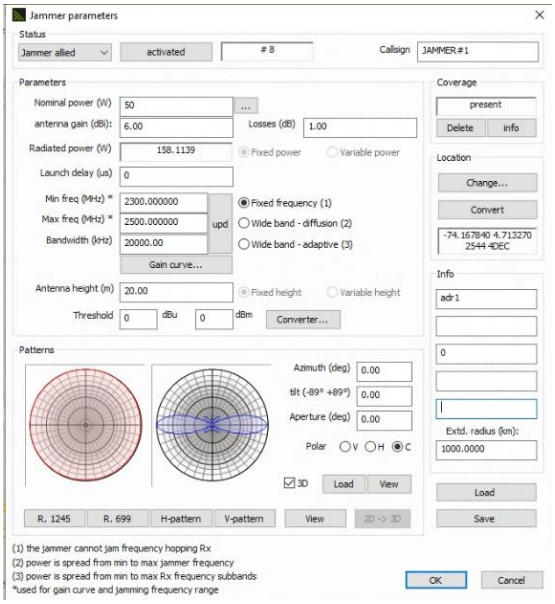


Figura 16. Parámetros de simulación de los Jammers.

La figura 16 muestra la ventana de configuración de un transmisor de interferencia (*jammer*) en el entorno de simulación HTZ Warfare. A continuación, se describen los parámetros establecidos para esta simulación, orientados a la neutralización de drones mediante interferencia electromagnética:

1. **Potencia y Ganancia**

- **Potencia nominal (Nominal power)**: Se configuró en **100 W**, equivalente a **50 dBm**, lo cual proporciona una fuente de interferencia potente adecuada para escenarios abiertos.
- **Ganancia de antena (antenna gain)**: Se estableció en **6.00 dBi**, asumiendo el uso de una antena omnidireccional con ganancia moderada.
- **Pérdidas (Losses)**: Consideradas en **1.00 dB** para incluir pérdidas en conectores, cables y condiciones de instalación.
- **Potencia radiada (Radiated power)**: Calculada automáticamente en **316.23 W EIRP**, considerando las ganancias y pérdidas del sistema.

2. Frecuencia y Ancho de Banda

- **Frecuencia mínima y máxima**: El *jammer* opera entre **2300 MHz** y **2500 MHz**, cubriendo completamente la banda ISM de 2.4 GHz, utilizada habitualmente por drones comerciales para enlaces de control (C2) y transmisión de video.
- **Ancho de banda (Bandwidth)**: Configurado en **20 MHz (20,000 kHz)**, lo que permite cubrir múltiples canales dentro del rango seleccionado.
- **Modo de frecuencia**: Se seleccionó **"Wide band - diffusion"**, lo que implica que la señal de interferencia se dispersa sobre todo el rango

definido, aumentando la probabilidad de bloquear múltiples enlaces simultáneamente.

2. **Altura, Retardo y Cobertura**

- **Altura de antena (Antenna height)**: Fijada en **20 metros**, simulando una instalación sobre estructura elevada dentro del perímetro aeroportuario.
- **Launch delay**: Establecido en **0 µs**, indicando que el transmisor entra en operación inmediatamente al inicio de la simulación.

4. Ubicación y Polarización

- **Ubicación georreferenciada**: Coordenadas aproximadas de ubicación del jammer dentro del Aeropuerto Internacional El Dorado: **Latitud:** -74.167840, **Longitud:** 4.713270
- **Polarización**: Se utilizó polarización **circular**, con patrones de radiación H y V visibles en la parte inferior de la ventana.

Con los parámetros de simulación obtenidos, y teniendo en cuenta el resultado obtenido con la herramienta Site Searche, se ubicaron los jammers en las siguientes ubicaciones, como se observa en la Figura 17.

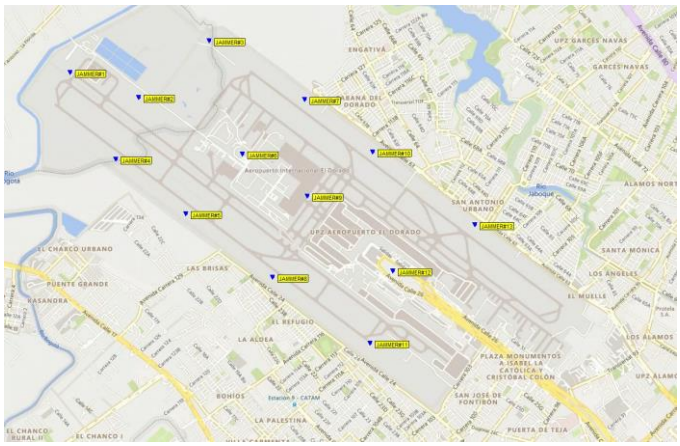


Figura 17. Ubicación de los Jammers dentro del aeropuerto.

Se distribuyeron **12 jammers (J1–J12)** de forma estratégica, cubriendo tanto pistas como áreas operativas y de acceso, buscando maximizar el área de interferencia con el mínimo número de transmisores.

Una vez ubicados los Jammers dentro del aeropuerto, se procede a correr la simulación, como se observa en la Figura 18.

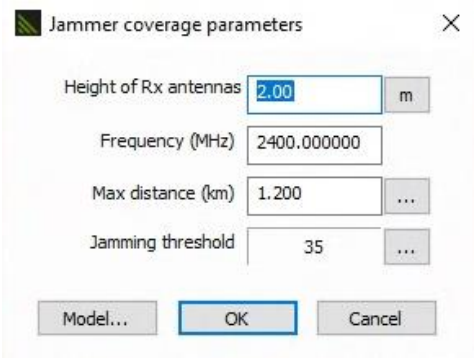


Figura 18. Parámetros de simulación de Cobertura.

En la ventana de "Jammer Coverage Parameters", se definieron los siguientes valores clave:

- Altura de antenas receptoras (Rx): desde los 2m hasta los 100 metros.
  Este valor representa la altitud estimada de los drones en vuelo dentro del espacio aéreo cercano al aeropuerto, permitiendo evaluar el efecto de la interferencia en condiciones realistas de operación.
- Frecuencia de simulación: 2400 MHz (banda ISM típica usada por drones para control y video).
  Este rango está alineado con los sistemas de enlace C2 (Command & Control) de muchos drones comerciales y representa un objetivo común de jamming.
- Distancia máxima de cobertura: 1.2 km.
  Este valor actúa como un límite superior teórico para la simulación. La atenuación real del campo radiado, el modelo de propagación y el umbral de interferencia definen la cobertura efectiva, que típicamente es mucho menor en entornos urbanos complejos.
- Umbral de jamming: 35 dBµV/m.
  Este umbral representa el nivel mínimo de intensidad de campo electromagnético necesario para que la interferencia sea efectiva sobre el receptor del dron. Es un valor crítico que determina el límite de cobertura funcional del jammer.

En la ventana **"Threshold"**, como se observa en la Figura 19, se definió el modo de umbral global (Global threshold) con las siguientes características:

- **Threshold (dBµV/m):** 35
  Este valor reafirma el nivel de intensidad de campo necesario para que una señal de interferencia sea considerada efectiva. Se aplica de forma uniforme a toda el área de cobertura.
- **Threshold (dBm):** -121
  Este valor es la conversión del umbral en términos de potencia recibida, útil para correlacionar con la sensibilidad de los receptores de drones típicos.
- **Impedancia de referencia:** 75 ohmios
  Se eligió esta configuración para simular adecuadamente el entorno de recepción RF en bandas ISM, en línea con muchas implementaciones comerciales.

- **Frecuencia de referencia:** 2400 MHz Coincide con la frecuencia objetivo del jammer, asegurando consistencia en la simulación.
- **Modelo de ganancia Rx:** Ganancia de antena receptora establecida en 0 dB para evaluar el peor caso (sin ganancia adicional en el receptor del dron).

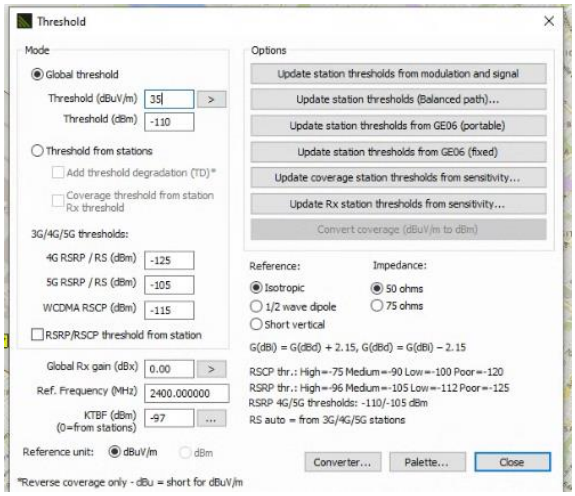


Figura 19. Parámetros del Threshold para la simulación de cobertura.

IV. RESULTADOS Y DISCUSIÓN

A. Resultados técnicos de la simulación.

Una vez realizada la simulación, se obtuvo la siguiente mancha de cobertura (Figura 20 a la Figura 23.) en la que se observa el área de cobertura de los jammers ubicados dentro del aeropuerto.

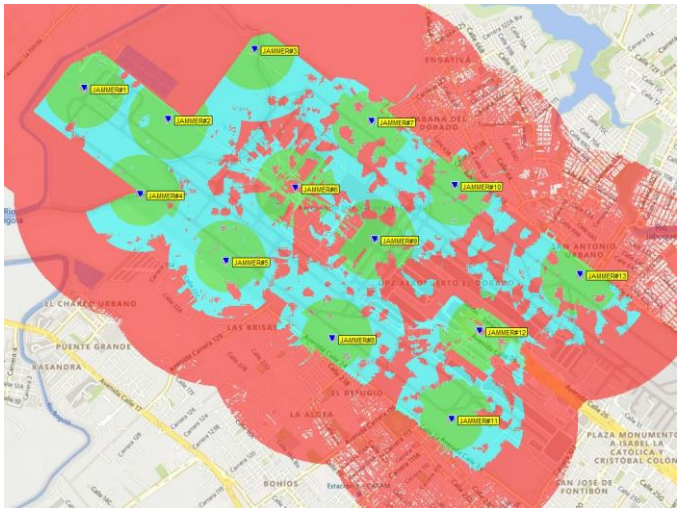


Figura 20. Mancha de cobertura de los Jammers simulando un dron volando a 2m de altura.

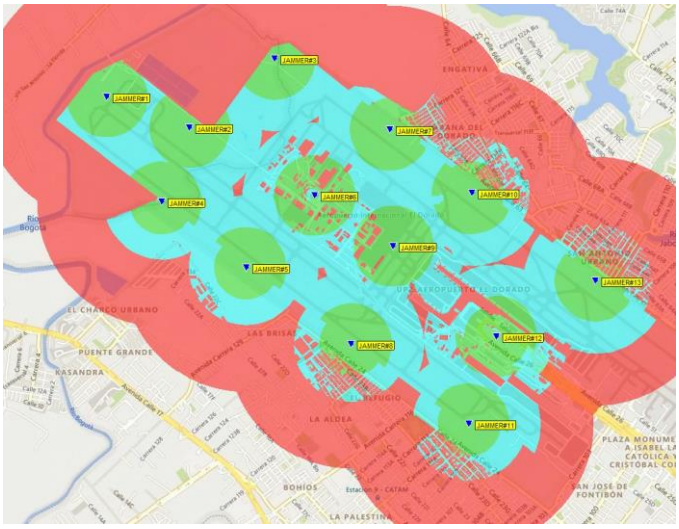


Figura 21. Mancha de cobertura de los Jammers simulando un dron volando a 25m de altura.

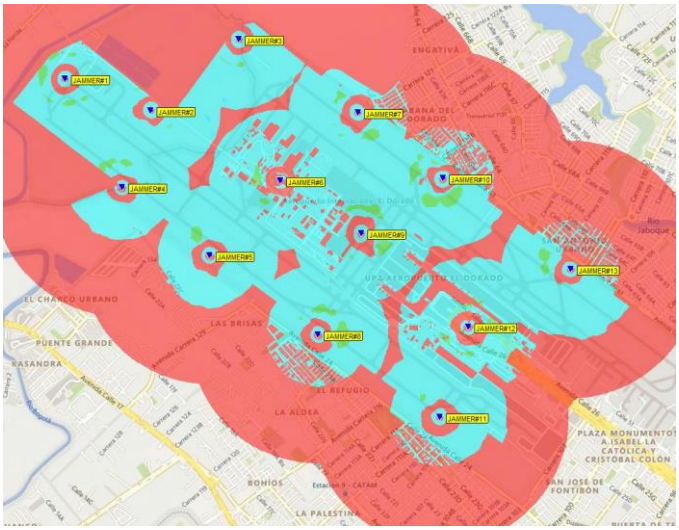


Figura 22. Mancha de cobertura de los Jammers simulando un dron volando a 75m de altura.

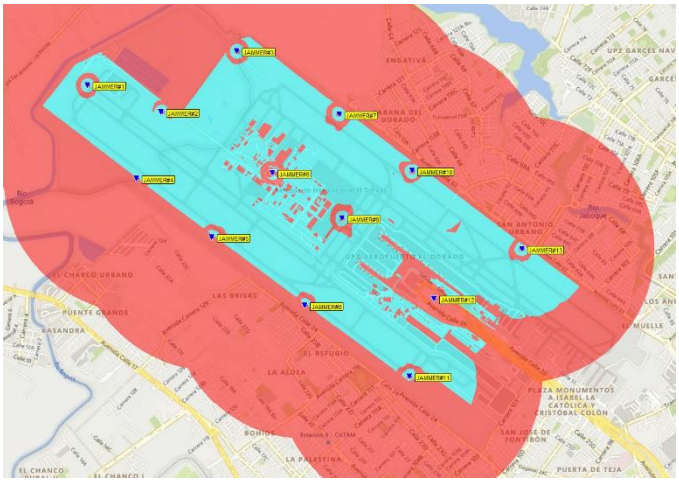


Figura 23. Mancha de cobertura de los Jammers simulando un dron volando a 120m de altura.

La mancha de cobertura generada representa el **nivel de efectividad de las señales de interferencia** emitidas por los jammers. Se utilizaron tres rangos de intensidad de señal expresados en **dBm**, codificados por colores conforme a la siguiente leyenda, en la Figura 24 y Tabla 7.

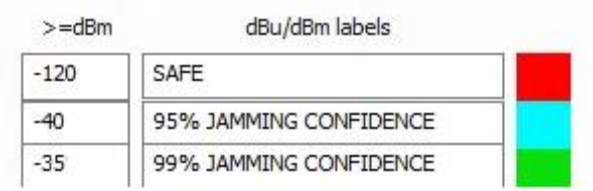


Figura 24. Paleta de colores cobertura.

TABLA 7
NIVELES DE JAMMING

Nivel (dBm)	Confianza de jamming	Color
>= -35	99% Jamming Confidence	
>= -40	95% Jamming Confidence	
>= -120	Zona segura (sin jamming)	

B. Validación del Diseño C-UAS

Un experto en telecomunicaciones evaluó el diseño del sistema C-UAS desarrollado en HTZ Warfare y concluyó que el modelo presenta una **fiabilidad estimada del 98%**, siempre y cuando se mantenga la coherencia y precisión de los insumos técnicos empleados. Esta alta fiabilidad no es inherente únicamente al motor de simulación del software, sino que depende de manera crítica de la calidad y exactitud de los datos suministrados, entre los que se destacan:

- **Modelo Digital del Terreno (DTM)** con resolución adecuada para representar variaciones de elevación.
- **Archivos .BGL** que integran las alturas reales de las edificaciones y obstáculos en el entorno aeroportuario.
- **Clutter vectorial o raster** que define el tipo de superficie y densidad de vegetación o infraestructura.
- **Modelo de propagación ITU-R P.452-18**, ajustado para el rango de frecuencias (1–50 GHz) y validado para entornos urbanos y periurbanos.
- **Precisión cartográfica y georreferenciación**, basada en imágenes satelitales de alta resolución y sistemas de referencia como WGS 84 / UTM.
- **Parámetros técnicos reales de los transmisores**, incluyendo potencia radiada (EIRP), tipo de antena, altura de instalación y orientación.
- **Experiencia comprobada del desarrollador (ATDI)** y validación del entorno de simulación en múltiples proyectos críticos de defensa y seguridad.

El experto también indicó que, si bien la simulación es altamente confiable en entornos virtuales, **es indispensable realizar una visita técnica en campo** para verificar la viabilidad física de instalar los jammers en las ubicaciones propuestas, considerando obstáculos no modelados, accesibilidad y requerimientos de infraestructura.
Adicionalmente, el despliegue final del sistema depende de los **permisos y regulaciones emitidos por la Aeronáutica Civil**, dado que las emisiones intencionales de interferencia en el espectro radioeléctrico requieren autorización expresa, especialmente en entornos aeroportuarios civiles.

C. Encuesta de percepción y conocimiento sobre drones y C-UAS

Con el fin de evaluar el conocimiento general sobre los Sistemas de Aeronaves No Tripuladas (UAS) y los sistemas de contramedidas (C-UAS), se diseñó y aplicó una encuesta de 10 preguntas cerradas a una muestra de 20 participantes, con perfiles diversos en cuanto a edad y formación. La encuesta fue aplicada a través de Microsoft Forms y su objetivo principal fue recoger datos que permitieran contextualizar la necesidad de implementar sistemas de mitigación en instalaciones críticas como aeropuertos.

Principales resultados de la encuesta:

- **Conocimiento de drones:** El 65% de los encuestados reconocen correctamente que un dron es una aeronave pilotada a distancia, aunque un 35% aún desconoce su definición técnica.

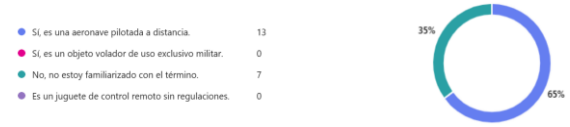


Figura 25. Resultado pregunta sobre conocimiento de drones.

- **Familiaridad con sistemas C-UAS:** El 70% de los encuestados no ha escuchado hablar sobre sistemas antidrone, lo cual evidencia un vacío de conocimiento en esta área crítica de seguridad.



Figura 26. Resultado pregunta sobre conocimiento de sistema C-UAS.

- **Percepción de amenaza:** El 55% considera que los drones representan una amenaza alta, mientras que un 20% opina que no representan peligro alguno.

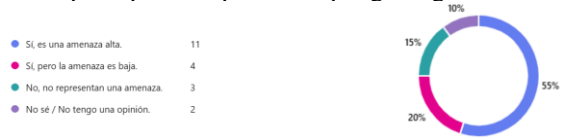


Figura 27. Resultado pregunta sobre conocimiento de la amenaza de un dron.

- **Experiencia personal:** Solo el 35% ha operado drones, en su mayoría de manera recreativa.



Figura 28. Resultado pregunta sobre conocimiento de drones.H

- **Conocimiento regulatorio:** Un 70% desconoce completamente la normativa aeronáutica vigente (RAC 100).



Figura 29. Resultado pregunta sobre conocimiento normativa aeronáutica sobre drones.

- **Factores de amenaza:** El 75% identifica el tamaño reducido de los drones como el principal reto para su detección.



Figura 30. Resultado pregunta sobre conocimiento detección de drones.

- **Métodos preferidos de neutralización:** El 85% identifica correctamente el "jamming" o interferencia de RF como el método más adecuado.



Figura 31. Figura 25. Resultado pregunta sobre conocimiento de drones.

- **Percepción sobre la regulación:** El 55% cree que se requiere una actualización normativa urgente para abordar los desafíos de los drones.



Figura 32. Resultado pregunta sobre conocimiento regulación de drones.

- **Drones en aeropuertos:** El 55% reconoce el riesgo de colisión con aeronaves como una amenaza concreta, y un 30% identifica la posibilidad de interferencia con comunicaciones.



Figura 33. Resultado pregunta sobre riesgo del vuelo de un drone.

Estos resultados justifican la necesidad de implementar simulaciones técnicas y estudios operativos sobre la eficacia de tecnologías como los jammers, en zonas sensibles como los aeropuertos, donde el conocimiento general no refleja el nivel de riesgo real ni las capacidades tecnológicas requeridas.

D. Matriz DOFA del diseño C-UAS

TABLA 8
MATRIZ DOFA DISEÑO DE SISTEMA C-UAS

FORTALEZAS	OPORTUNIDADES
• El software HTZ Warfare cuenta con una fiabilidad del 98%, validado por experto, gracias a la precisión de insumos como DTM, BGL, clutter, modelo de propagación, parámetros de antena y experiencia de ATDI. • Modelado detallado del entorno aeroportuario con datos reales (altura de edificios, zonas críticas, delimitación SIG con QGIS). • Simulación combinada de subsistemas de detección (DF) y neutralización (jammers), con análisis espacial detallado.	• Alta preocupación de las autoridades y usuarios sobre amenazas de drones en aeropuertos, lo que impulsa la adopción de soluciones C-UAS. • Posibilidad de escalar el modelo a otros aeropuertos en Colombia o América Latina con ajustes mínimos. • Colaboración potencial con la Aeronáutica Civil y entes de seguridad nacional para implementación real. • Disponibilidad de fondos y programas de seguridad aeroportuaria a nivel nacional e internacional.

DEBILIDADES	AMENAZAS
• La efectividad real depende de visitas en campo para validar accesibilidad, visibilidad, suministro eléctrico y seguridad de las ubicaciones propuestas para los jammers. • La percepción de riesgo por parte de la población puede generar rechazo si no se comunica adecuadamente la utilidad y seguridad del sistema. • Dependencia de precisión de insumos geoespaciales (si se actualizan o cambian, deben regenerarse capas vectoriales y clutter).	• Restricciones normativas: uso de jammers requiere autorización expresa de la Aeronáutica Civil, y puede tener implicaciones legales. • Posible interferencia colateral con sistemas aeronáuticos si los parámetros del jammer no se regulan adecuadamente. • Evolución de tecnologías de drones puede superar rápidamente las capacidades actuales del sistema simulado. • Cambios en normativas internacionales (ITU, ICAO) podrían afectar la viabilidad de ciertos métodos de neutralización.

V. CONCLUSIONES

El presente trabajo logró diseñar y simular un sistema C-UAS enfocado en la neutralización de amenazas mediante jammers en el Aeropuerto Internacional El Dorado de Bogotá, empleando el software HTZ Warfare con insumos de alta precisión. La simulación permitió identificar zonas críticas de cobertura, validando la eficacia del sistema en entornos urbanos complejos, sin interferir con las rutas aeronáuticas.

La validación por parte de un experto en telecomunicaciones indicó que el diseño cuenta con un 98% de fiabilidad, atribuida a la calidad de los insumos utilizados: el modelo digital del terreno (DTM), el archivo BGL con alturas de edificaciones, las capas de uso del suelo (clutter), la base cartográfica precisa, el modelo de propagación ITU-R P.452-18 y la experiencia operativa del software HTZ Warfare, respaldado por ATDI. No obstante, el experto también resaltó que esta fiabilidad está condicionada a la validación en campo de las ubicaciones propuestas para los jammers, así como a la viabilidad legal, regulatoria y operativa exigida por la Aeronáutica Civil.

Adicionalmente, se aplicó una encuesta de percepción a actores civiles y profesionales, cuyos resultados reflejan una actitud favorable hacia la implementación de sistemas C-UAS, reconociendo su necesidad ante el creciente riesgo que representan los drones en zonas críticas. Esto refuerza la aceptabilidad social del proyecto y su relevancia en la coyuntura actual.

Desde un enfoque estratégico, se construyó una matriz DOFA, donde se identificaron como fortalezas la alta precisión técnica del modelo y el uso de herramientas reconocidas a nivel internacional. Las debilidades incluyen la falta de pruebas de campo y la dependencia de autorizaciones institucionales. Entre las oportunidades, se destaca la posibilidad de escalar el modelo a otros aeropuertos del país y su integración con futuras tecnologías de detección. Las amenazas se relacionan con restricciones normativas, posibles interferencias colaterales y limitaciones presupuestales.

El artículo evidencia que la integración de herramientas de simulación y planificación técnica puede ser una solución efectiva, escalable y anticipatoria para mitigar amenazas UAS en infraestructuras críticas, siempre y cuando se complemente con validaciones en campo y adecuaciones normativas. Este enfoque híbrido entre tecnología, regulación y percepción social constituye un pilar esencial para avanzar en la protección del espacio aéreo civil colombiano.

REFERENCIAS

[1] J. Wang, Y. Liu, and H. Song, “Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends,” IEEE Aerospace & Electronic Systems Magazine, vol. 36, no. 3, pp. 4 30, Mar. 2021.

[2] G. Lykou, D. Moustakas, and D. Gritzalis, “Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies,” Sensors, vol. 20, no. 3537, Jun. 2020.

[3] A. D. Brown, “Radar Challenges, Current Solutions, and Future Advancements for the Counter Unmanned Aerial Systems Mission,” IEEE A&E Systems Magazine, Sep. 2023.

[4] ATDI, Anti-Drone System planning simulation and optimization. ATDI software documentation.

[5] K. Malon et al., “Evaluation of Safety Zones Created by Hybrid UAV Detection and Jamming System,” Proc. IEEE EUROCON, 2025.

[6] D. F. Díaz, L. C. Vargas, and G. D. Castellanos, “Training Model For Localization of Interfering and Illegal Transmission for Military Forces in UHF Bands,” Proc. IEEE Conf., 2020.

[7] S. Sánchez Díaz, “Capacidades de los medios disponibles C-UAS frente a la amenaza de enjambres de drones,” TFG, Univ. Zaragoza, 2022.

[8] D. Díez García, “Sistemas de detección y neutralización C-UAS,” TFG, Univ. Zaragoza, 2022.

[9] J. L. Hermosa López, “Detección, identificación, seguimiento y neutralización de UAS en ausencia de señal de control y/o GNSS,” TFG, Univ. Zaragoza, 2023.

[10] Aeronáutica Civil de Colombia, Resolución 04201 de 2018 (regulación UAS).

[11] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) Agencia Nacional del Espectro (ANE), normativa sobre uso del espectro y inhibidores.

[12] ATDI, HTZ Warfare Specific Tools. ATDI, 2020. [Online]. Available: Internal documentation PDF.

[13] ATDI, Hybrid Localization from Measurements. ATDI, 2020. [Online]. Available: Internal documentation PDF.

[14] ATDI, Radars in ATDI Tools. ATDI, 2020. [Online]. Available: Internal documentation PDF.

[15] Fathom & TES America Andina, Recap of Meeting with TES America Andina. Fathom, 2024. [Internal Report, PDF].

[16] UAEAC, *Reglamentos Aeronáuticos de Colombia RAC 100: Operación de Sistemas de Aeronaves no Tripuladas UAS*, Resolución 01983, 27 septiembre 2023. Aeronáutica Civil de Colombia.

[17] UAV Coach, “Drone Laws in Colombia (2025)”, UAV Coach. [Online]. Available: https://uavcoach.com/drone-laws-in-colombia

[18] QGIS Project, “Creación de nuevos datos vectoriales: capas de polígonos,” QGIS 3.40 Training Manual, 2024. [Online]. Available: https://docs.qgis.org/3.40/es/docs/training_manual/create_vector_data/create_new_vector.html

[19] “El Dorado International Airport,” Wikipedia, accessed Aug. 2025. [Online]. Available: https://en.wikipedia.org/wiki/El_Dorado_International_Airport

[20] LogCluster, “Colombia – El Dorado Aeropuerto Internacional,” LogCluster LCA, accessed Sep. 2025. [Online]. Available: https://lca.logcluster.org/es/221-colombia-el-dorado-aeropuerto-internacional.