

REPÚBLICA DE COLOMBIA
AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO
FUERZA AÉREA COLOMBIANA



GUÍA

SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)



**Versión 01
Mayo 2022**

TABLA DE CONTENIDO

INTRODUCCIÓN	4
CAPÍTULO A. DEFINICIONES, ABREVIATURAS Y REFERENCIAS	5
CAPÍTULO B. SISTEMAS AÉREOS NO TRIPULADOS (UAS)	11
1. Denominaciones a través de la historia.	11
2. Aplicaciones y empleos.	12
3. Generalidades y conceptos.	13
4. Clasificación.....	15
5. Componentes y funcionamiento.	19
6. Identificación de amenazas y riesgos.	25
CAPÍTULO C. SISTEMAS CONTRA UAS (C-UAS).....	27
1. Antecedentes e importancia de los C-UAS.....	27
2. Categorización de la amenaza.	27
3. Definición Sistemas Contra U-AS.	29
4. Clasificación C-UAS.	31
4.1 Tipos de tecnología C-UAS.	31
4.2 Sistemas de Defensa Aérea y sus limitaciones.	31
4.3 Sistemas de detección, seguimiento e identificación.....	32
5. Recomendaciones para la adquisición e implementación de C-UAS.	37
Anexo 1: Características y limitaciones de sistemas C-UAS de mayor empleo.....	40
Anexo 2: Consideraciones técnicas para la selección de C-UAS.....	44

INTRODUCCIÓN

El presente documento constituye una guía para los Entes de Aviación de Estado (EAE) y propende actualizar los conceptos relacionados a los Sistemas Aéreos No Tripulados (UAS: *Unmanned Aerial Systems*, por sus siglas en inglés), afianzar los conocimientos sobre generalidades y funcionamiento de los mismos en la Aviación de Estado (AE), advertir sobre los riesgos y amenazas inherentes al desarrollo tecnológico de la Aviación No Tripulada en el mundo, así como, propender por el alcance de los más altos niveles de seguridad operacional para la AE.

En el mismo sentido, busca dar a conocer el concepto C-UAS (Sistema Contra UAS) LSS (*Low, Slow and Steady*), entendiéndose este como la capacidad integral que permitirá prevenir, detectar, identificar, decidir y, cuando sea necesario, neutralizar la amenaza que representa el empleo imprudente y/u hostil de aquellos UAS que, por su diseño y características, vuelan a baja altura y velocidad siendo difíciles de detectar, identificar y neutralizar por los medios tradicionales de Defensa Aérea.

De otra parte, propende difundir a los EAE, información relevante sobre la operación de UAS de forma tal que su personal tenga herramientas para identificar posibles usos ilícitos de esos sistemas y/o situaciones que pongan en riesgo la seguridad de las unidades militares y de policía, con el fin que puedan actuar como parte integral del sistema de seguridad, realizar reportes oportunos de avistamiento y coadyuvar en el proceso de actuación y neutralización de una amenaza potencial o inminente. En dicho sentido, es necesario sensibilizar al personal de los EAE respecto de la necesidad de percibir esta amenaza como un reto tecnológico, que requiere disponer de sistemas C-UAS, procedimientos y estrategias organizacionales capaces de hacerle frente con eficacia y seguridad, evolucionando al ritmo que lo hacen los UAS LSS y gestionando correctamente las vulnerabilidades de los EAE.

Lo anterior, en observancia al artículo 8 del Convenio de Aviación Civil Internacional (Convenio de Chicago aprobado por el Congreso de Colombia con la Ley 12 de 1947) el cual establece respecto de las aeronaves sin piloto que “(...) *Cada Estado contratante se compromete a asegurar que los vuelos de tales aeronaves sin piloto en las regiones abiertas a la navegación de las aeronaves civiles sean controladas de forma que se evite todo peligro a las aeronaves civiles.*”, y en concordancia con el artículo 37 del citado Convenio el cual refiere que “*Cada Estado contratante se compromete a colaborar, a fin de lograr el más alto grado de uniformidad posible en las reglamentaciones, normas, procedimientos y organización relativos a las aeronaves, personal, aerovías y servicios auxiliares, en todas las cuestiones en que tal uniformidad facilite y mejore la navegación aérea.*”.

CAPÍTULO A. DEFINICIONES, ABREVIATURAS Y REFERENCIAS

1. Definiciones y abreviaturas.

Las siguientes definiciones y abreviaturas aplican al contenido de la presente guía.

AAES: Autoridad Aeronáutica de Aviación de Estado

AE: Autoridad Aeronáutica

Aeronave no tripulada: Aeronave destinada a volar sin piloto a bordo.

Aeronave pilotada a distancia –RPA: “Aeronave no tripulada que es pilotada desde una estación de pilotaje a distancia por un Piloto remoto, emplazado en una estación de control ubicada fuera de la aeronave (es decir en tierra, en barco, en otra aeronave, en el espacio, entre otros)” (OACI, 2015).

Aeronavegabilidad: Estado de una aeronave, motor, hélice o pieza que se ajusta al diseño aprobado correspondiente y está en condiciones de operar de modo seguro.

Clasificación de UAS amenaza: Es la asignación por parte de la tecnología C-UAS (ya sea de forma autónoma o por un operador) de un UAS objetivo potencial de alto nivel, en la que se indica el tipo de UAS, fabricante y/o protocolo de comunicación específico.

Captura directa (*Snagging*): Método que permite la captura del UAS a través del empleo de redes expulsadas desde otras aeronaves pilotadas remotamente o elementos ubicados en tierra.

Carga útil: Todos los elementos del UAS/RPAS que no son necesarios para volar pero que son transportados para el cumplimiento de la misión específica que tienen encomendada. La carga útil puede estar relacionada con vigilancia, armas, comunicaciones, detección aérea, o carga propiamente dicha.

Centro de Comando y Control: Hace referencia a la dependencia, oficina o entidad encargada de centralizar las comunicaciones y dirigir el flujo de comunicación en el aeródromo o zona restringida, para que los encargados tomen decisiones tendientes a proteger los recursos asignados.

Contra medidas de UAS: Sistemas dotados con la capacidad de interrumpir, deshabilitar, destruir, tomar el control y/o proporcionar instrucciones de vuelo alternativas a un UAS objetivo.

Cetrería: Técnica relacionada con la cría, amaestramiento y cuidado de aves rapaces para la casa de otras especies.

DA. Acrónimo para Defensa Aérea

Dazzling: Empleo de un haz de luz de alta intensidad o láser para "cegar" la cámara del UAS.

Detección de UAS: Es una declaración de que un UAS está en presencia de un sensor. Algunos sistemas, dependiendo de cómo estén configurados, pueden señalar cualquier objeto a su vista como detección (es decir, pájaros, aviones comerciales, entre otros.), o pueden alertar al operador únicamente de los objetos que se consideran UAS, basados en sus capacidades.

Drone: Expresión popular para referirse a cualquier aeronave no tripulada.

Electro-óptica: Es una rama de la ingeniería eléctrica y física de la materia que involucra componentes, dispositivos (por ejemplo, láseres, leds, guías de onda, entre otros.) y los sistemas que utilicen la propagación y la interacción de la luz con diversos materiales adaptados.

EAE: Ente de Aviación de Estado.

Enlace de mando y control. (C2) Enlace de datos entre la aeronave pilotada a distancia y la estación de pilotaje a distancia para fines de dirección del vuelo.

Estación de Control en Tierra (GCS). Estación en la cual el Operador dirige el vuelo de una aeronave no tripulada. "Puede variar desde un dispositivo manual hasta una estación con varias consolas. Puede estar emplazada en el interior o en el exterior; puede ser estacionaria o móvil (instalada en un vehículo/barco/aeronave)" (OACI, 2015).

Hacking: Búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes.

Identificación de UAS amenaza: Es la asignación por parte de la tecnología C-UAS (ya sea de forma autónoma o por un operador) de un nombre o categoría más específicos, como la dirección física del módem o la marca / modelo exacto del UAS.

Interferencia intencionada (Jamming): Interferencia producida deliberadamente por emisiones destinadas a hacer ininteligibles o falsear en todo o en parte una señal deseada.

Láser: Dispositivo óptico que genera un haz luminoso de una sola frecuencia, monocromático, coherente y muy intenso, mediante la estimulación eléctrica o térmica de los átomos, moléculas o iones de un material

Latencia: Tiempo que tarda en transmitirse un paquete dentro de la red, y es un factor clave en las conexiones a Internet.

LSS (Low, Slow and Steady): UAS de superficie radar equivalente reducida, baja firma infrarroja y/o acústica, vuelo a baja altura y velocidad.

Meaconing: Un sistema de recepción de señales de radio baliza que las retransmite en la misma frecuencia para confundir la navegación. Las estaciones de medición hacen que las aeronaves y estaciones terrestres obtengan datos imprecisos.

Mitigación de UAS: Describe los métodos utilizados para eliminar o reducir la amenaza que representa un UAS. Estos métodos incluyen medios técnicos, como interferencia de RF o GNSS, suplantación / secuestro y ataque cinético.

Modo autónomo de vuelo: Configuración de vuelo que le permite al UAS/RPAS volar sin la intervención de un Piloto Remoto u Operador, ejecutando acciones basadas en información suministrada por algoritmos, sensores y software previamente programados en la aviónica del Sistema.

NBQR: Nuclear, Biológico, Químico, Radioactivo

Operador UAS: Personal capacitado, calificado y entrenado para operar de manera segura una aeronave no tripulada de la Clase I-A y/o I-B, con la capacidad de cumplir las misiones típicas y operacionales de cada uno de los EAE.

Operador al Mando. Personal designado por el EAE para estar al mando y encargarse de la realización segura de un vuelo.

Peso máximo de despegue (MTOW: Maximum Takeoff Weight). Equivale al peso vacío de la aeronave + 100% de carga útil + 100% de su capacidad de combustible.

Operación con visibilidad directa visual (VLOS): Operación en la cual el Piloto Remoto y/u Operador mantiene contacto visual directo, sin ayudas ópticas y/o electrónicas, con la aeronave pilotada a distancia.

Operación con visibilidad directa visual extendida (EVLOS): Operación en las que el contacto directo con la aeronave se realiza con la ayuda de observadores RPA que se mantienen en contacto permanente por radio con el Piloto Remo y/u Operador.

Operación con visibilidad más allá de la línea de vista (BVLOS): Cuando ni el piloto a distancia ni los observadores RPA puedan mantener contacto visual directo sin ayudas con la RPA, las operaciones se consideran BVLOS. Los requisitos de equipo mínimo para apoyar las operaciones BVLOS aumentan considerablemente a medida que aumenta el alcance y la complejidad de tales operaciones, así como los costos involucrados en asegurar la solidez del enlace C2. Es fundamental contar con capacidad para detectar tránsito en conflicto u obstáculos y adoptar las medidas apropiadas.

Piloto Remoto: Persona designada y avalada por el EAE mediante certificado de habilidad para desempeñar funciones esenciales para la operación de una aeronave pilotada a distancia y para operar los controles de vuelo, según corresponda, durante el tiempo de vuelo.

Probabilidad de derribo (Pk): Es la probabilidad de derribo de un sistema de armas específico. Se mide en un rango entre 0 y 1, siendo 0 el 0 % de posibilidad de derribar un objetivo y 1 el 100 %. Depende de numerosos factores como la probabilidad de que el armamento impacte contra el objetivo (Phit) o la probabilidad de detección de la amenaza (Pd) entre otros.

Radar: Es un sistema que usa ondas electromagnéticas para medir distancias, altitudes, direcciones y velocidades de objetos estáticos o móviles como aeronaves, barcos, vehículos motorizados, formaciones meteorológicas y el propio terreno. Su funcionamiento se basa en emitir un impulso de radio, que se refleja en el objetivo y se recibe típicamente en la misma posición del emisor. A partir de este "eco" se puede extraer gran cantidad de información. El uso de ondas electromagnéticas permite detectar objetos más allá del rango de otro tipo de emisiones. Entre sus ámbitos de aplicación se incluyen la meteorología, el control del tráfico aéreo y terrestre y gran variedad de usos militares.

Radiación Infrarroja (IR): Es un tipo de radiación electromagnética, de mayor longitud de onda que la luz visible, pero menor que la de las microondas. Consecuentemente, tiene menor frecuencia que la luz visible y mayor que las microondas. Su rango de longitudes de onda va desde unos 0,7 hasta los 1000 micrómetros.

Radiofrecuencia (RF): También denominado *espectro de radiofrecuencia*, es un término que se aplica a la porción menos energética del espectro electromagnético, situada entre los 3 hercios (Hz) y 300 gigahercios (GHz).

Sistema aéreo no tripulado (UAS: *Unmanned Aerial System*): Aeronave y sus elementos asociados, la cual es operada sin piloto a bordo.

Sistema Contra UAS (C-UAS: *Counter Unmanned Aircraft System*): Conjunto

de sistemas, integrados por sensores, sistema de mando y control (C2) y sistemas de armas que permiten la detección, identificación y neutralización de UAS.

Sistema de Aeronaves Pilotadas a Distancia (RPAS: Remotely- Piloted Aircraft System). Aeronave pilotada por un “Piloto Remoto”, ubicado en una estación remota localizada fuera de la aeronave (ejemplo: en tierra, barco, otra aeronave, en el espacio); quien monitorea la aeronave todo el tiempo y puede responder a las instrucciones de ATC, efectuar comunicaciones apropiadamente vía voz o enlace de datos de acuerdo a la operación o espacio aéreo, y es responsable por la conducción segura de la aeronave durante su vuelo. Comprende un conjunto de elementos configurables incluyendo una RPA, sus estaciones de piloto remoto conexas, los necesarios enlaces C2 y todo otro elemento del sistema que pueda necesitarse, en cualquier punto durante el vuelo. Otras características podrían comprender soporte lógico, vigilancia de la salud, equipo de comunicaciones ATC, sistema de determinación de vuelo y elementos de lanzamiento y recuperación (OACI, 2011).

Suplantación (Spoofing): Método que permite sustituir las señales de posicionamiento del UAS para hacer creer a la aeronave que se encuentra en una posición distinta a la real.

Telemetría: Sistema automatizado de comunicación (alámbrico o inalámbrico) que le permite al UAS/RPAS almacenar información, procesarla y trasmitirla hasta el lugar donde se monitorea y controla el sistema. Para esto, se requiere de varios sensores que miden magnitudes físicas, químicas, entre otras, y que transforman esta información en señales análogas o inalámbricas para su envío y procesamiento.

Ubicación de UAS: Es un informe o visualización estimada de dónde se encuentra una GCS o UAS en un momento dado.

UAS: *Unmanned Aerial System.* Sistema Aéreo no Tripulado

UAV: *Unmanned Aerial Vehicle.* Vehículo Aéreo no Tripulado (Termino en desuso, OACI 2015)

VTOL (Vertical Take-off and Landing). Capacidad de ciertas aeronaves, tripuladas y no tripuladas, para efectuar las maniobras de despegue y aterrizaje de forma vertical, mientras que en vuelo recto y nivelado se utiliza el método de propulsión horizontal.

Zona restringida: Espacio aéreo de dimensiones definidas sobre el territorio o las aguas jurisdiccionales de un Estado, dentro del cual está restringido el vuelo de las aeronaves, de acuerdo con determinadas condiciones.

2. Referencias.

- OACI (2011), Circular 328 AN/190, *Sistemas de Aeronaves No Tripuladas (UAS)*.
- OACI (2015), Doc. 10019 AN/507, *Manual sobre Sistemas de Aeronaves Pilotadas a Distancia (RPAS)*.
- FAA (2019), *Unmanned Aircraft System Detection-Technical Considerations*.
- Ministerio de Defensa de España (2019), *Concepto Nacional C-UAS LSS*, Centro Conjunto de Desarrollo de Conceptos, Madrid-España.
- Ministerio de Defensa de España (2018), *GT Tecnología- Concepto Contra Sistemas Aéreos No Tripulados*, Centro Conjunto de Desarrollo de Conceptos, Madrid-España.
- Autoridad Aeronáutica de Aviación de Estado (2019), *Circular Informativa No. 003-19 Funcionamiento y Generalidades Sistema No Tripulado*, Bogotá-Colombia.
- Austin, R (2010). *Unmanned Aircraft Systems, UAV design, development and deployment*. Wiley.
- Barnhart, Hottman, Marshall, Shappee (2012). *Introduction to Unmanned Aircraft Systems*. CRC Press.
- Calvo, C (2014). *Perfiles IDS: De los UAV a los RPAS*.
- Michel (2019), *Counter-drone Systems*.

CAPÍTULO B. SISTEMAS AÉREOS NO TRIPULADOS (UAS)

1. Denominaciones a través de la historia.

El concepto de UAS (*Unmanned Aerial Systems*, por sus siglas en inglés), tal y como se emplea actualmente, ha evolucionado a través de la historia en consideración a numerosos factores. Al finalizar la Primera Guerra Mundial se conocían como “aeronaves robóticas”, “torpedos aéreos” o “aeronaves automáticas”. En la década de 1930 se comenzó a utilizar la denominación “*drone*” que, traducido literalmente del inglés, significa “zángano” y que se utilizó de forma extendida hasta la década de los 50. En los años 60 apareció la denominación RPV (*Remotely Piloted Vehicle*), es decir, vehículo pilotado a distancia. Durante los 80, la Autoridad de Aviación Civil norteamericana introdujo cambios conceptuales al concepto RPV, aplicando la denominación “*Remotely Operated Aircraft*” (ROA), sustituyendo las palabras “vehículo” por “aeronave” y “pilotado” por “operado”.

Si bien el término UAV (*Unmanned Aerial Vehicle*, por sus siglas en inglés), se adoptó a finales de los 80, a principios del siglo XXI se introdujo la denominación UAS, la cual además del vehículo aéreo, involucra de forma integral a los componentes asociados para la operación del mismo. En el 2011, mediante la publicación de la Circular 328 AN/190, la Organización de Aviación Civil Internacional (OACI) suscribió la primera referencia sobre regulación de UAS a nivel mundial, definiendo, entre otros aspectos, que “(...) *un vehículo aéreo no tripulado es una aeronave que vuela sin un piloto al mando a bordo y que se controla a distancia y plenamente desde otro lugar (tierra, otra aeronave, espacio) o que ha sido programada y es plenamente autónoma*”. Mencionada Circular también consideró que para integrar los UAS en el espacio aéreo no segregado y en aeródromos no segregados, debería haber un piloto responsable de la operación de los mismos, por lo cual, estableció una subcategoría de los UAS, conocida en la actualidad como Sistemas de Aeronaves Pilotadas a Distancia-RPAS (*Remotely Piloted Aircraft Systems*, por sus siglas en inglés).

Posteriormente, en el año 2015, y en consideración a la problemática legal y regulatoria de los UAS, la OACI publicó además el Documento 10019 AN/507 “*Manual sobre Sistemas de Aeronaves Pilotadas a Distancias (RPAS)*”, en el cual se contemplaron todos los aspectos inherentes a la operación segura de estos sistemas, específicamente, lo relacionado al factor humano. En tal sentido, determinó que “(...) *una RPA es una aeronave pilotada por un “Piloto remoto”, titular de licencia, emplazado en una “estación de piloto remoto” ubicada fuera de la aeronave (es decir, en tierra, en barco, en otra aeronave, en el espacio) quien monitorea la aeronave en todo momento y puede responder a las instrucciones expedidas por el ATC, se comunica por enlace de voz o datos según corresponda*

al espacio aéreo o a la operación, y tiene responsabilidad directa de la conducción segura de la aeronave durante todo su vuelo”.

Actualmente, los términos UAS y RPAS son los conceptos técnicos, adoptados por la AAAES, aplicables a la AE, y empleados comúnmente en la comunidad aeronáutica a nivel mundial para la estructuración de documentos y regulaciones sobre Sistemas Aéreos No Tripulados.

2. Aplicaciones y empleos.

Antes de analizar en detalle el funcionamiento de los UAS es apropiado enumerar, entre otros, algunos de los usos para los que se destinan, tanto en actividades de carácter civil como en el ámbito militar y policial.

Aplicaciones Civiles

- **Aerofotografía:** Filmación, video, fotos, entre otras.
- **Agricultura:** Seguimiento y fumigación de cultivos; control y conducción de rebaños.
- **Guardacostas:** Búsqueda y salvamento, seguimiento de costas y rutas marítimas.
- **Conservación:** Monitoreo de contaminación y vigilancia de terrenos.
- **Aduanas e Impuestos Especiales:** Vigilancia de importaciones ilegales
- **Compañías eléctricas:** Inspección de líneas eléctricas.
- **Servicios contra incendios y silvicultura:** Detección de incendios, control de incidentes.
- **Pesca:** Protección pesquera.
- **Empresas de suministro de gas y petróleo:** Estudio de la tierra y seguridad de los oleoductos.
- **Servicios de información:** Cubrimiento de noticias y eventos.
- **Servicios Meteorológicos:** Muestreo y análisis de atmósfera para predicción.
- **Agencias de tráfico vehicular:** Seguimiento y control del tráfico vial.

Fuente: Construcción AAAES basado en Documento OACI 10019 AN/507 “Manual sobre Sistemas de Aeronaves Pilotadas a Distancias (RPAS)”

Aplicaciones militares/policiales

- Detección de embarcaciones enemigas, incluyendo submarinos.
- Señuelos de misiles mediante la emisión de firmas artificiales.
- Inteligencia electrónica.
- Transmisión de señales de radio.
- Protección de puertos contra ataques en alta mar.
- Reconocimiento.
- Vigilancia de la actividad enemiga.
- Monitoreo de la contaminación nuclear, biológica, química o radioactiva (NBQR).
- Designación y seguimiento de objetivos.
- Ubicación y destrucción de minas terrestres.
- Vigilancia de largo alcance y gran altitud.
- Eliminación de artefactos explosivos sin detonar.
- Evaluación de daños en aeródromos.
- Búsqueda de personas desaparecidas, seguridad y vigilancia de incidentes, persecución de personas y vehículos.

Fuente: Construcción AAAES basado en Documento OACI 10019 AN/507 "Manual sobre Sistemas de Aeronaves Pilotadas a Distancias (RPAS)"

3. Generalidades y conceptos.

Un UAS es aquel sistema compuesto por una serie de componentes entre los que se incluyen: una o varias aeronaves, denominadas Vehículos Aéreos No Tripulados (UAV), sus cargas útiles, las estaciones de control en tierra (y, a menudo, otras estaciones remotas), sistemas de lanzamiento y recuperación de aeronaves, sistemas de soporte, comunicación, transporte y el componente humano requeridos para su operación. Así mismo, deben considerarse como parte de un entorno de operación aérea con sus normas, regulaciones y disciplinas.

Respecto a las aeronaves como tal, el Departamento de Defensa de Estados Unidos, definió que un UAV es "(...) un vehículo propulsado que no dispone de operador humano, que puede operarse de forma autónoma o por control remoto, que puede ser recuperable y que puede llevar una carga letal o no letal".

Generalmente, los UAS cuentan con los mismos mecanismos y dispositivos que requiere la operación de las aeronaves tripuladas, la diferencia es que estos sistemas, desde su concepción, se diseñan para ser operados sin una tripulación a bordo, la cual es reemplazada por un componente de inteligencia y control

electrónico. Así mismo, es importante comprender que los UAS se subdividen en varias categorías, de acuerdo al nivel de interacción humana que requieren para volar de forma autónoma:

Sistemas de Aeronaves Pilotadas a Distancia (RPAS): Se consideran como un integrante igualitario del sistema de aviación civil, capaz de interactuar con el control de tránsito aéreo (ATC) y otras aeronaves en tiempo real, por lo cual, exige la intervención directa y constante de un Piloto Remoto, el cual debe ser titular de un certificado de habilidad de vuelo. Cuentan con un alto grado de “inteligencia” al estar en la capacidad de reportar información al piloto (telemetría) en tiempo casi real, entre la que se incluye los datos de vuelo (posición actual, velocidad, altitud, cantidad de combustible), condición general (fallas de los sistemas) e imágenes o productos obtenidos con la carga útil (dependiendo del tipo de sensor abordo).

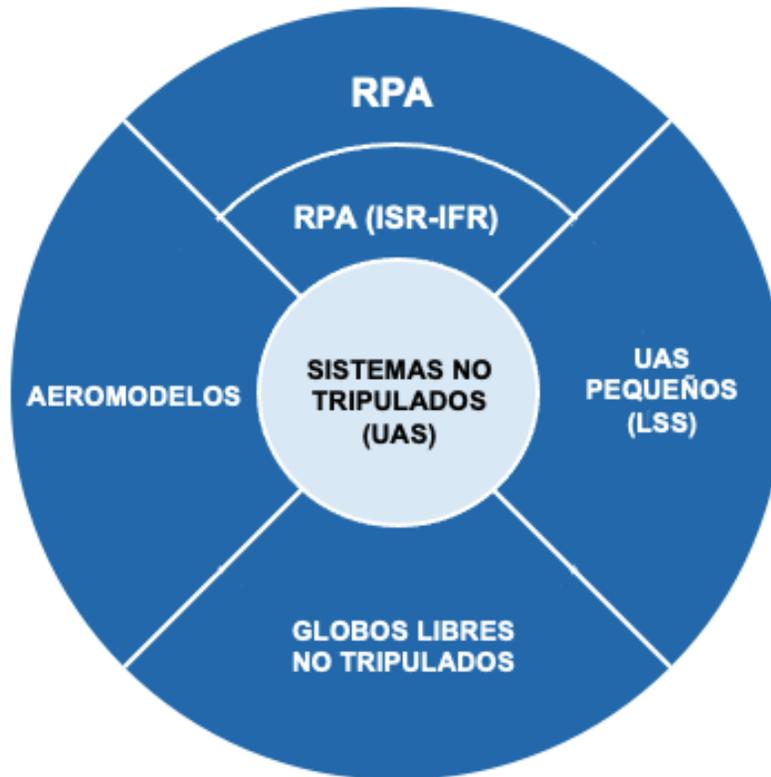
Aeronaves autónomas: Son programadas para ejecutar patrones de vuelo sin la intervención del operador o piloto. Pueden volar fuera del alcance del mismo, pero no tienen un Subsistema de Inteligencia como tal. Simplemente, son empleados para una misión preprogramada, la cual incluye las rutas que debe seguir y su regreso al punto de lanzamiento o despegue. Durante el vuelo, no retransmite datos sobre la misión, por lo cual, los resultados se obtienen generalmente cuando ésta es recuperada.

Aeromodelos: Si bien son controlados por radio, se usa sólo con fines recreativos y/o deportivos. Por consiguiente, es indispensable que permanezca a la vista del operador. Éste generalmente se limita al control horizontal y vertical de la aeronave, mientras se encuentre en vuelo.

Lo anterior, como se muestra en el siguiente gráfico:

INTENCIONALMENTE EN BLANCO

Imagen 1: Subcategorización UAS



Fuente: Construcción AAAES basado en ICAO Safety Bulletin 2020/1 <https://www.icao.int/safety/UA/Documents/ICAO%20UA%20Bulletin%202020%201a.pdf>

4. Clasificación.

A diferencia de lo que sucede con otros tipos de sistemas, para los UAS no existe una clasificación universalmente aceptada sino múltiples taxonomías que se acostumbra a entrelazar, teniendo en cuenta su diversidad y las múltiples misiones que pueden desempeñar.

La necesidad de elaborar una taxonomía estándar para los UAS responde, únicamente, a la búsqueda de un método que permita agruparlos de forma simplificada, y está estrechamente ligada al desarrollo de la normatividad que permita su empleo de forma segura, en espacios aéreos compartidos con las aeronaves tripuladas.

Algunos de los métodos típicos de clasificación, son:

Por las características físicas del UAS: Dentro de este tipo, los UAS pueden clasificarse de acuerdo a su masa o tamaño (nano, mini y micro, entre otros), método de generación de sustentación (ala fija, ala rotatoria, VTOL), autonomía, velocidad, techo de operación, entre otros. También se incluye la categorización de los UAS en función de su *Peso Máximo de Despegue (MTOW)* el cual está relacionado, por un lado, con la capacidad máxima de carga, la autonomía de vuelo y otros parámetros propios del UAS; y por otro, con la energía cinética en el momento de un eventual impacto sobre el suelo, que determinará el riesgo asociado a los accidentes de los sistemas.

De igual forma, los UAS pueden clasificarse de acuerdo a su autonomía y altitud máxima de vuelo, así:

INTENCIONALMENTE EN BLANCO

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

Tabla 1. Clasificación UAS según su autonomía y alcance vertical

CATEGORÍA	ALCANCE	EMPLEO
HALE (High Altitude Long Endurance) o Resistencia larga a gran altitud	Más de 15.000 m de altitud y más de 24 horas de autonomía de vuelo.	Capacidad extendida para sensores avanzados de inteligencia abordo y sistemas de armas. Usualmente empleados por Fuerzas Militares.
MALE (Medium Altitude Long Endurance) o Resistencia larga a mediana altitud	De 5.000 a 15.000 m de altitud y 24 horas de autonomía de vuelo.	Generalmente los mismos que la categoría HALE, pero en distancias más cortas.
TUAV (Medium Range or Tactical UAV) o Rango medio/UAV táctico	Entre 100 y 300 km de altitud.	Empleados por Fuerzas Militares, con sistemas más simples.
Close-Range UAV/UAV de rango corto	Más de 100 km de altitud	Empleados, tanto en la parte militar como en la civil, para actividades tácticas como vigilancia y reconocimiento de áreas específicas.
MUAV o Mini UAV	Aproximadamente 30 m de altitud. Menos de 20 Kg.	Empleados, tanto en la parte militar como en la civil, para actividades tácticas como vigilancia y reconocimiento de áreas específicas. No requieren equipos de lanzamiento y recuperación.
Micro UAV o MAV	Envergadura inferior a 150 mm . Menos de 6 Km de altitud	Usualmente empleados en ambientes urbanos, capaces de mantener bajas velocidades, por lo cual son vulnerables a las condiciones de viento.
NAV (Nano Air Vehicles)	300 metros de altitud	Desarrollados para ejecutar misiones de inteligencia
<p>Algunas de estas categorías, posiblemente hasta el tamaño del TUAV, también se pueden relacionar con sistemas de ala giratoria, conocidos como helicópteros pilotados a distancia (RPH).</p>		
RPH, Remotely Piloted Helicopter or VTUAV, vertical take-off UAV o helicóptero pilotado a distancia o UAV de despegue vertical	Aproximadamente 10 Km	Los sistemas de ala giratoria también son menos susceptibles a las turbulencias del aire en comparación con los de ala fija, aeronaves de poca carga alar.

Fuente: Reg Austin- Unmanned Aircraft Systems (2010)

Por la misión específica del UAS: El componente más importante de un UAS, respecto a su estructura física, es la carga útil a bordo, puesto que determina las capacidades y misiones que puede desarrollar. Por consiguiente, los sistemas se clasifican en función de las mismas en UCAS (UAS de combate) o UAS ISTAR (UAS de Inteligencia, Reconocimiento, Vigilancia y Adquisición de objetivos).

Por el nivel de conducción de las operaciones militares: Otro tipo de clasificación, propio del ámbito militar, es aquel dado en función del nivel de la guerra para los que pueden ser empleados (Táctico, Operacional o Estratégico), como la elaborada por la Organización del Tratado del Atlántico Norte (OTAN) (Ver tabla 2 “Clasificación UAS OTAN”).

En cualquier caso, debe tenerse en cuenta que no existen barreras perfectamente delimitadas. Por ello, para cada ámbito hay que buscar una clasificación funcional o taxonomía adecuada a la actividad que se pretenda realizar.

Tabla 2. Clasificación UAS OTAN.

CLASIFICACIÓN UAV OTAN				
Clase (MTOW)	Categoría	Empleo	Altitud de operación AGL	Radio de Misión
CLASE I ≤ 150 Kg	MICRO < 2 kg	Táctico (Sección)	Hasta 200 pies	5 km (LOS)
	MINI 2-20 Kg	Táctico (Compañía)	Hasta 1.000 pies	25 km (LOS)
	LIGEROS >20 kg	Táctico (Batallón)	Hasta 1.200 pies	50 km (LOS)
CLASE II ≤600 Kg	TÁCTICO	Táctico (Brigada)	Hasta 10.000 pies	200 Km (LOS)
CLASE II >600 Kg	MALE (Medium Altitude Long Endurance)	Operacional	Hasta 45.000 pies	Sin límite (BLOS)
	HALE (High Altitude Long Endurance)	Estratégico	Hasta 65.000 pies	Sin límite (BLOS)
	Combate	Estratégico	Hasta 65.000 pies	Sin límite (BLOS)

Fuente: JCGUAS “UAV Classification Guide”. NNAG. (2011)

5. Componentes y funcionamiento.

Un UAS comprende una serie de elementos, o subsistemas, que funcionan de forma integral y que son indispensables para el vuelo de la aeronave. De manera general, los componentes de un UAS pueden representarse con la siguiente estructura:

Imagen 2: Estructura Funcional UAS



Fuente: Construcción AAAES

El **segmento aéreo** está constituido por la plataforma aérea, su carga útil y la parte del sistema de comunicaciones que lleva embarcado, tanto para el control en vuelo como para la transmisión de datos obtenidos.

El **segmento terrestre** está conformado por la estación de control en tierra (GCS), incluyendo el software para la interacción del sistema de control con las plataformas, equipos de comunicaciones, terminales de transferencia de datos en tierra (GDT), equipos de soporte en tierra (GSE), interfaces que reciben la información obtenida por los sensores, la analizan y transmiten a los usuarios, además de los dispositivos que permiten la comunicación con la entidad de control de tránsito aéreo y otras aeronaves. Así mismo, podría incluir los sistemas de lanzamiento y recuperación de

las plataformas aéreas y el equipamiento necesario para su despliegue y protección. Implícitamente, se incluye en este segmento el componente humano, como elemento indispensable para el empleo del sistema.

Entre los dos segmentos, se disponen los enlaces de comunicación *Uplink* (de la GCS hacia la aeronave) y *Downlink* (de la aeronave a la GCS), lo cual permite obtener la telemetría (datos) de vuelo de la aeronave, conocer su estado (parámetros de vuelo, fallas, entre otros) en tiempo real y explotar los productos obtenidos con la carga útil (cámaras, radares, sistemas de inteligencia de señales, entre otros).

Lo anterior, se resume en la siguiente tabla:

Tabla 3. Componentes Sistemas Aéreos No Tripulados

Componente	Descripción
Vehículo aéreo	La plataforma debe reunir unas características que le permitan explotar las capacidades de los sensores, armamento o carga útil.
Carga útil	Sensores, armamento para las misiones asignadas y todo tipo de cargas útiles.
Comunicaciones	Data links para control (LOS y BLOS) e intercambio de datos de misión.
Estación de control	Desde donde es operado o controlado por los operadores.
Equipos de apoyo	Lanzamiento y recuperación, kit de despliegue, etc.
Interfaz C2	Con los centros de operaciones y el ATC.
Componente humano	Pilotos, operadores de equipos especiales o sensores, comandantes de misión, técnicos de mantenimiento.

Fuente: Revista PERFILES. Edición febrero 2014-IDS, Madrid-España.

Específicamente, el funcionamiento de los componentes principales del UAS es el siguiente:

La plataforma aérea.

La constituye el vehículo aéreo capaz de sustentarse en el aire, así como todos los medios y sistemas generales que le permiten realizar esta labor de forma segura y eficiente. Está formado por el fuselaje (incluyendo los subsistemas que proveen la

información de vuelo como los pitot-estáticos, eléctricos, de combustible, superficies de control, entre otros), los sistemas de propulsión, control de vuelo, navegación de precisión y detección; y es el medio para transportar y emplear la carga útil para el cumplimiento de la misión. Pueden ser de ala fija o ala rotatoria y su diseño depende básicamente del empleo que se le pretenda dar.

El sistema de control de vuelo, conocido generalmente como aviónica (la cual incluye al piloto automático), es el cerebro de la aeronave y su función principal es controlar y gestionar todos los sistemas a bordo, garantizando que el UAS siga automáticamente el vuelo pre-programado o los comandos de dirección ordenados remotamente desde una estación de control en tierra o embarcada.

Así como es indispensable para el Operador o Piloto remoto conocer la posición exacta de la aeronave en tiempo real durante todo el vuelo, para el UAS, dependiendo de su configuración, puede ser indispensable conocer la ubicación exacta de la GCS, sobre todo cuando se presenta algún tipo de degradación del desempeño del sistema o en situaciones de emergencia en las cuales el Piloto remoto pierde conexión con la aeronave y no la puede controlar. El Sistema de Navegación (GNSS, INS, entre otros), especialmente en el caso de los RPAS, le permite a la aeronave regresar de forma segura a la base de lanzamiento o la ubicación de la GCS, cuando presenta pérdida de conexión con la misma, cumpliendo con la lógica que tiene preprogramada en su *software*.

El pilotaje de un UAS/RPAS puede ser, en algunos casos, similar al de una aeronave convencional, ya que, si bien la tripulación no se encuentra a bordo de la aeronave, esta dispone de la misma instrumentación y de los mismos sistemas de navegación empleados en aeronaves convencionales. Sin embargo, la aeronave también puede volar de forma autónoma.

En el caso de los RPAS, y dada la complejidad de sus sistemas y los tipos de misión en los que son empleados, además del piloto automático se requiere de la interacción humana constante con el Piloto Remoto. En especial en situaciones de emergencia, el Piloto remoto debe tomar el control de la aeronave, anulando al piloto automático y ejecutar cambios en los parámetros de vuelo que permitan sortear situaciones críticas y llevar la aeronave a un aterrizaje seguro.

Una característica de seguridad de la mayoría de los sistemas de piloto automático de los UAS, es que estos tienen la capacidad de realizar un procedimiento de "enlace perdido" en caso que la comunicación, entre la estación de control en tierra (GCS) y la aeronave, se vea interferida impidiendo la transmisión de datos entre las dos partes. Hay muchas formas diferentes en que estos sistemas ejecutan este procedimiento el cual, generalmente, implica crear un perfil de vuelo especial en el cual se establecen y cargan, a la memoria del sistema, los parámetros (altitudes, trayectoria de vuelo y velocidades) que deberá seguir la aeronave para su retorno seguro al punto de lanzamiento.

Otros ejemplos de procedimientos de “enlace perdido” son:

- Que la aeronave proceda a un punto de referencia, donde la intensidad de la señal sea segura para volver a adquirir conectividad.
- Que la aeronave regrese al último punto de la ruta programada de vuelo, permanezca en éste mientras se intenta recuperar la señal y luego, de no ser exitoso el procedimiento, regrese al punto de origen para aterrizar.
- Que la aeronave permanezca en el rumbo actual durante un período de tiempo predeterminado.
- Que la aeronave ascienda para recuperar el enlace.

La carga útil.

El tamaño y el peso de las cargas útiles es una de las mayores consideraciones que se tienen en cuenta al momento de diseñar un UAS. Este componente está constituido por los dispositivos embarcados requeridos para la misión los cuales, generalmente, son intercambiables o fácilmente reemplazables y pueden incluir desde cámaras electroópticas (EO) e infrarrojas (IR) hasta radares de apertura sintética (SAR), designadores lásericos y diferentes tipos de sistemas de armamento y sus municiones. Por lo general, un UAS tiene capacidad para transportar más de una carga útil al mismo tiempo, las cuales a su vez pueden almacenar y posteriormente entregar información a la GCS para su análisis y explotación. La carga útil, por tanto, al ser el fin último de la misión, se convierte en la parte más importante del UAS.

Sistema de control en tierra o estación.

Designada comúnmente por las siglas GCS (*Ground Control Station*) o UCS (*UAS Control Station*), incluye el conjunto de equipos y sistemas que asumen las tareas de planificación y control de la misión (control de vuelo, control de la carga útil, entre otros), así como, la distribución o diseminado de la información a usuarios exteriores y comunicaciones con el ATC (*Air Traffic Control*). Cuenta además con sistemas de navegación, pantallas de monitoreo del diagnóstico y estado del sistema, aviónica de vuelo, sistemas de cartografía, de comunicaciones seguras y procesadores de datos internos.

La GCS, en tierra o embarcada, es una parte integral del UAS que controla al vehículo en el espacio aéreo. Ésta aloja al Operador o Piloto remoto del UAS, así como a otros miembros de la tripulación que deben interactuar con los diferentes sistemas a bordo de la misma. Por lo anterior, la GCS debe poseer comunicaciones

seguras no solo con la aeronave, sino también con todo tipo de agencias de control del espacio aéreo, ya sean locales, regionales, nacionales o internacionales, si es el caso.

Sistemas de lanzamiento y recuperación.

Los sistemas de Lanzamiento y Recuperación (*Launch and Recovery System, LRS*), que forman parte del segmento terrestre, son los dispositivos empleados para las maniobras de despegue o lanzamiento y aterrizaje o recuperación del UAS.

Dependiendo del tipo de UAS, los procedimientos de lanzamiento y recuperación pueden ser complejos o prácticamente inexistentes. Los RPAS, por ejemplo, generalmente tienen procedimientos que requieren de personal para la preparación, lanzamiento y recuperación de la aeronave. Los de mayor envergadura, pueden requerir longitudes de pista de hasta 10,000 pies y equipos de apoyo como remolcadores de tierra, camiones de combustible y unidades de potencia para poder realizar estas maniobras. Otros RPAS de menor tamaño emplean equipos auxiliares como catapultas, redes y dispositivos diseñados para operar en un área determinada con el fin de lanzar o recuperar la aeronave. Así mismo, algunos UAS pequeños pueden ser lanzados con la mano y recuperados mediante métodos de pérdida de sustentación controlada o paracaídas, de acuerdo al diseño del sistema.

Comunicación y enlace de datos.

El requisito principal, y probablemente el más exigente durante el diseño del UAS, es el sistema de comunicaciones encargado de proporcionar los enlaces de datos, *Uplink* (desde la GCS hacia la aeronave) y *Downlink* (desde la aeronave hacia la GCS), que finalmente permite la interacción entre el Operador y/o Piloto Remoto y la aeronave. Generalmente para esto se emplean radiofrecuencias, pero también es posible a través de señales satelitales.

La importancia de estos enlaces para la operación de la aeronave está relacionada con el tipo de información que se transmite a través de cada uno, así:

- (a) Enlace ascendente (*Uplink*):
 - i) Transmite los comandos de ruta de vuelo, que son almacenados posteriormente en el sistema de control de vuelo automático de la aeronave.
 - ii) Transmite comandos de control de vuelo en tiempo real cuando es indispensable la intervención humana.

- iii) Transmite comandos de control a las cargas útiles y accesorios a bordo de la aeronave.
 - iv) Transmite información posicional de la GCS actualizada a la aeronave.
- (b) Enlace descendente (*Downlink*):
- i) Transmite datos posicionales de la aeronave a la GCS en tiempo real.
 - ii) Transmite imágenes y / o datos de carga la útil a la GCS para su explotación.
 - iii) Transmite datos de la condición general de la aeronave, por ejemplo, cantidad de combustible disponible, temperatura del motor, nivel de energía eléctrica, fallas entre otros.

La complejidad en el diseño del sistema de comunicaciones y, por lo tanto, el tipo de dispositivos requeridos para tal fin (por ejemplo, antenas, GDT, SATCOM, entre otros), están determinados por el rango de operación del UAS desde la GCS, el nivel de sofisticación exigido para la transmisión de datos de la carga útil y el nivel de seguridad de la información requerida por tipo de misión.

Con respecto a este último aspecto, por razones de seguridad, es habitual que los sistemas, especialmente los RPAS, dispongan de dos canales de comunicación. El canal primario es el encargado de la operación en condiciones normales, por lo que su velocidad de transferencia de datos y su latencia deben permitir el monitoreo en tiempo real de los principales parámetros de la aeronave, así como, hacer llegar los comandos de los Pilotos Remotos desde la GCS hasta la plataforma aérea con el menor retardo posible. El canal secundario se usa en caso de degradación del primario como medida de seguridad y sus requisitos de velocidad y latencia suelen ser menos exigentes que los del primario.

Componente Humano.

El elemento más importante del UAS, que no hace parte de su estructura física, es por supuesto, el humano. Lo anterior, teniendo en cuenta que la interacción humana; tanto del Operador/Piloto remoto, operador de sensores y técnicos de mantenimiento; es indispensable para el control, explotación, sostenimiento y aeronavegabilidad del sistema. El número de personas requeridas para la operación de los UAS y, de manera especial, de los RPAS, está determinado por la complejidad de cada sistema. Es posible que, en el futuro, el elemento humano disminuya a medida que la capacidad tecnológica aumente.

6. Identificación de amenazas y riesgos.

En procura de salvaguardar la Seguridad Operacional de las aeronaves de Estado, la infraestructura aeronáutica y crítica de los Entes de Aviación de Estado (EAE) y de la nación, así como de los bienes e integridad física de los miembros de la Fuerza Pública y la ciudadanía en general, es necesario reconocer la operación irregular de los UAS (entiéndase hostil, ilícita y/o imprudente) como un riesgo, teniendo en cuenta la diversidad de empleos que pueden tener y que advierten una amenaza creciente para las instalaciones militares. Citados riesgos se deben conocer, analizar y socializar en procura de implementar sistemas de seguridad integrados, capaces de detectar, identificar y, de ser necesario, neutralizar cualquier posible amenaza que se suscite producto del empleo de este tipo de sistemas.

Un UAS equipado con sensores infrarrojos y electro-ópticos es capaz de realizar vuelos de reconocimiento y obtención de inteligencia, que no solo crea una desventaja estratégica, sino que también puede encontrar los puntos más vulnerables de aquello que sobrevuela. Si a los elementos que conforman la carga útil, se adapta algún tipo de explosivo, se obtiene un arma letal, con un rango de acción muy amplio, de bajo costo y de gran facilidad de adquisición, estando su compra al alcance de cualquier persona.

Se requieren conocimientos básicos de ingeniería para adaptar un sistema de armamento rudimentario a un UAS. Sin embargo, al convertirse en objeto bélico al servicio de grupos delictivos, las consecuencias producto de la materialización de este riesgo podrían ser catastróficas. Por lo anterior, y si bien es importante referenciar y conocer los eventos hostiles en los que, a nivel mundial, se han empleado UAS¹, también es indispensable prever situaciones potenciales, incluso de mayor gravedad, en las que se emplee este tipo de sistemas para causar daño a la población civil de manera indiscriminada, por ejemplo, la adecuación de dispositivo tipo rociador, con la capacidad de esparcir agentes de carácter NBQR (Nuclear, Biológico, Químico, Radioactivo), sobre áreas pobladas.

Adicionalmente, es importante mencionar que existen antecedentes del empleo de UAS para el transporte de alucinógenos a instituciones carcelarias del país, vulnerando los sistemas de seguridad de estas zonas restringidas, así como también, los numerosos eventos por intrusión de UAS en diferentes Aeropuertos

¹ Hasta la fecha el incidente más grave conocido es el ataque perpetrado el 15 de septiembre de 2019 contra las instalaciones de 2 refinерías de la empresa saudí ARAMCO, responsable de la producción de un alto porcentaje de Petróleo a nivel mundial y para lo cual se emplearon 18 vehículos aéreos no tripulados y 7 misiles de crucero, disminuyendo la capacidad productiva de la infraestructura objetivo hasta en un 50%.

alrededor de mundo, ocasionado el cierre de operaciones de los mismos, y, por ende, pérdidas económicas considerables.

INTENCIONALMENTE EN BLANCO

CAPÍTULO C. SISTEMAS CONTRA UAS (C-UAS)

1. Antecedentes e importancia de los C-UAS.

El desarrollo exponencial de las tecnologías de uso recreativo o entretenimiento aplicadas al sector de los UAS; la gran oferta en el mercado, bajo costo, simplicidad, entre otros que facilitan su adquisición; las capacidades de las plataformas y sus sensores, así como la falta de medidas de control para la adquisición y operación de los UAS, han provocado un cambio significativo en el entorno operacional.

Dentro de los eventos objeto de referencia de este capítulo, son relevantes las intrusiones de UAS, en aeropuertos de alto flujo operacional como Singapur, Frankfurt, Dublín, Madrid y Londres, situaciones que han resultado en el cierre de sus pistas, paralizando las operaciones aéreas, ocasionado el retraso y cancelación de vuelos programados y generando grandes pérdidas, tanto para las empresas operadoras como para los usuarios, además de riesgos considerables para la seguridad de las aeronaves tripuladas. Así mismo, los eventos operacionales por intrusión de UAS en diferentes Aeropuertos de Colombia, especialmente en el Aeropuerto Internacional “El Dorado” de Bogotá y los avistamientos de sistemas de este tipo en las inmediaciones de las Unidades Militares, de Policía y algunas edificaciones consideradas infraestructura crítica de la Nación.

Finalmente, el ataque perpetrado el 15 de septiembre de 2019 contra las instalaciones de 2 refinerías de la empresa saudí ARAMCO, responsable de la producción de un alto porcentaje del Petróleo mundial y para lo cual se emplearon 18 vehículos aéreos no tripulados y 7 misiles de crucero.

Adicionalmente, es importante considerar que el empleo de UAS como aeronaves de la AE, generalmente destinadas al desarrollo de operaciones de inteligencia y vigilancia es cada vez mayor, lo cual convierte a estos activos aeronáuticos en objetivos a neutralizar por parte del enemigo, a través del uso de sistemas C-UAS.

2. Categorización de la amenaza.

Existen múltiples clasificaciones y categorías de UAS en función del peso, altitud de vuelo, alcance, nivel de empleo, entre otras, pero en general, las diferentes clases de UAS se establecen en relación con el peso máximo de despegue (*MTOW: Maximum Takeoff Weight*).

Sin embargo, debido a la proliferación exponencial, cuantitativa y cualitativa, de los UAS y la amplitud del espectro para su modificación, algunas de estas clasificaciones se consideran un tanto decimonónicas y, en este sentido, resulta un desafío establecer una categorización de la amenaza que sea perdurable y que no esté sujeta a constantes actualizaciones.

Imagen 2: Categorización de la amenaza

	UAS CLASE IA	UAS CLASE IB	RPAS CLASE IC Y ID
			
Peso	200 g a <7 Kg	7kg a <15 Kg	15Kg a < 80 Kg
Altitud	<400 pies AGL	<1000 pies AGL*	>15000 pies AGL
Velocidad	Hasta 40 Kts	Hasta 50 kts	Hasta 80 Kts
Autonomía	<40 minutos	3-4 horas	>16 horas

*La altitud de operación de los UAS de la Aviación de Estado es de 400 pies AGL en espacios aéreos Clase G.

Fuente: Construcción AAAES

Por lo tanto, para los efectos de este capítulo, la categorización de la amenaza “se enfocará en aquellos sistemas que, debido a sus características de reducida superficie radar equivalente, baja firma infrarroja y/o acústica, o vuelo a baja altura y velocidad, denominados UAS LSS, hacen que se sitúen fuera de la envolvente de detección, seguimiento, identificación y neutralización de los sistemas actuales de Defensa Aérea (DA)” (Centro Conjunto de Desarrollo de Conceptos, 2019), ocasionado que los medios disponibles para la DA y Protección de los EAE no resulten eficaces.

Por lo anterior, se consideran dos escenarios fundamentales:

- (a) **Unidades e instalaciones militares en operaciones transitorias:** Incluye las Unidades a flote, fuerzas desplegadas y demás Unidades militares y de policía móviles sobre las cuales se proyecta una amenaza creciente debido a la evolución del empleo hostil de UAS LSS, desde su utilización como

sensores de vigilancia de la actividad propia, hasta el uso como vector de armamento improvisado.

- (b) **Unidades e instalaciones militares fijas:** En este tipo de unidades militares y de policía, factores tales como el entorno urbano, la presencia de población civil, la proliferación del uso recreativo de estos sistemas, la posible vulnerabilidad de las infraestructuras críticas y la alarma social que podría provocar esta amenaza en territorio nacional, implican una mayor complejidad y la aparición de nuevos aspectos a considerar.

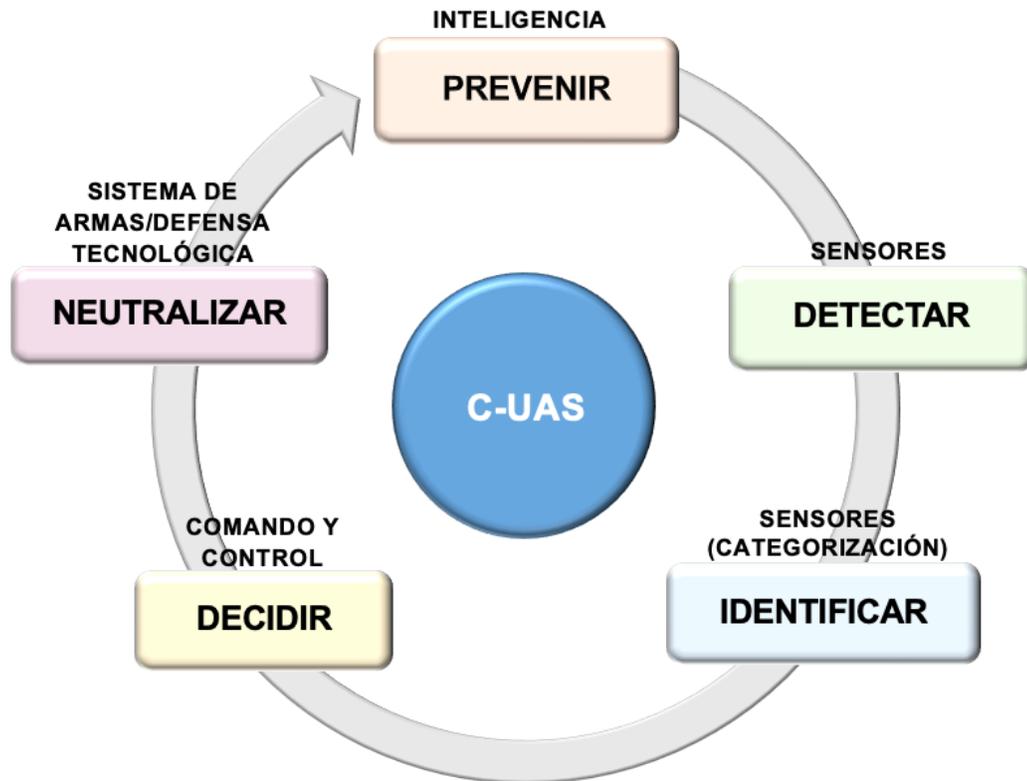
3. Definición Sistemas Contra U-AS.

La *Tecnología de contraataque* (Michel, 2019), también conocida como contra-UAS o simplemente C-UAS, se refiere a sistemas que se utilizan para detectar y/o deshabilitar aeronaves no tripuladas. Es un “*sistema de sistemas*” formado por diferentes sensores, interface de mando y control (C2) y sistemas de armas, diseñados para las diferentes fases de lo que se denomina *Ciclo C-UAS*.

Las fases del Ciclo C-UAS son: prevención, detección, identificación, decisión y neutralización (Centro Conjunto de Desarrollo de Conceptos, 2019) como se muestra en la siguiente imagen:

INTENCIONALMENTE EN BLANCO

Imagen 1: Diagrama Fases Ciclo C-UAS



Fuente: Ministerio de Defensa de España (2018), *GT Tecnología- Concepto Contra Sistemas Aéreos No Tripulados*, Centro Conjunto de Desarrollo de Conceptos, Madrid-España.

Para cada una de las fases, existen tecnologías y sensores disponibles en el mercado o en proceso de desarrollo. Sin embargo, al momento de definir cuál de estas se adapta más a las necesidades de cada área objeto de protección, deberán considerarse las ventajas e inconvenientes que presenta cada tipo de sensor, especialmente en lo relacionado a la posible interferencia que pueda generarse para las comunicaciones aeronáuticas y sistemas de ayudas para la navegación aérea.

Así mismo, durante los procesos de adquisición de UAS para la Fuerza Pública, es necesario identificar las vulnerabilidades propias de los sistemas frente al empleo de C-UAS y las medidas que deberán tomarse en el desarrollo de operaciones aéreas con el fin de mitigar los riesgos asociados.

4. Clasificación C-UAS.

4.1 Tipos de tecnología C-UAS.

Si bien, la oferta tecnológica de C-UAS en el mundo es difícil de dimensionar, es posible categorizarla en dos grupos: Cinética y No cinética.

La **tecnología cinética** es representada por los sistemas de DA actuales (Ej.: Sistemas Patriot, F-100, NASAMS, HAWK, Misil Mistral, entre otros), mientras que la **tecnología No cinética** puede sub clasificarse en sistemas de detección, seguimiento e identificación (medios pasivos) y sistemas de mitigación (medios reactivos).

4.2 Sistemas de Defensa Aérea y sus limitaciones.

Los Sistemas de Defensa Aérea actuales emplean mayoritariamente sistemas de armas cinéticos para neutralizar amenazas aéreas, los cuales son totalmente válidos para amenazas convencionales, así como para RPAS categorías II y III, debido a su similitud a las aeronaves tripuladas. Sin embargo, su utilización frente a UAS de categoría I, tipo MICRO y MINI o UAS LSS presenta una serie de limitaciones que deben ser evaluadas. Entre estas limitaciones es posible destacar:

- (a) **Daño colateral:** La neutralización de UAS LSS por medio de sistemas de armas cinéticos en entornos urbanos puede ir en contra del daño colateral aceptable, por lo que su uso puede estar restringido.
- (b) **Economía:** Los costos de empleo del armamento de los Sistemas de DA frente a un enemigo convencional son relativamente equilibrados y en muchos casos beneficiosos, por lo que su operación es asumible y justificable. Sin embargo, dado el bajo costo de los UAS LSS, emplear este tipo de sistemas para su neutralización resulta poco factible.
- (c) **Cantidad:** Actualmente ningún sistema de armas cinético puede hacer frente a un ataque masivo de UAS y, en el caso de que pudiera hacerle frente, el costo económico y de material sería inasumible.
- (d) **Efectividad:** Para los sistemas de armas cinéticos, un objetivo UAS LSS supone un verdadero reto por sus características especiales, por

lo que la probabilidad de derribo (P_k) esperada frente a esta amenaza podría ser en algunos casos elevada y en otros prácticamente nula, dependiendo del perfil de vuelo del objetivo, así como de diversos condicionantes.

4.3 Sistemas de detección, seguimiento e identificación.

Se encargan de identificar las señales del UAS, determinar su ubicación y, en algunos casos, un vector hacia su punto de control.

Dentro de estos sistemas encontramos los radares, receptores de ondas de radio, sensores acústicos y sensores ópticos, cuyas características son:

INTENCIONALMENTE EN BLANCO

Tabla 1: Sistemas C-UAS de detección, seguimiento e identificación

TIPO DE SISTEMA	DESCRIPCIÓN
Radar	Detecta la presencia de UAS LSS por su firma de radar, generada cuando la aeronave encuentra pulsos de radiofrecuencia emitidos por el elemento de detección. Estos sistemas a menudo emplean algoritmos para distinguir entre UAS y otros objetos pequeños, como pájaros.
Radio-Frecuencia	Detecta, localiza y, en algunos casos, identifica UAS cercanos escaneando las frecuencias en las que se sabe que operan la mayoría de estos.
Electro-óptico (EO)	Identifica y rastrea UAS en función de su firma visual.
Infrarrojo (IR)	Identifica y rastrea UAS en función de su firma de calor.
Acústico	Detecta UAS al reconocer los sonidos únicos producidos por sus motores. Se basan en una biblioteca de sonidos producidos por UAS conocidos, que luego se comparan con sonidos detectados en el entorno operativo.
Sensores Combinados	Muchos sistemas integran una variedad de diferentes tipos de sensores para proporcionar una mayor capacidad de detección, seguimiento e identificación.
Cetrería	Adiestramiento de aves rapaces para la captura o interceptación de UAS en vuelo.

Fuente: Michel (2019), *Counter-drone Systems*

Los sistemas basados en radar se pueden usar como un medio principal de detección; sin embargo, generalmente se enfrentan a la falta de automatización y dependen en gran medida de un operador capacitado para darse cuenta de identificaciones nuevas o cambiantes, trazar y rastrear geolocalizaciones, y elegir la configuración de sistema adecuada.

Este tipo de sistemas también enfrenta dificultades cuando se emplean con UAS que solo se mueven verticalmente o se desplazan en su lugar. Algunos sistemas radar pueden activar un sistema electroóptico secundario que apunta los sensores ópticos automáticamente en la dirección del objetivo de interés detectado. Esta característica puede ser inefectiva, en ocasiones, si el sistema detecta inadvertidamente un avión tripulado más grande como un nuevo objetivo.

Los sensores de radar están especialmente ajustados para identificar objetivos pequeños a distancias cortas, medias o largas; por lo tanto, pueden ser necesarios múltiples radares con diferentes rangos de detección para cubrir las áreas objetivo.

Así mismo, los sensores electroópticos (EO) e infrarrojos (IR) no suelen servir como sistemas de detección primarios para identificar y rastrear un UAS. Sin embargo, pueden ser herramientas secundarias importantes de validación visual para objetivos detectados por sensores primarios. Aunque hay sistemas EO avanzados, que pueden proporcionar la capacidad de hacer seguimiento automático a imágenes de objetivos potenciales detectados; son vulnerables ante la posibilidad de ser redirigidos a objetivos falsos, como pájaros o aviones tripulados que cruzan el campo de visión.

4.4 Sistemas de mitigación.

Son sistemas dotados con la capacidad de interferir con la señal de control entre el UAS y su operador, afectar el rendimiento del mismo, neutralizarlo e incluso suplantar su señal de control con el fin de detener cualquier actividad que realice. Algunos ejemplos de este tipo de tecnología son:

Tabla 2: Sistemas C-UAS de mitigación

TIPO DE SISTEMA	DESCRIPCIÓN
<i>Jamming</i> de RF	Interrumpe el enlace de radiofrecuencia entre el UAS y su operador al generar grandes volúmenes de interferencia en la RF. Una vez que se corta el enlace RF, que puede incluir enlaces WiFi, el UAS generalmente descenderá al terreno o iniciará una maniobra de "regreso a casa".
<i>Jamming</i> de GNSS	Interrumpe el enlace satelital que el UAS utiliza para la navegación, como GPS o GLONASS. Los UAS que pierden su enlace satelital generalmente mantienen su posición actual, aterrizan o regresan al punto de control, lo cual facilita la identificación de la ubicación del operador.
<i>Spoofing</i> y/o <i>Meaconing</i>	Permiten suplantar las señales de posicionamiento del UAS para hacer creer a la aeronave que se encuentra en una posición distinta a la real, ocasionando errores en la ejecución de los comandos programados por el Operador.
<i>Dazzling</i>	Emplea un haz de luz de alta intensidad o láser para "cegar" la cámara del UAS.
Láser	Destruye segmentos vitales de la aviónica del UAS usando energía dirigida, lo que hace que impacte contra el terreno.
Microondas de alta potencia	Dirige pulsos de energía de microondas de alta intensidad al UAS, deshabilitando los sistemas electrónicos de la aeronave.
<i>Snagging</i>	Redes expulsadas desde otras aeronaves pilotadas remotamente o elementos ubicados en tierra con el fin de capturar al UAS en vuelo y obligarlo a aterrizar de manera controlada.
<i>UAS de colisión</i>	UAS diseñados para colisionar directamente contra otros clasificados como adversarios.
<i>Hacking</i>	Empleo de software malicioso que ataca las vulnerabilidades de seguridad en sistemas o redes necesarios para la operación del UAS, afectando su rendimiento.

Fuente: Michel (2019), *Counter-drone Systems*

Nota 1: Los fabricantes o vendedores de C-UAS usualmente ofrecen equipos que pueden operarse tanto en modo pasivo como activo, lo cual, en teoría, garantiza que únicamente interferirán en el rendimiento de las señales de Radio Frecuencia (RF) empleadas en la operación aérea cuando se tenga la intención de neutralizar un UAS catalogado como hostil. Sin embargo, se debe tener en cuenta que algunos sistemas pueden emitir señales durante los procesos de actualización de su software, la instalación del equipo en el sitio o durante las calibraciones del sistema. Por esta razón, no es posible asumir categóricamente que el sistema de detección emite energía de RF de forma completamente controlada lo cual puede representar un riesgo para la Seguridad Operacional.

Nota 2: Consulte las capacidades, limitaciones, ventajas y desventajas de los Sistemas C-UAS más utilizados en el Anexo 1 de esta Guía “Características y limitaciones del Sistemas C-UAS de mayor empleo”.

4.5 Tipos de plataformas C-UAS.

Existen diferentes tipos de plataformas C-UAS entre las que destacan las 3 siguientes:

- a) **Basadas en tierra (ground-based):** Son sistemas diseñados para ser utilizados desde una estación fija o móvil en tierra, esta categoría incluye sistemas instalados en sitios fijos, sistemas móviles, y sistemas montados en vehículos móviles.
- b) **Portátiles o de mano (Hand-held):** Sistemas que son diseñados para ser operados por una persona o por sistemas automatizados muy simples que no requieren grandes infraestructuras, muchos de estos sistemas se asemejan a rifles u otras armas pequeñas.
- c) **Basada en UAS:** Sistemas diseñados para estar montados en un UAS los cuales pueden estar en las proximidades del objetivo con el fin de emplear una interdicción al UAV enemigo intentando realizar un cerramiento del rango de operación.

5. Recomendaciones para la adquisición e implementación de C-UAS.

Los EAE deberán tener en cuenta las siguientes consideraciones para la adquisición y empleo de C-UAS:

- (a) Los EAE deben propender porque todos sus C-UAS cuenten con una póliza de seguro vigente para responder por eventuales daños y perjuicios a terceros, de conformidad con lo dispuesto en el *Código de Procedimiento Administrativo y de lo Contencioso Administrativo*, y demás normas que regulen la materia. En todo caso, la operación de C-UAS de la AE deberá incluirse dentro de las Pólizas de Seguro que amparan los procedimientos de los EAE, de acuerdo a sus funciones, roles, misiones y capacidades distintivas.
- (b) Un factor clave para determinar la viabilidad de instalar un sistema de detección en o alrededor de un área objetivo (Unidad Militar y/o policial, aeropuerto, edificio, entre otros) es la cantidad de sensores necesarios para lograr la cobertura deseada del espacio aéreo. Debido a que el volumen de cobertura depende de las características y requisitos únicos de cada objetivo y del tipo de sistema, la cantidad de sensores variará. La distancia de cobertura para muchos tipos de tecnologías de detección también limita la eficacia de dichos sistemas para determinar las ubicaciones de los UAS y su punto de control. Además, es posible que las áreas de cobertura necesiten abarcar ángulos más amplios, ya que, el Piloto Remoto y/u Operador pueden no estar cerca del UAS.
- (c) No existe una única solución tecnológica C-UAS LSS que sea efectiva contra toda amenaza, en todo momento y lugar, por lo que se debe considerar qué tipo de sistema es más adecuado para cada escenario de empleo del EAE, entorno y situación general del objetivo a proteger. En este sentido, se debe evaluar no solo la protección de los activos estratégicos y la infraestructura crítica de la nación, sino también de las unidades e instalaciones militares y de policía dentro de territorio nacional, entre las que destacan principalmente las bases aéreas y aeródromos de operación de la Fuerza Pública por su complejidad y el impacto que podría llegar a tener la acción de UAS LSS sobre la actividad aérea que en ellas se desarrolla.
- (d) Así mismo, la protección de los buques y demás Unidades a flote de la Armada Nacional, tanto atracados y durante las entradas y salidas de puerto, como durante las navegaciones, requerirá de sistemas C-UAS LSS adecuados a dichas situaciones.

- (e) Los sistemas C-UAS LSS deberán ser modulares, escalables, rápidamente actualizables para adaptarse a la evolución de la amenaza; que permitan la integración de diferentes tipos de sensores para la detección, identificación, decisión, y de sistemas para la neutralización; que se basen en la cooperación de tecnologías complementarias (radar, optrónica, acústica, energía dirigida, submunicaciones, entre otros); que tengan fácil movilidad, portabilidad y que cumpla con los requerimientos mínimos para su puesta en funcionamiento tras un cambio de ubicación (Centro Conjunto de Desarrollo de Conceptos, 2019).
- (f) Los sistemas C-UAS LSS más complejos deberán disponer de un alto grado de automatización, que permita un proceso de decisión ágil. Debido al escaso tiempo de respuesta del que disponen los sistemas C-UAS LSS, las fases de detección, identificación y la recomendación de decisión (neutralizar o no) deberían realizarse de forma automática. La fase de neutralización se debería poder configurar en modos de operación manual, semiautomático y automático, dependiendo de la amenaza, escenario, entorno, situación, estado de alerta y reglas de enfrentamiento vigentes. Así mismo, las interfases de los sistemas deben poder ser integradas desde centros de monitoreo y así mismo poder interactuar con los demás sistemas electrónicos de seguridad disponibles. (Centro Conjunto de Desarrollo de Conceptos, 2019).
- (g) Si bien los sistemas C-UAS LSS podrían llegar a tener la capacidad de interconectarse e integrarse mediante un sistema de C2 con el resto de los sistemas de Defensa Aérea (DA) y de Protección a Fuerza (PF), se considera que en el corto y medio plazo la integración debería ser como mínimo a nivel local de cada sistema C-UAS LSS, para asegurar un ciclo de decisión del operador adecuado en cuanto a la neutralización o no del UAS LSS detectado. Hasta que la tecnología no permita una integración completa de los sistemas C-UAS LSS en el Sistema de Defensa Aérea, ésta se llevará a cabo mediante procedimientos y comunicaciones directas.
- (h) Se deberá buscar la sencillez en la operación y el mantenimiento, con el fin de que su empleo solo requiera un determinado nivel de especialización y no de especificidad, reducir las necesidades de Instrucción y Adiestramiento (I+A) y la huella logística para el despliegue.
- (i) Los sistemas C-UAS LSS deberán tener un alto grado de disponibilidad operativa, que les permita su funcionamiento en ciclos de 24/7, lo que requerirá de sistemas con una alta fiabilidad y mantenimientos programados que se puedan ejecutar con rapidez.

- (j) La capacidad C-UAS LSS debe ir más allá de los sensores y sistemas necesarios para la detección, identificación y neutralización de los UAS LSS. Se considera necesario actuar contra el adversario que ha decidido emplearlos de forma hostil contra el EAE. Para ello, la explotación técnica de la información obtenida de los componentes y capacidades de los UAS LSS neutralizados, apoyaría la fase de prevención del ciclo C-UAS LSS. De la misma forma es vital que los EAE generen y compartan con sus estamentos de inteligencia datos estadísticos de las detecciones de UAS hostiles a la AE y/u organismos civiles. Esto servirá como un insumo para que los organismos de inteligencia institucionales y nacionales realicen búsquedas de información puntuales que fortalezcan los productos que generan estas agencias.
- (k) Las necesidades de infraestructura vendrán condicionadas por el tipo de sistema C-UAS LSS (portátil/fijo/móvil), los diferentes sistemas que lo compongan (sensores de detección e identificación, sistema C2, sistema de neutralización) y el nivel de integración que se determine (aislado, local, C2, total). Se considera que el mantenimiento de los sistemas C-UAS LSS se podría realizar en las infraestructuras actuales. No obstante, se debería procurar que las necesidades de instalación sean las mínimas posibles y limitadas al emplazamiento físico del sistema.
- (l) La nueva capacidad C-UAS LSS implicará tener que revisar y adaptar la doctrina existente conjunta, específica y combinada, sobre la utilización de las diferentes capacidades afectadas por la misma, así como analizar la posibilidad de creación de una doctrina particular. La evolución será muy rápida, por lo que se debería desarrollar en paralelo a los nuevos sistemas, para que la solución al problema no pierda eficacia o se quede obsoleta en un corto periodo de tiempo.
- (m) El Anexo 2 de esta guía “Consideraciones Técnicas para la selección de C-UAS”, provee una orientación con preguntas que pueden ser empleadas por los EAE, dentro de los procesos de elección de Sistemas C-UAS, con el fin de orientar adecuadamente la información que requiere el EAE por parte de las empresas fabricantes para tomar decisiones adecuadas en la adquisición de este tipo de equipos, propendiendo por una estandarización tecnológica que favorezca la escalabilidad de los equipos, el desarrollo y línea logística asociada a estos equipos.

ANEXO 1
CARACTERÍSTICAS Y LIMITACIONES DE SISTEMAS C-UAS DE MAYOR EMPLEO

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
<p>Láser Ejemplos: Boeing YAL-1 / ABL (Airbone Laser) AN/SEQ-3 Laser Weapon System (XN-1 LaWS) MEHEL Rheinmetall HEL</p>	<p>Un láser es un dispositivo que produce un haz intenso y unidireccional de luz coherente. A diferencia de la luz ordinaria, generada por el sol o una bombilla, el rayo láser es coherente y casi uniforme en longitud de onda, y viaja en una sola dirección. Hay dos formas por las cuales un láser puede destruir un objetivo: destrucción térmica y destrucción mecánica.</p> <p>La destrucción térmica se produce cuando la energía térmica dirigida por un arma láser permanece en el mismo punto en un objetivo, es absorbida por la superficie objetivo y, por lo tanto, da como resultado el calentamiento por el efecto Joule. Con suficiente precisión y tiempo de permanencia, tras la fusión empezará a vaporizarse.</p> <p>La destrucción mecánica o «destrucción por impulso» ocurre cuando los pulsos de láser cortos e intensos interactúan con la superficie del objetivo, creando una onda de choque que penetra en el objetivo, pudiendo causar un colapso estructural y destruir componentes mecánicos internos.</p>	<p>Reducción drástica de los costes tanto de adquisición, como de operación y empleo.</p>	<p>El haz láser en su desplazamiento se ve afectado por las partículas presentes en la atmosfera como vapor de agua, dióxido de carbono, humo o calima.</p>
		<p>Concepto de sistemas de armas con mantenimiento y piezas de repuesto reducido.</p>	<p>Existen materiales resistentes a la acción del láser, por lo que podría ser inefectivo frente amenazas revestidas de materiales que reflejen la energía láser.</p>
		<p>Al ser un arma electromagnética el desplazamiento del rayo láser se produce a la velocidad de la luz, por lo que su efecto es casi instantáneo.</p>	<p>A diferencia de gran multitud de sistemas de armas cinéticos, necesita mantener constantemente la línea de visión sobre el objetivo.</p>
		<p>A diferencia de un sistema de armas cinético, el número de disparos disponible únicamente dependerá de la capacidad del sistema de armas de suministrar corriente eléctrica y de la refrigeración del mismo.</p>	<p>No puede iluminar a varios objetivos a la vez, por lo que en caso de multiamenaza son necesarios varios sistemas láser o complementarlo con otros sistemas de armas.</p>
		<p>Flexibles y modulares.</p>	<p>La potencia alcanzada hasta ahora en los sistemas de armas láser es insuficiente para amenazas aéreas no tripuladas de Clase II o superior.</p>
		<p>Pueden operar a cualquier nivel de potencia hasta su máximo nominal, por lo que permite al operador adaptar el efecto deseado en función de la situación táctica.</p>	

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
<p>Sistemas de armas de microondas de alta potencia (HPM)</p> <p>Ejemplos: RANETS-E PHASER HPEM counter UAS Counter-electronics High Powered Advanced Missile Project (CHAMP)</p>	<p>Son otro tipo de arma de energía dirigida, que tiene una longitud de onda mucho más larga y una frecuencia mucho más baja que el láser.</p> <p>Las armas HPM generalmente se subcategorizan como sistemas de banda estrecha (NB) o banda ultra ancha (UWB).</p> <p>Los sistemas de HPM de banda estrecha tienen mejores características de transmisión y menos problemas con el fratricidio que los sistemas de banda ultra ancha. Además, los sistemas de banda estrecha requieren un conocimiento previo de la amenaza para identificar la frecuencia específica de interés y son más susceptibles a contramedidas.</p> <p>Las armas HPM de banda ultra ancha proporcionan un amplio rango de capacidades incluso con poco o ningún conocimiento del objetivo. Dado que la destructividad de las armas HPM de banda ultra ancha depende de su distancia al objetivo, tienen un alcance efectivo más corto que las armas de banda estrecha que generalmente tienen una mayor potencia radiada.</p> <p>La energía de HPM puede afectar a cualquier cosa que responda a tensiones y corrientes inducidas electromagnéticamente.</p>	<p>Al igual que las armas láser, son una opción económica en comparación con los sistemas de armas cinéticos.</p> <p>Como arma electromagnética su acción es casi instantánea. A diferencia del láser no le afectan las condiciones atmosféricas para su operación.</p> <p>A diferencia de los láseres, las armas HPM pueden atacar a múltiples objetivos y para que sean efectivas no necesitan tanta precisión como un láser. Es por ello por lo que son muy efectivas frente a enjambres de UAS.</p> <p>Permiten diferentes efectos sobre los objetivos dependiendo de la potencia de emisión. Incluso pueden producir daños en equipos apagados.</p>	<p>El alcance de las armas HPM es muy discreto en comparación con muchos sistemas de armas cinéticos. Este depende de la frecuencia generada, la distancia al objetivo y la susceptibilidad del objetivo</p> <p>Existen multitud de posibilidades para proteger un sistema frente al ataque por HPM. Instalación de cajas de Faraday, filtros, conductores de fibra óptica, antenas específicas o uso de láminas conductoras sobre uniones.</p> <p>A diferencia del láser, el riesgo de fratricidio con armas HPM es elevado. Cualquier cosa susceptible al HPM en su rango de cobertura será afectada. Son necesarios procedimientos o conos de cobertura en los que no operen fuerzas amigas, así como medidas de protección propias frente a este tipo de armas.</p> <p>Emiten una firma electrónica fácilmente localizable, por lo que pueden delatar la posición al enemigo y ser objeto de ataque por parte de este.</p>

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
<p style="text-align: center;">Interferencia electromagnética (Electromagnetic Jamming)</p> <p>Ejemplos: J4SKY-T Virtual-Fence AUDS Anti-UAV Defence System R-330ZH DroneGun</p>	<p>La interferencia puede ser vista como una señal no deseada dentro del rango de operación de un determinado sistema de comunicación. La calidad de un sistema de telecomunicación está directamente ligada a la relación entre la potencia de señal deseada y la potencia de ruido más la interferencia (SINR - <i>Signal to Interference plus Noise Ratio</i>) captada por el receptor dentro de la banda de transmisión. De esta manera, cualquiera que sea el tipo de interferencia, se tendrá una reducción de esa relación y, consecuentemente, una degradación en la calidad de la comunicación.</p> <p>Las interferencias intencionales son aquellas generadas de forma deliberada, a fin de inviabilizar el establecimiento de enlaces de comunicación en determinadas frecuencias.</p> <p>El jamming es la radiación deliberada, reradiación o reflejo de la energía electromagnética con el fin de prevenir o reducir el uso efectivo del espectro electromagnético por parte del enemigo, con la intención de degradar o neutralizar la capacidad de combate del mismo.</p> <p>Su efectividad dependerá de la técnica usada y de las características del objetivo. Los UAS LSS, generalmente, si son controlados a distancia están transmitiendo señales de RF, bien sean de control, de video o de posición. Por otro lado, si siguen una ruta de vuelo preprogramada, en la que vuelan de forma autónoma, utilizan señales de alguno de los sistemas globales de navegación por satélite para seguir la misma.</p>	<p>Jamming link de datos</p> <p>Como arma electromagnética su acción es casi instantánea. Además, son sistemas muy económicos y efectivos frente a amenazas no protegidas.</p>	<p>Jamming link de datos</p> <p>Las bandas de RF en las que operan son utilizadas por sistemas de telefonía móvil, telecomunicaciones o redes Wi-Fi entre otros, por lo que su acción puede afectar a sistemas propios o sistemas no deseados.</p>
		<p>Hay disponibles sistemas de <i>jamming</i> tanto direccionales para una amenaza localizada, como omnidireccionales para cubrir grandes áreas.</p>	<p>En diversos países hay bandas de frecuencia que están protegidas, por lo que su interferencia solo puede ser autorizada por el Gobierno.</p>
		<p>Permiten una acción dirigida pudiendo atacar el enlace de datos de video, telemetría y control.</p>	<p>Actualmente existen multitud de desarrollos tecnológicos tanto civiles como militares para evitar las interferencias en su sistema de comunicación.</p>
		<p>Generalmente neutralizan la amenaza sin destruirla. En este sentido puede permitir capturar el UAS enemigo (por ejemplo, si la aeronave entra en modo pérdida de link y efectúa aterrizaje de emergencia) o incluso localizar al operador en el caso de UAS LSS (por ejemplo, persiguiendo a un dron en situación de <i>Regreso a casa</i>).</p>	<p>Dado un caso de <i>jamming</i> sobre una amenaza por UAS LSS en el que esta revierte a modo seguro de retorno a punto de origen, si el atacante selecciona como punto de origen las coordenadas del objetivo deseado se daría la situación en la que el <i>jamming</i> del sistema de armas aproxime la amenaza al objetivo.</p>
		<p>Son altamente flexibles pudiéndose instalar en localizaciones fijas o móviles.</p>	<p>Gran número de UAS pueden ser programados para operar autónomamente sin la necesidad de un link de datos con el operador, por lo que los sistemas de armas <i>jamming</i> en este caso serían totalmente inefectivos.</p>
		<p>Jamming señal GNSS</p>	<p>Jamming señal GNSS</p>
		<p>Sistemas muy económicos y tecnológicamente sencillos.</p>	<p>Su empleo con sistemas omnidireccionales puede afectar a sistemas propios o no deseados.</p>
		<p>Altamente efectivos para UAS que operan de manera autónoma, inhabilitando su guía u obligando al operador a tomar el control. Para UAS de ala fija la información de los sistemas GNSS es vital en la maniobra de aterrizaje (un error del sistema de navegación de 1 metro se traduce en una imprecisión de 10 metros en el punto de aterrizaje).</p>	<p>Actualmente existe multitud de sistemas de navegación dual GNSS/inercial, de tal manera que si el UAS pierde la señal satélite pasa a navegación autónoma con sistema inercial. El sistema inercial es menos preciso que el satelital, pero puede ser suficiente en el caso de UAS hostiles atacando objetivos de dimensiones moderadas.</p>
		<p>Para el caso de los UAS LSS, una pérdida de señal válida de un sistema GNSS puede provocar la colisión contra el terreno o contra objetos colindantes.</p>	<p>Existen antenas con tecnología anti-<i>jamming</i> de GNSS. Por otro lado, hay numerosos programas que están desarrollando soluciones tecnológicas para evitar el <i>jamming</i> GNSS.</p>
		<p>Pueden ser direccionales u omnidireccionales, cubriendo grandes áreas.</p>	<p>La acción del <i>jamming</i> de la señal GNSS sobre un UAS controlado por un operador puede no ser suficiente para neutralizarlo.</p>
<p>Altamente efectivos frente a enjambres de UAS.</p>			
<p>Son altamente flexibles, pudiéndose instalar en sitios fijos o móviles.</p>			

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
Spoofing	<p>Es un tipo de ataque a la lógica de las aplicaciones. El tipo más común frente a drones es el <i>spoofing</i> de la señal GNSS.</p> <p>Consiste en la transmisión deliberada de una señal falsa de GNSS con la intención de engañar a un receptor proporcionándole información falsa de posición, velocidad y tiempo.</p> <p>El objetivo del ataque spoofing es forzar de manera inadvertida al receptor GNSS a seguir la señal modificada con el objetivo de inducir un error de posición.</p> <p>Realizar spoofing sobre las bandas encriptadas de los sistemas GNSS como la banda P (Y) de GPS o la banda PRS del Galileo es prácticamente imposible. Sin embargo, en estos casos un tipo de ataque efectivo es el Meaconing, que consiste en grabar señales encriptadas y re-radiarlas posteriormente. Si el receptor interpreta estas señales como válidas, estará asumiendo un error.</p>	Proveen un tipo de ataque muy económico y tecnológicamente sencillo.	Su empleo con sistemas omnidireccionales puede afectar a sistemas propios o no deseados.
		Altamente efectivos para drones que operan de manera autónoma con sistema GNSS no encriptado.	Necesita de operadores con conocimientos avanzados a diferencia de otros sistemas de armas no cinéticos.
		Accesibles tanto en el mercado civil como el militar.	Frente a señales GNSS encriptadas sus efectos son limitados. Para estos casos se puede emplear <i>Meaconing</i> .
		Pueden permitir el control y captura de un UAS o su destrucción, guiando al mismo a un área de control o haciéndole volar a un lugar donde colisione.	Existen numerosos desarrollos tecnológicos para detectar ataques <i>spoofing</i> .
		Pueden pasar inadvertidos para el enemigo, de tal manera que no sepa que sus UAS estén siendo atacados con sistemas de <i>spoofing</i> .	La acción del <i>spoofing</i> de la señal GNSS sobre un UAS controlado por un operador puede no ser suficiente para neutralizarlo.
	En el caso de un ataque por enjambre y una sola antena para <i>spoofing</i> disponible, la señal enviada será similar para todas las aeronaves del enjambre independientemente de su posición, por lo que es necesario un estudio situacional para evitar que alguno de los UAS se dirija al lugar a proteger.		
	Su alcance es limitado.		
Hacking <i>Ejemplo: Maldrone</i>	<p>Tanto UAS como estaciones en tierra (GCS) son susceptibles a ciberataques en sus diferentes segmentos o subsistemas.</p> <p>Entre los ataques más comunes destacan la exposición a virus informáticos de las GCS, ataque sobre el link de comunicaciones entre aeronave y GCS o ataque al sistema operativo propio del UAS.</p>	Son un tipo de ataque muy económico.	Necesita de operadores altamente especializados y con amplios conocimientos de la plataforma a atacar.
		Altamente efectivos para UAS no protegidos frente a ciberataques.	Ante UAS protegidos frente a ciberataques su acción puede ser extremadamente compleja.
		Pueden permitir el acceso a información de sensores, control o destrucción del UAS.	Existen numerosos desarrollos tecnológicos para protegerse frente a ciberataques, como sistemas de comunicaciones encriptadas, cortafuegos...
		Pueden pasar inadvertidos para el enemigo.	

Fuente: Instituto Español de Estudios Estratégicos. (2018). *El sistema de defensa aérea no cinético, clave para la defensa anti drone*. Madrid.

**ANEXO 2
CONSIDERACIONES TÉCNICAS PARA LA SELECCIÓN DE C-UAS**

En referencia al documento “*Unmanned Aircraft System Detection-Technical Considerations*” de la FAA, se consolidan en esta guía una serie de preguntas que pueden ser empleadas por los EAE durante los procesos de estructuración de procesos cuyo fin sea el de optar por la adquisición de equipos C-UAS para la protección de Unidades Militares y/o Policiales, especialmente cuando estas cuentan con aeródromos como parte integral de su infraestructura.

PARTE 1: MITIGACIÓN

La mitigación o contramedidas de UAS incluyen la capacidad de interrumpir, deshabilitar, destruir, tomar el control y/o proporcionar instrucciones de vuelo alternativas a un UAS objetivo. Algunos sistemas de detección de UAS pueden tener estas capacidades integradas, con la posibilidad de ser desactivadas, mientras que otros pueden ofrecerlas como una capacidad modular opcional.

<i>Pregunta</i>	<i>Información Adicional</i>
¿El sistema de mitigación UAS tiene alguna capacidad para realizar actividades de contramedida?	Si es así, ¿cómo se desactiva?
¿Qué tecnologías o métodos de contramedidas emplea el sistema?	Ej: Cinético, Cinética híbrida, no cinética, RF, Jamming, Laser, entre otros.
¿Qué tipo de interferencia o afectación se puede generar a las comunicaciones aeronáuticas o frecuencias usadas por los sistemas de navegación en tierra y/o a bordo de las aeronaves cuando se activan las contramedidas?	
¿Qué frecuencias se emplean para la operación de las contramedidas?	
¿Se tiene conocimiento o se han evidenciado consecuencias no esperadas y/o planeadas al activar las contramedidas durante el tiempo en que han sido implementadas?	

PARTE 2: DETECCIÓN PRIMARIA (RF Y RADAR)

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

Un factor clave para determinar la viabilidad de instalar un sistema de detección en o alrededor de un área objetivo (unidad militar o policial, aeropuerto, edificio, entre otros) es la cantidad de sensores necesarios para lograr la cobertura deseada del espacio aéreo. Debido a que el volumen de cobertura depende de las características y requisitos únicos de cada objetivo y del tipo de sistema, la cantidad de sensores variará. La distancia de cobertura para muchos tipos de tecnologías de detección también limita la eficacia de dichos sistemas para determinar las ubicaciones de los UAS y su punto de control. Además, es posible que las áreas de cobertura necesiten abarcar ángulos más amplios, ya que, el piloto al mando y/u operador pueden no estar cerca del UAS.

Así mismo, los fabricantes o vendedores pueden identificar los sistemas que empujan RF como no emisores (a menudo usando el término "pasivo") aunque el producto podría incluir y emplear regularmente tales capacidades de emisión, que podrían interferir con otras facilidades necesarias para la operación aérea.

<i>Pregunta</i>	<i>Información Adicional</i>
¿Cuáles son las áreas de cobertura, las ubicaciones críticas del sitio y los volúmenes de espacio aéreo que se deben monitorear?	
¿Cuáles son las tecnologías o sensores utilizados como medio principal para la detección?	Ej: Radar, RF, EO / IR, acústicos, entre otros.
¿Cuáles son las tecnologías o sensores utilizados como medios secundarios o de apoyo para validar la actividad detectada por los sensores primarios?	Ej: Radar, RF, EO / IR, acústicos, entre otros.
¿Se ha realizado un análisis de RF para este sitio específico?	¿Quién realizó el análisis? ¿Las emisiones de RF fueron simuladas o reales?
¿Cuál es el área de cobertura por sensor o del Radar?	¿Azimut? ¿Altitud? ¿Distancia?
¿Cuántos de cada tipo de sensor se requieren para el área requerida para el área objetivo?	
¿Cuáles son las capacidades de filtrado que utiliza el sistema para reducir la RF de fondo y la interferencia con otros sistemas?	

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

¿El sistema de detección depende de una base de datos de firmas de RF o radar conocidas?	En caso afirmativo, ¿con qué frecuencia se actualiza la base de datos? ¿Cuál es el proceso para actualizar la base de datos? ¿Hay un costo continuo para las actualizaciones de la base de datos?
¿El sistema puede detectar una operación de UAS o quién está saltando o cambiando intencionalmente las frecuencias a una velocidad aleatoria y / o rápida para evadir la detección?	
¿El sistema intercepta la transmisión de video en vivo de la UAS?	
¿El sistema diferencia y rastrea múltiples objetivos simultáneamente?	Si es así, ¿cuál es el límite superior en el número de objetivos que puede rastrear?
¿Se han realizado evaluaciones de la propagación de RF durante el día y la noche para tener en cuenta cualquier posible interferencia electromagnética que pudiera generarse?	
¿Cuál es la potencia de transmisión del radar?	
¿Cuáles son las bandas de frecuencia del radar?	¿Cuál es el tipo de escaneo del radar?
¿Cómo afectan las condiciones meteorológicas al radar?	

Es importante considerar, además, que ciertos modos de vuelo de la aeronave (por ejemplo, el vuelo estacionario) y el grado de autonomía de vuelo pueden limitar la efectividad del sistema de detección.

<i>Pregunta</i>	<i>Información Adicional</i>
¿Qué tipos de UAS puede detectar el sistema? RF y RADAR	Ej: Ala fija, multirrotor, entre otros.
¿Cuánto tiempo tarda el sistema en detectar un UAS que está dentro del alcance? RF y RADAR	Ej: Cinético, Cinética híbrida, no cinética, RF, Jamming, Laser, entre otros.

Así mismo, es probable que se necesite mano de obra dedicada y capacitación especializada para operar el equipo y ayudar a discernir falsos positivos, teniendo

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

en cuenta que el sistema de detección puede identificar incorrectamente otro objeto en movimiento como un UAS.

<i>Pregunta</i>	<i>Información Adicional</i>
¿Cómo diferencia el sistema entre la detección de un posible elemento de interés y un UAS?	
¿El sistema detecta UAS semiautónomos (es decir, UAS que usan navegación preprogramada, pero que son capaces de transmitir información por RF)?	¿Si es así, cómo?
¿Detecta el sistema UAS totalmente autónomo (es decir, UAS sin capacidades de RF que pueden navegar sin comandos en vuelo)?	¿Si es así, cómo?
¿Puede el sistema detectar UAS encendidos, antes que hayan iniciado el vuelo?	¿Si es así, cómo?
¿Puede el sistema detectar y geolocalizar la estación de control terrestre (GCS)?	Si es así, ¿cómo logra esto?
¿El sistema solo tiene capacidad de línea de visión (LOS)?, es decir, ¿los árboles y los edificios inhibirán las capacidades del sistema?	
¿Qué personal debe operar el sistema?	¿Qué tipo de entrenamiento es necesario para usar el sistema? ¿Qué entrenamiento está incluido?
¿Qué soporte operacional está incluido dentro del proceso de adquisición del sistema y su garantía?	¿El soporte incluye actualizaciones de software para abordar la evolución de la tecnología UAS?
¿Es el sistema una instalación fija o se puede instalar fácilmente?	¿El personal que no está familiarizado con el fabricante o vendedor del sistema, podría instalarlo fácilmente?
¿Es el sistema fácilmente transportable a cualquier entorno?	

¿Cuáles son las especificaciones o requisitos del sistema en cada punto de instalación?	Especificaciones Requisitos por tamaño (incluida la altura de la antena / sensor) Despliegue de almacenamiento físico Configuración Comunicaciones Fuente de energía Conexión a tierra eléctrica Calibración Almacenamiento físico
---	--

PARTE 3: DETECCIÓN SECUNDARIA (EO/IR o ACÚSTICOS)

Las especificaciones para sistemas EO son similares a las de cualquier cámara digital moderna; la calidad del lente, el campo de visión, las capacidades varifocales, el tamaño de píxel y la densidad de píxeles, tienen un papel en la calidad general de la imagen y su utilidad para validar elementos de interés. Algunas métricas, como la densidad de píxeles, anteriormente utilizadas para determinar la calidad de la imagen ya no son precisas: "más megapíxeles" no significa una mejor imagen. La industria de la videovigilancia utiliza una métrica comúnmente aceptada, *Pixels Per Foot* (PPF), como un nivel más predecible de calidad de imagen.

<i>Pregunta</i>	<i>Información Adicional</i>
¿Cuáles son las capacidades de movimiento horizontal, vertical y zoom (PTZ) de los dispositivos EO / IR?	
¿Cómo se automatizan las capacidades de PTZ en coordinación con sensores de detección primarios?	
¿Cuál es el campo de visión del dispositivo EO / IR?	
¿Qué tipos y niveles de estabilización de imagen, si corresponde, se utilizan para los dispositivos EO / IR?	
¿Cuál es la cantidad de píxeles por pie (PPF) que proporciona el dispositivo EO?	
¿Qué longitudes de onda detecta el dispositivo IR?	

PARTE 4: DATOS E INFORMACIÓN

AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO

GUÍA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS)

La gestión de datos e información juega un papel crucial en los sistemas de detección UAS. Además de las "mejores prácticas" comunes para la gestión de la tecnología de la información y la seguridad de los datos, podrían considerarse otros factores, como los paneles estadísticos, la información histórica y la portabilidad de los datos, considerados de gran importancia.

<i>Pregunta</i>	<i>Información Adicional</i>
¿Cómo distinguirá el sistema entre UAS autorizados y no autorizados?	
¿Cómo maneja el sistema objetivos duplicados de sensores múltiples o superpuestos?	
¿Cómo se verifican o validan los datos de actividades sospechosas?	
¿Cómo se generan, informan y distribuyen los datos de actividades sospechosas?	
¿Cómo se gestionan los sistemas la información histórica o que proporcionan análisis estadísticos y minería de datos?	
¿Cuál es la tasa de actualización de los sensores al sistema y del sistema a la interfaz?	
¿Cuáles son las características de alerta y alarma de la interfaz?	
¿El fabricante, el vendedor o el integrador del sistema tienen acceso a los datos capturados, derivados, transmitidos o almacenados?	
¿El fabricante, vendedor o integrador del sistema tiene una solución (geolocalización) del sistema de detección?	
¿El fabricante, el vendedor o el integrador del sistema tienen la capacidad de iniciar actualizaciones de software (con o sin consentimiento)?	

<p>¿El sistema, los componentes o el software tienen la capacidad de implementar o mantener una lista blanca de UAS sin el conocimiento del operador u organización gubernamental?</p>	
--	--

PARTE 5: SOLUCIONES INTEGRADAS

Algunos sistemas pueden denominarse una solución integrada, que emplea múltiples tipos de tecnologías de sensores y proporciona sus datos en una única interfaz de usuario. Otros sistemas pueden proporcionar capacidades para incorporar los elementos de hardware y software existentes de una organización.

<i>Pregunta</i>	<i>Información Adicional</i>
<p>Si hay varios sistemas, ¿el sistema proporciona una interfaz gráfica fusionada para el usuario con una fuente autorizada?</p>	
<p>¿Cómo podría integrarse el sistema durante mucho tiempo con los centros e infraestructura de operaciones de seguridad existentes, como cámaras de seguridad, conectividad de datos y sistemas de visualización?</p>	
<p>¿Cómo se puede integrar la información externa, como los informes del personal de tierra o las fotos, con la información del sistema?</p>	