Universitat Autònoma de Barcelona

escola d'enginyeria

DRONES. INCIDENCIA EN LAS OPERACIONES AÉREAS. SOLUCIONES Y PLAN MODELO DE RESPUESTA.

Memoria del Trabajo Final del
Máster Universitario en Gestión Aeronáutica
realizado por
Daniel Juan Pérez Carmona
y dirigido/supervisado por
Romualdo Moreno Ortiz
Sabadell, 14 de septiembre de 2020

Resumen.

En los últimos años, se ha producido un crecimiento exponencial en el mercado de los drones domésticos y profesionales, adaptándose a cada bolsillo y necesidad, lo que ha venido aparejado de un incremento similar en los incidentes aéreos en los que estos dispositivos se ven involucrados. Este documento afronta esta problemática teniendo en cuenta todos los aspectos para, tras analizar las conclusiones obtenidas, proponer un modelo de respuesta anti dron que consiga mantener la seguridad de las operaciones aéreas y de la propia instalación aeroportuaria.

Abstract.

In recent years, there has been an exponential growth in the domestic and professional drone market, adapting to every pocket and need, which has been accompanied by a similar increase in air incidents in which these devices are involved. This document addresses this problem taking into account all aspects and, after analyzing the conclusions obtained, proposing an anti-drone response model that manages to maintain air operations safety and airport facility security.

Resum.

En els últims anys, s'ha produït un creixement exponencial en el mercat dels drons domèstics i professionals, adaptant-se a cada butxaca i necessitat, el que ha vingut aparellat d'un increment similar en els incidents aeris en els quals aquests dispositius s'han vist involucrats. Aquest document afronta aquesta problemàtica tenint en compte tots els aspectes per, després d'analitzar les conclusions obtingudes, proposar un model de resposta anti dron que aconsegueixi mantenir la seguretat de les operacions aèries i de la mateixa instal·lació aeroportuària.

El abajo firmante, Romualdo Moreno Ortiz

Profesor de los estudios de Máster Universitario en Gestión Aeronáutica de la UAB,

CERTIFICA:

Que el trabajo al que corresponde la presente memoria ha sido realizado bajo su dirección por Daniel Juan Pérez Carmona

Y para que conste firma la presente.

ROMUALDO MORENO ORTIZ - DNI 38435075M

Firmado digitalmente por ROMUALDO MORENO ORTIZ - DNI 38435075M
Fecha: 2020.09.14 10:39:19 +02'00'

Firmado: Romualdo Moreno Ortiz

Sabadell, 14 de septiembre de 2020

GLOSARIO DE SIGLAS.

ADS-B	Automatic Dependent Surveillance Broadcast (Sistema de Vigilancia Dependiente Automática
AESA	Agencia Estatal de Seguridad Aérea
ATC	Air Traffic Controller (Controlador de Tráfico Aéreo)
BOE	Boletín Oficial del Estado
CCA	Centro de Coordinación de Actuación
CTA	Control Traffic Area (Área de Control de Táfico)
CTR	Control Traffic Region (Región de Control de Tráfico)
EASA	European Aviation Safety Agency (Agencia Europea de Seguridad de la Aviación)
EO	Electro-óptico
ESM	Electromagnetic Spectrum Monitoring (Monitorización del espectro electromagnético
FAA	Federal Aviation Administration (Administración Federal de Aviación)
FFCCSE	Fuerzas y Cuerpos de Seguridad del Estado
FIR	Flight Information Region (Región de Información de Vuelo)
GC	Guardia Civil
GPS	Global Positioning System (Sistema de Posicionamiento Global)
HPM	High Power Microwave (Microondas de alta potencia)
HVE	High Visibility Event (Evento de Alta visibilidad)
IFR	Instrumental Flight Rules (Reglas de Vuelo Instrumental)
IR	Infrarrojo
LÁSER	Light Amplification by Stimulated Emission of Radiation (Luz Amplificada por Emisión Estimulada de Radiación
LSS	Low, Small, Slow (Bajo, Pequeño, Lento)
LUC	Light UAS operator Certificate (Certificado de Operación de UAS Ligeros)
NOTAM	Notice to Airmen (Avisos para Aviadores)
OACI	Organización de Aviación Civil Internacional
RCS	Radar Cross Section (Corte Transversal de Radar)
RED	Responsable de Evento Dron

RF	Radio Frecuencia
RPAS	Remotely Piloted Aircraft System (Sistema Aéreo Pilotado Remotamente)
RTH	Return To Home (Vuelta a Casa)
TCAS	Traffic Alert and Collision Avoidance System (Sistema de Alerta de Tráfico y Evitación de Colisión)
TEDAX	Técnico Especialista en Desactivación de Artefactos Explosivos
TMA	Terminal Manoeuvring Area (Área de Maniobra Terminal)
UAS	Unmanned Aircraft System (Sistema Aéreo no Tripulado)
UE	Unión Europea
VFR	Visual Flight Rules (Reglas de Vuelo Visual)

ÍNDICE DE FIGURAS

Figura 1. Proyección del crecimiento del mercado de drones comerciales. Página 1. (Statista,2019)

Figura 2. Número de incidentes relacionados con drones por año. Página 2. (UK Airprox Board, 2020)

Figura 3. Estructura genérica de espacio aéreo. Página 7. (Plan director del aeropuerto de Santander)

Figura 4. Consecuencias del impacto de un dron contra un perfil alar. Página 10. (University of Dayton, 2018)

Figura 5. Actores afectados por las incursiones dron. Página 13. (WillisTowersWatson, 2019)

Figura 6. Vista del software de DJI cuando un dron se encuentra en zona protegida por geofencing. Página 16. (DroneLife, 2017)

Figura 7. Representación de avión cercano en el sofware de DJI. Página 17. (YouTube,2018)

Figura 8. Fases de gestión de la amenaza dron. Página 18 y 33. (ICAO, 2019)

Figura 9. Distancias máximas teóricas de detección visual. Página 19. (NLR, 2019)

Figura 10. Espectro electromagnético. Página 20. (CC BY-NC-SA; anonymous by request)

Figura 11. Distancias teóricas de detección radar. Página 21. (NLR, 2019)

Figura 12. Características de los dispositivos LSS. Página 21. (Elaboración propia).

Figura 13. Distancias máximas teóricas de detección acústica. Página 22. (NLR,2019)

Figura 14. Triangulación por sensores acústicos. Página 22. (SquareHead, 2020)

Figura 15. Distancias máximas teóricas de detección por RF. Página 23. (NLR, 2019)

Figura 16. Triangulación por detector de RF. Página 25. (MyDefence, 2019)

Figura 17. Radar del sistema Drone Dome. Página 30. (Rafael, 2019)

Figura 18. Sensor RF del sistema Drone Dome. Página 31. (Rafael, 2019)

Figura 19. Cámara EO e IR del sistema Drone Dome. Página 31.
(Rafael, 2019)

Figura 20. Perturbador del sistema Drone Dome. Página 31.
(Rafael, 2019)

Figura 21. Sistema mando y control del sistema Drone Dome. Página 32.
(Rafael, 2019)

Figura 22. Munición anti dron Skynet. Página 32.
(LessLethal, 2020)

Figura 23. ATZ y CTR de Almería. Página 38.
(AIP España, 2020)

Figura 24. Representación gráfica de las áreas y zonas de protección del aeropuerto. Página 39.
(Elaboración propia, basada en mapas de FEGA).

Figura 25. Cuadrícula para localización de dron. Página 40.
(Elaboración propia, basada en mapas de FEGA)

Figura 26. Cuadrícula ampliada para la localización precisa del dron. Página 41.
(Elaboración propia, basada en mapas de FEGA)

Figura 27. Formulario recogida de datos. Página 44.
(Elaboración propia)

TABLA DE CONTENIDOS

1. Introducción……..…1
   1.1 Motivación…… 1
   1.2 Objetivos…….……3
   1.3 Organización de la memoria……3
2. Fundamentos……5
   2.1 Normativa y clasificación……..5
   2.2 Espacio aéreo…….6
3. Incidencia e impacto de los drones……...9
   3.1 Incidencia en eventos de alta visibilidad……...9
   3.2 Consecuencia impacto dron……9
   3.3 Incidencia en aeropuertos……11
   3.4 Cobertura de los seguros……14
4. Medidas de mitigación de la amenaza……..16
   4.1 Seguridad integrada en los drones……..…16
   4.2 Gestión de la amenaza. Fases……...18
   4.3 Detección y seguimiento……..…19
   4.4 Clasificación y localización……...23
   4.5 Neutralización……25
5. Modelo plan actuación ante amenaza dron……..…30
   5.1 Cuerpo general……..…….30
   5.2 Áreas del aeropuerto……36
   5.3 Procedimiento de actuación……42
   5.4 Formulario recogida de datos……..44
6. Conclusiones……45
7. Referencias……48
8. Bibliografía…….....51

1. INTRODUCCIÓN

1.1 MOTIVACIÓN

Durante los últimos años, se han venido aplicando una serie de términos distintos para definir los dispositivos que vuelan sin piloto o controlados remotamente. Según la circular OACI 328-AN/190, lo correcto es aplicar los términos UAS (Unmanned Aircraft System) y RPAS (Remotely Piloted Aircraft System). Los RPAS son una subclase de UAS y constan de una serie de equipos (como estaciones de tierra, sistemas de comunicaciones y control, etc) que les da la posibilidad de, si disponen del equipamiento necesario, ser incluidos en un futuro en espacios aéreos compartidos con aeronaves tripuladas. Por ser de uso común, a lo largo de este documento se incluirá con frecuencia la palabra dron para referirse a los términos anteriormente mencionados.

El uso de estas aeronaves ha experimentado un crecimiento exponencial en los últimos años, pasando de tener un uso puramente gubernamental a llegar a muchos hogares, siendo este hecho el responsable de que el número de incidentes con drones haya tenido una tendencia similar.

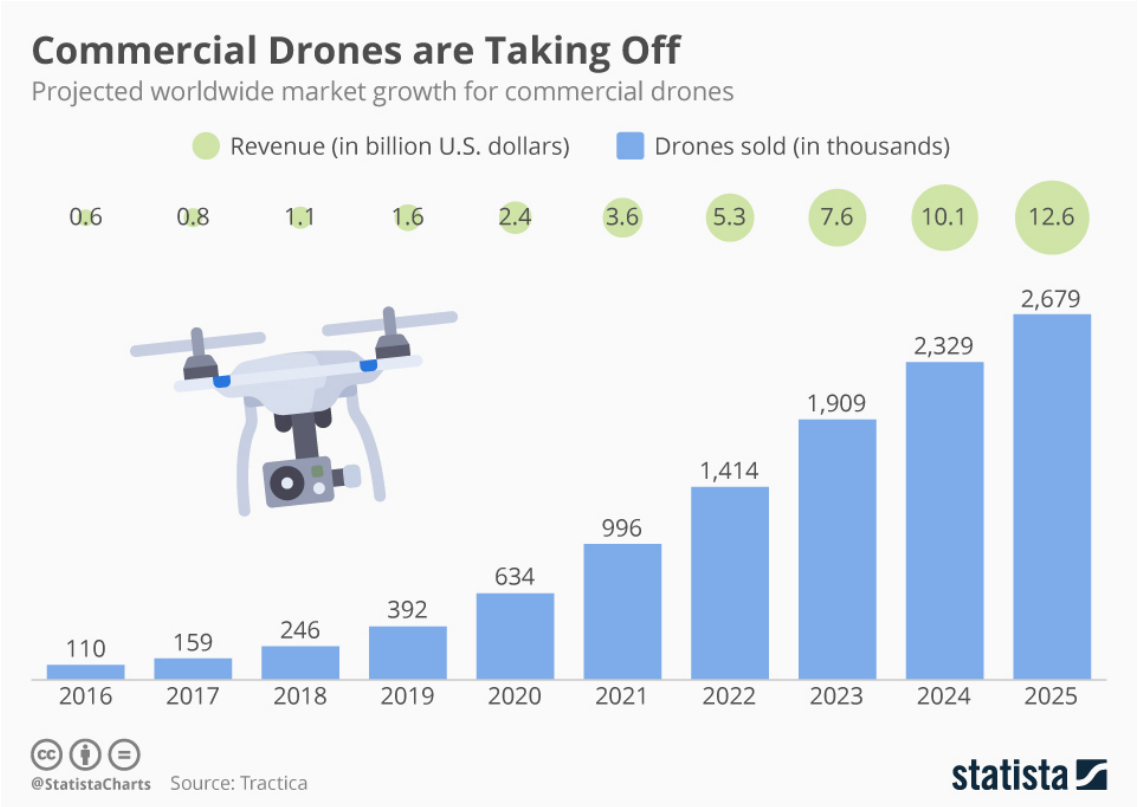


Figura 1. Proyección del crecimiento del mercado de drones comerciales. (Statista,2019)

Estos drones, enfocados al uso doméstico, están en su mayoría operados por personas con pocos o nulos conocimientos acerca del uso del espacio aéreo y sus restricciones, dando lugar, en ocasiones, a un uso inadecuado e incluso ilegal por desconocimiento. Asimismo, dada la capacidad de transporte de pequeñas cargas,

como por ejemplo videocámaras, están siendo utilizados por grupos terroristas para perpetrar sus atentados, convirtiéndose en una prioridad para las Fuerzas y Cuerpos de Seguridad del Estado, especialmente en eventos de alta visibilidad (HVE por sus siglas en inglés)

Dada su baja RCS (Radar Cross Section) y baja velocidad, suponen un desafío para los sistemas convencionales de detección, ya que están enfocados al control de aeronaves de una velocidad y tamaño superior.

Lo anteriormente expuesto ha tenido una repercusión significativa en el número de incidentes aéreos registrados en la última década, lo que los ha puesto en el punto de mira de las agencias de seguridad aérea de todos los países. Como se puede apreciar en la figura 2, el número de incidentes aéreos que involucran a drones, se multiplicó por cuatro en el periodo del 2015 al 2018, reduciéndose en 2019 a niveles del 2018 y no considerándose significativo el 2020 por haber transcurrido únicamente la mitad del año y la bajada del tráfico aéreo por la crisis sanitaria.

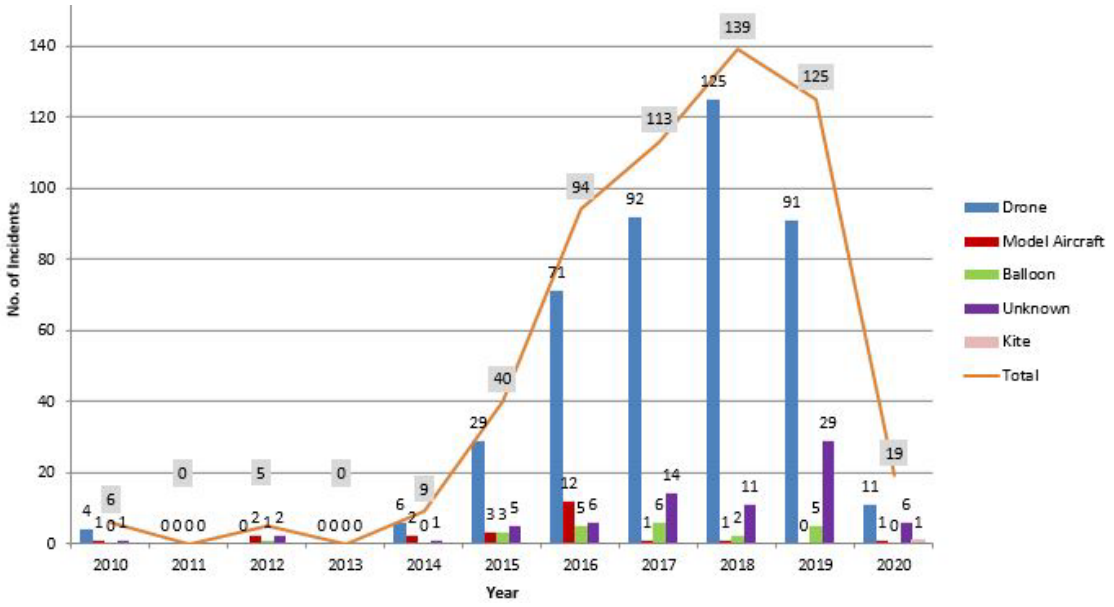


Figura 2. Número de incidentes relacionados con drones por año. (UK Airprox Board, 2020)

La necesidad de mantener un espacio aéreo seguro para la operación de aeronaves ha propiciado la creación de diversos sistemas, tanto externos como de los propios fabricantes de drones. Debido a que no se puede confiar únicamente en los sistemas que instalan los fabricantes, ya que pueden no ser todo lo efectivos que sería deseable o incluso puede ser *hackeados*, es necesario que las agencias gubernamentales, especialmente aquellas que se encargan de dar seguridad a estructuras que se pueden considerar de interés para la defensa nacional, tengan la capacidad de defensa ante este tipo de amenaza.

1.2 OBJETIVOS

En primer lugar, dada la cantidad de actores involucrados en un incidente dron, como pueden ser pilotos, personal ATC (Air Traffic Controller), operadores aficionados o profesionales, cuerpos y fuerzas de seguridad del estado, un objetivo que se persigue es dar una visión global del entorno en donde se produce el vuelo de este tipo de dispositivos, tanto normativamente como entrando en unas nociones básicas sobre la tecnología disponible y posibles medidas de mitigación.

En segundo lugar, se está produciendo una toma de conciencia de este problema y cómo afecta a las operaciones aéreas, con lo que, en un corto plazo de tiempo, los aeropuertos que no hayan creado un plan para enfrentarse a las incursiones dron, tendrán que crearlo desde cero, probablemente con conocimientos justos en alguno de los campos que aquí se tratan. Por ello, se ha redactado un plan modelo, tomando como referencia un aeropuerto y sistema anti dron existentes, para dar una idea de cómo gestionar y estructurar la toma de decisiones en un evento dron.

1.3 ORGANIZACIÓN DE LA MEMORIA

La estructuración se ha dividido en cinco partes principales:

- Fundamentos.

  Se incluyen nociones básicas sobre la normativa vigente en lo relativo al uso de drones y un repaso general de la estructuración del espacio aéreo para obtener unos conocimientos mínimos que permitan entender el problema desde un punto de vista técnico.

- Incidencia e impacto de los drones.

  En muchas ocasiones, la sociedad no es consciente de hasta qué punto un dispositivo de este tipo es capaz de causar un daño, tanto de forma intencionada por parte de su operador, como por imprudencias o desconocimiento. Por tanto, en este capítulo, se hace un análisis de la afectación que supone un incidente de este tipo en distintos ámbitos, centrándose fundamentalmente en lo que atañe a las operaciones aéreas.

- Medidas de mitigación de la amenaza.

  Conociendo ya las bases del problema, se pasa a exponer las medidas de las que actualmente se dispone para controlar este problema de seguridad. Se analizan tanto las medidas que están empezando a integrar los dispositivos, como un sistema de varias fases para el análisis del grado de amenaza y posibilitar una toma de decisiones óptima.

- Modelo plan de reacción.

  Teniendo en cuenta todos los aspectos teóricos y normativos, se propone un modelo para la situación en la que un gestor aeroportuario tenga que hacer frente a una incursión dron que pueda causar un problema de seguridad en las operaciones o en las propias instalaciones.

- Conclusiones.

  Una vez que se ha obtenido una visión conjunta del problema, se analizan los probables escenarios futuros atendiendo a los plausibles cambios de tendencias, decisiones de fabricantes y gobiernos, y comprensión del problema por parte del grueso de la sociedad.

2. FUNDAMENTOS

2.1 NORMATIVA Y CLASIFICACIÓN

Actualmente, la operación tanto lúdica como profesional de los drones en España se rige por el Real Decreto 1036/2017, de 15 de diciembre que modifica el anteriormente vigente que databa del año 2014 (BOE, 2017). Ésta tiene un carácter bastante restrictivo y está bastante enfocada a la protección de las operaciones aéreas y de las personas. Las principales restricciones son las siguientes:

Uso profesional

- Habilitación por parte de AESA (Agencia Estatal de Seguridad Aérea)
- Seguro de responsabilidad civil
- Licencia de piloto de RPAS
- Necesidad de autorización para vuelos nocturnos, sobre poblaciones o aglomeraciones de personas y en espacios aéreos controlados.

Uso recreativo

- No hace falta licencia, pero sí que el operador o supervisor sea un adulto.
- Mantener siempre contacto visual con el dron.
- Volar siempre a menos de 120 m de altura, evitando aglomeraciones y poblaciones.
- Se recomienda un seguro de responsabilidad civil.
- No volar a menos de 8km de ningún aeropuerto o aeródromo.

Adicionalmente se plantean ciertos requisitos a los operadores profesionales para que puedan recibir autorización para volar en condiciones especiales como sobre ciudades, a menos de 8km de distancia de un aeropuerto, etc. Dependiendo del peso del dron, puede ser exigible para estas actividades un certificado de aeronavegabilidad y un estudio de seguridad para cada exención a la normativa general que se autorice.

La normativa regulatoria más reciente sobre este tipo de dispositivos, es la que se ha redactado por parte de la Unión Europea a través del Reglamento Delegado (UE) 2019/947 (Diario Oficial de la UE, 2019), dando lugar a una nueva clasificación en la que se distinguen 3 categorías principales, cuyas diferencias se pueden simplificar de la siguiente manera:

A) Open.

- Masa máxima inferior a 25 kg
- Distancia segura de personas y evitando sobrevolarlas.
- El piloto mantiene en todo momento contacto visual con el dron, a excepción del modo “sígueme” o siendo necesario que haya un observador.
- Altura máxima de 120 m sobre el suelo, a excepción del sobrevuelo de obstáculos.
- El dron no podrá transportar cargas peligrosas ni dejar caer un objeto.

- Esta categoría se subdivide en A1, A2 y A3 en función de las limitaciones operacionales, los requisitos aplicables al piloto y requisitos técnicos aplicables al dron.

B) Específica.

- Cuando no se cumpla uno de los requisitos para ser incluido en la categoría "Open"
- Será necesario solicitar una autorización operacional, a la cual se adjuntará unas medidas de atenuación del riesgo.
- Si la autoridad considera que los riesgos están suficientemente atenuados, emitirá una autorización.
- Esta autorización especificará si cubre uno o varios vuelos determinados o se concede un LUC (Light UAS operator Certificate)

C) Certificada

- Tiene una dimensión característica igual o superior a los 3 metros.
- Implica el vuelo sobre concentraciones de personas.
- Conlleva el transporte de éstas.
- Implica el transporte de mercancías peligrosas que puedan entrañar un riesgo elevado para terceros en caso de accidente.

Esta normativa ya está en vigor a excepción del apartado 3 del artículo 15, que prorroga su aplicación al 1 de julio de 2021, a efectos de permitir que los países que autoricen una zona de vuelo de drones, tengan tiempo para adaptar sus sistemas informáticos y puedan proveer información pública de éstas.

Los fabricantes y operadores de terceros países se ven también afectados por el Reglamento Delegado (UE) 2019/945 (Diario Oficial de la UE, 2019) que regula las características técnicas de los dispositivos que se comercializan en la UE, asignándoles unas determinadas etiquetas. También establece las normas que son de aplicación a los drones que se vayan a utilizar en la categoría "abierta" y establece normas aplicables a los operadores de drones dentro del espacio aéreo del cielo único europeo.
El anexo 7 de OACI (Organización de Aviación Civil Internacional), referente a la normativa que regula las marcas de nacionalidad y de matrícula de aeronaves, fue actualizado en 2012, en su sexta edición, para incluir a este tipo de dispositivos (OACI, 2012).

2.2 ESPACIO AÉREO

El conocimiento de la división del espacio aéreo es un tema bastante desconocido entre los usuarios lúdicos de drones, lo que hace que en numerosas ocasiones se produzca un uso potencialmente peligroso de forma inconsciente.

De forma general, el espacio aéreo tiene una división distinguida por letras, las cuales se asignan en función de la altura y posición geográfica de ese volumen de

espacio. En general, las capas bajas tienen clasificación en España como tipo “G”, lo que lo incluye dentro de los espacios aéreos no controlados, lo que implica que tanto vuelos IFR (Instrumental Flight Rules) como VFR (Visual Flight Rules) se permiten, recibiendo estos únicamente servicio de información de vuelo si lo solicitan.

Sin embargo, la mayoría del territorio español se encuentra incluido dentro de otros volúmenes de espacio aéreo que suponen unas restricciones mayores (ENAIRE, 2020). En el siguiente diagrama se muestran para su mejor comprensión

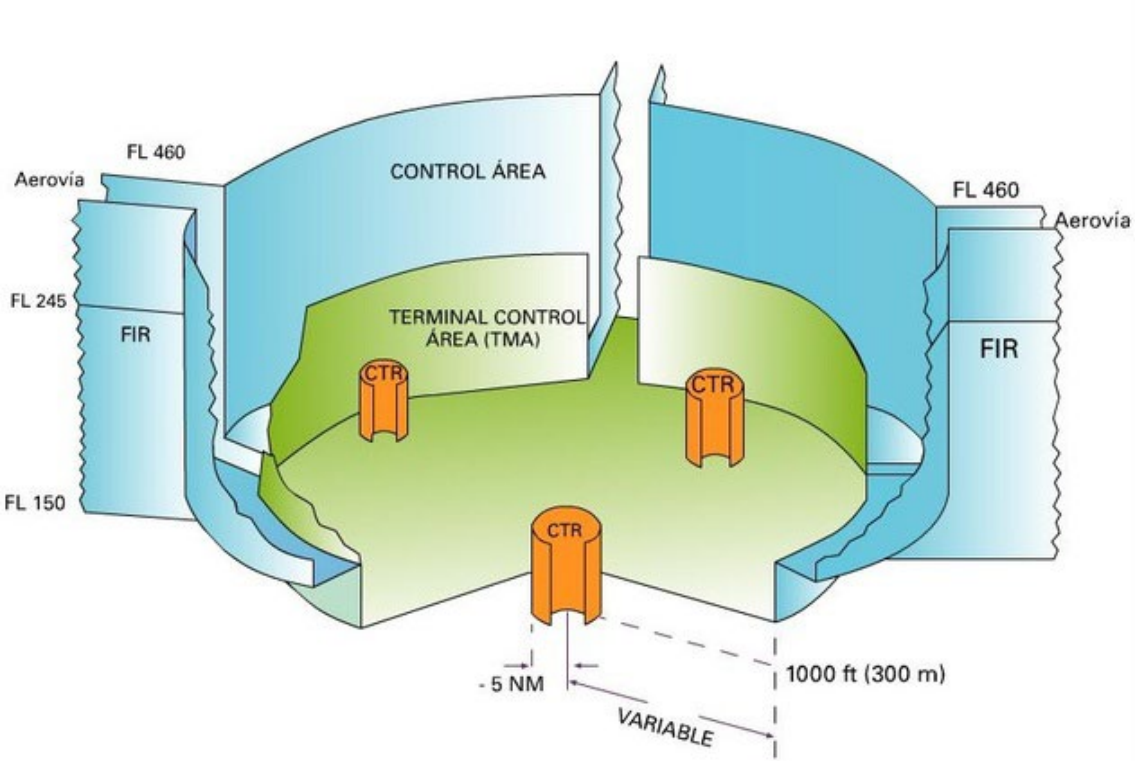


Figura 3. Estructura genérica de espacio aéreo. (Plan director del aeropuerto de Santander)

FIR: Flight Information Region.

Divisiones del espacio aéreo que incluyen zonas incluso que no son espacio aéreo nacional, donde se provee información al vuelo y servicios de alerta. Su extensión se extiende desde el suelo hasta FL245, donde pasa a denominarse UIR (Upper Information Region) al superar dicho nivel. En España existen tres, Madrid, Barcelona y Canarias.

CTA: Control Traffic Area

Volumen de espacio donde se da servicio de control aéreo, puede incluir una TMA o encontrarse aislada para controlar las aproximaciones y salidas de aeropuertos con poco volumen de tráfico.

TMA: Terminal Manoeuvring Area.

Zona que puede englobar varios aeropuertos o uno con un gran volumen de tráfico donde se coordina el flujo de llegadas y salidas.

CTR: Control Traffic Region.

Espacio que incluye normalmente un aeropuerto, se extiende desde el suelo hasta una altura determinada y se usa para dar protección y control a los tráficos en llegada o salida.

De todos éstos, los que más problemas presentan por las características del vuelo de drones son las TMA, CTA y especialmente las CTR. Al fin y al cabo, normalmente las dos primeras no se extienden hasta el suelo, llegando habitualmente hasta los 1000’ (330 m). Sin embargo, la CTR llega hasta el nivel del suelo, lo que por regla general hace que el espacio aéreo a ese nivel sea controlado y asigna a la agencia de control la potestad y responsabilidad de proveer separación entre tráficos y separación entre ellos, siendo los drones dispositivos que no se encuentran habitualmente en coordinación con estas agencias.

Actualmente, los esfuerzos se están centrando en mantener las CTR despejadas de drones que puedan interferir con los aviones que despegan o aproximan, por lo que todos los aeropuertos están desarrollando procedimientos con dicho fin.

Aunque la aviación comercial sólo se ve afectada durante estas maniobras, los vuelos de aficionados o militares suelen transitar las capas bajas de espacio aéreo “G”, las cuales se encuentran en la envolvente de vuelo de los drones, por lo que habrá que tener este aspecto en cuenta una vez que se haya puesto una solución a las áreas más críticas.

3. INCIDENCIA E IMPACTO DE LOS DRONES

3.1 INCIDENCIA EN EVENTOS DE ALTA VISIBILIDAD.

Uno de los peligros que impulsó el desarrollo temprano de sistemas anti dron, fue el de que se produjera un atentado en un evento con alta afluencia de personas o altos cargos de un gobierno. Los primeros prototipos fueron de desarrollo militar debido al tipo de amenaza que se encontraron en los escenarios más recientes, como puede ser la lucha contra el DAESH, cuyos combatientes descubrieron lo fácil y barato que resultaba la adquisición de un dron con una capacidad de carga limitada pero lo suficientemente grande para llevar una cantidad suficiente de explosivo para efectuar el daño que deseaban. Inicialmente se usaban armas ligeras, pero la necesidad de detección temprana y de poder usarlo en entornos urbanos, hicieron que pasaran a plantearse alternativas no destructivas que pudieran evitar daños colaterales.

En el 2018 se pudo apreciar un claro ejemplo, cuando en Caracas (Venezuela) durante un desfile conmemorativo de la creación de la Guardia Nacional Bolivariana, se produjo un ataque con dos drones DJI con un kilogramo de explosivo C4 cada uno contra el presidente de Venezuela, Nicolás Maduro. Se desconoce si por fallo de los drones o acierto de las fuerzas de seguridad venezolanas, las explosiones se produjeron a relativa distancia de su objetivo, causando únicamente 7 heridos leves (CNN, 2018).

Desde antes, ya se estaban implementando medidas en el resto del mundo para proteger este tipo de eventos de ataques con drones que se han ido perfeccionando y extendiendo su uso a desfiles militares, finales de competiciones de diversos deportes, actos destacados gubernamentales, etc.

3.2 CONSECUENCIAS IMPACTO DRON.

Los drones no son los únicos riesgos para las aeronaves a baja cota, existen también distintos tipos de aves que suponen un peligro para las operaciones aéreas. Desde hace muchos años se identificó este peligro y se comenzó a poner solución, resultando uno de los métodos más efectivos la cetrería, que a día de hoy se sigue manteniendo en múltiples instalaciones aeroportuarias. Pero, ¿tiene las mismas consecuencias un impacto contra un dron o un pájaro?

La respuesta a esa pregunta va a depender de varios factores, siendo el más importante, a igualdad de situaciones, el peso y cómo se encuentra distribuido éste a lo largo del tamaño del objeto. La Universidad de Dayton distribuyó un vídeo de un impacto reproducido en su laboratorio de investigación de física del impacto (University of Dayton, 2018).

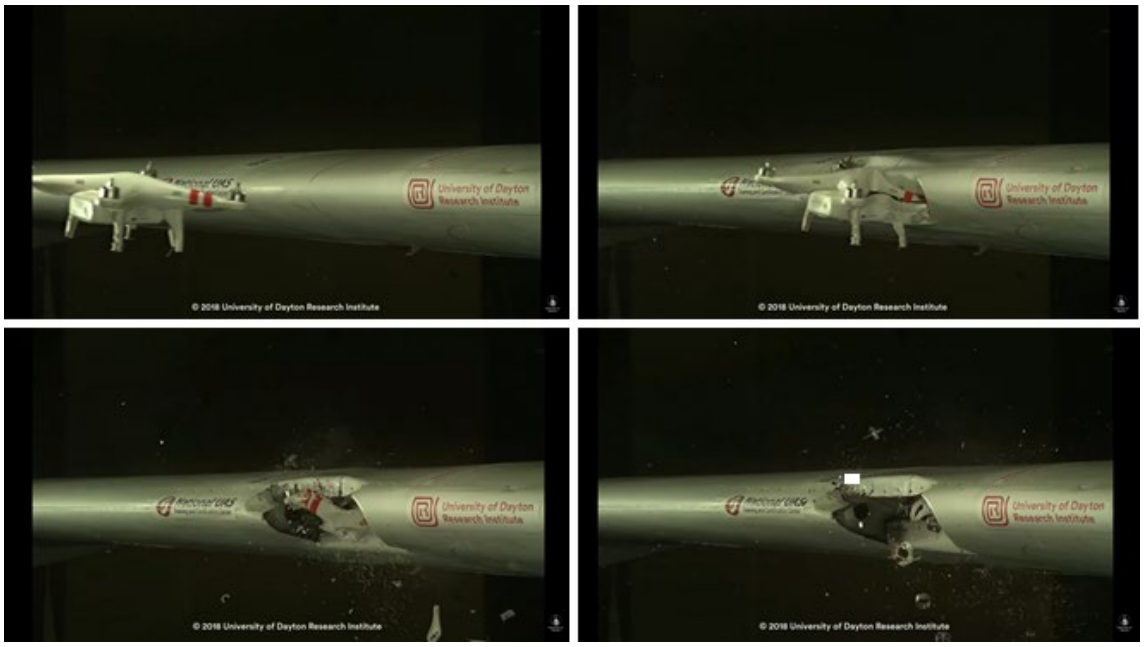


Figura 4. Consecuencias del impacto de un dron contra un perfil alar. (University of Dayton, 2018)

Como se puede apreciar en la figura 4, el dron produce un daño significativo en el borde de ataque del perfil alar, aunque al simular el impacto con un pájaro de peso similar, los daños en el ala fueron más extensos en el caso del ave. Sin embargo, los investigadores pudieron apreciar que, debido a la concentración de la masa del dron, éste pudo penetrar significativamente más, llegando a dañar el larguero principal, por lo que la integridad estructural del ala se pudo ver comprometida.

Un par de años antes, el gobierno británico encargó otro estudio (MAA y col., 2016) referente a la evaluación de daños que se podían producir al impactar una aeronave contra un dron de un tamaño pequeño que oscilaba de peso entre 400 gramos y 4 kg y las velocidades de impacto se establecieron a lo que se determinó como factible teniendo en cuenta la envolvente de vuelo de la mayoría de drones. Los resultados que arroja este estudio son los siguientes:

- Impacto contra parabrisas de helicópteros no certificados contra impacto de pájaros.

  La penetración a través del parabrisas se produjo incluso a velocidades bastante inferiores a la de crucero habitual, llegando incluso a producirse cuando el helicóptero se encontraba en vuelo estacionario y únicamente se tenía en cuenta la velocidad de acercamiento del dron.

- Impacto contra parabrisas de helicóptero certificados contra impacto de pájaros.

  Se apreció que a velocidades habituales de crucero e incluso significativamente inferiores en los casos en que el dron se desplazaba contra el helicóptero a su máxima velocidad, se produjeron daños en el parabrisas que permitió la entrada al habitáculo del dispositivo. Sin embargo, en vuelo estacionario, la resistencia fue suficiente para evitar daños dentro de la cabina.

- Impacto contra rotor de cola.

En este caso, el estudio fue a través de modelado, llegando a la conclusión de que, debido a las grandes velocidades que alcanzan las hélices, podría producirse un daño crítico en éstas.

- Impacto contra parabrisas de avión de línea aérea.

El diseño de estos parabrisas es más complejo que el de los helicópteros, no apreciándose rotura con drones de 1,2 kg, sin embargo, se produjo una rotura con el de 3,5 kg, determinándose que en el caso de los de 4 kg era posible que los daños fueran suficientes para que se produjera la entrada del dron en la cabina.

Uno de los aspectos que subrayó este estudio fue el papel clave que jugaba el tipo de construcción del dron en la severidad de los daños causados. En los casos que las piezas plásticas hacían contacto en primer lugar, los daños eran significativamente menores que en los que lo hacían las piezas metálicas. Adicionalmente, se comprobó que los daños que causaba un dron de un determinado peso a una determinada velocidad, eran significativamente mayores a los de un ave equivalente, debido a la dureza de los materiales metálicos empleados en éstos, por lo que una certificación de resistencia a impacto con ave, no debería ser extrapolable a los drones.

3.3 INCIDENCIA EN AEROPUERTOS.

Al ser el lugar donde hay una mayor afluencia de tráfico aéreo en niveles bajos del espacio aéreo, es donde más informes de avistamiento y colisión se producen. Mientras que la amenaza de las aves es bien conocida y controlada, los drones suponen un nuevo escenario para el que se dispone de pocas armas. Además, por su difícil detección es complicado determinar el momento en el que un dron que ha sido avistado deja de ser un problema de seguridad, ya que su autonomía oscila entre 20 minutos y 2 horas, siendo muy fácil perder su rastro en ese periodo de tiempo.

Han sido numerosos los incidentes con drones que han supuesto bien daños materiales o pérdidas de dinero por interrupción de las operaciones aéreas por todo el mundo. Teniendo en cuenta los más significativos, se pueden destacar los siguientes:

- Frankfurt (The Local, 2019). El aeropuerto con más tráfico de Alemania se vio obligado a parar su actividad el 9 de mayo de 2019 debido a un avistamiento de dron. De acuerdo a las autoridades, un total de 143 salidas y llegadas fueron canceladas y otros 50 aviones tuvieron que ser desviados a otros aeropuertos alternativos de un total de 1500 vuelos programados para ese día.

- Londres (The Guardian, 2018). En Heathrow se produjeron una serie de avistamientos de drones que forzaron su cierre durante largos periodos entre el 19 y 21 de diciembre de 2018. La policía sospechaba que había sido un acto deliberado por parte de alguien que conocía bien los procedimientos operacionales. Se estima que afectó a unos 82000 pasajeros, suponiendo un perjuicio total de unos 50 millones de libras, aunque otras estimaciones lo reducen a 15 millones.

- Madrid (La Vanguardia, 2020). Barajas se vio también afectado el día 3 de febrero del 2020 por una notificación de que un dron se encontraba en las proximidades. Esto obligó a establecer el “rate 0” de despegues y aterrizajes, lo que supuso una paralización del aeropuerto que rondó las dos horas, obligando a desviar 17 vuelos que se encontraban con destino Barajas, pudiendo posteriormente reactivarse el tráfico.

- Dubai (Arabian Business, 2016). En 2016, el aeropuerto internacional de Dubai sufrió 3 cierres por avistamiento de drones, sumando una duración total de 115 minutos. Se estima que las pérdidas ascendieron a unos 95000$ por minuto.

- Quebec (BBC, 2017). En las cercanías de este aeropuerto canadiense, se produjo en 2017 un impacto de dron con una avioneta comercial que transportaba a 6 pasajeros y dos tripulantes. La aeronave sufrió daños que no le impidieron aterrizar de forma segura en su destino.

- Nueva York (NY Post, 2017). Un helicóptero Black Hawk del ejército americano sufrió un impacto cuando se encontraba volando a unos 500 pies, pudiendo aterrizar en un aeropuerto cercano sin que se produjeran daños personales, aunque una de las palas del rotor principal se vio afectada.

Adicionalmente, se producen miles de notificaciones de avistamientos, sospechas de impacto o lo que se conocen comúnmente como “near miss” (accidentes que no se produjeron por muy poco). La FAA (Federal Aviation Administration) edita trimestralmente un informe (FAA, 2020) recopilando todos los incidentes notificados, siendo casi 1800 los registrados el último año. Todos estos incidentes no se limitan a tener un impacto económico en las compañías aéreas o en el propio aeropuerto, si no que muchas partes se ven involucradas y afectadas de distintas formas (WillisTowersWatson, 2019).

Figura 5. Actores afectados por las incursiones dron. (WillisTowersWatson, 2019)

1. Pasajeros. Si se produce una pérdida de confianza de los viajeros en la capacidad de gestión de imprevistos por parte del gestor aeroportuario, en caso de poder escoger otro aeropuerto desde el que viajar lo harán, pudiendo causar un daño que perdure a lo largo del tiempo, siendo especialmente crítico en ciudades que disponen de varios aeropuertos.

2. Compañías aéreas. Aunque son completamente dependientes de estas infraestructuras, no dejan de ser clientes, con lo que, si empiezan a tener problemas con las instalaciones e incidentes que se prolongan en el tiempo, empezarán a buscar otras alternativas.

3. Agencias reguladoras. El cierre de un aeropuerto es siempre crítico, ya que pertenece a un sistema en el que cualquier imprevisto actúa como una reacción en cadena, con lo que agencias como AESA, EASA (European Aviation Safety Agency), Eurocontrol y otras gubernamentales podrían llegar a plantearse imponer algún tipo de sanción a instalaciones aeroportuarias que den problemas recurrentemente.

4. Empleados. De la misma forma que los pasajeros, el gestor aeroportuario tiene que cuidar de la gran cantidad de empleados tanto propios como de las compañías a los que pone en una situación delicada al ser incapaz de gestionar la amenaza de los drones. Los pilotos son los encargados de la seguridad de vuelo en última instancia, con lo que podrían incluso a negarse a operar desde un aeropuerto.

5. Medios de comunicación. Cuando se produce un incidente, es muy importante la forma en la que el gestor aeroportuario reacciona, siendo necesario que la exposición del problema sea clara, transparente y sobre todo rápida, ya que

cualquier retraso, falta de información o incoherencia podría ser aprovechado para crear especulaciones o bulos.

6. Inversores. Muchos aeropuertos, sobre todo fuera de España, son de propiedad privada e incluso algunos cotizan en bolsa, con lo que cualquier incapacidad para gestionar un problema que se perciba, puede causar una falta de confianza de los inversores, lo que sería catastrófico tanto para la financiación del aeropuerto, como para el resto de inversores al verse mermado el valor de la acción.

3.4 COBERTURA DE LOS SEGUROS.

Uno de los aspectos más controvertidos sobre esta nueva amenaza para las operaciones aéreas reside en dirimir quién se hace responsable de los daños ocasionados. Como se ha podido ver, las cifras que se manejan son astronómicas, por lo que todos los actores implicados van a intentar por todos los medios evitar tener que responsabilizarse de la compensación.

En lo que se refiere a daños a las propiedades la situación es clara, pasando la aseguradora a reparar el daño, además siendo los drones en general ligeros y pequeños, los daños que se pueden producir en las propiedades son en general pequeños. Sin embargo, el mercado está creando drones más pesados y con una capacidad de carga mayor, con lo que estos daños potenciales también se incrementan. Hay una cláusula que resulta clave y es si el dron lleva algún tipo de explosivo, lo que convierte el incidente en un acto terrorista, eximiendo habitualmente a la aseguradora de cualquier tipo de responsabilidad.

En este caso existen en el mercado pólizas específicas que cubren este tipo de incidentes, muchos de los cuales llegan incluso a cubrir ataques bacteriológicos, radiológicos y nucleares, siempre que no se produzca en el contexto de una guerra. Dado que el terrorismo yihadista ya ha empezado a usar los drones como forma de ataque, no es descabellado pensar que en algún momento se pueda producir un ataque de ese tipo en algún país occidental.

Sin embargo, la responsabilidad por pérdidas asociadas a una interrupción del tráfico aéreo por un dron en las proximidades es mucho más ambigua. Normalmente para que un seguro de interrupción de la actividad pueda aplicarse, se necesita que haya algún tipo de daño que haya forzado dicha interrupción. Por ejemplo, si un dron ha impactado contra un vehículo en el parking del aeropuerto y las autoridades pausan la actividad por el riesgo de que pueda haber más, la aseguradora podría alegar que la actividad podría haber continuado ya que los daños no imposibilitaban la operación.

Recientemente se está contemplando una cláusula conocida como “amenaza por acto delictivo” en la que la aseguradora puede ofrecer cobertura en caso de evacuaciones, intervenciones o cierres decretados por los FFCCSE (Fuerzas y Cuerpos de Seguridad del Estado). Aquí se podrían incluir también las pausas de la actividad que se decreten por sospecha o notificación de actividad cercana por parte de un dron, aunque al final resulte no ser real y las medidas tomadas hayan sido razonables.

Respecto al caso de las actuaciones que se puedan producir por parte de terceros, como pueden ser los pasajeros o aerolíneas, el seguro de responsabilidad que suscribe una instalación aeroportuaria suele tener clausulas muy poco concretas. Hay tres claves que hacen que la cobertura se active (WillisTowersWatson, 2019):

- Se produzca un suceso tal y como se define en la póliza.
- Éste haya causado algún daño personal o material.
- El aeropuerto sea responsable total o parcial ante el daño sufrido por un tercero.

En algunos tipos de incidentes con dron puede ser aplicable, como en caso del impacto con una instalación del aeropuerto, pero en sucesos como el cierre de Barajas por avistamiento de dron, es mucho más complicado demostrar que se ha producido un daño o incluso que fuera un dron lo que lo ha causado, ya que por sus características se pueden confundir con aves y es muy complicado mantener un seguimiento de su trayectoria. Sin embargo, en cuanto se produjera un daño en una aeronave, por mínimo que fuera, serviría para poder activar la cobertura.

Los pasajeros tienen también la potestad de redactar reclamaciones a las aerolíneas por los retrasos y cancelaciones acumuladas, lo que probablemente éstas intenten repercutir en el gestor aeroportuario en caso de haber sido causadas por un dron. En este caso, las coberturas actuales no lo contemplarían a no ser, como se ha comentado anteriormente, que se haya producido algún daño.

Por tanto, se puede afirmar que las pólizas actuales son útiles para los casos en los que se produzca un impacto, pero sin embargo son en general ineficientes en los casos en los que la pérdida se produzca únicamente como consecuencia de sospechas y por precaución. Se espera que en los próximos años haya un desarrollo en el negocio de los seguros contra dron, lo que hará que haya clausulas mucho más específicas que permitan abandonar el limbo legal en el que actualmente se encuentran este tipo de sucesos.

4. MEDIDAS DE MITIGACIÓN DE LA AMENAZA

4.1 SEGURIDAD INTEGRADA EN LOS DRONES

Tras los numerosos informes y creciente preocupación por los problemas tanto de security, safety y vulneraciones del derecho a la intimidad, los fabricantes se han visto en la necesidad de implementar sistemas que garanticen una mayor seguridad en la operación. En caso de que no hubieran tomado medidas y los sucesos sigan incrementándose, es factible pensar que las autoridades tomen medidas, imponiendo restricciones aún más duras, haciendo que los drones se conviertan en un mercado menos atractivo, afectando directamente a los fabricantes. Actualmente, las medidas que están aplicando los fabricantes son las siguientes:

- Geofencing.

Consiste en "vallar" de forma virtual el espacio aéreo para que no se puedan producir incursiones, usando varios sistemas de geolocalización de los drones. Para ello se definen una serie de puntos que forman una zona en la que el dron emite un aviso al operador, aterriza de forma automática o prohíbe el despegue para evitar cualquier peligro.

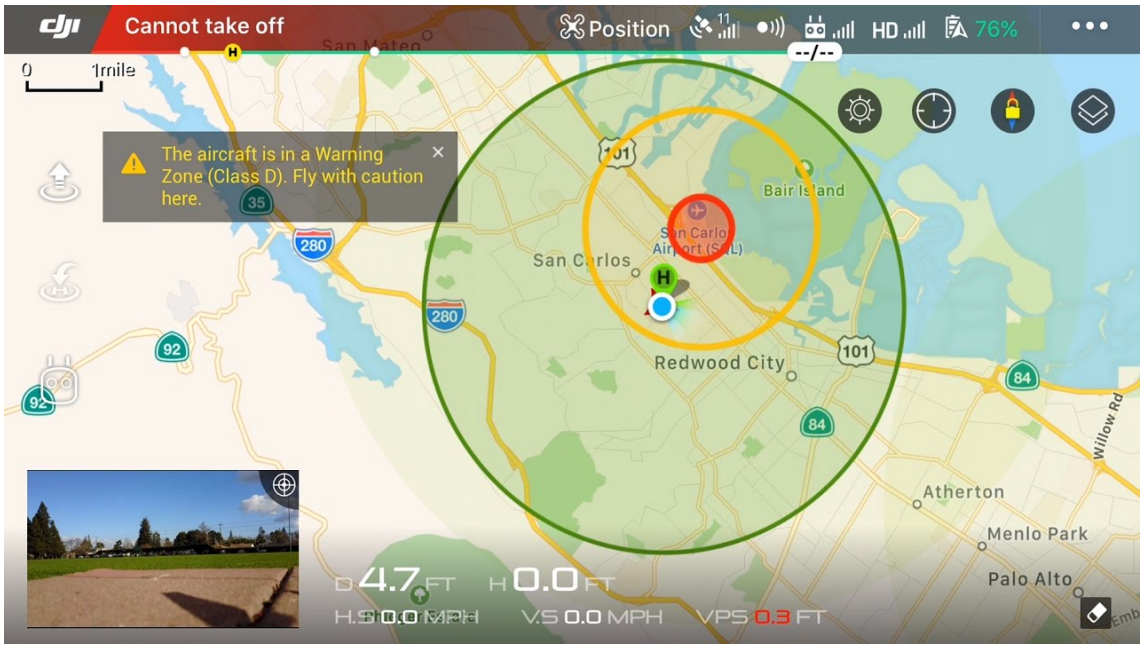


Figura 6. Vista del software de DJI cuando un dron se encuentra en zona protegida por geofencing (DroneLife, 2017)

Este sistema es muy útil para operadores que no tienen mucho conocimiento del espacio aéreo en el que están volando, pudiendo el mismo software limitarles la altura de vuelo y evitar la entrada en espacios aéreos restringidos, manteniendo el vuelo del aficionado dentro de la legalidad.

Sin embargo, hay maneras de evitar la restricción, como puede ser la desconexión del GPS (Global Positioning System) por lo que el dron pasa a un modo inercial en el que gestiona su vuelo a través de giróscopos o de forma puramente manual. Por lo tanto, ante una actuación de una persona irresponsable o con intenciones maliciosas, es inefectivo. Existe la posibilidad de hacer aún más restrictiva esta herramienta por

ejemplo no permitiendo que el dron vuele sin señal GPS, pero esto haría que el vuelo en circunstancias concretas como en interiores fuera imposible. Además, la legislación actual y la que se plantea para el futuro, permite bajo autorización de las agencias gubernamentales, volar en zonas restringidas, con lo que se necesita que exista alguna forma de permitir la operación.

- Receptor ADS-B

El ADS-B (Automatic Dependent Surveillance Broadcast) es un sistema por el cual una aeronave emite continuamente sus datos exactos de posición, altura y velocidad. Esto es útil tanto para los servicios de tránsito como para el resto de usuarios del espacio aéreo. Está diseñado para ser el sustituto del transpondedor, que funciona de forma similar pero únicamente emite la información al recibir una interrogación por parte de un radar secundario. Este sistema está siendo implantado rápidamente por todo el mundo, especialmente Europa y EEUU, donde está previsto que haya una implantación mayoritaria en 2020 con algunas excepciones.

DJI, fabricante que representa el 75% de las ventas mundiales, ha integrado un sistema en su software, el cual denomina “AirSense”. Se basa en un receptor ADS-B para representar cualquier aeronave que pueda entrar en conflicto con el dron.

Figura 7. Representación de avión cercano en el software de DJI. (YouTube,2018)

Es importante recalcar que el dron dispone únicamente de receptor, con lo que el avión que se representa en la pantalla, no dispone de información de la posición del dron, con lo que los sistemas TCAS (Traffic Alert and Collision Avoidance System) son inútiles para gestionar situaciones peligrosas en las que se vea implicado un dron. Esta tecnología tiene un futuro prometedor y es posible que sea obligatorio en un futuro. Probablemente se necesite que pase de ser un sistema puramente informativo a uno intrusivo, en el que, bajo ciertas circunstancias, el piloto automático del dron tome el control y maniobre para posicionarse de forma segura. De esta forma, se evitarían los acercamientos intencionales a otras aeronaves que operadores inconscientes pudieran intentar. En cuanto a la información adicional que ofrece este sistema y puede servir para intentar acercarse a aviones aprovechándola, realmente está desde hace tiempo disponible en otras aplicaciones como Flight Radar. También existen receptores ADS-B disponibles en el mercado, pudiéndose visualizar la información en cualquier ordenador.

4.2 GESTIÓN DE LA AMENAZA. FASES.

A lo largo de los años en el ámbito militar se han ido desarrollando varias teorías para responder a una amenaza, llegándose en los últimos años a un modelo que, con ciertas variaciones, se puede adaptar a todos los procesos de toma de decisiones. Posteriormente se ha ido adoptando en la vida civil, especialmente en los cuerpos y fuerzas de seguridad.

El proceso distingue 3 fases principales: detección, clasificación y neutralización.

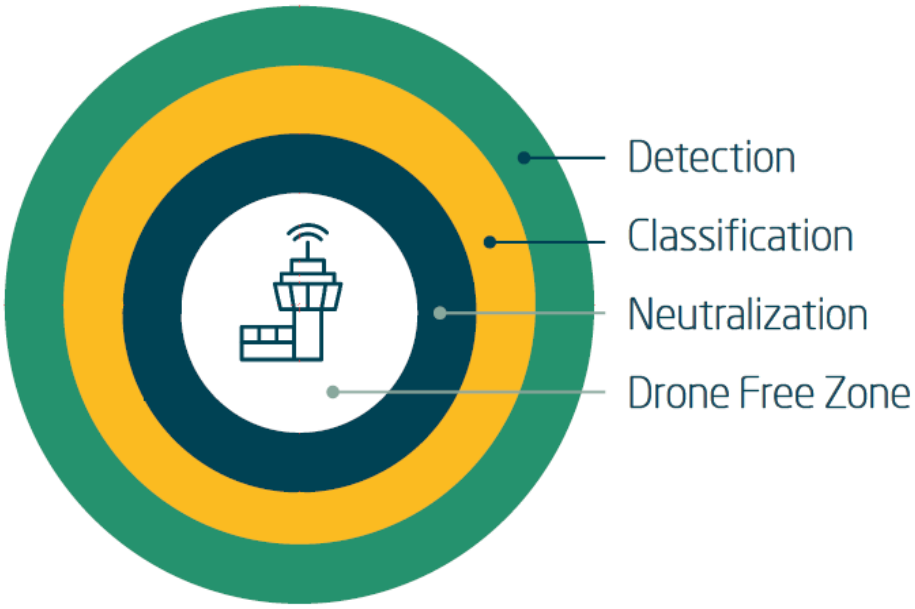


Figura 8. Fases de gestión de la amenaza dron. (ICAO, 2019)

Aunque los sistemas actuales anti dron tienden a cubrir todas las fases, la realidad es que muchos están enfocados sobre todo a la neutralización de la amenaza. El

sistema ideal es capaz de cubrir todas las etapas en tiempo suficiente y ofreciendo la información adecuada, lo que hace que la toma de decisiones se produzca con la mayor de las garantías de que es una respuesta adecuada y proporcional a la amenaza que se presenta.

4.3 DETECCIÓN Y SEGUIMIENTO.

En esta primera fase, se produce una primera señal de la presencia de un dron en las proximidades del área de interés. Puede ser detectado de múltiples formas y es necesario que se pueda mantener su seguimiento a lo largo del tiempo para poder tener la certeza de la envergadura de la amenaza a la que se está haciendo frente y tomar las medidas adecuadas. Un seguimiento inestable dará lugar a una incertidumbre sobre el número de dispositivos y el recorrido que está realizando.

Los métodos de detección actualmente disponibles son:

- Observadores.

  En los recintos aeroportuarios hay multitud de personal que conoce la necesidad de notificar si observan un dron en una zona prohibida en la que el tráfico aéreo se puede ver afectado. Pueden ser pilotos, controladores, trabajadores de handling, oficinistas, gente que se encuentre desplazándose por carreteras aledañas, etc. Es muy importante que las vías de comunicación con la torre de control y responsables de las operaciones sean claras y funcionen correctamente. Dada la centralización con el número único de emergencias 112, se facilita mucho esta comunicación. En caso de pilotos, el enlace directo por radio con la torre agiliza cualquier notificación, facilitando una rápida actuación.
  Para evitar una saturación de avisos y un exceso de paralizaciones de la actividad, es necesario clasificar según su fiabilidad y exactitud los avisos que se reciben. Por ejemplo, no es lo mismo que un piloto llame avisando de que 1 milla náutica en final de la aproximación a 200 pies ha observado un dron que haya un aviso al 112 de una persona sin una cualificación aeronáutica que no aporte apenas datos.

	ROTARY WING	FIXED WING
Nano (< 0.5 kg)	100	100
Micro (0.5 - 2 kg)	200	500
Mini (2 - 20 kg)	300	1000
Small (20 - 150 kg)	800	1200

*Notional maximal visual detection ranges (m)**

Figura 9. Distancias máximas teóricas de detección visual. (NLR, 2019)

- Visual.

  El uso de cámaras en los sistemas anti dron es habitual, siendo necesario combinar dispositivos que sean capaces de analizar distintas longitudes de

onda, cubriendo principalmente desde el ultravioleta, pasando por la luz visible por el ojo humano, hasta el infrarrojo. Suelen estar montadas en soportes giratorios para poder ofrecer una visión prácticamente omnidireccional.

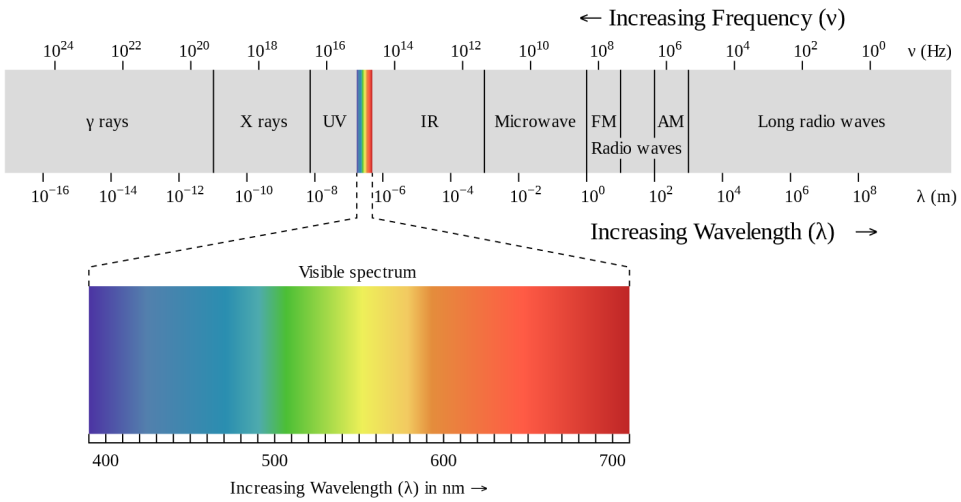


Figura 10. Espectro electromagnético (CC BY-NC-SA; anonymous by request)

Aunque actualmente es un sistema que funciona mejor en la identificación, se están haciendo mejoras muy importantes para incrementar la fiabilidad de detección, a través de sistemas basados en técnicas de *neural networks* o *deep learning* que permiten que los ordenadores aprendan de datos observados a lo largo del tiempo, mejorando continuamente los algoritmos de detección. Estos métodos han demostrado capacidad para detectar y seguir drones, pero debido a la similitud del vuelo de éstos con las aves, se producen un gran número de falsos positivos, lo que produce una saturación del sistema si éste no está equipado con otro tipo de sensor que permita la confirmación automáticamente.

- Radar (Radio Detection and Ranging).

El uso de este sistema para detectar aeronaves, se remonta a la segunda guerra mundial, habiéndose llegado actualmente a un desarrollo anteriormente impensable de esta tecnología, con radares de barrido electrónico con unas distancias de detección impresionantes. Se basa en el envío de una señal electromagnética para una vez que se ha recibido la onda que el aparato refleja, obtener datos como rumbo, distancia, altura y velocidad. Estos sistemas están diseñados con una o varias antenas, siendo capaces de detectar y mantener el seguimiento de múltiples objetivos simultáneamente. Sus mayores ventajas residen en la capacidad todo tiempo (no se ven apenas afectados por las condiciones meteorológicas), distancia de detección (variando dependiendo del tamaño entre 3 y 10 km) y la precisión de los datos obtenidos.

	Active Radar ROTARY WING	Active Radar FIXED WING	Laser Enabled
Nano (< 0.5 kg)	3000	6000	300
Micro (0.5 - 2 kg)	3000	6000	300
Mini (2 - 20 kg)	3000	6000	300
Small (20 - 150 kg)	10000	10000	2000

Notional maximal detection ranges (m)

Figura 11. Distancias teóricas de detección radar (NLR, 2019)

Su mayor desventaja reside en las características del dispositivo que intenta encontrar. Los drones tienen las características de los dispositivos conocidos por el acrónimo LSS (Low, Small, Slow).

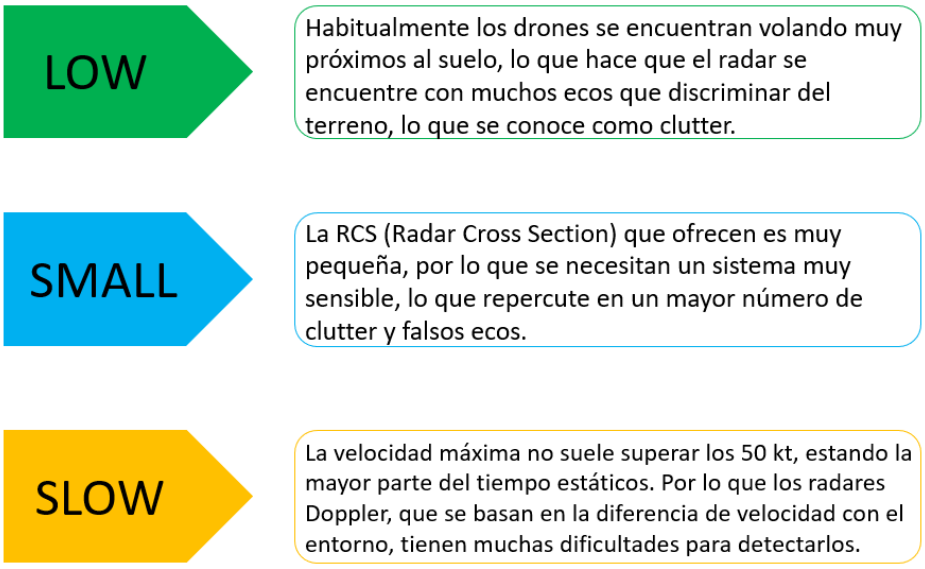


Figura 12. Características de los dispositivos LSS (Elaboración propia).

Una dificultad añadida es que es necesario que el sistema tenga un nivel de automatización bastante alto y unos operadores con un entrenamiento suficiente para que las capacidades que ofrece este sistema de detección sean aprovechadas completamente. Este tipo de sensor suele ser el más caro de los que integran el conjunto del sistema de detección. Además, es el único que no es pasivo, por lo que se necesita estar seguro que no va a causar interferencias con otros sistemas que se usen en las inmediaciones y debe ser aprobado su uso por las autoridades.

- Detección acústica.

Se basan en una serie de micrófonos de alta sensibilidad que se encuentran enlazados a unos programas de análisis de audio para detectar los sonidos

producidos por los drones. Es incluso posible, usando una librería de sonidos, saber el modelo de dron que se encuentra en el radio de detección de la estación. Esto funciona en condiciones ideales, pues la onda sonora es muy sensible a cualquier cambio de temperatura, obstáculos, viento, etc.

El problema fundamental de este sistema, es que es muy fiable en lugares aislados, donde no hay contaminación acústica. En un aeropuerto, donde se producen ruidos intensos y suelen estar comunicados con grandes carreteras con mucho flujo de tráfico, la distancia a la que es capaz de detectar un dron, se verá muy mermada.

	Acoustics
Nano (< 0.5 kg)	150
Micro (0.5 - 2 kg)	250
Mini (2 - 20 kg)	350
Small (20 - 150 kg)	500

Notional maximal detection ranges (m)

Figura 13. Distancias máximas teóricas de detección acústica. (NLR, 2019)

Evidentemente, una señal en un micrófono únicamente dará una intensidad que permitirá saber que se encuentra a una distancia determinada del dispositivo acústico, por lo que se sabrá que se encuentra en un área formada por un círculo alrededor de éste. Para obtener una posición fiable, es necesario que haya una serie de sensores distribuidos a lo largo de la instalación a proteger para que se pueda obtener la posición a través de la triangulación de la información recibida por varios micrófonos.

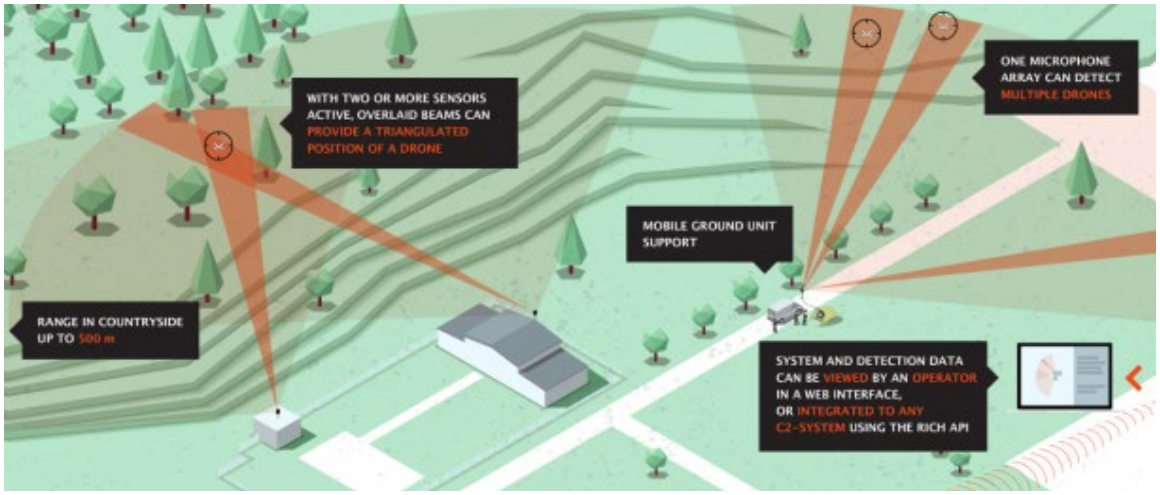


Figura 14. Triangulación por sensores acústicos. (SquareHead, 2020)

- Detectores de radiofrecuencia (RF)

También conocido por el acrónimo ESM (Electromagnetic Spectrum Monitoring), se basa en la detección de la emisión de radiofrecuencia que se produce como consecuencia del intercambio de información del dron y la estación de control. La práctica totalidad de los drones que se encuentran en el mercado, emite en la frecuencia del Wi-Fi, es decir, entre 2.4GHz y 5.8GHz. El principal problema es que los aeropuertos se suelen encontrar en zonas donde hay muchísimos emisores en dichas frecuencias, lo que hace que la distancia a la que pueden detectarlos se reduzca considerablemente. Los sistemas actuales tienen un software que incorpora librerías con las frecuencias concretas que usa cada tipo de dron, lo que sirve para filtrar las emisiones recibidas y poder optimizar la búsqueda, mejorando considerablemente los resultados.

Cuenta con dos ventajas principales, la primera es que permite la detección en cuanto se encienden los dispositivos, permitiendo que se puedan tomar medidas mucho antes del primer aviso de cualquier otro sistema. La segunda reside en que es el único sistema que permite obtener la localización del operador.

	ESM
Nano (< 0.5 kg)	1500
Micro (0.5 - 2 kg)	1500
Mini (2 - 20 kg)	1500
Small (20 - 150 kg)	1500

*Notional maximal detection ranges (m)**

Figura 15. Distancias máximas teóricas de detección por RF. (NLR, 2019)

4.4 CLASIFICACIÓN Y LOCALIZACIÓN.

La clasificación de los dispositivos que entran en la zona de responsabilidad servirá para que la toma de decisiones sea efectiva y proporcional al peligro que suponen para las operaciones. Requerirá una fusión de los datos recibidos por los distintos sensores y la información obtenida por otros medios. Es necesario obtener una clasificación de la actividad en función de la posición, lo que determinará las medidas a tomar. También es posible, con autorización, que los drones vuelen en zonas restringidas, por lo que el flujo de información entre agencias gubernamentales y operadores de drones autorizados funcione, con el fin de no crear falsas alarmas que puedan hacer que se tomen medidas para controlar una situación que ya se encontraba controlada, pudiendo causar perjuicios a las operaciones aéreas o daños a drones privados autorizados.

- Información provista por observadores.

Es necesario establecer los canales de comunicación necesarios para que las personas que observen un dron, puedan dar los datos más exactos posibles

relativos a la localización, número de rotores, si es de ala fija o rotativa, color, tamaño aproximado, velocidad, dirección de movimiento etc. Esto servirá para tener una idea aproximada de donde buscar con el resto de sensores y saber si se está acercando a zonas críticas.

- Radar.

Una técnica que se está desarrollando y tiene un futuro prometedor es el microdoppler. Consiste en el análisis de las ondas de radar recibidas y que están condicionadas no por la firma radar del dron en sí, sino por la perturbación que genera en estas ondas las partes móviles de las que dispone el dispositivo. Esto permite, contando con una base de datos actualizada y detallada, saber el modelo de dron del que se trata, consiguiendo ofrecer información precisa, por ejemplo, del rango de frecuencias en la que está trabajando, para que la neutralización sea más sencilla y rápida. Además, elimina prácticamente en su totalidad, los falsos positivos que se puedan dar por detección de aves. En la actualidad, pocos equipos del mercado ofrecen esta herramienta.

- Sistemas acústicos.

De la misma forma que cada modelo de dron tiene una firma microdoppler, también emiten un sonido distinto. De nuevo, la base de datos de la que disponga el software es la parte más importante y debe ser actualizada continuamente. En entornos donde los ruidos se superponen, como los aeropuertos, la capacidad de identificación del modelo de dron, se puede ver muy reducida hasta hacerla inservible.

- Sistemas electro-ópticos.

Como en los anteriores sistemas, es necesario tener una librería actualizada de imágenes o unos operadores bien instruidos para conocer los drones que están en el mercado. La combinación de cámaras visuales e infrarrojas o térmicas, ofrece la posibilidad de identificar un dispositivo tanto de noche como de día, sin embargo, su desempeño ante las inclemencias meteorológicas es muy limitada.

- Detectores de RF.

A través de la señal que se detecta, es posible obtener muchísimos datos del dispositivo, como son:

▪ Datos de la señal. Todos los parámetros de la conexión son útiles para, en caso de necesidad, poder perturbarla o tomar el control del dispositivo. Además, cuantos más datos se tengan, la perturbación será más precisa, evitando interferencias indeseadas a otros sistemas y pudiendo usar potencias de emisión inferiores.

▪ Modelo de dron. A partir de los datos, es posible obtener fabricante, modelo e incluso, en un futuro, tener un registro obligatorio de drones con lo que se podrá saber quién es el propietario.

▪ Posición del operador. En los drones que se encuentran conectados a una estación remota que dirige sus movimientos, es posible obtener no solo la posición del dron, sino también del operador. Es necesario que haya al menos dos sensores de RF que se encuentren dentro de alcance para poder efectuar una triangulación. Es incluso posible integrar este tipo de sistemas en el software del que disponen los controladores, para obtener la posición del operador y mandar a fuerzas de seguridad u obtener incluso grabaciones de cámaras que consigan identificar a éste. Dado que no es un sistema activo que pueda medir la distancia como un radar, el operador se encontrará en la intersección del eje de las señales recibidas por los distintos sensores.

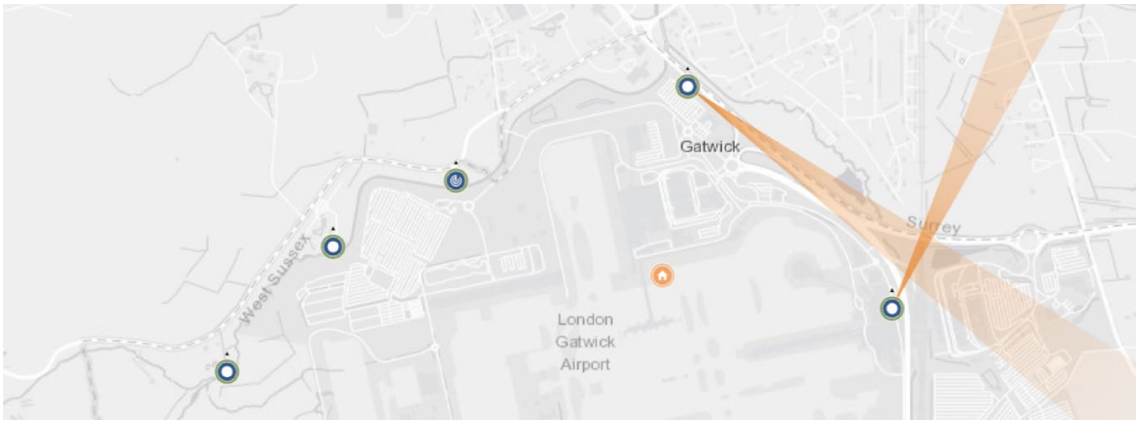


Figura 16. Triangulación por detector de RF. (MyDefence, 2019)

4.5 NEUTRALIZACIÓN.

Cuando, tras seguir los pasos anteriores, se llega a la conclusión de que el dron supone una amenaza que tiene que ser desactivada, existen una amplia variedad de métodos para lograr este fin. Se deben tener en cuenta los siguientes aspectos:

▪ Tipo de guiado.

En función de este aspecto, podremos evaluar si podemos intentar interferir en la señal de guiado, ya sea mandando una señal para hacerle aterrizar simulando ser la estación remota, o si está funcionando de forma autónoma, hacer que los sistemas de posicionamiento funcionen de forma incorrecta.

▪ Tamaño.

Uno de los aspectos más importantes a considerar es el tamaño y peso del objetivo, ya que la mayoría de sistemas de neutralización hacen que caiga al suelo con cierta velocidad, con lo que cuanto mayor sean estos parámetros, mayor será la energía del impacto pudiendo producir mayores daños a personas o instalaciones.

▪ Entorno.

Hay que estudiar si alguno de los métodos puede suponer un menor riesgo, evaluando si la zona es aislada, si hay edificios o personas en las cercanías, si quizás al interferir su señal de guiado puede que se desplace a una zona más crítica de la que se encontraba originalmente, etc. También se debe considerar cuando empleemos dispositivos que interfieran señales, o emitan energía, si podemos afectar a otros sistemas que se encuentren próximos.

▪ Carga.

Aunque no se han detectado todavía ataques con explosivos a instalaciones aeroportuarias, no es descartable en un futuro, siendo necesaria una actuación muy rápida en estos casos, necesitándose medios que derriben el dron de forma instantánea y con un corto tiempo de reacción.

Los métodos actuales para la neutralización de drones son los siguientes:

● Perturbación de señal GPS.

Para que este sistema tenga efecto, es imprescindible que la nueva señal que se le manda al dron, sea más intensa que la que recibe de los satélites reales, con lo que se requieren altas potencias de emisión o bien que sean muy direccionales. Dado el entorno en el que se va a usar, se debe usar de forma controlada y cuando no pueda interferir a otros sistemas, como pueden ser los sistemas de posicionamiento y guiado de los aviones.

Otro factor a tener en cuenta es el movimiento errático que se puede crear al introducir perturbaciones en esta señal, como quedó reflejado en un experimento por un aficionado (Robinson, 2015). Este efecto se veía incrementado cuando hacía viento y además la característica RTH (Return To Home) de la que disponen algunos dispositivos, se volvía inservible. Por tanto, estos sistemas únicamente deben ser empleados cuando se estime que la zona está suficientemente libre de obstáculos y personal para que, en el trayecto errático del dron al suelo, no se produzca una situación peligrosa.

También es posible, alterando de forma dinámica las coordenadas de las que dispone el dron, controlar su vuelo, haciendo que aterrice de forma controlada en el lugar que se considere conveniente.

● Perturbación señal de Radio Frecuencia.

Como se ha expuesto anteriormente, la inmensa mayoría de los drones usan el rango de frecuencias del wifi para su comunicación con la estación de control, con lo que, si se consigue emitir una señal suficientemente potente, podemos interferir en esta comunicación, haciendo que el dron actúe asumiendo que ha perdido la conexión. En estos casos, dependiendo del diseño, el dron, bien caerá sin control, aterrizará de forma controlada en la posición en la que se encontraba o volverá al lugar de donde despegó.

En este último caso es posible seguir el vuelo del dron hasta llegar al lugar donde se encuentre el operador para tomar las medidas administrativas que correspondan.

De nuevo se presenta el problema de la gran cantidad de señales con las que el perturbador puede interferir en un entorno aeroportuario. Por ello, es necesario contar con un sistema con una precisión muy alta y que concentre su acción en el volumen de espacio establecido por el operador.

Es incluso posible, si se conoce la frecuencia exacta y el protocolo de comunicación, *hackear* el dron, con lo que se toma el control de este, pudiendo dirigirlo hacia una zona segura. Normalmente esta técnica requiere una mayor complejidad y suele tardar bastante más tiempo, no teniéndose garantía de éxito al iniciar el proceso debido a que en el encriptado de las comunicaciones en ocasiones imposibilita la conexión.

- Métodos físicos.

En este apartado se incluyen los sistemas que neutralizan físicamente un dron, ya sea a través de la emisión de energía o por otros medios. En este apartado se mezcla la más avanzada tecnología con los métodos más rudimentarios, pero en algunas ocasiones más efectivos.

- HPM (High Power Microwave).

Aunque no hay muchos sistemas en el mercado actualmente que utilicen esta tecnología, está teniendo un rápido desarrollo. Se basa en una emisión muy potente y concentrada de micro ondas que son capaces de producir daños suficientes en los sistemas de un dron para hacer que no pueda continuar con su vuelo. Este tipo de sistemas tiene dos problemas principales, el primero, que suponen una emisión de energía que en muchos países está prohibido y puede llegar a afectar a otras aeronaves o sistemas de comunicaciones. El segundo, es que tienen un coste elevado en comparación con otros sistemas más sencillos. La ventaja principal radica en su capacidad para, integrado con otros sistemas de seguimiento, derribar rápidamente cualquier dron sin importar el tipo de guía que tenga, si vuela de forma autónoma, etc.

Esta tecnología se ve afectada por la atenuación atmosférica, lo que hace que, para obtener resultados a una gran distancia, se necesite una potencia y concentración de la energía muy superior, con lo que los alcances en general no son muy altos, aunque para un aeropuerto probablemente sean suficientes.

- Láser (Light Amplification by Stimulated Emission of Radiation).

El uso del láser como arma es relativamente reciente, habiendo nacido y siendo usado hasta ahora prácticamente en exclusiva por los distintos ejércitos. Se basa en la emisión muy concentrada de energía que produzca un daño en los distintos componentes de un dron, consiguiendo en poco tiempo derribarlo. Al ser luz, se caracteriza por mantener la dirección en la que es emitida, con lo que no son necesarios sistemas de puntería que calculen la desviación, caída o efecto Coriolis para que la neutralización sea efectiva. Tiene un problema que limita las distancias a las que se puede emplear y es el efecto conocido como “Thermal Blooming”, que es la pérdida de energía que se produce por la interacción del haz láser con el entorno (en este caso

aire). Al igual que el HPM, requiere una emisión de potencia muy grande, lo que, en muchos casos, limita su movilidad al necesitar una gran fuente de energía.

Los tipos de láser que se pueden usar con este fin son (Freudenrich,2008):

▪ Láser de estado sólido. Su funcionamiento se basa en un cristal como pueden ser el rubí o neodimio que tienen en su interior.

▪ Láser “excimer”. Su nombre proviene de la contracción de exciter y dimer (excitador y dímero). El dímero es una especie química que consiste en la unión de dos compuestos generalmente idénticos. Este tipo de dispositivo usa habitualmente una combinación de un gas noble y otro reactivo para producir un haz en el espectro ultravioleta. Dependiendo de los gases usados, la longitud de onda resultante será distinta.

▪ Láser de tinte. Su nombre proviene del tinte que se usa como medio, habitualmente encontrándose en una solución líquida y puede generar una gama de longitudes de onda superior a los gases y sólidos.

▪ Láser de gas. En este caso, el medio usado para que circule la corriente es un gas, el cual varía dependiendo de la longitud de onda deseada y su fin. El “excimer” podría incluirse dentro de este tipo, aunque tiene unas características especiales.

- Cetrería.

La cetrería es una vieja conocida de los aeropuertos de todo el mundo, a los cuales lleva años proveyéndoles de protección contra las aves y el impacto para la operación que suponen. Su funcionamiento se basa en el vuelo diario de aves de presa en las instalaciones aeroportuarias para evitar que el resto de aves se establezcan y habitúen a volar en las inmediaciones. Es un sistema que en la actualidad se sigue usando a pesar de haberse hecho varios intentos para sustituirlas.

La teoría de su uso contra drones varía en cuanto a que no trata de disuadir su uso, si no que su finalidad es derribarlo. Actualmente hay compañías que ofrecen ya este servicio tanto para aeropuertos como en eventos susceptibles de ser amenazados por drones. Sus principales ventajas son:

▪ Rapidez. Cuando se detecta un dron se puede desplazar el vehículo del cetrero al lugar mientras se investiga y clasifica el tipo de amenaza que supone para que, si se decide neutralizar, poder hacerlo al instante.

▪ Precisión. No necesita caros sistemas de puntería para acertar en el objetivo ya que el entrenamiento que tienen las aves es suficiente para que sean efectivas.

▪ Ausencia de daños colaterales. Al ser un sistema que no consta de proyectiles ni emite energía electromagnética, su uso es plausible en una amplia variedad de situaciones.

Sin embargo, cuenta también con algunas desventajas:

▪ Amplio radio de maniobra.

Si el dron se encuentra cerca de la zona crítica de operaciones aéreas, es necesario paralizarlas, ya que puede que el ave se desvíe lo suficiente para poder causar problemas con un avión que esté maniobrando en las inmediaciones del aeropuerto.

▪ Sistema de reserva.

En general todos los sistemas pueden fallar, pero al depender de un ser vivo, en más necesario que nunca disponer de otro por si las cosas no van como se espera.

▪ Limitación a condiciones visuales.

Su uso es únicamente posible cuando las condiciones atmosféricas son favorables y hay luz diurna, con lo que en muchas ocasiones no es una opción válida.

● Proyectiles.

Cuando la amenaza de los drones comenzó, había pocas opciones que no fueran las armas de fuego. Estos sistemas han ido quedando en desuso o como última opción, aunque se ha ido desarrollando incluso municiones específicas contra dron, más similares a un cartucho de escopeta que a una bala de fusil o pistola. Existen también cartuchos que disponen de una malla en su interior que, al ser proyectada hacia un dron, se expande y consigue atascar las hélices, provocando así su caída. Se ha seguido con el desarrollo de misiles contra dron, pero su uso es exclusivamente militar en escenarios de conflicto.

● Drones.

Uno de los sistemas que han surgido ha sido el uso de otro dron para derribar a través del impacto al otro o con el lanzamiento de una red que atrapa al dron objetivo y lo deposita suavemente en el suelo.

Cuenta con grandes ventajas, pero necesita que el dron objetivo no realice maniobras muy bruscas para que su uso sea satisfactorio. Hay que tener en cuenta que este sistema no es compatible con otros, como puede ser la perturbación, ya que también se vería afectado.

5. MODELO PLAN ACTUACIÓN ANTE AMENAZA DRON.

5.1 CUERPO GENERAL.

5.1.1 Preámbulo.

El siguiente documento es un modelo que puede ser adaptable al plan de reacción de cualquier aeropuerto dependiendo de sus capacidades, dimensiones y flujo de tráfico aéreo. Por trabajar sobre un aeropuerto real se va a usar como referencia el de Almería, lo que será útil para ver cómo toda la teoría explicada anteriormente se adapta a un escenario existente y ofrece un ejemplo que pueda servir de guía para la implantación en otra instalación aeroportuaria. El modelo propuesto no está basado en ningún dato real de equipamiento, disposición de éste o tráfico aéreo, por lo que se garantiza que no pueda ser usado con fines delictivos. El equipamiento simulado es considerado el ideal para este tipo de amenaza, aunque para este caso está sobredimensionado. Estos procedimientos deben tener una clasificación de seguridad y deben ser conocidos por el número indispensable de personas para garantizar su funcionamiento.

5.1.2 Equipamiento lucha anti dron.

El equipo del que se dispone en el aeropuerto de Almería es:

- Sistema Drone Dome del fabricante israelí Rafael. Sus componentes son:

  ● Radar. Capacidad de seguimiento de varios objetivos simultáneamente. Sistema todo tiempo con una cobertura de 360º horizontales y 90º verticales.

Figura 17. Radar del sistema Drone Dome. (Rafael, 2019)

  ● Sensor de RF. Capacidad de detección en un gran ancho de bandas, alto rango dinámico y buena sensibilidad.

Figura 18. Sensor RF del sistema Drone Dome (Rafael, 2019)

● Cámara electroóptica e infrarroja. Sensor con capacidad de detección, seguimiento y reconocimiento automático de objetivo.

Figura 19. Cámara EO e IR del sistema Drone Dome. (Rafael, 2019)

● Perturbador. Capacidad de bloqueo e interferencia de las señales recibidas por el control remoto, incluyendo vídeo. Posibilidad de perturbación de señal de geolocalización del dron.

Figura 20. Perturbador del sistema Drone Dome. (Rafael, 2019)

● Centro de mando y control. Instalado e integrado en los sistemas de la torre de control de tráfico aéreo.

Figura 21. Sistema mando y control del sistema Drone Dome. (Rafael, 2019)

- Armas de fuego con munición anti dron “Skynet”.
  La patrulla que de la GC que se encuentra en las instalaciones del aeropuerto dispone de este tipo de munición, la cual despliega una malla metálica que provoca la caída inmediata del dron.

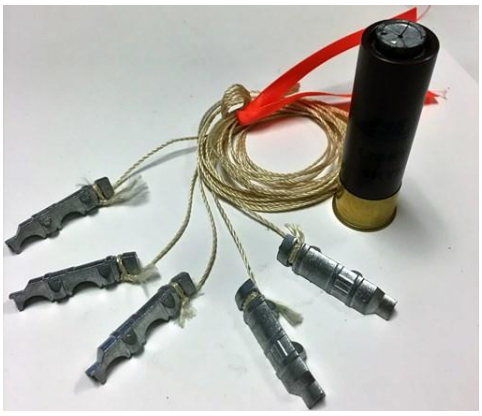


Figura 22. Munición anti dron Skynet. (LessLethal, 2020)

5.1.3 Mando y control.

El Centro de Coordinación de Actuación (CCA) del aeropuerto de Almería estará conformado por:

● Responsable de Evento Dron (RED). Será el director del Aeropuerto, en su ausencia el Jefe de servicio de la Torre de Control.
● Jefe de Seguridad de la Guardia Civil.
● Jefe del equipo anti drones.
● Personal ATC.

Los cometidos son los siguientes:

● RED: Toma de decisiones y responsable de la gestión de la amenaza.

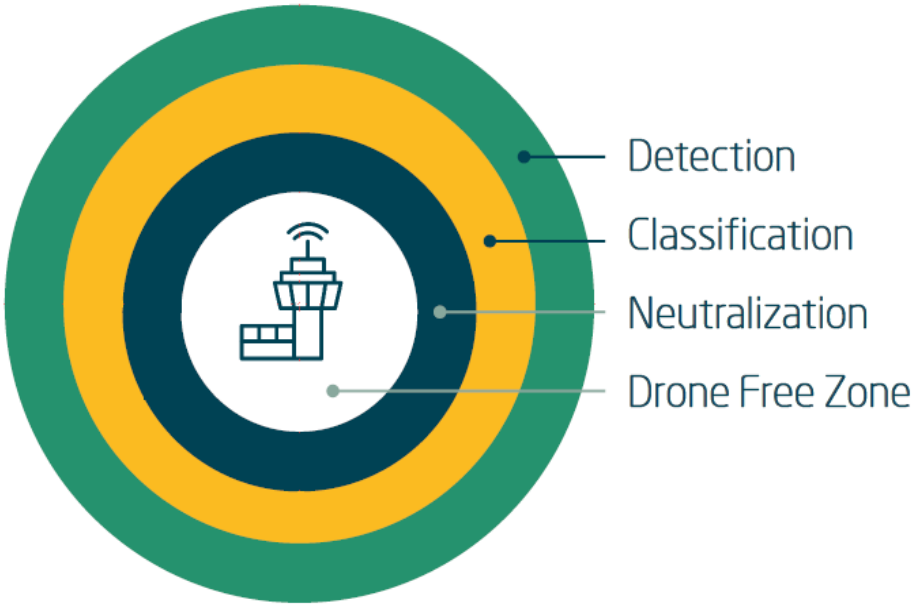
● Personal de Servicio ATC: Distribución de la información, siendo la vía de entrada de información al CCA, como la transmisión de las órdenes o actuaciones que se tomen. Gestionará sus recursos para ofrecer la forma más segura de operación al tráfico aéreo. Redactará el modelo de notificación de amenaza dron, contemplado en el anexo C.

● Jefe del equipo anti drones. Responsable del funcionamiento correcto del equipamiento c-uas, de ofrecer al RED la información actualizada y un asesoramiento técnico para todas las fases de la gestión de la amenaza. Cumplimentará el informe final a AENA.

● Jefe de Seguridad de la Guardia Civil. Responsable de la patrulla equipada con armas de fuego para la neutralización de drones y protección de la zona. Nexo de unión con el resto de FFCCSE que puedan ser necesarios.

5.1.4 Criterios de reacción.

Para determinar los criterios de reacción ante una amenaza de este tipo es necesario verificar la presencia de la misma y evaluar la situación antes de actuar. El procedimiento se basará en las fases de Detección y seguimiento, clasificación e identificación y neutralización. Ninguna de estas fases debe omitirse para que el resultado de la actuación sea satisfactorio.



5.1.5 Detección y seguimiento.

Se considera que una incursión dron está verificada cuando la notificación y/o detección del dron en espacio o zona no autorizada proviene de un observador cualificado o uno de los sistemas anti dron instalados en el aeropuerto.
Se define como observador cualificado a pilotos, personal ATC, personal que opera en la plataforma de aeronaves, a los componentes de las FFCCSE y a los miembros del aeropuerto que Almería que el director de éste determine.

En caso de que la información provenga de otra fuente (observador no cualificado) deberá ser confirmada por otro medio o un segundo observador, lo que no impide que se puedan adoptar las medidas de precaución necesarias.

El seguimiento se llevará a cabo preferiblemente a través de los sensores del sistema c-uas y cuando no sea posible se desplazará una patrulla con comunicación directa con la torre de control.

En los casos en que un dron sea detectado por un observador, se rellenará un formulario de avistamiento con los datos obtenidos, tal y como viene reflejado en la figura 27 de este documento, siendo transmitida esta información directamente al jefe del equipo anti dron. Para detallar la posición del dron, se utilizarán coordenadas, referencias visuales o preferiblemente las cuadrículas expuestas en las figuras 25 y 26.

- Para observador cualificado:
  - -Iniciar el Procedimiento.
  - -Confirmar presencia de dron con sensores C-UAS
- Para observador no cualificado:
  - -Informar a los miembros del CCA.
  - -Iniciar búsqueda con sensores C-UAS.
  - -Enviar una patrulla al lugar para confirmar presencia de dron.
  - -En caso de encontrarse fuera de la zona de amenaza del aeropuerto, enviar patrullas Policía Local/Nacional.

5.1.6 Clasificación e identificación.

En este paso se tratará de establecer por todos los medios disponibles las características del dron, discriminación de falsos positivos y comprobación cruzada con los datos disponibles respecto a autorizaciones de vuelo por parte de AESA o publicación de NOTAM (Notice to Airmen) con el fin de saber si es un vuelo de un dispositivo coordinado previamente. En este sentido, se establece una clasificación de la amenaza de:

1. Riesgo CRÍTICO. Situaciones que requieran una actuación inmediata, principalmente si hay sospecha de que el dron está transportando un explosivo o puede ser usado con fines terroristas.

2. Riesgo ELEVADO. Cuando el dispositivo haya invadido las áreas de protección de la pista o el área de operaciones aéreas.

3. Riesgo MODERADO. El dron se encuentra en la zona de amenaza del aeropuerto.

4. Riesgo MENOR. La ubicación del aparato se encuentra dentro de la zona de vigilancia dron.

5. Sin Riesgo. Se ha detectado un dron y bien tiene autorización o se encuentra fuera de las zonas anteriormente descritas, pero dentro de la CTR.

En caso de activación preventiva del plan de actuación por notificación no contrastada o dron del que no se dispongan datos de su posición, se adoptarán las medidas correspondientes al Riesgo Moderado.

Asimismo, se usarán los distintos sensores para averiguar fabricante y modelo de dron, ofreciendo datos sobre su peso, techo, velocidad máxima, tipo de control y reacción esperada a la perturbación.

Además de a los miembros del CCA, durante esta fase se pre-alertarán otros organismos por si fuera necesaria su intervención. Estos servicios son:
● Servicio de Bomberos.
● Servicio de Sanidad.
● Equipo TEDAX (Técnico Especialista en Desactivación de Artefactos Explosivos).

En cualquier caso, el nivel de clasificación de la amenaza podrá ser ajustado siempre por el RED en función del comportamiento que esté teniendo el dron.

5.1.7 Neutralización.

El procedimiento se iniciará cuando se haya clasificado la amenaza como de riesgo elevado, moderado o dadas las circunstancias el RED, consideren necesaria la neutralización inmediata del dispositivo.

En caso de no ser considerada necesaria la neutralización, se coordinará para mandar patrullas de los FFCCSE a la zona para intentar localizar al operador cuando el dron aterrice e iniciar las acciones correspondientes.

El método usado se decidirá por el RED que contará con el asesoramiento del Jefe del Equipo anti drones. Se tendrán en cuenta aspectos como:

- Tráfico aéreo cercano.
- Tamaño del dron.
- Si hay peligro de que haya personas que sufran daños.
- Sistemas críticos que se pudieran ver afectados por perturbación.

Tras la neutralización del dron, siempre que sea posible y con las medidas de precaución adecuadas, se procederá a la recogida del dron o de sus restos, para iniciar la investigación que corresponda a cargo del Jefe de Servicio de la GC. Si hubiera alguna sospecha de que pudiera transportar explosivos, se acordonará la zona hasta la llegada de los TEDAX.

5.1.8 Restablecimiento de la situación.

El objeto de esta fase es restaurar y recuperar las operaciones en el aeropuerto de Almería. El CCA es el responsable de decidir la restauración y recuperación normal de las operaciones. Previo a la toma de decisiones, se tendrá en cuenta el análisis de la

información facilitada por el Jefe de Equipo anti dron y Jefe de Servicio de la Guardia Civil relativo a:

- Discriminación de si fue un uso imprudente de un operador aficionado o pudo tener un fin delictivo o terrorista.
- Posibilidad de que haya más dispositivos en vuelo o próximos a despegar.
- Nivel de la amenaza que se llegó a alcanzar.

Si se llegó a neutralizar la amenaza, se valorará restablecer las operaciones normales inmediatamente. En caso de no llegarse a neutralizar, los tiempos de referencia para volver a una situación normal son:

● Riesgo CRÍTICO: 60 minutos
● Riesgo ELEVADO: 30 minutos.
● Riesgo MODERADO: 15 minutos.
● Riesgo MENOR: no requiere actuación.

Tras la decisión de restablecer la situación de inicio, el personal ATC iniciará el flujo de llamadas a los miembros del CCA, y otros servicios que se hubieran puesto en pre aviso con la fórmula “Finalización de amenaza dron en el aeropuerto de Almería”

5.1.9 Análisis e informes

Una vez finalizado el evento dron, las partes implicadas remitirán a AENA, a la mayor brevedad un informe sobre el incidente. Dicho informe deberá contener:

1. Información cronológica del suceso con actuaciones, medidas adoptadas y resultados.
2. Identificación del operador (incluyendo actuaciones concretas) y del tipo de dron.
3. Recopilación de evidencias.
4. Análisis del impacto en las operaciones del aeropuerto.
5. Aprendizaje obtenido durante la activación del plan de reacción.

5.2 ÁREAS DEL AEROPUERTO.

A) ÁREAS RIESGO ELEVADO.

Será valorada como riesgo ELEVADO la presencia o incursión dron en el Área Recinto Aeroportuario o en el Área Protección Dron Pista.

El Área Recinto Aeroportuario se ha definido como todo el espacio correspondiente a las instalaciones del aeropuerto de Almería, incluyendo el parking de vehículos y las carreteras de acceso.

El Área Protección Dron Pista se define como el área trapezoidal definida por las aproximaciones instrumentales y visuales, extendiéndose hasta 5 NM (8 km) en sentido de la pista contado desde cada umbral. Se considera que, a partir de esa distancia, la

altura de las aeronaves es mayor a la de operación normal de drones y por tanto la probabilidad de impacto con estos dispositivos se reduce considerablemente.

B) ÁREAS RIESGO MODERADO.

Será valorada como riesgo MODERADO la presencia o incursión dron en la Zona de amenaza del aeropuerto. Esta área está comprendida entre el vallado del aeropuerto y 2 km alrededor del mismo, con forma rectangular.

.

C) ÁREAS RIESGO MENOR.

En el Área Vigilancia Dron la amenaza por presencia o incursión dron será valorada como riesgo MENOR. El Área Vigilancia Dron está comprendida por el rectángulo limitado por dos lados paralelos al eje de la pista a 5 km del mismo y por otros dos lados perpendiculares situados a 8 km. Tiene una extensión superior en algunos puntos a la ATZ, sin llegar a cubrir la CTR, dada la capacidad de detección y actuación contra drones. Independientemente de esto, cualquier dron del que se tenga constancia dentro de la CTR, será objeto de seguimiento y advertencia al tráfico aéreo.

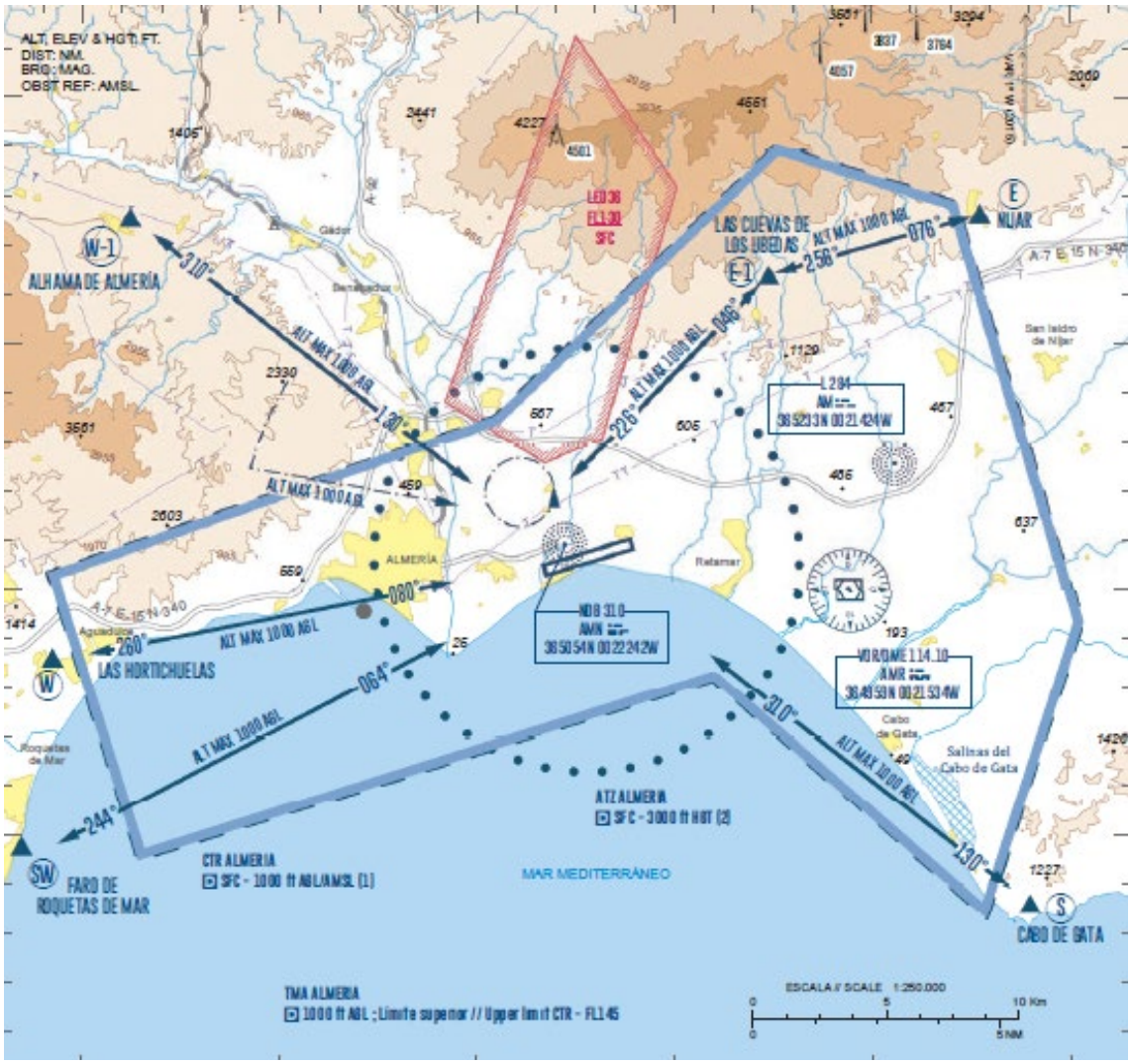


Figura 23. ATZ y CTR de Almería (AIP España, 2020)

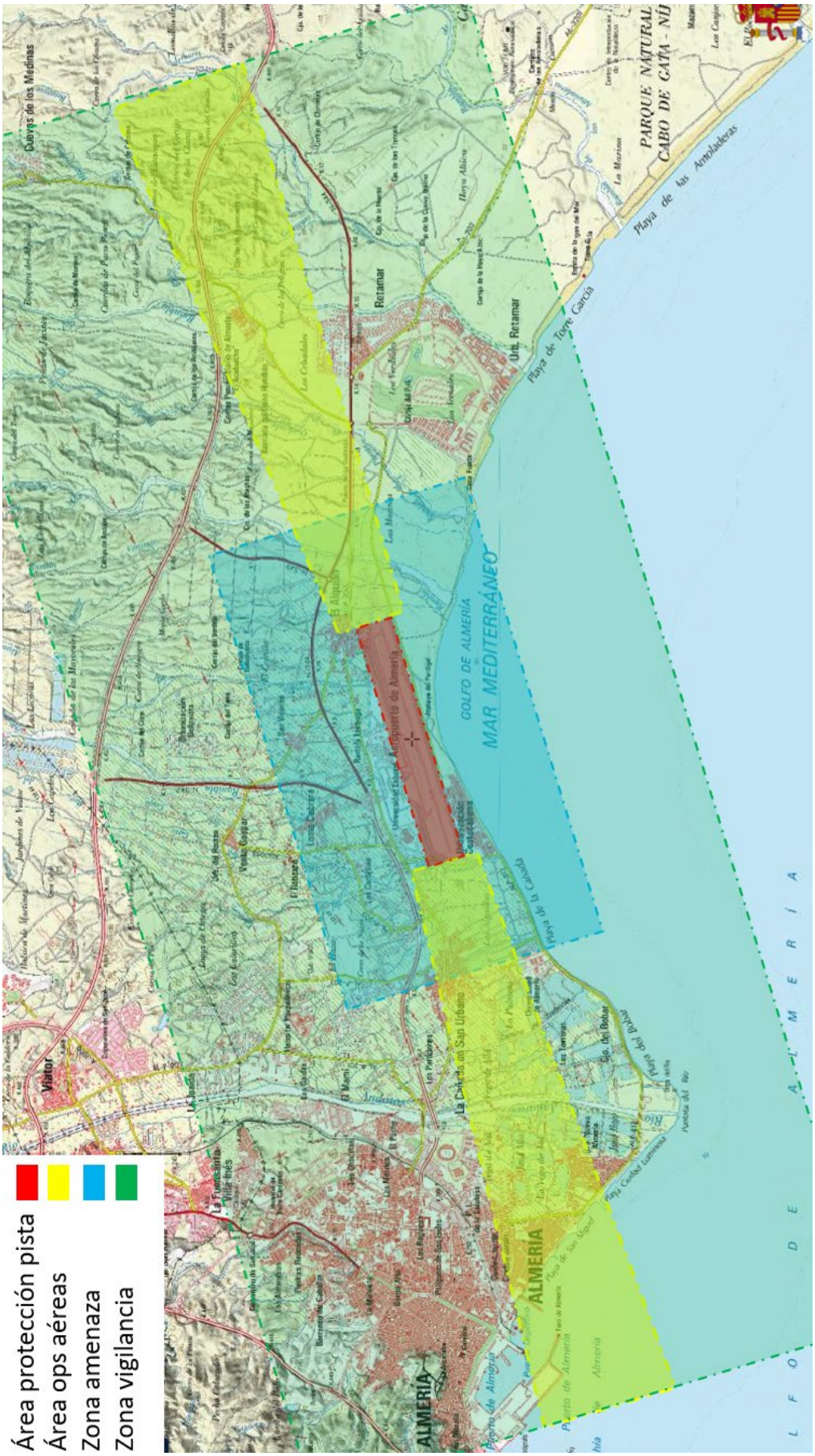


Figura 24.Representación gráfica de las áreas y zonas de protección del aeropuerto (Elaboración propia, FEGA, 2020)

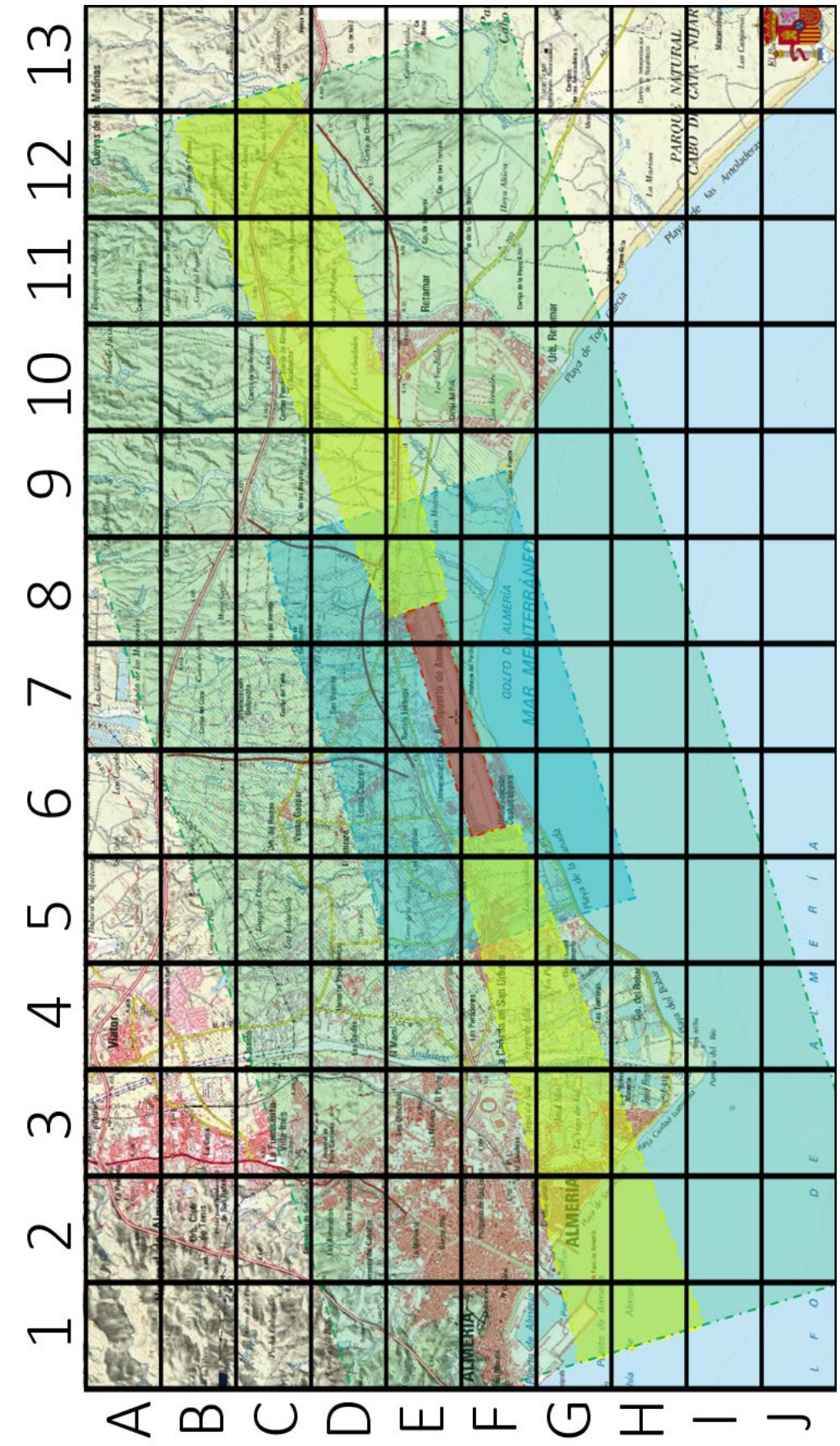


Figura 25. Cuadrícula para localización de dron (Elaboración propia, FEGA, 2020)

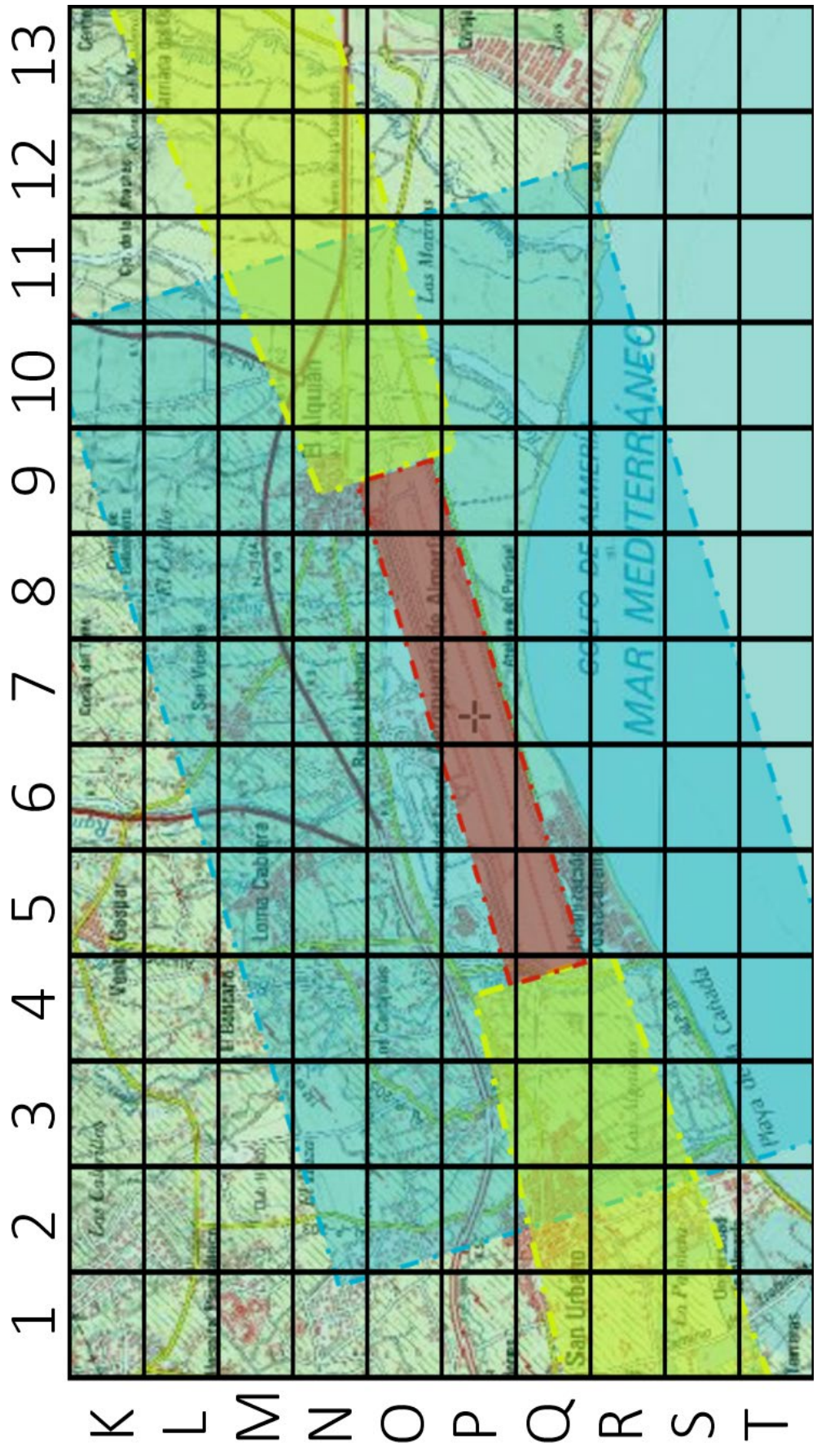


Figura 26. Cuadrícula ampliada para la localización precisa del dron (Elaboración propia, FEGA,2020)

5.3 PROCEDIMIENTOS DE ACTUACIÓN.

Como observador cualificado, el control de tránsito aéreo puede tener conocimiento de la presencia no autorizada de un dron en el entorno del aeropuerto de Almería.
Una vez se constate dicho evento dron y cerciorado de que se trata de un dron no autorizado en su área de responsabilidad iniciará el Procedimiento.

Recogerá y compartirá, al menos, la siguiente información:

● Zona de observación y trayectoria.
● Número de drones avistados.
● Indicará si se trata de una observación propia o confirmada de otra fuente.
● Tomará las acciones preventivas con el resto del tránsito aéreo que estime convenientes en tanto no se declare un estado de amenaza concreto por parte del CCA.

A continuación, se recogen las actuaciones según el nivel de riesgo del evento dron.

A) RIESGO CRÍTICO.

● Evacuar las aeronaves que se encuentren en plataforma y el aeropuerto.
● Implementar las medidas de riesgo ELEVADO, MODERADO y MENOR.

B) RIESGO ELEVADO.

● Suspender las operaciones aéreas.
● Monitorizar la evolución del dron dentro del Área Recinto Aeroportuario.
● Interceptar e identificar al operador dentro de la Zona de Seguridad.
● Estar preparados para neutralizar el dron.
● Recoger y custodiar evidencias en el interior de la Zona de Seguridad.
● Coordinar actuaciones con los FFCCSE.
● Implementar las medidas de riesgo MODERADO y MENOR.

C) RIESGO MODERADO.

● Restringir las operaciones aéreas en la zona de localización del dron (en estrecha coordinación entre el Control de Aproximación y Torre).
● Adoptar medidas de precaución tales como frustrar a una aeronave en una aproximación hacia la zona de riesgo, contemplar la posibilidad de usar la otra pista o mandar al tráfico a orbitar en una espera.
● Desplazar la patrulla de la GC a la posible zona de incursión.
● Implementar las medidas de riesgo MENOR.

D) RIESGO MENOR

● Compartir con el CCA todas aquellas actividades en curso de las que tenga conocimiento que puedan suponer un incremento del riesgo (repostajes en plataforma, embarques de personal VIP…) y que deban ser valoradas.
● Realizar los avisos a la navegación necesarios a las aeronaves de la presencia de un dron no autorizado.
● Alertar a la Patrulla de Seguridad.
● Informar al observador que colabore quedándose en el lugar hasta que hagan presencia los FFCCSE.

● Preavisar a los equipos necesarios.
● Monitorizar la actividad del dron y alertar de los cambios significativos en su comportamiento.

E) SIN RIESGO.
Operaciones normales, manteniendo vigilancia en cualquier dispositivo que pueda haber por la zona y optimizando las operaciones para garantizar la seguridad

5.4 FORMULARIO RECOGIDA DE DATOS.

Fecha	Hora notificación
Localización (Coordenadas, referencias, cuadrícula)	
Datos observador (Empleo, nombre, teléfono)	Número de dispositivos
Características físicas dron	
Altura y velocidad estimadas	¿Transporta alguna carga visible?
¿Está viendo al operador? En caso afirmativo, localización, descripción física y de un posible vehículo, matrícula, etc.	
Datos adicionales.	

Figura 27. Formulario recogida de datos. (Elaboración propia)

6. CONCLUSIONES.

El reto al que se enfrentan las administraciones no es sencillo. Se está por fin acometiendo un problema que en los últimos años no ha dejado de crecer, creando problemas de *security* y *safety* que se han ido agravando con la popularización de los drones. Los gobiernos y agencias gubernamentales de todo el mundo han optado por intentar compaginar una legislación implacable contra los que actúen de forma imprudente, temeraria o delictiva, con un marco legislativo que permita un desarrollo de esta tecnología que ha llegado para quedarse en nuestras vidas.

El uso de los drones se puede extender a prácticamente todos los ámbitos de nuestras vidas, incluyendo campos tan diversos como la agricultura, salvamento marítimo, logística, televisión, industria cinematográfica y así hasta el infinito. Sin embargo, la legislación actual es muy conservadora, lo que limita muchísimo las aplicaciones actuales que podrían tener los drones en pro de un uso seguro de estos.

Es cierto que existen cauces para que las autoridades permitan operaciones que habitualmente no se autorizan, como puede ser vuelo dentro de espacios controlados o sobrevuelos de ciudades y aglomeraciones de personas, pero los requisitos son en muchas ocasiones de una complejidad y coste excesivo, siendo normalmente autorizaciones individuales y puntuales, lo que limita muchísimo el desarrollo de esta tecnología.

Un mercado que está teniendo un desarrollo exponencial es el referente a los sistemas de seguridad para equipar en drones que amortiguan o disipan la energía del impacto del dron contra el suelo en caso de fallo o accidente. Hay una gran variedad de sistemas, desde paracaídas a cámaras hinchables que se activan en caso de emergencia. Para poder optar a realizar actividades con drones que están restringidas, hay que equipar estos sistemas y hacer además estudios exhaustivos de seguridad para su aprobación final. En la actualidad, esta tecnología no está suficientemente desarrollada, pero sería muy bueno para la industria del dron que, en un futuro cercano, las agencias aeronáuticas autoricen el vuelo a modelos de dron que tengan equipados dispositivos concretos de seguridad, abaratando y facilitando muy significativamente las operaciones que actualmente se encuentran restringidas.

Todo esto no es nuevo, ya que ante todas las tecnologías que ha ido desarrollando el ser humano se han ido enfrentando al status quo, hasta que poco a poco han ido encontrando un hueco. Tanto la sociedad como las leyes han sabido ir evolucionando para acoger las nuevas tecnologías, con lo que esta ocasión no va a ser una excepción.

Uno de los aspectos más importantes para llegar a este punto, va a ser la concienciación de los operadores de drones aficionados sobre lo que se puede y no se puede hacer. Actualmente, el desconocimiento es generalizado y las marcas deben implicarse en este aspecto, puesto que una disminución de los incidentes con drones llevará previsiblemente a una legislación más permisiva que aumente las ventas y por tanto el beneficio de las compañías. Algunas como DJI ya hemos visto que han dado un primer paso implantando sensores ADS-B en algunos de sus dispositivos, pero probablemente deban evolucionar para ser más intrusivos y no permitir cierto tipo de operaciones que puedan poner en peligro a otras aeronaves.

El esfuerzo no debe quedarse únicamente en este punto, sino que es necesario concienciar a través de las instrucciones y anuncios de lo que permite y no permite la ley y las consecuencias de su incumplimiento.

Con estas medidas, a medio plazo, se podrá conseguir que los vuelos que hagan incursiones en espacios aéreos no autorizados por desconocimiento se reduzcan significativamente y se mantengan los vuelos que puedan tener intenciones delictivas o terroristas.

Por tanto, es necesario un desarrollo sólido y continuado en el tiempo de tecnologías anti dron que permitan seguir el ciclo de detección, identificación y neutralización, asegurando que ningún eslabón es más débil que otro, ya que podrá llevar a tomar medidas que no son adecuadas, causen daños no deseados en dispositivos autorizados o no sean lo suficientemente efectivos para la neutralización de drones que supongan una amenaza.

En este sentido, los dispositivos anti dron que causan perturbaciones en la geolocalización o en la comunicación por radio frecuencias, están prohibidos en muchos países, con lo que, si se quiere un desarrollo sólido de los drones junto con la tecnología adecuada para controlarlos, es necesario que las leyes se adapten para permitirlo. No se trata de dar carta blanca para que todo el mundo pueda perturbar el espectro electromagnético, pero sí que las agencias gubernamentales, con personal cualificado y entrenado, tengan la capacidad de ofrecer este servicio.

En cuanto a los sistemas disponibles, como se ha visto todos tienen sus ventajas e inconvenientes, puntos fuertes y débiles. Por tanto, no existe un único sistema que nos pueda garantizar cubrir el proceso de análisis de amenaza completamente, con lo que algo básico es la complementación entre sensores y sistemas. Disponer de un software que combine de forma satisfactoria toda la información y se la muestre al operador de forma *user friendly* es imprescindible. Cuanto más fiable y precisa sea la información de la que dispone el organismo a cargo del análisis de amenazas, las actuaciones serán más adecuadas.

Hay multitud de fabricantes y no existe un protocolo estandarizado para que los distintos sensores fusionen la información, por tanto, interesa más encontrar un sistema en el mercado que integre los sensores que consideramos necesarios, pues el software estará desarrollado específicamente para ellos. Esto es fundamental en las fases de detección y clasificación, disponiéndose de mayor libertad en la fase de neutralización, pues podría considerarse más independiente que las dos anteriores.

La actualización de los sistemas anti dron deberá ser continua e ir adaptándose a los avances tecnológicos y legislativos que se vayan produciendo. La irrupción del 5G y las nuevas posibilidades que ofrece esta red para el control de los drones de nueva generación son las nuevas amenazas que se ciernen en un futuro cercano. Este futuro parece inevitable, ya que las ventajas que ofrece esta tecnología querrán ser aprovechadas por los fabricantes, como son el ancho de banda y la baja latencia, lo que permitirá que no haya retrasos en el intercambio de información entre el dron y la estación de control, abriendo un nuevo mundo de posibilidades y aplicaciones.

Es de esperar un avance tecnológico en el equipamiento del que disponen los drones para integrarse en el espacio aéreo controlado junto con otras aeronaves. Muy

probablemente se requerirán nuevas capacidades sobre sistemas de comunicaciones, interrogadores y sistemas de control resistentes a la perturbación, lo que supondrá un desafío para los fabricantes.

El futuro que tiene ante sí la industria del dron es muy prometedor siempre que pueda garantizar la seguridad de su operación. Sin avances tecnológicos suficientemente notorios en este sentido, únicamente encontrará trabas en la legislación, lo que limitará sus posibilidades.

7. REFERENCIAS.

1. Statista. Commercial drones are taking off. Febrero 2019) https://www.statista.com/chart/17201/commecial-drones-projected-growth/

2. UK Airprox Board. Airprox involving UAS Drones. Junio 2020. https://www.airproxboard.org.uk/Reports-and-analysis/Statistics/Airprox-involving-UAS-Drones/

3. Boletín Oficial del Estado. Real Decreto 1036/2017 de 15 de diciembre. https://www.boe.es/eli/es/rd/2017/12/15/1036

4. Diario Oficial de la Unión Europea. Reglamento de ejecución (UE) 2019/947 de la Comisión de 24 de mayo de 2019. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0945&from=ES

5. Diario Oficial de la Unión Europea. Reglamento delegado (UE) 2019/945 de la Comisión de 12 de marzo de 2019. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0945&from=ES

6. Organización de Aviación Civil Internacional (OACI). Anexo 7, julio 2012. https://www.anac.gov.ar/anac/web/uploads/normativa/anexos-oaci/anexo-7.pdf

7. ENAIRE. AIP (Servicio de Información Aeronáutica). Agosto 2012. https://ais.enaire.es/aip/

8. CNN. Detalles exclusivos del plan para asesinar a Maduro con drones en agosto. Marzo 2019. https://cnnespanol.cnn.com/2019/03/14/detalles-exclusivos-del-complot-para-asesinar-a-maduro-con-drones/

9. University of Dayton Research Institute. Impact test prove large aircraft won´t always win in collision with small drones. Septiembre 2018. https://udayton.edu/udri/news/18-09-13-risk-in-the-sky.php

10. MAA, BALPA and Department for Transport. Small remotely piloted aircraft systems (drones). Mid air collision study. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/871672/small-remotely-piloted-aircraft-systems-drones-mid-air-collision-study.pdf

11. The Local. Update: 143 flights cancelled at Frankfurt Airport due to drone sighting. Mayo 2019.
https://www.thelocal.de/20190509/disruption-after-frankfurt-airport-halts-flights-due-to-drone-sighting

12. The Guardian. Thousands forced to spend night at airport as chaos continues – as it happened. Diciembre 2018.
https://www.theguardian.com/uk-news/live/2018/dec/20/gatwick-airport-drone-travel-chaos-disruption-live-updates

13. La Vanguardia. La presencia de drones obliga a cerrar el espacio aéreo de Barajas durante dos horas. Febrero 2020.
https://www.lavanguardia.com/local/madrid/20200203/473278294504/barajas-drones.html

14. Arabian Business. Shutting down Dubai International Airport due to a drone costs $100.000 a minute. Julio 2017.
https://www.arabianbusiness.com/content/375851-drone-costs-100000-minute-loss-to-uae-airports

15. BBC. Drone collides with comercial aeroplane in Canada. Octubre 2017
https://www.bbc.com/news/technology-41635518

16. NY Post. Civilian drone collides into Army helicopter. Septiembre 2017.
https://nypost.com/2017/09/22/army-helicopter-hit-by-drone/

17. FAA. UAS sighting report. 2020.
https://www.faa.gov/uas/resources/public_records/uas_sightings_report/

18. WilllisTowersWatson. Drone disruption at airports. A risk mitigation and insurance response. 2019.
https://www.willistowerswatson.com/-/media/WTW/Insights/2019/07/drone-disruption-at-airports-a-risk-mitigation-and-insurance-response.pdf?modified=20190731151924

19. DroneLife. DJI, Hackers, Conspiracy Theories and the Geofencing controversy. Julio 2017.
https://dronelife.com/2017/07/17/defence-dji-hackers-wrong/

20. YouTube. ADS-B in receiver on DJI Matrice 210 (DJI Airsense) for manned aircraft avoidance. Junio 2018.
https://youtu.be/zZibkxLQs8o

21. ICAO. ARMS – Anti RPAS Multisensor System. Junio 2019.
https://www.icao.int/NACC/Documents/Meetings/2019/NACCDCA9/NACCDCA9P08.pdf

22. NLR. C-UAS Detection, Tracking and Intent. Octubre 2019.
https://www.eurocontrol.int/sites/default/files/2019-10/9-nlr-poppinga.pdf

23. CC BY-NC-SA; anonymous by request. https://chem.libretexts.org/Courses/Harper_College/CHM_110%3A_Fundamentals_of_Chemistry/02%3A_Radiation-_Pros_and_Cons/2.08%3A_The_Electromagnetic_Spectrum

24. SquareHead. Drone detection. 2020. https://www.sqhead.com/drone-detection/

25. MyDefence. Protecting airports against drones. Febrero 2019. https://mydefence.dk/wp-content/uploads/2019/02/White-Paper-Protecting-airports-against-drones.pdf

26. Michael Robinson. Knocking my neighbor´s kid´s cruddy drone offline. 2015. https://academic.csuohio.edu/yuc/mobile/GPS-Knocking-My-Neighbors-Kid-Drone-compressed.pdf

27. Craig Freudenrich, Ph.D. How Laser Weapons Work. Marzo 2008. https://science.howstuffworks.com/laser-weapon.htm

28. Rafael. Drone Dome. Marzo 2019) https://www.rafael.co.il/wp-content/uploads/2019/03/Drone-Dome-Updated-march-19-1.pdf

29. LessLethal. Skynet Mi-5. 2020. https://www.lesslethal.com/products/12-gauge/als12skymi-5-detail

30. FEGA. Visor SIGPAC. 2020. http://sigpac.mapama.gob.es/fega/visor/

31. Imagen de portada. Lukas Godja. https://www.shutterstock.com/es/image-photo/drone-flying-near-commercial-airplane-danger-1023444085

8. BIBLIOGRAFÍA.

1. Ministerio de Defensa de España. Concepto nacional C-UAS LSS. Enero 2019. https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/01_CONCEPTO_NACIONAL_C-UAS_LSS_xPARA_WEBx.pdf

2. Cátedra ISDEFE. Estado del Arte de las Tecnologías Antidrón. Junio 2018. https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/08_ESTADO_DEL_ARTE_DE_TECNOLOGIAS_ANTIDRON_JUN_18.pdf

3. EASA. Concept of Operations for Drones. https://www.easa.europa.eu/sites/default/files/dfu/204696_EASA_concept_drone_brochure_web.pdf

4. HM Government. UK Counter-Unmanned Aircraft Strategy. Octubre 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf

5. Arthur Holland Michel. Counter-Drone systems. Diciembre 2019. https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

6. Homeland Security. Counter-Unmanned Aircraft Systems. Septiembre 2019. https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf

7. María José Cervell Hortal. La defensa contra sistemas aéreos no tripulados (C-UAS): Una reflexión jurídica preliminar desde el punto de vista del uso de la fuerza. Noviembre 2018. http://www.ieee.es/publicaciones-new/documentos-de-investigacion/2018/DIEEEINV11-2018.html

8. EASA. Research Programme on Collisions with Drones. 2017. https://www.easa.europa.eu/sites/default/files/dfu/QinetiQ%20-%20EASA.2016.LVP_.50%20UAS%20Collisions%20-%20Report%20WA1-%20Issue%204.0%20-%20For%20publication%20-%20NS.pdf

9. Georgia Lykou y col. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. Junio 2020. https://www.researchgate.net/publication/342401654_Defending_Airports_from_UAS_A_Survey_on_Cyber-Attacks_and_Counter-Drone_Sensing_Technologies

PEREZ CARMONA DANIEL JUAN - 75725571A

Firmado digitalmente por PEREZ CARMONA DANIEL JUAN - 75725571A
Fecha: 2020.09.14 10:32:55 +02'00'

Daniel Juan Pérez Carmona

Almería, 14 de septiembre de 2020