INTERPOL

MARCO DE INTERVENCIÓN ANTE INCIDENTES CON DRONES

Para equipos de primera intervención y laboratorios forenses digitales

Enero de 2020

La redacción de este documento ha estado a cargo del Laboratorio Forense Digital
del Centro de Innovación de INTERPOL (Singapur)

Para consultas, observaciones o sugerencias, diríjanse a:

INTERPOL Global Complex for Innovation
18 Napier Road
Singapur 258510

Correo electrónico: dfl@interpol.int

Teléfono: +6565503462

PREFACIO DEL SECRETARIO GENERAL DE INTERPOL MARCO DE INTERVENCIÓN ANTE INCIDENTES CON DRONES

Con el rápido desarrollo de las tecnologías empleadas para su fabricación, los drones se han vuelto más asequibles y están utilizándose cada vez más no solo en el ámbito recreativo o comercial, sino también con fines delictivos.

Evidentemente, esta situación ha creado desafíos importantes para la comunidad policial mundial. Actualmente, los drones suponen una presencia constante en el entorno de la labor policial y su utilización y repercusiones se incrementarán todavía más en el futuro.

No obstante, muchos profesionales de la aplicación de la ley no conocen bien todavía las tecnologías relacionadas con los drones. Dado que la utilización indebida de drones supone un grave riesgo para la seguridad pública, es fundamental que los agentes cuenten con la formación y los conocimientos necesarios para actuar de manera segura y eficaz ante incidentes relacionados con drones. Por otro lado, los drones contienen información muy valiosa que puede ser extraída y analizada a fin de obtener evidencias útiles para una investigación.

INTERPOL está en contacto con especialistas en drones, procedentes de organismos encargados de la aplicación de la ley, entidades privadas e instituciones académicas de todo el mundo. Esta red de expertos es la que ha impulsado la creación del presente marco de intervención ante incidentes con drones, destinado a los equipos de primera intervención y los profesionales de laboratorios forenses digitales.

Este documento, concebido como una herramienta de referencia para las fuerzas del orden de todo el mundo, es una muestra de la labor permanente de INTERPOL orientada a promover la innovación y consolidar las buenas prácticas utilizadas en nuestros países miembros.

Doy las gracias a todas las personas que han contribuido a la elaboración del presente documento, que se enmarca en nuestro empeño permanente por hacer del mundo un lugar más seguro.

Jürgen Stock
Secretario General de INTERPOL

CARTA DE LA DIRECTORA DEL CENTRO DE INNOVACIÓN DE INTERPOL

En el ámbito internacional, los avances tecnológicos y la irrelevancia de las fronteras en nuestro mundo interconectado han incrementado el riesgo de muchos delitos tradicionales y han conllevado la aparición de nuevos tipos de actividades delictivas. Esta tendencia ha aportado un mayor grado de complejidad a los desafíos que afrontan las fuerzas del orden en todo el mundo.

Ante esta situación, en 2017 INTERPOL estableció un Centro de Innovación en Singapur, con miras a impulsar el desarrollo de tecnologías avanzadas que resultaran útiles para la labor policial mundial. Dentro del Centro de Innovación existe un Laboratorio Forense Digital que ha organizado diversas actividades de formación para mejorar los conocimientos en esta materia en los países miembros de INTERPOL.

Estoy convencida de que el trabajo de los laboratorios forenses digitales constituye un elemento crucial de la actividad policial, sobre todo en la investigación de actos delictivos relacionados con drones. En efecto, los profesionales de la ciencia forense digital deben formarse de manera continuada para conocer bien las tecnologías emergentes, entre ellas la de los drones.

Por este motivo, en los últimos tres años el Laboratorio Forense Digital ha organizado encuentros en los que especialistas procedentes de organismos encargados de la aplicación de la ley, empresas privadas e instituciones académicas han compartido información, conocimientos y buenas prácticas en materia de drones. La existencia de esta red mundial de especialistas en drones ha sido muy útil para facilitar una actuación eficaz en nuestros países miembros. Gracias a la colaboración permanente con esa comunidad de expertos, tengo el honor de presentar este marco de INTERPOL para la intervención ante incidentes con drones, dirigido a equipos de primera intervención y laboratorios forenses digitales.

En el presente documento se ofrece una perspectiva general sobre los drones y otros dispositivos asociados, se dan orientaciones para la actuación inicial ante un incidente relacionado con drones y se ofrecen pautas para los profesionales encargados de adquirir, examinar, analizar y presentar evidencias electrónicas relacionadas con drones. Esperamos que este marco contribuya a mejorar los conocimientos y las capacidades especializadas de las fuerzas del orden en todo el mundo, en particular los equipos de primera intervención y los laboratorios forenses digitales, para actuar de manera segura y eficaz ante este tipo de incidentes.

Con la esperanza de impulsar la disciplina de la ciencia forense digital para que llegue a ser una parte fundamental de la labor policial, el Centro de Innovación de INTERPOL se esforzará en insuflar un espíritu innovador en los laboratorios forenses digitales de los países miembros, a fin de ayudarlos a superar los complejos desafíos de la seguridad mundial.

Anita Hazenberg
Directora del Centro de Innovación de INTERPOL

Agradecimientos

Son muchas las personas y entidades que han contribuido a elaborar este marco de INTERPOL para la intervención ante incidentes con drones. En primer lugar, INTERPOL desea dar las gracias a los miembros del grupo de trabajo sobre drones que inspiró la elaboración de este documento. En noviembre de 2018, representantes de 6 países y de 4 organismos estadounidenses se reunieron en Denver para abordar los desafíos relacionados con la utilización delictiva de drones. El resultado de aquella reunión es este documento, que esperamos sirva de guía para la intervención de las fuerzas del orden de los países miembros ante incidentes relacionados con drones.

Además, en el presente documento se ofrecen pautas básicas para la gestión de escenarios de incidentes, extraídas de la guía para la primera intervención en lugares de comisión de delitos publicada por el Instituto Nacional de Justicia de los Estados Unidos.

INTERPOL desea expresar un especial agradecimiento a Steve Watson, organizador del taller sobre drones para equipos de primera intervención y laboratorios forenses digitales donde se planteó la elaboración de este marco. En esa actividad, representantes de 9 países miembros de INTERPOL tuvieron ocasión de determinar la estructura y el contenido del presente documento y compartir datos y materiales válidos para toda la comunidad.

Merecen también nuestro reconocimiento Harry Blackie, de la Universidad de Gales del Sur, por detallar las ubicaciones de ficheros de datos en los drones, basada en información recopilada por Steve Watson; Matt Service, por elaborar la introducción técnica empleada como referencia en el presente documento; y Dronelogbook.com, por autorizarnos a reproducir su diagrama sobre la geometría de los drones.

Finalmente, damos las gracias a los especialistas encargados de la revisión técnica del documento, cuyas valiosas observaciones ayudaron a colmar lagunas de información y mejorar la redacción final: Alexandra Clare Alder, Jamie Allan, Priscilla Cabuyao, Christopher Church, Taurean Dennis, Greg Dominguez, Albert Drijfhout, Daniel Halliwell, Graeme Horsman, Bruce Keeble, David Kovar, Alan McConnell, Alan McDevitt, Joseph Majersky, Geoff Moore, Michal Naglowski, Vincent Olsthoorn, Dale Richards, Fahad E. Salamh, Alan Tan y Antonio Sousa Lamas.

Aprovechamos la ocasión para agradecer a todos aquellos especialistas en drones y en labor policial que, a pesar de no haber sido mencionados, también contribuyeron a desarrollar y dar forma al presente marco de intervención.

SUMARIO Página

PREFACIO DEL SECRETARIO GENERAL DE INTERPOL 3
CARTA DE LA DIRECTORA DEL CENTRO DE INNOVACIÓN DE INTERPOL 4
Agradecimientos 5
1. INTRODUCCIÓN 11
1.1 Propósito del documento 11
1.2 Destinatarios 11
1.3 Aplicación del documento 11
2. PERSPECTIVA GENERAL SOBRE LOS DRONES 11
2.1 Los drones en el mundo actual 11
2.2 Incidentes con drones 12
2.3 Clasificación de las aeronaves no tripuladas 13
2.4 Componentes de las aeronaves no tripuladas 14
2.4.1 Componentes físicos ***14***
2.4.2 Software ***15***
2.5 Carga útil de los drones 16
2.6 Entender los drones y otras fuentes de material probatorio 17
2.7 Datos de los drones 19
2.7.1 Tipos de datos ***19***
2.7.2 Acceso a diferentes soportes de información ***20***
2.7.3 Consideraciones para la investigación de datos de drones ***21***
2.8 Delitos que pueden cometerse con la ayuda de drones 22
2.9 Visión general de la normativa sobre drones 22
2.10 Pautas para el manejo seguro de drones 23
2.11 Ejemplos de drones y dispositivos asociados 25
3. PAUTAS PARA LOS EQUIPOS DE PRIMERA INTERVENCIÓN 30
3.1 Primera intervención y recepción de información 30
3.2 Procedimientos de seguridad 31
3.3 Atención de emergencia 32
3.4 Cierre del lugar de los hechos y control de las personas presentes 32
3.5 Traspaso de responsabilidades en el lugar de los hechos y transmisión de información a los encargados de la investigación 33
3.6 Documentación de acciones y observaciones 33
3.7 Establecimiento de un puesto de mando (sistema de control de incidentes) y envío de notificaciones 34
3.8 Manejo de los testigos 35
3.9 Evaluación del lugar de los hechos 35
3.10 Delimitación del perímetro: determinar, establecer, proteger y precintar 36

3.11 Exploración del lugar de los hechos y documentación inicial 37
3.12 Toma de notas y elaboración de registros 38
3.13 Embargo preventivo de drones 40
3.14 Proceso de investigación 45
3.14.1 Investigación en profundidad 47
4. NOCIONES Y PRINCIPIOS DEL ANÁLISIS FORENSE DIGITAL 47
4.1 Descripción general 47
4.2 Principios del análisis de evidencias digitales 48
4.3 Características de un laboratorio de análisis forense digital 48
4.3.1 Recepción de la solicitud 49
4.3.2 Registro del caso 49
4.3.3 Registro de las muestras 49
4.3.4 Toma de fotografías 50
4.3.5 Realización del análisis 50
4.3.6 Devolución de las muestras 50
4.3.7 Cierre del caso 50
5. ANÁLISIS DIGITAL DE DRONES 51
5.1 Descripción general 51
5.1.1 Dispositivos asociados a drones 51
5.2 Adquisición 52
5.2.1 Tipos de extracción de datos 53
5.2.2 Herramientas de extracción 54
5.2.3 Formato del fichero de extracción 54
5.2.4 Secuencia del proceso 54
5.2.5 Otras fuentes de evidencias 60
5.3 Examen 61
5.4 Análisis 61
5.4.1 Procedimientos para el análisis de trazas digitales 61
5.5 Presentación 64
5.5.1 Admisibilidad de las evidencias electrónicas 64
5.5.2 Redacción del informe 65
5.5.3 Testimonios periciales 65
6. EJEMPLOS DE DATOS DE DRONES 66
6.1 Registros de vuelo 66
6.2 Ubicación de ficheros multimedia 66
6.3 Aplicaciones móviles asociadas 67
6.3.1 Aplicación móvil DJI 68
6.3.2 Aplicación móvil Parrot 69
6.3.3 Aplicación móvil Yuneec 71
6.3.4 Aplicación móvil Yuneec para la cámara del dron 73

6.4 Nota sobre las ubicaciones del almacenamiento en los drones 74
7. HERRAMIENTAS HABITUALES EN EL ANÁLISIS FORENSE DE DRONES 75
7.1 Cellebrite/MSAB XRY/Oxygen/CFID 75
7.2 CsvView y DatCon (http://datfile.net/) 75
7.3 DRone Open source Parser (DROP) (https://github.com/unhcfreg/) 75
7.4 Google Earth Pro (https://www.google.co.uk/earth/versions/#download-pro) 75
7.5 ST2Dash y Dashware (https://github.com/ajpierson/st2dash; http://www.dashware.net/) .. 75
7.6 DJI Assistant 75
7.7 FTK Imager 76
7.8 VLC Player 76
8. SITIOS WEB ÚTILES 76
Anexos 77
Anexo A: Tipos de drones 77
Anexo B: Registro de actuaciones del equipo de primera intervención ante un incidente con drones 80
Anexo C: Hoja de registro de incidente con dron 83
Anexo D: Registro de examen de dron 86
Anexo E: Tarjeta de seguridad de las baterías LiPo 93
Anexo F: Lista de comprobación del equipamiento básico para actuar ante un incidente con drones 94
Anexo G: Competencias básicas de los equipos de primera intervención y los especialistas en análisis forense digital 95
Anexo H: Competencias básicas de los agentes de primera intervención 97
Anexo I: Competencias básicas de los agentes de primera intervención no especializados 98
Anexo J: Competencias básicas de los agentes de primera intervención de nivel técnico 99
Anexo K: Competencias básicas de los agentes de primera intervención de nivel técnico avanzado 100
Glosarios 101
Glosario I: Abreviaciones de aviación generales 102
Glosario II: Abreviaciones técnicas 105
Glosario III: Glosario de análisis forense de drones 106
Glosario IV: Glosario de aeronaves no tripuladas 112

Lista de figuras

Figura 1 - Accidente de un dron cargado con drogas 12
Figura 2 - Aeronaves no tripuladas de uso recreativo 13
Figura 3 - Aeronaves no tripuladas de uso comercial 13
Figura 4 - Aeronaves no tripuladas hechas a medida 14
Figura 5 - Dispositivos de control remoto de drones 17
Figura 6 - Dispositivos de control remoto conectados a móviles o tabletas 17
Figura 7 - Gafas de visión en primera persona 18
Figura 8 - Tarjeta de memoria micro-SD 18
Figura 9 - Iconos de almacenamiento en la nube 18
Figura 10 - Huella dactilar 19
Figura 11 - Infografía de la Autoridad de Aviación de Singapur sobre la utilización segura de drones 24
Figura 12 - Infografía de la Autoridad Federal de Aviación de EE.UU. sobre el uso de aeronaves no tripuladas 25
Figura 13 - Control remoto integrado 25
Figura 14 - Componentes de un cuadricóptero 26
Figura 15 - Componentes de un dron de ala fija 26
Figura 16 - Control remoto sin pantalla 27
Figura 17 - Control remoto con conexión a teléfono móvil 27
Figura 18 - Aplicación móvil para el control de drones 28
Figura 19 - Planificador de misiones 29
Figura 20 - Precauciones recomendables antes de aproximarse a un dron 41
Figura 21 - Precauciones de seguridad en el manejo de drones 43
Figura 22 - Secuencia del manejo de drones 43
Figura 23 - Advertencia de seguridad de una batería LiPo 43
Figura 24 - Conservación de evidencias digitales 44
Figura 25 - Recopilación de evidencias digitales 44
Figura 26 - Documentación en el lugar del incidente 45
Figura 27 - Diagrama del proceso de investigación 46
Figura 28 - Analista forense examinando un dron 48
Figura 29 - Proceso seguido en el laboratorio forense digital 49
Figura 30 - Modelo de análisis utilizado en laboratorios forenses digitales 51
Figura 31 - Dron en proceso de examen 53
Figura 32 -Proceso de extracción de datos válido para drones y dispositivos de control remoto 54
Figura 33 - Etiqueta de identificación de un dron 55
Figura 34 - Organigrama del examen de un dron 59
Figura 35 - Organigrama del examen de un control remoto 60
Figura 36. Otras fuentes de evidencias 61
Figura 37 - Control remoto Yuneec 74
Figura 38 - Ubicaciones de datos en el Yuneec Typhoon Q500 4K 74

List of Tables

Cuadro 1 - Consideraciones para la investigación de datos de drones 21
Cuadro 2 - Pautas para el manejo seguro de drones 23
Cuadro 3 - Secuencia de actuaciones en el lugar de los hechos 30
Cuadro 4 - Procedimiento para la primera intervención y la recepción de información 31
Cuadro 5 - Procedimiento de seguridad 31
Cuadro 6 - Procedimiento de la atención de emergencia 32
Cuadro 7 - Procedimiento para cerrar el lugar y controlar a las personas presentes 33
Cuadro 8 - Procedimiento para transferir responsabilidades en el lugar de los hechos e informar a los encargados de la investigación 33
Cuadro 9 - Procedimiento para documentar las acciones y observaciones 34
Cuadro 10 - Procedimiento para establecer un puesto de mando (sistema de control de incidentes) y enviar notificaciones 34
Cuadro 11 - Procedimiento para el manejo de testigos 35
Cuadro 12 - Procedimiento para la evaluación del lugar de los hechos 36
Cuadro 13 - Procedimiento para la delimitación del perímetro: determinar, establecer, proteger y precintar 37
Cuadro 14 - Procedimiento para la exploración del lugar de los hechos y la documentación inicial 38
Cuadro 15 - Procedimiento para la toma de notas y elaboración del registro 39
Cuadro 16 - Procedimiento para el embargo preventivo de drones 41
Cuadro 17 - Riesgos asociados a los drones 42
Cuadro 18 - Tres aspectos que deben tenerse en cuenta en una investigación en profundidad 47
Cuadro 19 - Principios básicos del tratamiento de evidencias digitales 48
Cuadro 20 - Tipos de datos contenidos en los dispositivos de control remoto 51
Cuadro 21 - Métodos de aislamiento de drones y controles remotos 56
Cuadro 22 - Soportes de información en drones y controles remotos 56
Cuadro 23 - Trazas que pueden estar presentes en un dron o dispositivo de control remoto 57
Cuadro 24 - Criterios generales de admisibilidad de evidencias digitales 64
Cuadro 25 - Ubicación de registros de vuelo en algunos modelos de dron 66
Cuadro 26 - Ubicaciones de ficheros multimedia en algunos modelos de dron 66
Cuadro 27 - Aplicación móvil DJI Go 4 68
Cuadro 28 - Características de la aplicación Freeflight de Parrot 71
Cuadro 29 - Características de la aplicación móvil Yuneec 72
Cuadro 30 - Características de la aplicación para cámara Yuneec 73

1. INTRODUCCIÓN

1.1 Propósito del documento

El *Marco de intervención ante incidentes con drones* elaborado por INTERPOL ha sido concebido como una guía para el personal de equipos de primera intervención y laboratorios forenses digitales encargado de actuar cuando se produzca un incidente relacionado con drones. Su propósito es ofrecer pautas técnicas para la gestión de este tipo de incidentes.

Con la presente guía, se pretende que los países miembros dispongan de la información necesaria para llevar a cabo una actuación óptima ante un incidente con drones. Las pautas sugeridas son una referencia para el nivel estratégico y táctico y deben servir como modelo para que cada país, en función de sus propias leyes, prácticas y procedimientos nacionales, determine el tipo de intervención ante incidentes que más se adecúe a sus necesidades.

1.2 Destinatarios

El presente documento está destinado a los países miembros de INTERPOL. En su elaboración se han tenido en cuenta dos tipos de público: los equipos encargados de la primera intervención ante un incidente, y los especialistas en ciencia forense que traten las evidencias digitales con posterioridad a un incidente.

Este documento puede ser útil también para fiscales, jueces y abogados, al ayudarlos a conocer mejor el funcionamiento de un dron, el tratamiento del incidente y las peculiaridades de los casos relacionados con drones.

1.3 Aplicación del documento

No es pretensión de este marco imponer límites a los equipos de primera intervención o los profesionales técnicos, quienes deben guiarse por sus respectivas normativas nacionales. Las pautas propuestas están supeditadas a las leyes y reglamentos vigentes en cada país.

2. PERSPECTIVA GENERAL SOBRE LOS DRONES

2.1 Los drones en el mundo actual

Hoy en día, los drones se han popularizado enormemente y se utilizan con múltiples finalidades, desde el entretenimiento infantil hasta la distribución de artículos ilegales por parte de delincuentes. Sea cual sea nuestro interés en esa tecnología, los drones se han vuelto omnipresentes en nuestra vida cotidiana, ya sea como pasatiempo en los parques o como mecanismo de grabación de imágenes para la prensa, las redes sociales, la televisión y el cine. Todos los días se publican noticias, tanto positivas como negativas, que reflejan los beneficios que los drones pueden aportar a la industria y al público general, pero también sus posibles peligros.

Los cambios en la percepción ciudadana, la proliferación de fabricantes y modelos disponibles, la disminución de los precios y el rápido avance de la tecnología han popularizado el uso de drones entre miles de personas de todo el mundo. El término más utilizado por el público y la prensa es el de “dron”, pero en los organismos encargados de la aplicación de la ley se emplean también otras denominaciones: “aeronave no tripulada”, “sistema aéreo no tripulado”, “pequeño vehículo aéreo teledirigido”, “sistema de aeronave pilotada a distancia”, etc. En el presente documento se utilizarán indistintamente “dron” y “aeronave no tripulada”.

El aumento de la utilización recreativa y comercial de las aeronaves no tripuladas en todo el mundo

indica que los organismos de policía y las fuerzas del orden en general deberán enfrentarse con mayor frecuencia en los próximos años a este tipo de vehículos y a sus operadores.

2.2 Incidentes con drones

Los drones pueden tener diferentes formas y tamaños y utilizarse para multitud de finalidades, desde la obtención de fotografías y vídeos aéreos hasta el transporte de artículos de un lugar a otro. En los últimos años se ha incrementado su disponibilidad, lo cual ha ido acompañado de su empleo para cometer infracciones como las siguientes: invasión de la intimidad, contrabando de drogas, operaciones terroristas o destrucción de infraestructuras críticas, entre otras. Por ejemplo, se han utilizado drones para:

- Introducir artículos de contrabando en ámbitos prohibidos (p. ej., cárceles).
- Sobrevolar zonas restringidas para espiar o grabar imágenes destinadas al uso personal.
- Obstaculizar actividades cotidianas, por ejemplo al sobrevolar un aeropuerto.

Figura 1 - Accidente de un dron cargado con drogas

En los últimos años se han registrado varios incidentes con drones en todo el mundo. A modo de ejemplo, en diciembre de 2018 hubo un incidente grave en el aeropuerto de Gatwick (Reino Unido), cuando una aeronave no tripulada accedió sin autorización al recinto del aeropuerto y ocupó una trayectoria de vuelo. Este incidente alteró durante tres días el funcionamiento del aeropuerto, afectó a miles de personas y costó millones de libras. Por otro lado, en una misma semana de junio de 2019, en el aeropuerto Changi de Singapur hubo dos incidentes con drones que interrumpieron el tráfico aéreo durante varias horas, obligaron a cancelar 65 vuelos y afectaron a numerosos pasajeros.

Este tipo de incidentes han tenido repercusión en múltiples sectores en todo el mundo. Teniendo en cuenta tan solo las noticias publicadas en el primer semestre de 2019, pueden citarse casos en los siguientes lugares:

En aeropuertos:

- Singapur, Inglaterra, Irlanda, Escocia, Canadá, Alemania, Italia, Dubái, Estados Unidos de América, México, Nueva Zelanda y Noruega.

En cárceles

- Estados Unidos de América, Italia, Escocia, Irlanda, Inglaterra y Canadá.

Aparte de estos incidentes recogidos en la prensa, las aeronaves no tripuladas ofrecen innumerables posibilidades para la comisión de delitos, pero también para su prevención. En el futuro, el desarrollo de la tecnología y la disminución de los precios conllevará un aumento en la utilización de aeronaves no tripuladas que impondrá nuevos desafíos a los equipos de primera intervención, los especialistas en ciencia forense digital y la comunidad general de las fuerzas del orden.

2.3 Clasificación de las aeronaves no tripuladas

La diversidad de aeronaves no tripuladas disponibles en el mercado, junto con las grandes diferencias de precio, pueden dificultar la clasificación de los tipos de dispositivos disponibles. Según nuestros estudios, las aeronaves no tripuladas se enmarcan en tres categorías principales:

a) Aeronaves no tripuladas de uso recreativo

Este tipo de aeronaves no tripuladas son utilizadas con fines de entretenimiento por aficionados a esta tecnología, tanto adultos como niños, y su precio suele ser bajo. Las aeronaves no tripuladas de uso recreativo pueden tener especificaciones técnicas muy básicas y costar menos de 25 euros. Casi siempre están concebidas para ser usadas en exteriores y la duración de sus baterías es muy limitada. Por lo general, una aeronave no tripulada se considera de uso recreativo cuando su peso no llega a los 250 gramos. Actualmente se comercializan miles de modelos de aeronaves no tripuladas de uso recreativo, que pueden adquirirse en jugueterías, tiendas de artículos electrónicos e innumerables plataformas de venta por Internet.

Dado que la legislación sobre aeronaves no tripuladas se basa en la utilización prevista y no en las especificaciones del dispositivo, algunos modelos recreativos de alta gama pueden llegar a ser muy complejos. Por ello, en esta categoría se incluyen algunos drones particularmente caros, cuyo precio puede alcanzar los miles de euros.

Figura 2 - Aeronaves no tripuladas de uso recreativo

b) Aeronaves no tripuladas de uso comercial

Este tipo de aeronaves no tripuladas están pensadas para usos comerciales. Normalmente incluyen una carga útil (*payload*) correspondiente a la función prevista; por ejemplo, una cámara, utilizada para la fotografía profesional, la inspección de instalaciones industriales o el levantamiento topográfico. Tal como sucede con los dispositivos recreativos, el hecho de que una aeronave no tripulada se clasifique como comercial no depende de la capacidad del dispositivo sino de la finalidad prevista por el usuario; por ello, algunos drones muy baratos podrían englobarse en esta categoría. En todo caso, en diferentes países del mundo se fabrican drones diseñados para uso comercial y no recreativo, y la mayoría de los modelos cuestan varios miles de euros.

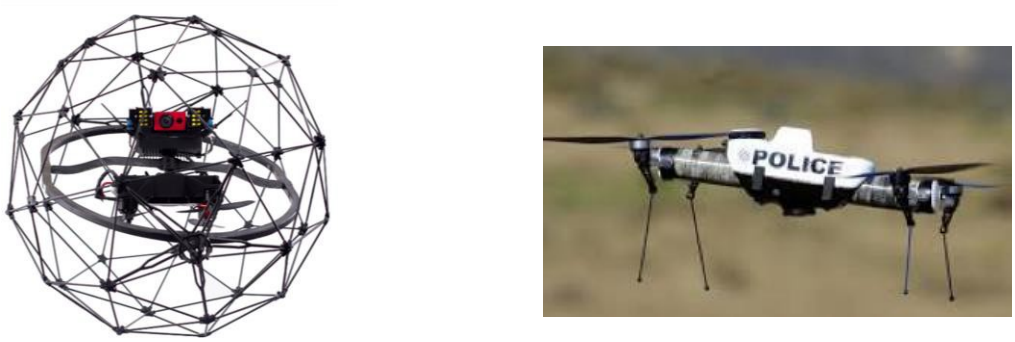


Figura 3 - Aeronaves no tripuladas de uso comercial

c) Aeronaves no tripuladas hechas a medida

Estas aeronaves no tripuladas no se adquieren como un dispositivo completo, sino que el propio usuario se encarga de ensamblar piezas compradas por separado. Aunque los modelos a la venta de aeronaves no tripuladas de uso recreativo o comercial ofrecen mayores funcionalidades e incorporan aplicaciones para su control, el mercado de los drones hechos a medida ha crecido rápidamente en años recientes porque hay una mayor disponibilidad de piezas sueltas, lo que reduce los costes.

En este caso, el usuario tiene la posibilidad de adquirir piezas procedentes de diferentes orígenes y construir y configurar la aeronave de acuerdo con su presupuesto o sus necesidades. El único límite es la capacidad de los componentes disponibles y los conocimientos y habilidades del constructor del dron, dos aspectos que están mejorando exponencialmente.

Por muy poco dinero se puede construir a medida una aeronave no tripulada para uso infantil, pero también es posible combinar piezas que se venden por miles de euros para diseñar y construir aeronaves tan sofisticadas como las de los principales fabricantes comerciales.

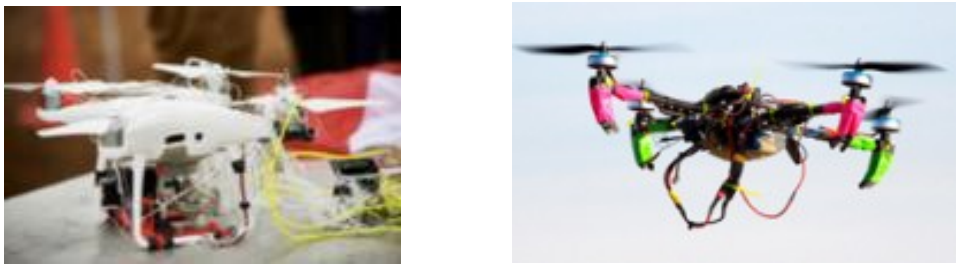


Figura 4 - Aeronaves no tripuladas hechas a medida

2.4 Componentes de las aeronaves no tripuladas

Cualquier aeronave no tripulada está formada por los siguientes dos tipos de componentes.

2.4.1 Componentes físicos

Los componentes físicos de una aeronave no tripulada son los que conforman el chasis y los mecanismos de vuelo, y pueden dividirse en las categorías indicadas a continuación. Estos componentes no están siempre presentes en su totalidad, pero todos ellos pueden formar parte de una aeronave no tripulada.

i) Chasis del dron

Fuselaje de la aeronave no tripulada, donde se alojan el resto de componentes.

ii) Controlador de vuelo

Se utiliza para controlar el vuelo del dron. Estabiliza la aeronave y, por lo general, recibe instrucciones de navegación transmitidas desde un dispositivo de radiocontrol. En los sistemas más sofisticados, este componente puede controlarse a distancia en tiempo real o bien programarse con antelación para un vuelo autónomo.

iii) Motores, rotores/hélices/alas y reguladores de velocidad

La combinación de estos componentes asegura la elevación y propulsión de la aeronave no tripulada. Pueden emplearse distintos diseños para conseguir, por ejemplo, mayor velocidad o una mayor duración de los vuelos.

iv) Carcasa protectora

La carcasa envuelve los motores y las hélices (las piezas más vulnerables de cualquier aeronave no tripulada) para evitar colisiones y pérdidas de control, con el consiguiente daño para el vehículo.

v) Receptor GPS

No es un componente imprescindible en toda aeronave no tripulada, pero suele estar presente en los modelos más avanzados. Permite manejar la posición de la aeronave con precisión, asegurar el regreso a la base y establecer rutas de vuelo autónomo.

vi) Receptor de radio (RX)

Se utiliza para recibir las señales enviadas desde el transmisor situado en tierra

vii) Transmisor (TX)

Transmite a la aeronave no tripulada las instrucciones del operador situado en tierra.

viii) Luces LED

Algunas aeronaves no tripuladas están equipadas con luces LED (normalmente, verdes y rojas) que ayudan al piloto a orientar el dron o permiten que este sea identificado por otros usuarios del espacio aéreo.

2.4.2 Software

Todos los drones incluyen algún tipo de aplicación o programa informático que controla el vehículo mientras está en funcionamiento. Aunque las aeronaves no tripuladas de uso comercial o recreativo suelen incluir aplicaciones ya configuradas, en el caso de los drones hechos a medida es el constructor el encargado de integrar algún componente electrónico que asegure el funcionamiento del vehículo. Actualmente, en Internet pueden descargarse multitud de aplicaciones de código abierto, fácilmente modificables, para el control de vuelo o el manejo desde tierra.

Independientemente del sistema o la configuración de *software* utilizada, las soluciones electrónicas empleadas en las aeronaves no tripuladas se enmarcan en dos categorías básicas:

a) Software de gestión de vuelos

Estos programas se instalan tanto en el controlador de vuelo incorporado a la aeronave no tripulada como en la estación de control remoto utilizada en el otro extremo. Cuando la aeronave está en funcionamiento, controlan el despegue, el vuelo y el aterrizaje. Normalmente, este tipo de *software* asegura las siguientes funciones: vuelo de la aeronave no tripulada, estabilización del vehículo e ingreso manual de instrucciones de navegación.

b) Software para el control desde tierra

Estos programas se utilizan para controlar trayectorias de navegación predeterminadas y planear horarios de vuelo, y es recomendable reservarlos para preparar el vuelo mientras la aeronave no tripulada se encuentra fuera de servicio. Además, los programas de control desde tierra permiten que otros usuarios que no sean el piloto hagan un seguimiento en directo del vuelo de la aeronave desde un ordenador, una tableta o un teléfono inteligente.

Aunque los drones hechos a medida pueden incluir componentes tecnológicos sofisticados, por lo general representan un riesgo mayor porque al construirlos se suele dar más importancia a los costes que a las cuestiones de seguridad. Por este motivo, a veces no cuentan con opciones básicas que sí están integradas en la mayoría de los dispositivos comerciales, como la detección de áreas restringidas, la evitación de obstáculos o el funcionamiento a prueba de averías. Estas opciones reducen el peligro que un fallo del sistema o un error del piloto podrían comportar para personas o bienes.

Aunque la anterior clasificación puede resultar difusa en ocasiones —por ejemplo, cuando un usuario particular utiliza con fines recreativos un dron de gama alta diseñado para fines comerciales—, a la hora de describir aeronaves no tripuladas y considerar sus capacidades es conveniente utilizar las categorías propuestas anteriormente.

2.5 Carga útil de los drones

Las aeronaves no tripuladas de uso comercial pueden llevar cargas útiles muy diferentes y de precios muy variados. Por lo general, se enmarcan en alguna de las categorías siguientes:

a) Cámaras de fotografía y vídeo

Si bien la mayoría de las aeronaves no tripuladas ya incorporan algún tipo de cámara en su diseño, los modelos comerciales incluyen dispositivos de obtención de imágenes más sofisticados y con más opciones: visión en primera persona (FPV por sus siglas en inglés), vídeo 4K, *zoom* óptico para aplicaciones de inspección, etiquetado GPS para cartografía en 3-D, etc. Los sistemas más avanzados pueden incorporar un *gimbal* o cardán que contrarresta los movimientos del vuelo para mantener la cámara nivelada y obtener imágenes de vídeo más estables y de calidad superior.

b) Cámaras térmicas, de infrarrojos y de visión infrarroja frontal

Los sistemas térmicos de obtención de imágenes, reservados tradicionalmente a los modelos de gama alta, pueden emplearse con diferentes fines, como la realización de censos agrícolas, controles sanitarios o vigilancia de seguridad o policial, además de en tareas de inspección y rescate. La tecnología de infrarrojos puede facilitar el manejo de las aeronaves no tripuladas en condiciones de poca luz o vuelos nocturnos. Los sistemas de visión infrarroja frontal (FLIR por sus siglas en inglés) utilizan una cámara térmica que percibe variaciones mínimas de la radiación infrarroja. Este tipo de cámaras son capaces de captar diferentes rangos de frecuencia, lo que les permite detectar la presencia de compuestos químicos mediante un radar óptico (sistema LIDAR) para determinar la posición exacta de los objetos y la distancia entre ellos.

c) Transporte y entrega

La utilización de aeronaves no tripuladas para efectuar entregas de manera rápida y eficaz ha ido en alza en los últimos años, siendo el ejemplo más notable el servicio Prime Air de Amazon.

Aunque sus posibilidades de aplicación comercial están sobre todo en las entregas de venta al por menor, la tecnología del transporte controlado por radio podría ser útil también en otros sectores, como el de la sanidad, donde las aeronaves no tripuladas podrían emplearse, por ejemplo, para enviar desfibriladores a demanda. Ahora bien, el uso de aeronaves no tripuladas como medio de transporte brinda también oportunidades a los delincuentes, ya que constituye una solución innovadora para distribuir drogas, armas y otros artículos. Esta táctica se ha detectado en cárceles de todo el mundo.

d) Armas

Las aeronaves no tripuladas tienen la capacidad de distribuir armas o llevar a cabo ataques desde la propia aeronave. Se están utilizando con este fin en el ámbito militar, donde los drones son apreciados como sistema de ataque porque aseguran una mayor precisión y un menor riesgo de muerte en comparación con otros métodos que requieren la intervención humana directa. Desde el punto de vista operativo, una aeronave no tripulada de rango medio puede transportar hasta 3 kg durante 16 minutos a una velocidad de 16 metros por segundo, lo cual la hace equivalente a un vehículo autónomo capaz de desplegar 3 kg de explosivos en un radio de 16 kilómetros.

e) Comunicaciones

El uso de dispositivos de comunicaciones como carga útil de drones aún no es habitual, pero podría popularizarse con la introducción de las redes 5G. Las aeronaves no tripuladas cargadas con un dispositivo de comunicaciones podrían emplearse para controlar, interrumpir o emular comunicaciones inalámbricas privadas legítimas; por ejemplo, manipulando las ondas emitidas por torres de telefonía o puntos de acceso inalámbrico.

2.6 Entender los drones y otras fuentes de material probatorio

A diferencia de muchos aparatos electrónicos, un dron requiere otros dispositivos de apoyo para funcionar. Entre ellos figuran los siguientes:

a) Control remoto

Estos dispositivos se emplean para controlar el dron a distancia.

Figura 5 - Dispositivos de control remoto de drones

b) Tabletas y teléfonos móviles

Estos dispositivos se utilizan para visualizar las imágenes fotográficas o de vídeo obtenidas por la cámara del dron.

Figura 6 - Dispositivos de control remoto conectados a móviles o tabletas

c) Gafas de visión en primera persona

Las gafas de visión en primera persona (FPV por sus siglas en inglés) se utilizan para visualizar las imágenes obtenidas por el dron y en algunos casos permiten controlar el dron con movimientos de la cabeza u otros gestos.

Figura 7 - Gafas de visión en primera persona

d) Tarjetas de memoria

En ocasiones se emplean tarjetas extraíbles para almacenar las imágenes y los vídeos obtenidos desde el dron. Estas tarjetas pueden contener también detalles de trayectorias o geoetiquetas de las fotografías, basadas en los metadatos EXIF (formato de fichero intercambiable) de las imágenes.

Figura 8 - Tarjeta de memoria micro-SD

e) Almacenamiento en la nube

Los drones pueden incluir alguna opción que emplee el dispositivo móvil asociado para cargar imágenes fotográficas o de vídeo en plataformas de almacenamiento en la nube, como iCloud o Google Photos.

Figura 9 - Iconos de almacenamiento en la nube

f) Indicios biológicos

Como cualquier otro elemento de prueba físico, los drones y sus dispositivos asociados pueden contener indicios biológicos; por ejemplo, huellas dactilares, ADN, etcétera.

Figura 10 - Huella dactilar

Aunque por lo general la principal fuente de evidencias será el propio dron, es fundamental disponer de las demás fuentes secundarias, como el control remoto, la tableta, el teléfono móvil o las tarjetas de memoria, para formarse una visión lo más amplia posible sobre los hechos y la información policial disponible.

Al intervenir ante un incidente relacionado con drones, es importante recopilar la máxima información sobre todos los hechos asociados, identificando a los principales testigos y determinando los lugares afectados y las condiciones del entorno. Algunos de esos datos pueden parecer superfluos inicialmente, pero podrían convertirse en elementos cruciales en el transcurso de la investigación.

2.7 Datos de los drones

Como sucede con cualquier otro dispositivo electrónico, la utilización de una aeronave no tripulada genera inevitablemente una huella digital, ya que se crean y almacenan datos, bien en el marco del servicio ofrecido o como resultado de la utilización del vehículo (p. ej., registros de uso).

2.7.1 Tipos de datos

En la investigación de un incidente con drones son útiles diferentes tipos de datos. Entre ellos figuran los siguientes:

a) Contenido audiovisual

En muchos casos, la primera y principal fuente de datos procedentes de una aeronave no tripulada de uso recreativo o comercial serán las imágenes digitales y de vídeo. Actualmente, la mayoría de los operadores de drones tratan de registrar imágenes con la máxima calidad para lograr ventajas competitivas, lo cual puede generar un volumen de datos significativo y requerir gran capacidad de almacenamiento, aunque el período de obtención de imágenes sea corto.

b) Horarios de vuelo

Cuando el sistema de control de la aeronave no tripulada permite programar vuelos con antelación para ofrecer mayor autonomía al usuario, esta información se conserva para que posteriormente sea posible verificar la actividad pasada, repetir horarios programados o modificar horarios previstos. A menudo, los datos generados durante el vuelo se descargan más tarde en un sistema o plataforma de control, donde se conservan para que el usuario pueda revisar la utilización del dron, cotejar mapas o hacer un seguimiento de la actividad de la aeronave.

c) Otros contenidos

Otros tipos de carga útil registran datos específicos para presentarlos al usuario o a alguna entidad. Aunque este tipo de información puede ser muy variada, un ejemplo son las aeronaves no tripuladas utilizadas con fines de transporte, donde puede ser necesario revisar horarios y ubicaciones de entrega o resultados de misiones programadas.

d) Registros de uso automatizados

Al igual que muchos otros dispositivos electrónicos, las aeronaves no tripuladas generan y almacenan automáticamente la información digital necesaria para asegurar su funcionamiento previsto. Si bien esta clase de información no está pensada para ser revisada por el usuario y suele estar oculta, hay que tener en cuenta que algunas aeronaves no tripuladas generan sistemáticamente registros de uso con detalles de misiones, fechas y horas de operaciones, puntos de referencia de navegación, etc. Por lo general, estos datos consisten en posiciones de GPS, velocidades de motor, altitudes y pautas de dirección.

2.7.2 Acceso a diferentes soportes de información

Muchos dispositivos electrónicos válidos como evidencia almacenan en soportes muy diversos grandes cantidades de datos relativos a su utilización que pueden ser útiles a los investigadores. Según nuestros estudios, en el caso de las aeronaves no tripuladas, el acceso a este tipo de datos varía mucho en función del fabricante y el modelo, desde las escasas posibilidades de recuperación de información de los drones recreativos de gama baja hasta los complejos volúmenes de datos que almacenan los modelos de uso comercial y los drones construidos a medida.

Además del volumen de información, su ubicación puede variar considerablemente según el modelo de dron y la configuración elegida por el usuario. Por ello, para estimar las posibilidades de obtención de información a partir de una aeronave no tripulada, es fundamental aplicar el principio de la tipificación digital (*digital profiling*), considerando los conocimientos técnicos y la competencia informática del usuario, las especificaciones del dron analizado, su carga útil y la configuración de control de vuelo utilizada. Sobre la base de esos factores, puede efectuarse evaluarse la mejor manera de obtener los datos digitales pertinentes para la investigación.

Los datos útiles para las investigaciones pueden encontrase en ubicaciones como las siguientes:

a) Almacenamiento a bordo

Para conservar la información, algunas aeronaves no tripuladas incorporan un microprocesador o dispositivo de memoria en el fuselaje o en el controlador de vuelo. Dependiendo de las especificaciones y los puertos de conexión de la aeronave, la extracción de datos puede ser muy sencilla, de tipo *plug and play* (enchufar y usar), o requerir técnicas forenses destructivas como el *chip-off* (retirada del microprocesador).

b) Almacenamiento extraíble

Dado el gran tamaño de los ficheros asociados, la mayoría de las aeronaves no tripuladas pensadas para obtener imágenes y vídeos en alta resolución llevan integrado algún dispositivo de almacenamiento extraíble. La solución más habitual son las tarjetas micro-SD de 2 TB, que ofrecen gran capacidad de almacenamiento en muy poco espacio. Esta posibilidad también debe tenerse en cuenta, ya que, aunque este tipo de soportes externos se utilizan principalmente para almacenar ficheros multimedia, pueden contener otros tipos de datos.

c) Dispositivos y aplicaciones móviles

Muchas aeronaves no tripuladas ofrecen la opción de controlar total o parcialmente el vehículo o su carga útil mediante una aplicación nativa instalada en un dispositivo inteligente conectado en red. Tampoco debe pasarse por alto esta posible fuente de datos asociados. Al llevar a cabo una tipificación digital, hay que tener en cuenta el contenido de los dispositivos móviles del sospechoso y la posibilidad de obtener información útil para la investigación a partir de aplicaciones relacionadas con aeronaves no tripuladas.

d) Dispositivos de control remoto

La mayoría de los drones se manejan con un dispositivo de control remoto específico. Dichos sistemas de control pueden contener datos residuales útiles para identificar otros dispositivos emparejados con el dron, como el móvil o la tableta empleados para visualizar las imágenes grabadas.

e) Estaciones terrestres

Los sistemas de control que establecen un enlace con tierra para asegurar la planificación de rutas, la visión FPV o el seguimiento visual también pueden registrar datos o imágenes en directo en un dispositivo de almacenamiento local, como el disco duro de un ordenador. Por lo general, el programa de visualización integrado en la fuente permite acceder a este tipo de datos, y cuando esto no es posible, se puede recurrir al *triage* (muestreo) o a otras técnicas típicas del análisis forense digital.

f) Plataformas de almacenamiento en la nube

La difusión comercial del almacenamiento en la nube hace necesario tener en cuenta este tipo de plataformas como otra posible fuente de información asociada a una aeronave no tripulada. El propio usuario puede optar por cargar datos en la nube para reducir la necesidad de almacenamiento local, o la aeronave no tripulada puede incluir alguna opción que envíe datos automáticamente a una plataforma.

g) Paquetes de datos de red

Es habitual que los sistemas de control utilicen las redes inalámbricas para comunicarse con el dron, lo cual genera paquetes de datos que también son útiles como evidencia forense. Posiblemente, la introducción del 5G facilitará el control de drones a través de redes de telefonía móvil, lo que generará otra fuente muy valiosa de material probatorio.

2.7.3 Consideraciones para la investigación de datos de drones

Debido a las características de la información digital y al hecho de que los drones requieren otros dispositivos secundarios para funcionar, en la investigación de un incidente con drones conviene tener en cuenta los siguientes elementos:

Consideraciones para la investigación de datos de drones
• Los datos pueden estar dispersos entre diferentes ubicaciones físicas, incluso en diferentes países.
• Es posible transferir datos de una zona jurisdiccional a otra en fracciones de segundo.
• Este tipo de datos son extremadamente inestables: es posible alterarlos, sobrescribirlos, dañarlos o destruirlos simplemente pulsando una tecla.
• Estos datos pueden ser copiados sin degradación.
• A diferencia de lo que sucede en otras disciplinas forenses, las evidencias digitales tienen una vida corta. Podría suceder que el dispositivo electrónico ya no pueda conectarse o utilizarse al cabo de tan solo cinco años.

Cuadro 1 - Consideraciones para la investigación de datos de drones

Por todos estos motivos, las evidencias obtenidas a partir de drones deben manejarse con las debidas precauciones.

En el módulo avanzado sobre análisis forense de drones que está desarrollando INTERPOL se incluirá información adicional sobre la identificación, adquisición, análisis e interpretación de datos procedentes de aeronaves no tripuladas.

2.8 Delitos que pueden cometerse con la ayuda de drones

La popularización de las aeronaves no tripuladas y el riesgo que plantean para el sector público y privado cuando se incumplen los reglamentos establecidos y los procedimientos de concesión de licencias han llevado a la aparición de nuevas infracciones en los últimos años. La consideración de esas infracciones varía según la jurisdicción, por lo que los equipos de primera intervención deben tener una idea clara de las leyes aplicables en cada lugar.

Entre las infracciones relacionadas con drones, cabe citar las siguientes:

- No mantener contacto visual directo con la aeronave no tripulada.
- Sobrepasar la altitud autorizada en cada lugar (p. ej., en el Reino Unido y en los Estados Unidos, la máxima altitud permitida para un dron es de 121 metros).
- Ocupar espacio aéreo sin autorización.
- Acceder a un espacio aéreo restringido: aeropuertos, bases militares o infraestructuras críticas (p. ej., centrales nucleares).
- Volar cuando las condiciones ambientales no sean seguras (p. ej., mal tiempo).
- Utilización no autorizada de una aeronave no tripulada con fines de vigilancia (p. ej., para espiar o invadir la intimidad).
- Poner en peligro aeronaves civiles (p. ej., volando a demasiada altura, en el recinto de un aeropuerto en un espacio aéreo restringido).

Además, en algunas jurisdicciones es ilegal sobrevolar aglomeraciones de personas, transportar una carga útil para la que el dron no haya sido diseñado o liberar cargamento desde un dron.

Para responder a un delito relacionado con drones hay que tener en cuenta los siguientes aspectos:

- Hechos que se deben establecer.
- Lugar de la infracción.
- Fecha y hora de la infracción.
- ¿Se ha localizado y detenido al piloto y a los demás sospechosos?
- ¿Cuál era el propósito de la utilización del dron?
- ¿El dron se dirigía hacia algún objetivo? En ese caso, ¿hacia qué o quién se dirigía y cuál era la intención del operador?

Aunque la principal amenaza sea el dron, otro aspecto importante que debe considerarse es la posibilidad de detener al piloto y demás sospechosos.

2.9 Visión general de la normativa sobre drones

Si bien la normativa aplicable a los drones puede diferir considerablemente según el lugar, hay ciertos elementos que se repiten. La mayoría de los países se basan en un enfoque de seguridad y requieren que el vehículo, el piloto o ambos estén registrados. Incluso en aquellos países donde existe normativa específica sobre drones, las leyes están en constante modificación. Puede haber normas aplicables al propio dron y otras aplicables al espacio aéreo donde está permitido utilizar estos vehículos. En la mayoría de los casos, se encarga de regular estos aspectos la autoridad de aviación civil. En algunos lugares está totalmente prohibido el uso de drones, por lo que pueden ser confiscados en la aduana o conllevar una multa o una pena de cárcel si se utilizan dentro del territorio del país.

En agosto de 2019, estaba prohibido utilizar drones en los siguientes países: Argelia, Barbados, Brunéi, Côte d'Ivoire, Cuba, Irán, Iraq, Kirguistán, Madagascar, Marruecos, Nicaragua, Senegal y Siria.

Los funcionarios de los organismos encargados de la aplicación de la ley deben conocer la legislación vigente en sus respectivos países. En la mayoría de los casos, la autoridad de aviación civil es la responsable de elaborar la legislación relativa a los drones.

La ausencia de legislación específica no implica necesariamente que se pueda pilotar un dron en cualquier momento o lugar. De hecho, por lo general, cuando no existe normativa es porque las autoridades se oponen totalmente a la utilización de drones en el país, en especial por parte de turistas. Lo mismo sucede con el tratamiento aduanero. A veces, cuando no existe legislación específica, es el propio funcionario de aduanas el que determina si un dron será confiscado o no. En los países donde sí está regulada la utilización de aeronaves no tripuladas, la formulación y aplicación de la normativa correspondiente suele estar a cargo de la autoridad nacional de aviación civil.

En caso de no conocer la legislación nacional aplicable, es recomendable consultar a la autoridad de aviación civil para conocer las normas vigentes. Actualmente, las plataformas Google Play (para Android) o Apple Store (para iPhone) ofrecen aplicaciones móviles que permiten conocer la normativa aplicable en cada país y consultar mapas de las zonas en las que sí está permitida la utilización de drones.

2.10 Pautas para el manejo seguro de drones

En los países donde no exista legislación específica, es conveniente aplicar como mínimo las pautas indicadas a continuación (extraídas de las recomendaciones para el manejo de drones de la Administración Federal de Aviación de los Estados Unidos y del código sobre drones de la Autoridad de Aviación Civil del Reino Unido):

Pautas para el manejo seguro de drones	
1	Mantener el dron dentro del alcance visual.
2	Volar cuando se den las condiciones climáticas especificadas por el fabricante del dron.
3	Mantener el dron como mínimo a 45 metros de distancia de personas y bienes. No volar directamente sobre personas.
4	Mantenerse a una distancia de 152 metros de aglomeraciones de personas o edificios.
5	Mantener una altura máxima de 60 metros (Singapur) o 121 metros (Estados Unidos).
6	Volar en horas de luz diurna o crepúsculo civil.
7	Respetar una velocidad máxima de 160 km/h.
8	No interferir en la trayectoria de aeronaves tripuladas.
9	No manejar el dron desde un vehículo en marcha.
10	No volar en un radio de 5 km en torno a un aeropuerto, una infraestructura civil crítica (p. ej., una central nuclear o eléctrica), una base militar o una zona restringida, según se designe en cada país.

Cuadro 2 - Pautas para el manejo seguro de drones

En caso de duda, consúltese a la autoridad de aviación civil del país correspondiente.

En las figuras 11 y 12 se presentan otras recomendaciones para el manejo seguro de aeronaves no tripuladas.

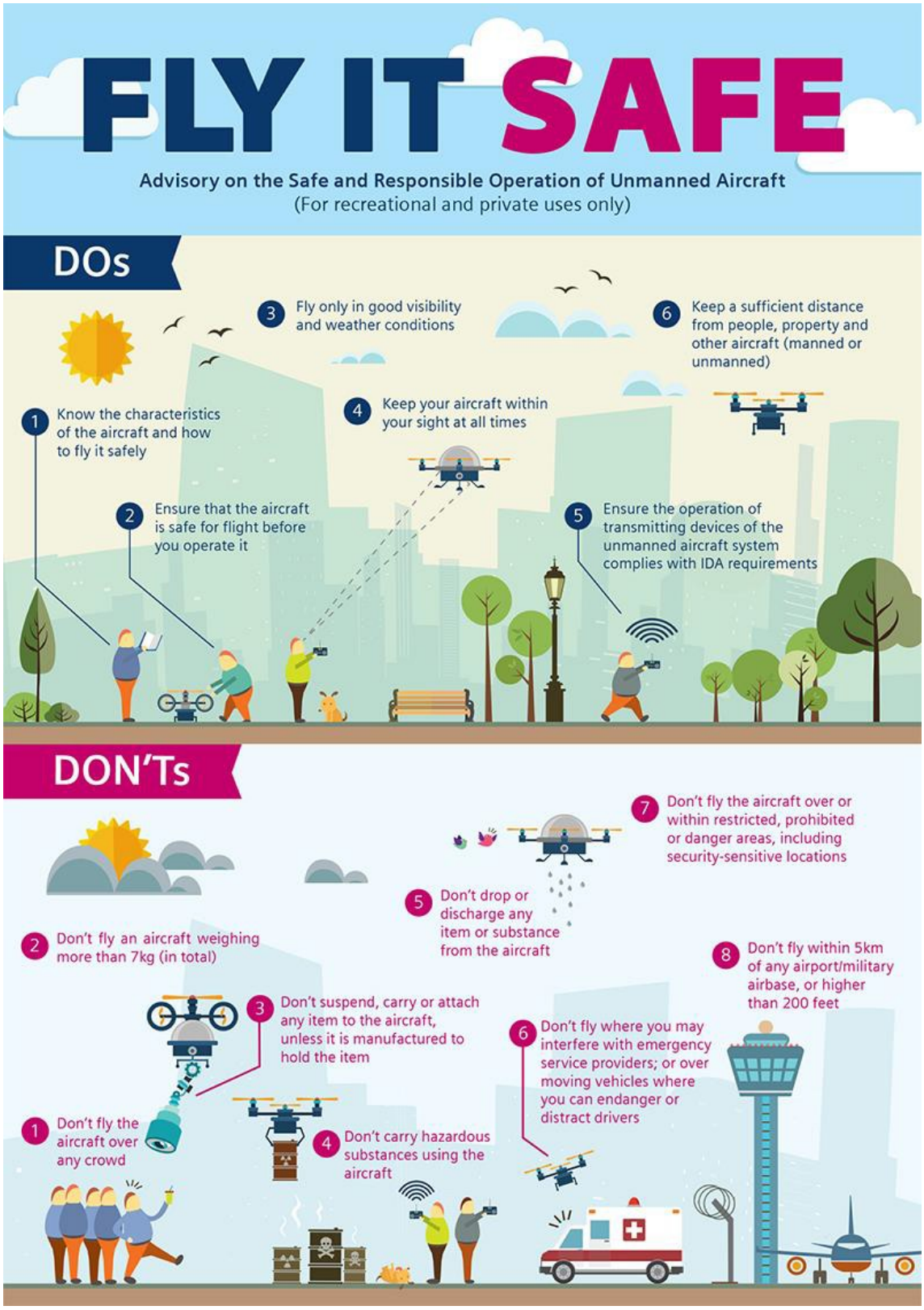


Figura 11 - Infografía de la Autoridad de Aviación de Singapur sobre la utilización segura de drones

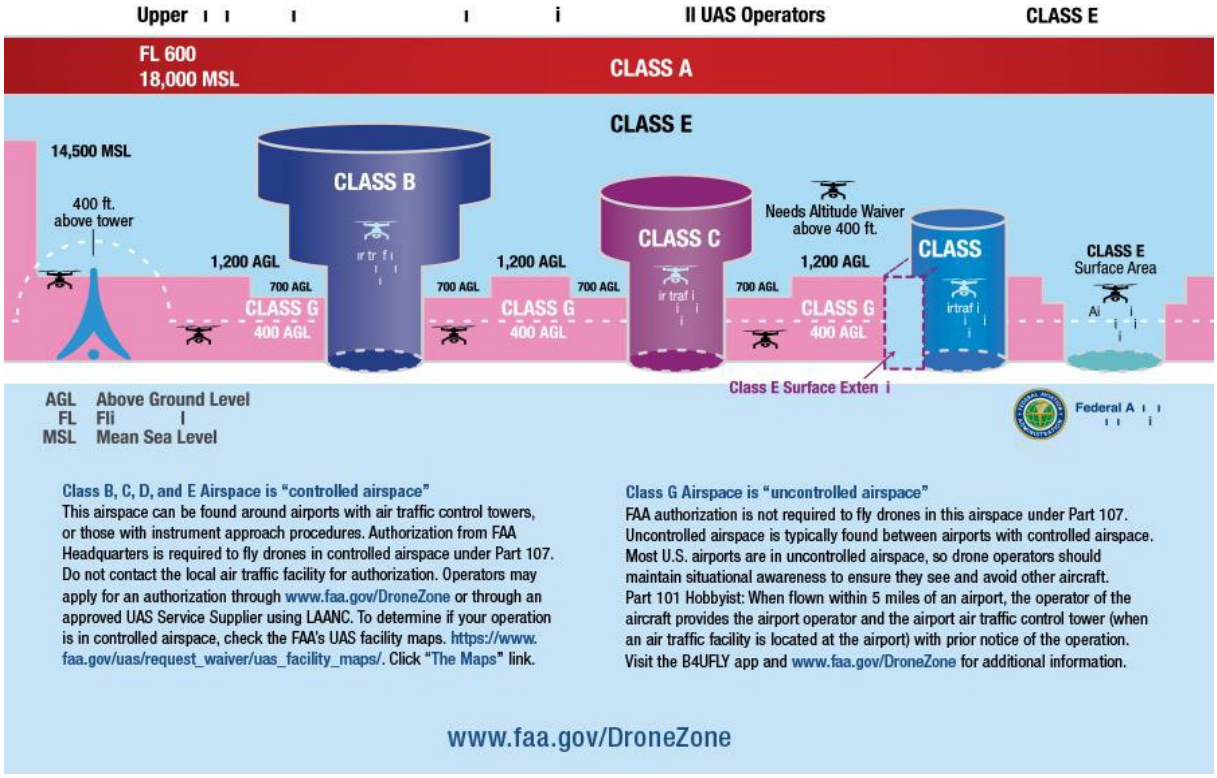


Figura 12 - Infografía de la Autoridad Federal de Aviación de EE.UU. sobre el uso de aeronaves no tripuladas

2.11 Ejemplos de drones y dispositivos asociados

Figura 13 - Control remoto integrado

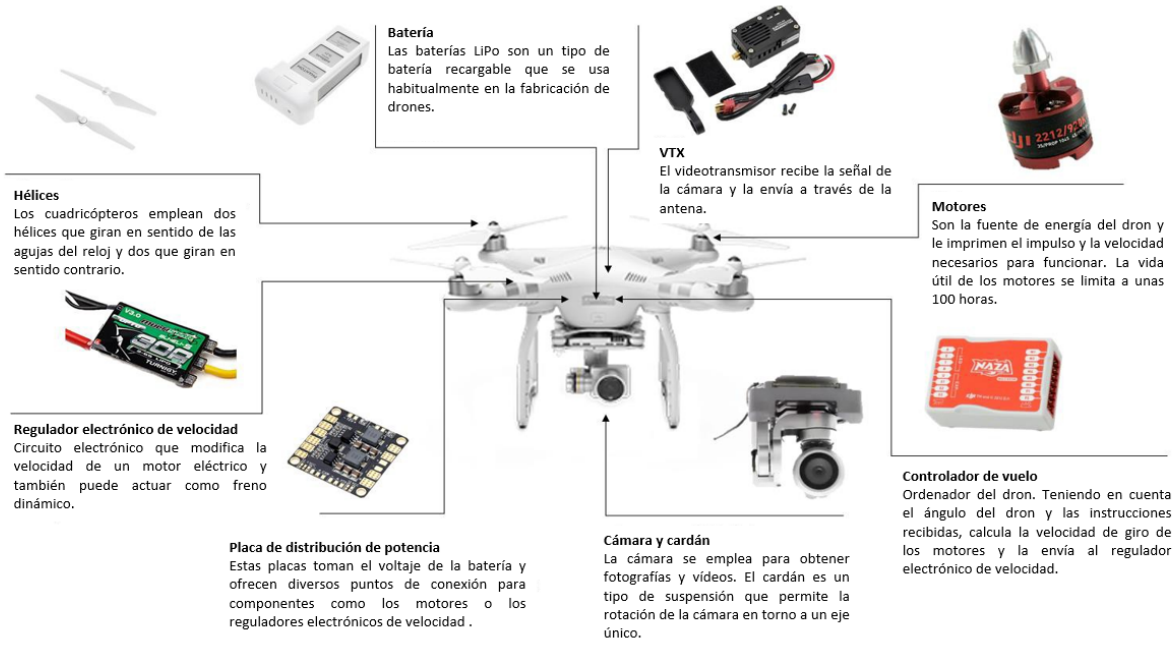


Figura 14 - Componentes de un cuadricóptero

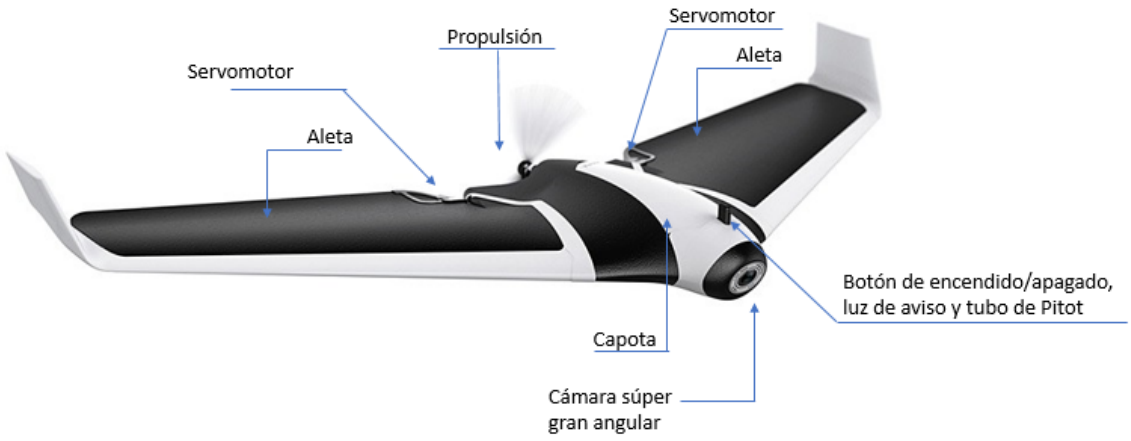


Figura 15 - Componentes de un dron de ala fija

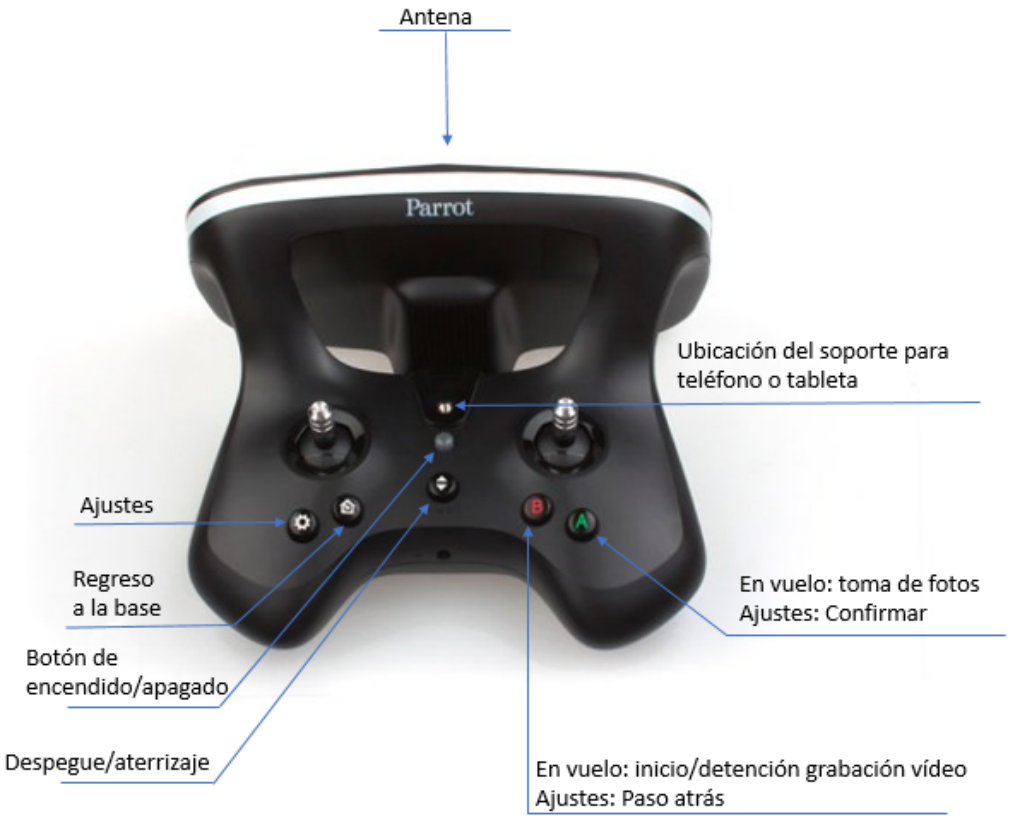


Figura 16 - Control remoto sin pantalla

Figura 17 - Control remoto con conexión a teléfono móvil

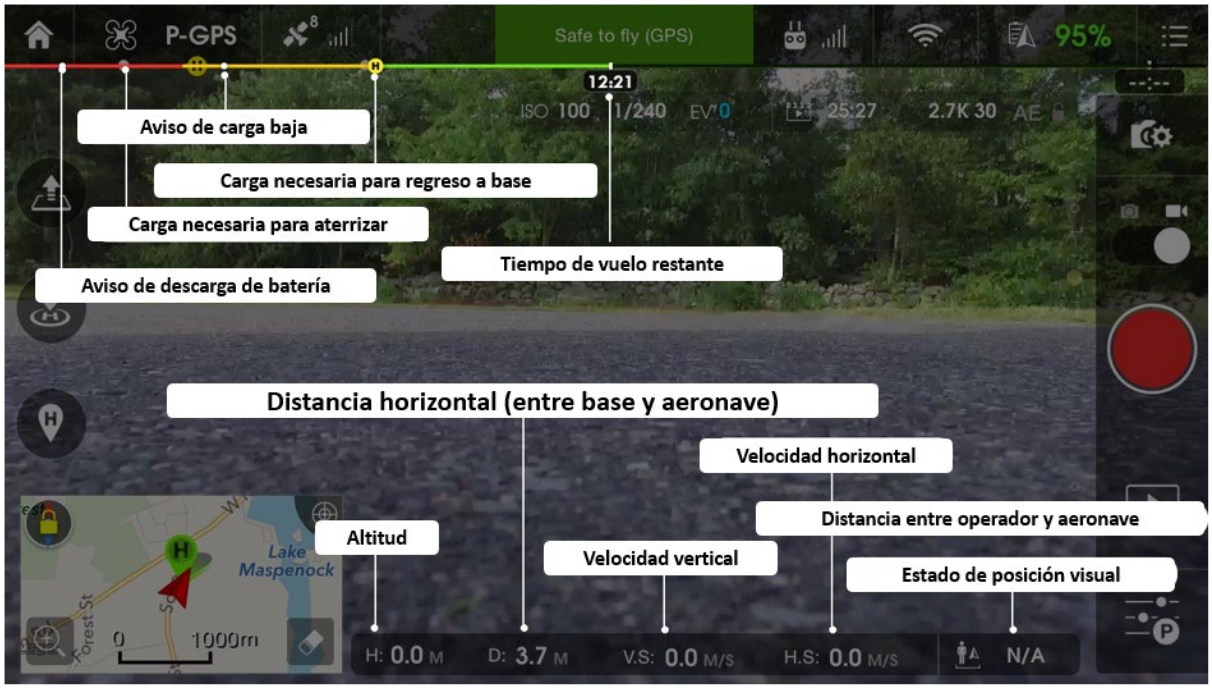


Figura 18 - Aplicación móvil para el control de drones

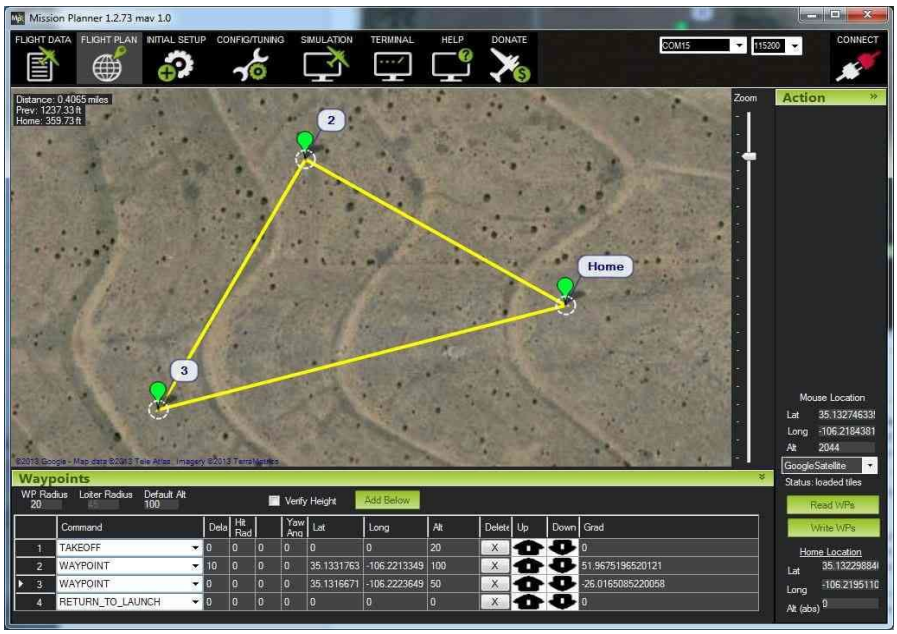


Figura 19 - Planificador de misiones

3. PAUTAS PARA LOS EQUIPOS DE PRIMERA INTERVENCIÓN

Las pautas presentadas a continuación tienen como objetivo maximizar las posibilidades de investigación y garantizar la seguridad de los investigadores y del público general.

Secuencia de actuaciones en el lugar de los hechos	
1	Primera intervención y recepción de información
2	Procedimientos de seguridad
3	Atención de emergencia
4	Cierre del lugar de los hechos y control de las personas presentes
5	Delimitación del perímetro: determinar, establecer, proteger y precintar
6	Traspaso de responsabilidades en el lugar de los hechos y transmisión de información a los encargados de la investigación
7	Documentación de acciones y observaciones
8	Establecimiento de un puesto de mando (sistema de control de incidentes) y envío de notificaciones
9	Manejo de los testigos
10	Evaluación del lugar de los hechos
11	Exploración del lugar de los hechos y documentación inicial
12	Toma de notas y elaboración de registros

Cuadro 3 - Secuencia de actuaciones en el lugar de los hechos

3.1 Primera intervención y recepción de información

Principio: Uno de los principales objetivos de la actuación en el lugar de los hechos es evitar al máximo la contaminación o la alteración de las pruebas físicas. Por ello, la primera intervención en caso de incidente debe ser rápida y metódica.

Pauta: A su llegada, el equipo de primera intervención debe evaluar la situación y tratar el espacio como el escenario de un delito. Es preciso acceder al lugar de los hechos con rapidez pero con las debidas precauciones y estar atentos a las personas y los vehículos presentes, los sucesos que tengan lugar, las condiciones ambientales y las posibles evidencias.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Anotar o registrar la información recibida (lugar, fecha, hora, tipo de llamada, partes implicadas).
b	Estar atentos a las personas y vehículos que abandonen el lugar de los hechos.
c	Aproximarse con precaución, observar con atención toda la zona y anotar otros posibles lugares de los hechos.
d	Estar atentos a las personas y vehículos de las inmediaciones que puedan tener relación con el delito. Efectuar las primeras observaciones (vista, oído y olfato) para evaluar el lugar de los hechos y garantizar la seguridad de los agentes antes de proceder.
e	Mantenerse vigilantes. Dar por supuesto que se está cometiendo un delito a no ser que se determine lo contrario.
f	Tratar el espacio como el lugar de comisión de un delito, a no ser que tras su examen se determine lo contrario.
g	Indicar a otros servicios cómo acceder con seguridad a la zona.

Cuadro 4 - Procedimiento para la primera intervención y la recepción de información

Resumen: Es fundamental que los equipos de primera intervención se mantengan vigilantes en el momento de aproximarse al lugar de los hechos, acceder al mismo o salir de él. Deberán velar por la seguridad de los agentes del orden y los ciudadanos presentes en el lugar de los hechos o en sus inmediaciones.

3.2 Procedimientos de seguridad

Principio: La prioridad básica del equipo de primera intervención debe ser la seguridad y la integridad física de los agentes y demás personas presentes en el lugar de los hechos o en sus proximidades.

Pauta: A su llegada al lugar del incidente, los equipos de primera intervención deben identificar y controlar todas las situaciones o personas que puedan suponer un peligro.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Cerciorarse de que no existen amenazas inmediatas para los demás agentes; observar la zona en busca de imágenes, sonidos u olores que puedan indicar un peligro para las personas (p. ej., materiales peligrosos, artefactos explosivos improvisados o riesgos biológicos). Si se detecta alguna carga consistente en armas biológicas o materiales que comporten un riesgo químico o radiológico, es necesario avisar al servicio u organismo pertinente antes de acceder al lugar de los hechos.
b	Aproximarse al lugar de los hechos tratando de minimizar el peligro para los agentes, a la vez que se asegura la máxima seguridad de víctimas, testigos y demás personas presentes en la zona.
c	Observar el lugar de los hechos para localizar posibles individuos peligrosos y controlar la situación.
d	Notificar al personal supervisor y solicitar asistencia o respaldo.

Cuadro 5 - Procedimiento de seguridad

Resumen: El control de los riesgos físicos garantiza la seguridad de los agentes y demás personas presentes.

3.3 Atención de emergencia

Principio: Una vez controladas las situaciones o personas peligrosas, la siguiente tarea del equipo de primera intervención es asegurarse de que los heridos reciban atención médica, minimizando en lo posible la contaminación del lugar de los hechos.

Pauta: Los equipos de primera intervención deben cerciorase de que se presta la atención médica necesaria, procurando minimizar la contaminación del lugar de los hechos.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Determinar si las víctimas precisan cuidados vitales y proporcionar atención médica inmediata.
b	Avisar al personal médico.
c	Indicar al personal médico cómo llegar hasta las víctimas evitando en lo posible contaminar o alterar el lugar de los hechos.
d	Señalar las posibles evidencias físicas a la atención del personal médico y explicarles cómo minimizar el contacto con las mismas (p. ej., pedir que conserven las prendas de vestir y otros efectos de las víctimas, sin recortar las partes con agujeros de bala, rasgaduras de arma blanca, etc.). Documentar los desplazamientos de personas u objetos por parte del personal médico.
e	Dar indicaciones al personal médico para que no limpie el espacio y no retire o altere objetos presentes en el lugar de los hechos.
f	Si el personal médico ha accedido al lugar antes que el equipo de primera intervención, anotar sus nombres y números de teléfono, así como los datos del centro médico al que se traslade a las víctimas.
g	Si la vida de las víctimas corre peligro, intentar obtener una declaración *in articulo mortis*. En algunos casos puede ser necesario obtener huellas dactilares e impresiones del calzado del personal médico para descartar las muestras no válidas.
h	Documentar todos los comentarios y declaraciones de víctimas, sospechosos o testigos presentes en la escena.
i	Si las víctimas o los sospechosos son trasladados a un centro médico, enviar a un agente para que documente sus comentarios y conserve las evidencias. (Si no hay ningún agente disponible, permanecer en el lugar de los hechos y solicitar al personal médico que conserve las evidencias y documente los comentarios de las personas atendidas.)
j	Preservar las evidencias, como la carga útil de la aeronave. Si se confiscan, aplicar los procedimientos previstos para la cadena de custodia.

Cuadro 6 - Procedimiento de la atención de emergencia

Resumen: Dar indicaciones al personal médico encargado de atender y retirar a los heridos disminuye el riesgo de contaminación o pérdida del material probatorio.

3.4 Cierre del lugar de los hechos y control de las personas presentes

Principio: Localizar, controlar y hacer salir a las personas presentes en el lugar de los hechos y limitar los accesos es una de las principales funciones del equipo de primera intervención.

Pauta: El equipo de primera intervención debe localizar a las personas presentes en el lugar de los hechos y controlar sus movimientos.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Controlar los movimientos, la ubicación y las actividades de todas las personas presentes en el lugar de los hechos para evitar que alteren o destruyan evidencias físicas y preservar la seguridad del lugar.
b	Localizar a todas las personas presentes en el lugar de los hechos: • Sospechosos: Confinarlos y aislarlos. • Testigos: Confinarlos y aislarlos. • Espectadores: Determinar si son testigos de los hechos. En ese caso, aplicar las consideraciones anteriores; si no son testigos, hacerlos salir del lugar de los hechos. • Víctimas, familiares y amigos: Controlarlos, mostrando compasión. • Agentes de policía, profesionales sanitarios y demás personal: Identificarlos.
c	Excluir del lugar de los hechos a todo el personal no esencial (p. ej., agentes de policía que no se ocupen del caso, políticos, periodistas...).

Cuadro 7 - Procedimiento para cerrar el lugar y controlar a las personas presentes

Resumen: Controlar los movimientos de los individuos presentes en el lugar de los hechos y limitar los accesos al mismo es esencial para garantizar la integridad del escenario, salvaguardar las evidencias y minimizar la posible contaminación.

3.5 Traspaso de responsabilidades en el lugar de los hechos y transmisión de información a los encargados de la investigación

Principio: Celebrar una sesión informativa con los responsables de la investigación es útil para asegurar el control del lugar de los hechos, determinar responsabilidades ulteriores y gestionar los recursos.

Pauta: Los equipos de primera intervención deben proporcionar información detallada sobre el lugar de los hechos a los investigadores presentes.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Celebrar una sesión informativa con los investigadores que asumirán el control del lugar de los hechos.
b	Ayudar a controlar el lugar de los hechos.
c	Transferir la responsabilidad de documentar las entradas y salidas.
d	Permanecer en el lugar de los hechos hasta ser relevados.

Cuadro 8 - Procedimiento para transferir responsabilidades en el lugar de los hechos e informar a los encargados de la investigación

Resumen: La sesión informativa brinda la oportunidad de trasladar la información inicial sobre el lugar de los hechos al siguiente equipo que asumirá el control y se ocupará de la investigación posterior.

3.6 Documentación de acciones y observaciones

Principio: Es necesario documentar lo antes posible todas las actividades y observaciones realizadas en el lugar de los hechos y preservar esta información.

Pauta: Los equipos de primera intervención deben registrar de manera permanente la información documentada.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Documentar las observaciones realizadas en el lugar de los hechos, entre ellas la ubicación de personas y objetos, así como el aspecto y las condiciones del lugar en el momento de acceder al mismo.
b	Documentar las condiciones del lugar a la llegada (luces apagadas o encendidas, persianas subidas o bajadas, puertas y ventanas abiertas o cerradas, olores, presencia de hielo o líquidos, muebles, clima, temperatura, efectos personales...).
c	Documentar la información aportada por testigos, víctimas y sospechosos y todas sus declaraciones o comentarios.
d	Documentar las acciones de testigos, víctimas, sospechosos y otras personas presentes.

Cuadro 9 - Procedimiento para documentar las acciones y observaciones

Resumen: Los equipos de primera intervención deben registrar de manera clara y concisa sus observaciones y actuaciones. Esta labor de documentación es esencial para las investigaciones y actuaciones judiciales posteriores.

3.7 Establecimiento de un puesto de mando (sistema de control de incidentes) y envío de notificaciones

Principio: Es recomendable establecer un espacio para coordinar las tareas de investigación y celebrar reuniones con los medios y con el equipo. El puesto de mando es el punto central desde el que se coordina la investigación y se evalúan los recursos disponibles. Además, el establecimiento de un puesto de mando permite mantener informados a otros profesionales que participen en la investigación e incorporarlos a las actividades a medida que sea necesario.

Política: Se debe determinar un lugar para coordinar las actividades de investigación y celebrar reuniones con la prensa y los miembros del equipo.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Establecer un puesto de mando provisional en un lugar donde la prensa pueda tomar fotografías sin poner en peligro la seguridad del lugar ni de las evidencias.
b	Facilitar a los investigadores y a otros servicios implicados (p. ej., Homicidios) la información recopilada en el lugar de los hechos. Este es el momento en que se deben proporcionar datos detallados sobre el lugar de los hechos.
c	Facilitar al servicio de comunicaciones los números de teléfono disponibles en el puesto de mando.
d	Solicitar al servicio de comunicaciones que avise a las unidades pertinentes y envíe teletipos regionales y nacionales si algún sospechoso huye del lugar de los hechos. En los avisos debe figurar una descripción del sospechoso y los vehículos involucrados, así como los detalles de contacto para comunicar su posible localización.
e	Informar al oficial supervisor cuando sea necesario.
f	Celebrar una sesión informativa final entre los equipos de primera intervención y los responsables de la investigación.
g	Asignar tareas y registrar cada asignación en el formulario pertinente.
h	Usar este mismo formulario para registrar las nuevas asignaciones realizadas durante la investigación. Facilitar la lista de asignaciones a otros miembros del personal que trabajen en el caso. Asignar el registro de evidencias y el registro de entradas y salidas (la misma persona se encargará de llevar un calendario de actividades).

i	Determinar la situación y ubicación de víctimas y sospechosos.
J	Determinar la situación de los comunicados sobre víctimas y sospechosos. Asegurarse de que se difunden avisos sobre los sospechosos huidos. Establecer un calendario de reuniones del el equipo de investigación (con la participación de todos los agentes uniformados) para determinar categorías, actualizar las asignaciones y comunicar la información básica.

Cuadro 10 - Procedimiento para establecer un puesto de mando (sistema de control de incidentes) y enviar notificaciones

Resumen: El establecimiento de un puesto de mando es fundamental para que los equipos de primera intervención, el servicio de comunicaciones y otras unidades puedan comunicar la información esencial a los encargados de la investigación.

3.8 Manejo de los testigos

Principio: Interrogar oportunamente a los testigos es esencial para la resolución de cualquier delito.

Pauta: Se debe determinar quiénes fueron testigos del delito, interrogarlos si es posible en el mismo lugar de los hechos y tratarlos de conformidad con la normativa correspondiente.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Interrogar por separado a cada testigo en el propio lugar de los hechos, para obtener información que pueda ser útil a la investigación.
b	Trasladar a los testigos a la comisaría sin que estén en contacto con los sospechosos o con los demás testigos.
c	Obtener declaraciones orales o escritas de cada uno de los testigos en comisaría.
d	Cuando sea posible, el oficial supervisor deberá: • Determinar la situación y ubicación de cada una de las víctimas y los sospechosos. • Determinar la situación de los comunicados difundidos sobre víctimas y sospechosos. Asegurar la pronta difusión de los avisos sobre sospechosos dados a la fuga.

Cuadro 11 - Procedimiento para el manejo de testigos

Resumen: Para obtener información sobre un delito, es importante interrogar oportunamente y por separado a cada uno de los testigos.

3.9 Evaluación del lugar de los hechos

Principio: La evaluación del lugar de los hechos permite determinar el tipo de incidente que se ha producido y el grado de investigación necesario.

Pauta: Se deben determinar responsabilidades concretas, difundir la información preliminar y elaborar un plan de investigación de conformidad con el reglamento de la sección a cargo y con la legislación local, regional y estatal.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Establecer contacto con los agentes que actuaron inicialmente para conocer sus actividades y observaciones.
b	Evaluar aspectos de seguridad que puedan afectar al personal que acceda al lugar de los hechos (patógenos, riesgos químicos...).
c	Evaluar la necesidad de efectuar registros o embargos preventivos y determinar si se requiere una autorización u orden.
d	Establecer rutas de entrada y salida del lugar de los hechos para el personal autorizado.
e	Evaluar el perímetro inicial del lugar de los hechos.
f	Determinar el número de lugares de los hechos y su extensión y establecer prioridades.
g	Establecer una zona protegida en las proximidades del lugar de los hechos para las consultas y la organización del equipo.
h	Si hay más de un lugar de los hechos, establecer y mantener una comunicación permanente entre el personal que se encuentre en cada uno de ellos.
i	Establecer una zona protegida para el almacenamiento temporal de las evidencias, respetando la cadena de custodia.
j	Determinar y solicitar cuando sea necesario recursos adicionales (servicios y personal especializado, abogados y fiscales, suministro de materiales).
k	Asegurar de manera permanente la integridad del lugar de los hechos (documentar las entradas y salidas del personal autorizado e impedir que nadie acceda sin autorización).
l	Localizar y aislar a los testigos del incidente (requerir documentos de identidad válidos).
m	Sondear la zona circundante y documentar los resultados. Obtener documentación y fotografías iniciales del lugar de los hechos, los heridos y los vehículos.

Cuadro 12 - Procedimiento para la evaluación del lugar de los hechos

Resumen: La evaluación del lugar de los hechos permite elaborar un plan y coordinar las tareas de determinación, recopilación y preservación de evidencias físicas y la identificación de los testigos. Además, facilita el intercambio de información entre el personal policial y el establecimiento de estrategias de investigación.

3.10 Delimitación del perímetro: determinar, establecer, proteger y precintar

Principio: Delimitar y controlar el perímetro del lugar de los hechos es otra medida útil para mantenerlo protegido. El número de lugares de los hechos y su extensión dependen de la ubicación del incidente y del tipo de delito cometido. Por lo general, inicialmente se delimita un perímetro más amplio con la idea de reducir su extensión posteriormente si es necesario, ya que resulta más difícil ampliarlo una vez establecido.

Pauta: Los equipos de primera intervención deben realizar una evaluación inicial de la extensión del lugar o lugares afectados y a continuación delimitar y proteger su perímetro.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Establecer el perímetro del lugar de los hechos, partiendo de un punto central para incluir: • El lugar de comisión del delito • Posibles vías de entrada y salida de sospechosos y testigos • Lugares de donde puedan haberse retirado víctimas o evidencias (observar la presencia de trazas y huellas).
b	Cerrar el lugar de los hechos. Colocar barreras físicas (cuerdas, conos, precintos policiales, vehículos, objetos u agentes) o aprovechar las existentes (puertas, verjas, muros...).
c	Documentar las entradas y salidas de todas las personas que accedan o salgan del lugar de los hechos una vez se haya establecido el perímetro.
d	Proteger el lugar de los hechos. Controlar la afluencia de personas y animales para asegurar la integridad del escenario.
e	Establecer medidas para preservar las evidencias, evitando que se deterioren o se extravíen (protegerlas de la lluvia, el viento y el sol, evitar que se enciendan aspersores o que se alteren pisadas o roderas...).
f	Documentar la ubicación inicial de las víctimas y los objetos que se hayan cambiado de lugar.
g	Considerar si se precisa un registro o un embargo preventivo y obtener la orden o autorización necesarias.

Cuadro 13 - Procedimiento para la delimitación del perímetro: determinar, establecer, proteger y precintar.

Nota: NO se permitirá que nadie fume, hable por teléfono, vaya al baño, coma, beba, retire objetos del lugar de los hechos (ni siquiera armas, a no ser que sea imprescindible para proteger a las personas presentes), modifique el termostato, abra puertas o ventanas (deben mantenerse las condiciones iniciales), toque nada que no sea esencial (se documentarán todos los movimientos de objetos) o reponga elementos dentro del perímetro establecido. Los sospechosos no podrán ir al baño ni modificar su aspecto (no pueden peinarse ni lavarse las manos).

Resumen: Delimitar el perímetro es fundamental para asegurar la integridad del material probatorio.

3.11 Exploración del lugar de los hechos y documentación inicial

Principio: La exploración a pie permite hacerse una idea general del lugar de los hechos, determinar posibles riesgos para su integridad y asegurar la protección de las evidencias físicas. Deben tomarse notas escritas y fotografías para documentar la situación. Este tipo de exploración solo se llevará a cabo cuando no pueda alterar el material probatorio. En ocasiones es necesario proceder previamente a la documentación y recopilación de evidencias.

Pauta: Los agentes encargados de actuar en el lugar de los hechos deben efectuar una exploración inicial, recorriendo a pie el lugar afectado.

Procedimiento:

Cometidos del equipo de primera intervención	
a	Utilizar las vías de acceso establecidas para no contaminar el lugar de los hechos.
b	Tener en cuenta si se necesitan equipos de protección personal (PPE).
c	Elaborar la documentación preliminar (notas, bocetos...), basándose en la observación del lugar de los hechos.
d	Localizar y proteger evidencias frágiles o perecederas (considerando las condiciones climáticas y las características del entorno). Cerciorarse de que todas las evidencias que puedan verse afectadas quedan documentadas y fotografiadas lo antes posibles.
e	Durante la exploración inicial, tomar nota de todo lo que se observe, por ejemplo: • Elementos exteriores: farolas, carteles, bancos... • Entradas y salidas de los edificios circundantes y condiciones ambientales locales. • Lugar de la colisión: ¿se han producido daños en los edificios o en el terreno? • Luces de la calle: ¿encendidas o apagadas? ¿Qué luces están encendidas? • Condiciones climáticas: momento del día, temperatura local, velocidad del viento, etc. • Condiciones del terreno. • Condiciones de iluminación en el exterior. • Olores: humo de tabaco, gas, pólvora, perfume, etc. • Descripción del autor de la infracción (si está presente). • Descripción de otras personas presentes involucradas en la infracción. • Descripción del personal sanitario o de rescate presente en el lugar. • Armas observadas. • Muebles presentes, indicando su ubicación respecto de la víctima y en el conjunto del lugar. • Elaborar una teoría general sobre los hechos ocurridos.

Cuadro 14 - Procedimiento para la exploración del lugar de los hechos y la documentación inicial

Resumen: En la exploración inicial, es posible formarse una idea general del lugar de los hechos. Es el momento de identificar evidencias que puedan ser frágiles o vulnerables y determinar las primeras tareas de investigación, además de observar y documentar sistemáticamente las condiciones del lugar. La situación inicial debe registrarse mediante fotografías y anotaciones escritas que puedan conservarse de manera permanente.

3.12 Toma de notas y elaboración de registros

Principio: Las anotaciones y registros permiten documentar de manera permanente las actividades realizadas en el lugar de los hechos.

Pauta: Todo el personal asignado al lugar de los hechos debe anotar y registrar las actividades que realice.

Procedimiento: Se creará un registro de entradas y salidas para documentar a las personas que transiten por el lugar de los hechos durante la investigación. Asimismo, hay que hacer constar qué personas se encontraban en el lugar de los hechos antes del inicio de la investigación.

Cometidos del equipo de primera intervención	
a	El oficial supervisor asignará a un agente la tarea de crear un registro y mantenerlo actualizado. El responsable del registro se ocupará de cumplimentarlo en detalle y se asegurará de que en el lugar de los hechos no entre ninguna persona que no deba cumplir una función específica.
b	El registro se colocará en un lugar visible para que lo utilicen todas las personas que entren o salgan del lugar de los hechos. Se registrará la siguiente información: • Ubicación del lugar de los hechos • Nombres de los testigos • Nombres de las víctimas • Nombres de los arrestados • Nombres y hora de llegada de los componentes del equipo de primera intervención • Nombre y hora de llegada del oficial supervisor (si llegó antes de iniciar el registro, indicar una hora aproximada).
c	Para cada una de las personas presentes en el lugar de los hechos, deben registrarse los datos indicados a continuación, reservando espacio en el papel en caso de no disponer de un cuaderno o formulario en formato normalizado: • Fecha de llegada • Hora de llegada • Nombre • Número de identificación y unidad • Organización (si no pertenece al departamento encargado de la investigación) • Motivo de su presencia en el lugar de los hechos (indicado la hora de llegada y de salida de todos los funcionarios que accedan al lugar, incluido el forense, el juez instructor y otros profesionales) • Documentar las personas presentes en el lugar de los hechos y los motivos de su presencia, indicando la ubicación del lugar de los hechos, el código del incidente, el número de unidad, los números de acreditación, los nombres de los componentes del equipo de primera intervención, los nombres del responsable del registro y del oficial superior, los nombres de víctimas, sospechosos y testigos, etc.
	• Antes de dejar el registro de entradas y salidas a disposición de las personas que accedan al lugar, anotar los detalles logísticos (ubicación, fecha y hora y nombres de víctimas, testigos y sospechosos). • Antes de que alguien abandone el lugar de los hechos, cerciorarse de que se registra la hora de salida. • Si alguien abandona el lugar de los hechos sin comunicarlo al responsable del registro, se podrá anotar una hora aproximada, indicando que se trata de una estimación. • Guardar el registro en un lugar seguro, según la normativa del departamento correspondiente.

Cuadro 15 - Procedimiento para la toma de notas y elaboración del registro

Resumen: La toma de notas y la elaboración de un registro de entradas y salidas permite documentar qué personas están presentes en el lugar de los hechos para efectuar tareas judiciales o de investigación.

3.13 Embargo preventivo de drones

Para proceder al embargo preventivo de una aeronave no tripulada respetando las buenas prácticas establecidas es conveniente seguir las siguientes indicaciones.

Antes de proceder, hay que hacer indagaciones para averiguar la marca y el modelo de la aeronave no tripulada, conocer sus características y determinar las posibles ubicaciones de datos digitales útiles como material probatorio. Antes de entrar en contacto con el usuario de la aeronave, es recomendable buscar la manera de obtener pruebas sobre la infracción que se haya presenciado o que se nos haya encomendado investigar.

Tras esta investigación inicial, si se considera conveniente embargar preventivamente la aeronave no tripulada, deben seguirse las pautas indicadas a continuación.

Embargo preventivo de un dron	
1	Antes de establecer contacto físico con la aeronave no tripulada o el dispositivo de control, deben considerarse las posibilidades de obtener indicios biológicos (huellas dactilares o ADN). Al aprehender o empaquetar los dispositivos, hay que procurar no alterar este tipo de pruebas. Se aconseja embalar el objeto con precaución, utilizando guantes y prestando atención a los elementos más proclives a contener indicios biológicos (botones de encendido, cables, palancas de mandos, etc.).
2	Considerar la posibilidad de que en las proximidades haya otros dispositivos asociados a la aeronave o utilizados para su control. Por lo general, las antenas de las aeronaves no tripuladas tienen un alcance corto, por lo que es probable que los controles remotos estén dentro de un radio pequeño alrededor de la aeronave. Se intentará localizar al piloto.
3	Si es posible, la aproximación al dron se hará desde atrás, tapando las cámaras para evitar ser vistos por el piloto. Se determinará si el dron está o no en marcha (lo indicará la presencia de luces o sonidos), documentando el estado del vehículo y si se ha visto que alguien lo conectara desde la llegada del equipo al lugar de los hechos. Si el vehículo se encuentra en marcha, regístrese de inmediato cualquier tipo de información que aparezca en el visor. Evite que el dron despegue, mediante algún sistema que no altere posibles evidencias (por ejemplo, volcando la aeronave de un puntapié o cubriéndola con una chaqueta gruesa), hasta tener la seguridad de que es posible desconectarla sin corromper los datos.
4	Anote los principales elementos de identificación del dron, como la marca, el modelo y el número de serie. Estos datos pueden figurar en distintos puntos, dependiendo del modelo. Algunas aeronaves no tripuladas incluyen un código QR escaneable para facilitar su identificación.
5	Si la aeronave no tripulada lleva una batería extraíble, retírela. Si la batería no es extraíble, pulse el botón de apagado una vez para desconectar el dron y a continuación, dependiendo del modelo, púlselo de nuevo y manténgalo presionado durante dos segundos (sistemas DJI) o colóquelo en posición “off”. Registre la hora en que lleva a cabo cada uno de estos pasos. **ATENCIÓN:** No toque ni retire la batería si hay indicios de deterioro o pérdida de líquido, por el posible riesgo de heridas o explosión.
6	Registre cualquier modificación visible en la aeronave no tripulada o la presencia en el vehículo o en sus inmediaciones de cargas útiles o elementos que puedan cumplir funciones adicionales.

Embargo preventivo de un dron	
7	Embale por separado la aeronave no tripulada y el dispositivo de control remoto, utilizando bolsas o cajas de Faraday para evitar la contaminación aérea y el borrado de información a distancia. Empaquete los dispositivos secundarios en bolsas de Faraday independientes y registre el lugar en el que se encontraron. Los dispositivos asociados al dron pero hallados a cierta distancia del mismo deben tratarse y empaquetarse como muestras independientes.

Cuadro 16 - Procedimiento para el embargo preventivo de drones

Es fundamental procurar que no se pierdan datos al manejar el dron y los dispositivos asociados, a fin de maximizar las posibilidades de obtener información histórica útil para identificar al usuario. Como ayuda para los equipos de primera intervención, INTERPOL ha elaborado un formulario para documentar las características de la infracción y los hechos asociados (véase el Anexo C).

Al intervenir ante un incidente con drones, es fundamental tener en cuenta los aspectos indicados a continuación. La principal prioridad debe ser uno mismo, los demás servicios de emergencia y el público general.

Al llegar al lugar de los hechos es preciso efectuar una evaluación y cerciorarse de que nadie corre peligro de morir o resultar herido. Antes de aproximarse al dron hay que preguntarse los motivos de su presencia en el lugar:

- ¿El dron sufrió un accidente, o tomó tierra de forma deliberada?
- ¿Se puede identificar el objetivo hacia el que se dirigía?
- ¿Se puede localizar al piloto?
- ¿El dron llevaba una carga útil? En ese caso, ¿existen riesgos asociados, como artefactos explosivos improvisados o sustancias que supongan peligro biológico?

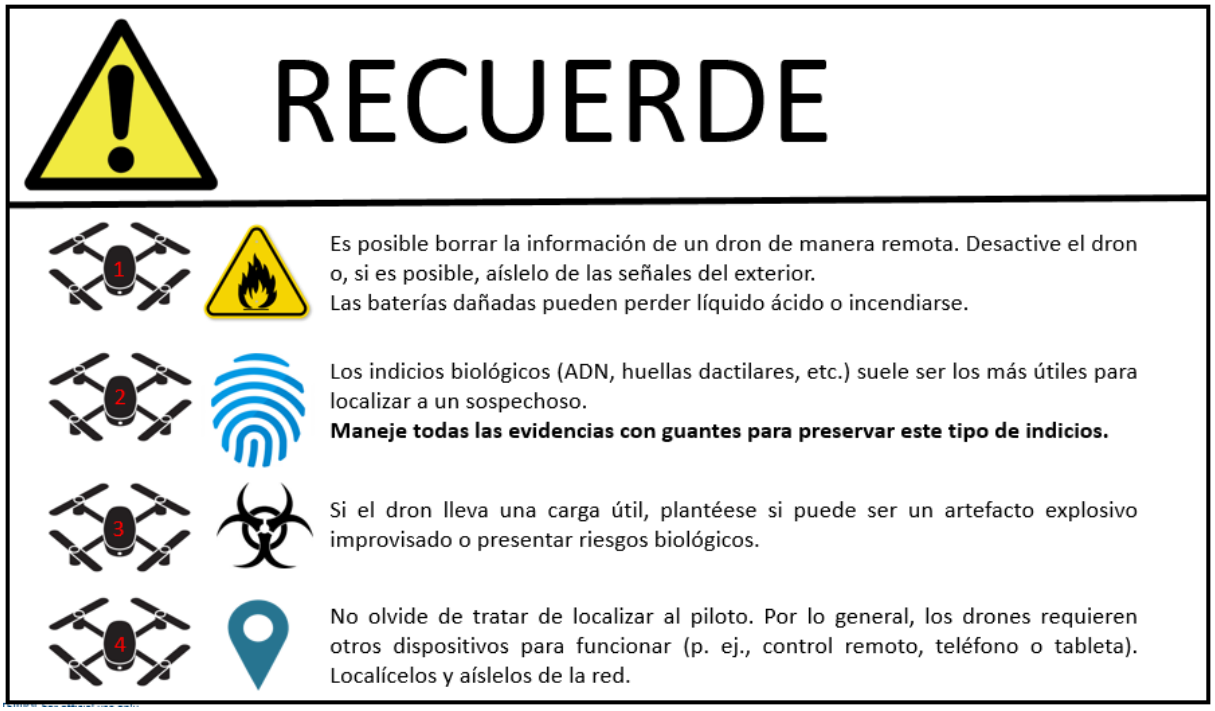


Figura 20 - Precauciones recomendables antes de aproximarse a un dron

Una vez se haya evaluado el lugar de los hechos y se tenga la seguridad de que no hay riesgos para uno mismo, los demás servicios de emergencia o el público general, puede plantearse la aproximación al dron.

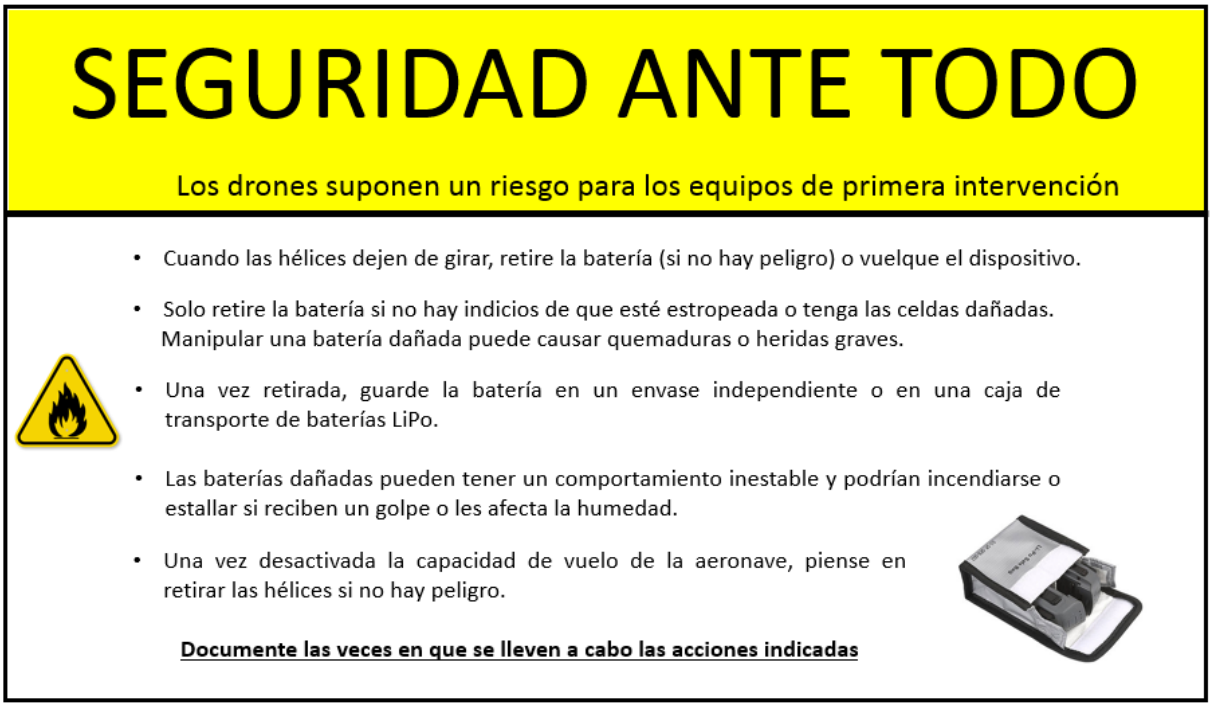
Para ello, es preferible aproximarse al dron desde atrás, de manera que el piloto no pueda vernos en las imágenes obtenidas por la cámara.

El peligro principal serán las hélices del dron, si todavía giran. Un dron aún en marcha podría elevarse repentinamente mientras nos acercamos. Para impedirlo, se puede volcar el dron de un puntapié o cubrirlo con una chaqueta gruesa o una manta.

En este caso, la prioridad debe ser proteger el lugar de los hechos y las posibles evidencias digitales que puedan ayudar a identificar a la los responsables del incidente.

Proceso de embargo preventivo de un dron
Hélices: si aún giran, eche una manta o una chaqueta gruesa sobre el dron para evitar que se eleve y pueda causar heridas. Si no giran, puede volcar el dron o bien retirar las hélices para evitar que el vehículo despegue.
Baterías: Los drones utilizan baterías LiPo (de polímeros de litio), que pueden volverse inestables si se dañan o se manejan incorrectamente. Si la batería está intacta y no hay señales de deterioro o fuga de líquidos, retírela si se considera que no hay peligro. En caso de duda, busque asesoramiento.

Cuadro 17 - Riesgos asociados a los drones



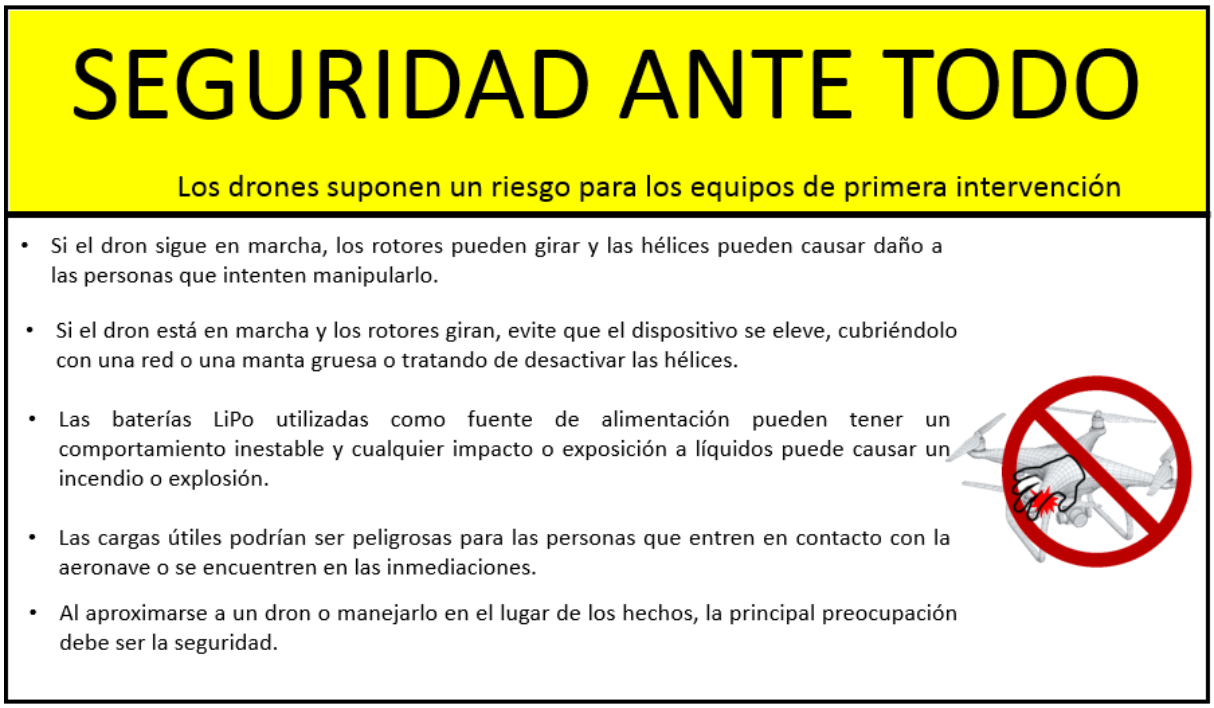


Figura 21 - Precauciones de seguridad en el manejo de drones

En el caso de los drones, el principal riesgo lo plantean las hélices y las baterías LiPo utilizadas como fuente de alimentación. Es necesario manejar estos elementos con precaución, a fin de que no supongan un peligro para usted mismo o para los demás.

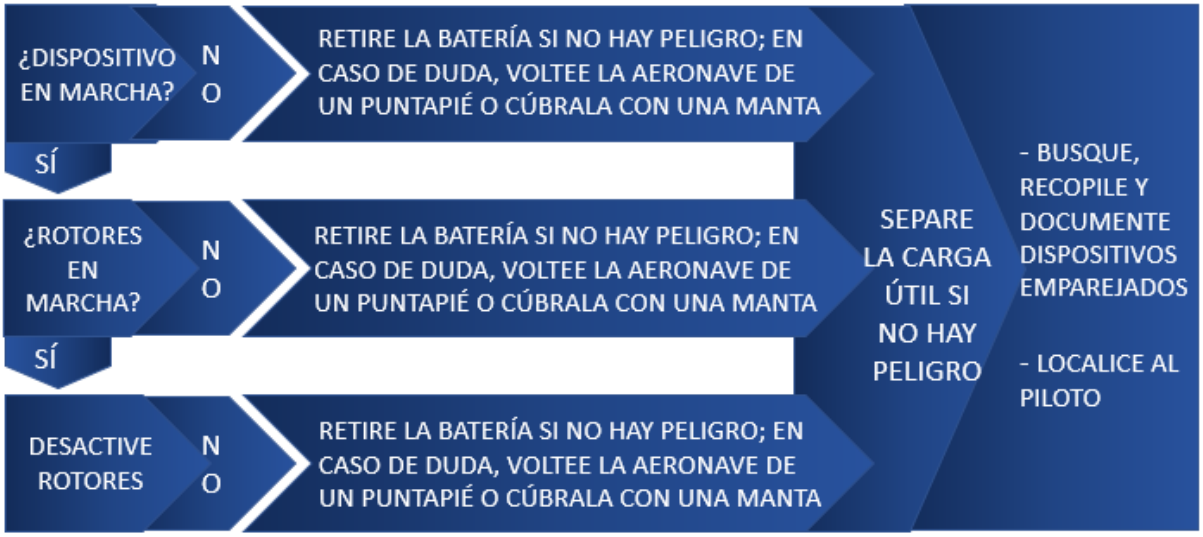


Figura 22 - Secuencia del manejo de drones

Figura 23 - Advertencia de seguridad de una batería LiPo

Figura 24 - Conservación de evidencias digitales

Figura 25 - Recopilación de evidencias digitales

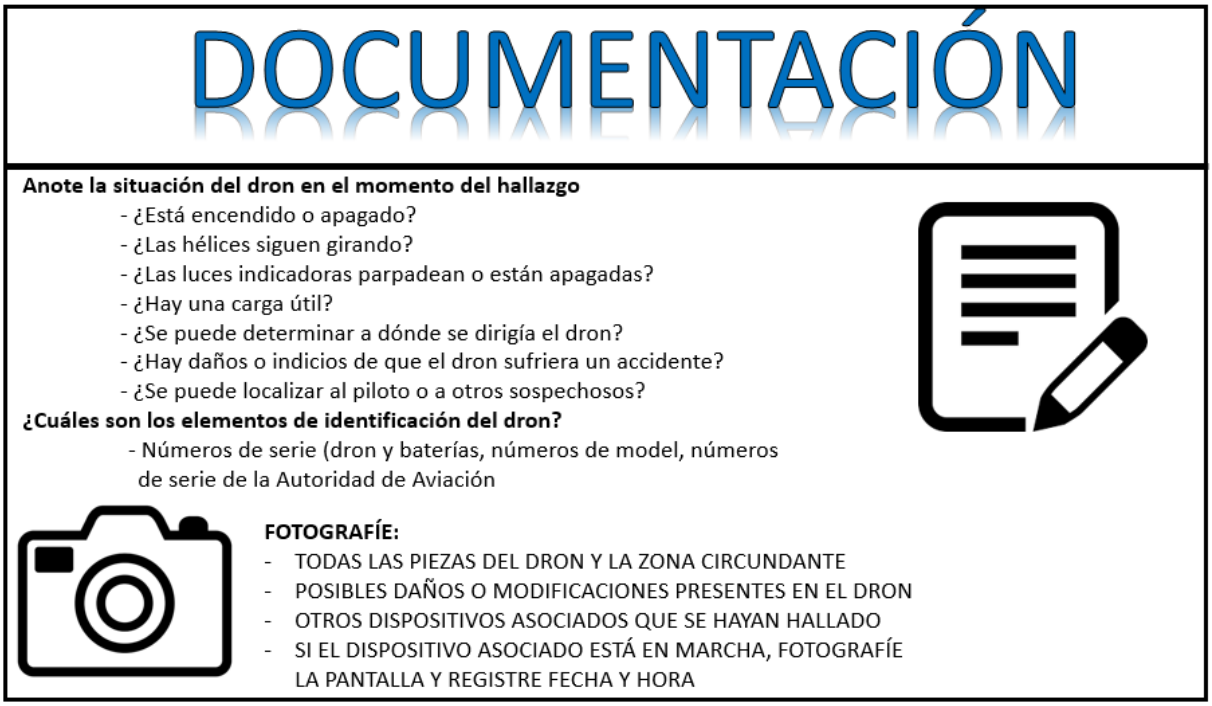


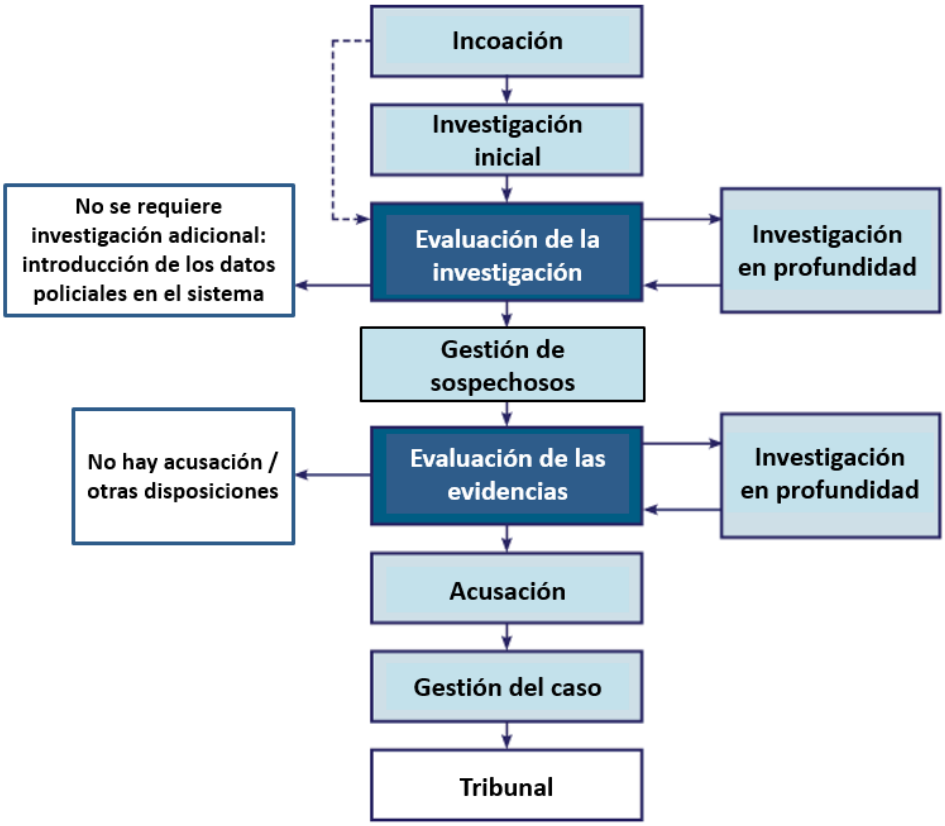
Figura 26 - Documentación en el lugar del incidente

3.14 Proceso de investigación

Una vez se haya analizado el lugar de los hechos y se hayan tomado las medidas necesarias, la actuación debe centrarse en la determinación de los autores, los motivos, el lugar y el momento de la infracción, a fin de localizar a los sospechosos de haber causado el incidente.

El tipo de materiales recopilados y la actuación de los investigadores puede variar en función del enfoque aplicado (reactivo o proactivo). En cualquier caso, los pasos son similares, como se muestra en el diagrama que figura más abajo.

Cada investigación es diferente y puede requerir una vía de actuación específica. Por ejemplo, a veces se conoce de antemano la identidad del infractor y la investigación puede centrarse desde el principio en el manejo de los sospechosos. En otros casos, puede ser que la identidad del infractor no llegue a conocerse nunca o solo se descubra tras una investigación en profundidad.



Las celdas azul claro representan actividades de la estrategia de investigación, las celdas azul oscuro representan los principales elementos de decisión, y las celdas blancas son los posibles resultados.

Figura 27 - Diagrama del proceso de investigación

La fase inicial de la investigación concluye cuando se han llevado a cabo las siguientes actuaciones:

- El equipo de primera intervención o los investigadores han tomado declaración a las víctimas y a los testigos disponibles.
- Se han atendido las necesidades inmediatas de las víctimas y los testigos.
- Se ha solicitado un examen del lugar de los hechos.
- Se han llevado a cabo los pasos de la actuación acelerada, según el material disponible.
- Se ha completado y revisado la documentación requerida por la normativa local.
- Se han presentado los datos policiales recopilados durante la investigación inicial.

Se indicará a los responsables de atender las llamadas, a los encargados de informar al público y a los oficiales de patrulla el tipo de información que deben obtener y las actuaciones que deben realizar. Al atender una denuncia, los agentes deberán registrar todos los detalles y trasladarlos a los responsables de la investigación. Los investigadores deben estar familiarizados con las técnicas de interrogatorio de víctimas y testigos, ya que de este modo podrán aprovechar oportunidades tempranas de obtener material probatorio, gracias a las declaraciones de las personas que denuncien la infracción.

La realización de registros detallados es útil para la investigación general, porque:

- Ayudan al investigador a llevar a cabo la evaluación de investigación.
- Ayudan a formarse una idea general de los lugares de comisión del delito.
- Permiten que los supervisores evalúen la calidad de la investigación.
- Facilitan el traspaso de responsabilidades en caso de que la investigación se asigne a otro equipo.

3.14.1 Investigación en profundidad

Cuando se considera que una infracción merece una investigación en profundidad, es necesario elaborar un plan que permita llegar a una conclusión adecuada. Dicho plan de investigación debe basarse en una evaluación rigurosa del material recopilado hasta el momento, teniendo en cuenta los aspectos indicados a continuación.

Aspectos que deben tenerse en cuenta para una investigación en profundidad
• Objetivos específicos de la investigación
• Estrategias que se emplearán para lograr esos objetivos
• Recursos necesarios: investigadores, especialistas en el examen del lugar de los hechos, especialistas en ciencia forense digital, analistas de datos policiales.

Cuadro 18 - Tres aspectos que deben tenerse en cuenta en una investigación en profundidad

Aunque el cuadro anterior no es exhaustivo, es útil como orientación. Las estrategias de investigación quedan fuera del alcance del presente marco y no se abordan en este documento.

Como se aprecia en el diagrama del proceso de investigación, hasta ahora se han descrito las etapas de la evaluación y la investigación inicial. En los siguientes apartados se tratará el proceso de evaluación de las evidencias y otras actuaciones útiles para la investigación de un incidente con drones. En el capítulo siguiente se detallan las estrategias y procedimientos del análisis forense digital aplicado a drones, como orientación para los equipos de primera intervención y el personal de laboratorios forenses digitales.

4. NOCIONES Y PRINCIPIOS DEL ANÁLISIS FORENSE DIGITAL

4.1 Descripción general

El análisis forense digital es una rama de la ciencia forense centrada en la identificación, adquisición, tratamiento, análisis y comunicación de datos almacenados en ordenadores, dispositivos electrónicos y otros tipos de soportes digitales. Su objetivo es obtener los datos contenidos en evidencias electrónicas, tratarlos para convertirlos en información útil y presentar los hallazgos ante los tribunales. En todas las fases del proceso deben utilizarse técnicas forenses reconocidas, a fin de que las conclusiones resulten admisibles ante un tribunal.

La aplicación del análisis forense digital a los drones y sus dispositivos asociados tiene como objetivo identificar trayectorias de vuelo, datos de usuario e imágenes y vídeos almacenados en los dispositivos, como ayuda para entender las características del dron y su utilización.

Por lo general, los incidentes que generan evidencias digitales son transfronterizos y pueden suceder en una fracción de segundo. Por ello, para obtener conclusiones a partir de evidencias electrónicas deben seguirse una serie de pautas normalizadas, que aseguren resultados admisibles no solo en una jurisdicción específica, sino también en el sistema internacional de justicia penal.

En los capítulos siguientes se describirán las buenas prácticas aplicables al tratamiento de aeronaves no tripuladas, válidas para toda la gama de drones recreativos, comerciales y hechos a medida y sus dispositivos de control. Cada capítulo está dedicado a un tema específico e incluye una descripción concisa de la normativa y las infracciones relacionadas con los drones. Además, se incluye un apartado dedicado a la preservación de la integridad de aeronaves no tripuladas, desde el primer punto de contacto inicial hasta el *triage* (muestreo) y el examen forense.

Es importante que los responsables de una investigación digital entiendan que, si bien los elementos de prueba requieren un tratamiento especial, los principios generales de la obtención y análisis de evidencias electrónicas son aplicables a todo el proceso de gestión del caso, desde el embargo preventivo hasta la comparecencia en el tribunal.

4.2 Principios del análisis de evidencias digitales

Figura 28 - Analista forense examinando un dron

Al manejar evidencias electrónicas, es necesario seguir los principios siguientes:

Principios del tratamiento de evidencias digitales
Principio 1
Las evidencias digitales deben obtenerse de manera acorde a las leyes.
Principio 2
El personal encargado de examinar evidencias digitales debe haber cursado un programa de formación específico sobre el manejo de materiales electrónicos.
Principio 3
Ninguna de las actuaciones realizadas con las evidencias digitales debe alterar los datos contenidos en ellas. Si es necesario acceder a los datos originales o modificar la configuración del sistema, deberá hacerlo personal competente y justificar sus actuaciones.
Principio 4
Al manejar evidencias electrónicas, se registrarán todas las actuaciones realizadas y se conservará el registro para su posible revisión. Si un tercero independiente repite las mismas actuaciones, debe poder llegar al mismo resultado.

Cuadro 19 - Principios básicos del tratamiento de evidencias digitales

Por consiguiente, es fundamental proceder al embargo preventivo del dron y los dispositivos asociados, para poder aprovechar al máximo las evidencias digitales disponibles.

4.3 Características de un laboratorio de análisis forense digital

Cuando un laboratorio de análisis forense digital recibe un dron y otros dispositivos asociados, debe disponer de un procedimiento para la gestión de este tipo de evidencias. Por lo general, se siguen los siete pasos descritos en la figura que aparece a continuación y detallados en los apartados siguientes. Antes de ocuparse del caso, el laboratorio debe cerciorarse de que la petición se ajusta a la legislación aplicable. El director o el profesional encargado del examen deberá contar con una orden o documento oficial que lo autorice a tratar evidencias digitales. El objetivo de la labor forense digital es emplear las evidencias electrónicas para demostrar o refutar una presunta infracción, por lo que la obtención de evidencias debe ser conforme a la normativa. Al finalizar la labor forense digital, las pruebas obtenidas deben ser admisibles y el informe forense debe poder ser aceptado en un tribunal.

Figura 29 - Proceso seguido en el laboratorio forense digital

4.3.1 Recepción de la solicitud

El trabajo del laboratorio forense digital comienza cuando una entidad presenta una solicitud oficial, que puede llegar en forma de carta, fax o correo electrónico. La solicitud debe contener la siguiente información: infracción investigada, hechos relacionados, detalles de las evidencias electrónicas, objetivo del caso y (si procede) orden de actuación.

A continuación, el director del laboratorio o el personal designado deben analizar la solicitud y determinar si el caso es factible, de acuerdo con los siguientes criterios:

a. El caso está dentro del alcance de la ciencia forense digital; esto es, las evidencias son de naturaleza electrónica y no de otro tipo (como ADN o huellas dactilares);
b. Se dispone de los métodos y herramientas necesarios;
c. Se dispone de personal para encargarse del caso;
d. Se cumplen los requisitos reglamentarios.

Tras valorar estos criterios, el laboratorio forense digital debe enviar una respuesta oficial, indicando si acepta o no el caso. Si la decisión es positiva, debe indicarse también la fecha en la que se devolverán las evidencias digitales a la entidad solicitante.

4.3.2 Registro del caso

Una vez el laboratorio haya decidido que el caso es factible, la entidad solicitante deberá aportar las evidencias electrónicas. A continuación, el laboratorio adjudicará un número único al caso y cumplimentará la hoja de registro.

Para poder examinar las evidencias electrónicas, la entidad solicitante debe proporcionar una petición detallada en relación con el caso. Dado que los dispositivos electrónicos pueden contener grandes cantidades de datos de todo tipo (documentos, vídeos, comunicaciones, datos de salud, ubicaciones, etc.), sería imposible examinar la información contenida sin disponer de una petición clara y específica.

Una vez conocida esta información, el encargado del examen puede establecer un plan para el tratamiento de las evidencias y determinar las herramientas y métodos que utilizará.

El formulario debe estar firmado por ambas partes, la entidad solicitante y el laboratorio forense digital. Una vez firmado, comienza oficialmente el trabajo. A continuación, el laboratorio debe crear una carpeta en un soporte de información para conservar todos los datos lógicos relacionados con el caso.

4.3.3 Registro de las muestras

Antes de transferir la custodia de las evidencias digitales (muestras) al laboratorio, es importante precintar las muestras. Para descartar cualquier duda razonable sobre la integridad de las evidencias, tanto la entidad solicitante como la entidad encargada del examen deben estar en condiciones de demostrar que nadie más ha tenido acceso a las muestras durante el proceso de transferencia de una parte a otra. En algunos organismos este requisito puede resultar muy novedoso o complicado, pero el laboratorio puede ayudarles a practicar el procedimiento, estableciendo un calendario y prestando el asesoramiento necesario.

Cada uno de los elementos electrónicos recibidos debe ser registrado y contar con un código de identificación específico que se documentará en el formulario de registro junto con los demás detalles de la muestra.

Este proceso de registro es aplicable también a subcomponentes, como las tarjetas SIM o las tarjetas de memoria. En este caso, el código de identificación debe reflejar su relación con el elemento del que proceden. Por ejemplo, si un teléfono móvil se etiqueta con el código 20190105(2)-MP01, su correspondiente tarjeta SIM se etiquetará como 20190105(2)-MP01-SIM01.

Cabe señalar que en el formulario de registro debe documentarse cualquier tipo de defecto que presente la muestra. El objetivo es proteger al laboratorio forense digital de posibles quejas o denuncias en el futuro.

Cualquier tipo de copia electrónica relacionada con la muestra se incorporará a la carpeta del caso.

En este momento comienza la cadena de custodia de las muestras, y el personal que las haya recibido debe ocuparse de cumplimentar el formulario correspondiente.

4.3.4 Toma de fotografías

Las muestras deben fotografiarse por los motivos siguientes: para registrar su estado inicial y para identificarlas adecuadamente en el futuro. Se tomarán fotografías generales de las muestras y también fotografías de detalle. Si hay alguna pantalla activa, se fotografiará también. Las fotografías se incorporarán a la carpeta del caso. Se recomienda fotografiar la muestra antes de devolverla a la entidad solicitante, como futura referencia de su estado.

4.3.5 Realización del análisis

En la realización del análisis debe seguirse el modelo de actuación para laboratorios forenses digitales (para más detalles, consúltese el capítulo 5). Durante el proceso, los responsables del examen deben estar en contacto con la entidad solicitante y comunicarle cualquier limitación o complicación que surja. Algunos profesionales tienen una larga experiencia en análisis forense digital y pueden localizar rápidamente los datos pertinentes tras recibir las indicaciones de la entidad solicitante.

4.3.6 Devolución de las muestras

Una vez completado el análisis, el laboratorio forense digital debe ponerse en contacto con la entidad solicitante para concertar la recogida de las muestras. Es habitual que el laboratorio devuelva las muestras a la entidad solicitante junto con el informe forense, para evitar viajes innecesarios. El laboratorio debe precintar las muestras antes de devolverlas. En el precinto deben figurar las iniciales del profesional encargado, el código de la muestra y la fecha y la hora en la que se precintó.

4.3.7 Cierre del caso

Tras el paso anterior, se considera que el proceso ha finalizado y el laboratorio forense digital puede cerrar el caso. Para cerrar el caso, ambas partes deben confirmar que el trabajo ha finalizado y que se ha enviado el informe a la entidad solicitante. Para ello, pueden firmar el formulario correspondiente.

5. ANÁLISIS DIGITAL DE DRONES

En esta sección se describirá el proceso del análisis forense digital aplicado a los drones y sus dispositivos de control. El examen de otros dispositivos asociados, como ordenadores portátiles, teléfonos móviles o tabletas, se describe en la Guía general de INTERPOL para laboratorios forenses digitales.

5.1 Descripción general

El presente capítulo se centra en el procedimiento empleado para el análisis forense digital de evidencias electrónicas relacionadas con drones. Se incluye un modelo cronológico donde figuran los pasos básicos del análisis digital de drones.

Por lo general, el análisis de evidencias electrónicas en un laboratorio forense digital se divide en cuatro etapas: adquisición, examen, análisis y presentación. A lo largo del proceso, debe actualizarse la cadena de custodia cada vez que las muestras cambien de manos, y debe garantizarse su integridad en todo momento. Las etapas de examen y de análisis deben repetirse hasta satisfacer lo solicitado para el caso.

Por lo general, se entiende que un análisis forense digital se divide en esas cuatro etapas; no obstante, no todas se emplean en todos los casos. En ocasiones se puede prescindir de la fase de adquisición y pasar directamente al *triage*, en la etapa de examen. Esto sucede, por ejemplo, cuando hay grandes conjuntos de datos y no es factible adquirir por separado cada elemento probatorio.

En la figura siguiente se presenta un modelo de análisis de laboratorio:

Figura 30 - Modelo de análisis utilizado en laboratorios forenses digitales

5.1.1 Dispositivos asociados a drones

En el siguiente apartado se describen en detalle las etapas del modelo de análisis empleado en los laboratorios forenses digitales. En el presente documento se explica el proceso de adquisición, examen y análisis aplicable a dos tipos de dispositivos:

I. Drones
II. Sistemas de control remoto

Tal como se indicaba en el apartado 2.5, los drones pueden aportar diferentes tipos de información, que además pueden almacenarse en soportes diversos, como el propio dron, tarjetas extraíbles, dispositivos móviles, servidores en la nube, etc. Como hemos visto, a veces quedan datos residuales en el propio sistema de control del dron y el encargado del examen puede tratar de recuperarlos en caso necesario. Estos datos pueden ser de los tipos indicados a continuación.

Tipos de datos presentes en los sistemas de control remoto	
Telemetría	Datos relativos a los vuelos, como posiciones GPS, fechas y horas de señales GPS, dirección, altitud, velocidad del motor e instrucciones introducidas por el usuario.
Dispositivos asociados	Datos de cualquier dispositivo emparejado o conectado al sistema de control, como tabletas o teléfonos móviles. Puede ser el código IMEI (Identidad Internacional de Equipo Móvil) del terminal o la identificación de *hardware* del dispositivo.
Cuentas de usuarios registrados	Las cuentas creadas para el contacto con el fabricante del dron pueden incluir direcciones de correo electrónico o nombres de usuario.
Parámetros de comunicación entre el dron y el dispositivo de control	Los registros de comunicación contienen información relativa a la potencia de señal establecida entre el dron y el dispositivo de control remoto.

Cuadro 20 - Tipos de datos contenidos en los dispositivos de control remoto

Para orientaciones específicas sobre el análisis forense digital aplicado a otros dispositivos asociados a drones (p. ej., teléfonos móviles u ordenadores), consúltese la Guía general de INTERPOL para laboratorios forenses digitales.

5.2 Adquisición

La adquisición, también conocida como captación de datos, es el proceso seguido para crear una copia forense de la evidencia digital (muestra), es decir, el dron, dispositivo de control, teléfono móvil u ordenador portátil, en forma de uno o varios ficheros imagen. A continuación, esos ficheros imagen pueden utilizarse en la fase de análisis. La adquisición se lleva a cabo para preservar la integridad de las pruebas digitales, ya que se obtiene una copia idéntica de los datos sin alterar en modo alguno el contenido de la evidencia electrónica. Es recomendable crear dos copias: una que se conservará como fichero maestro y otra que se empleará para el análisis forense.

La adquisición de evidencias electrónicas debe llevarse a cabo con técnicas forenses reconocidas. El carácter intangible de la información almacenada en formato electrónico la hace más fácil de manipular y más proclive a la alteración que otros tipos de evidencias tradicionales. Por ello, es fundamental utilizar un procedimiento de adquisición establecido y comprobado.

Una vez creado el fichero imagen, hay que registrar el valor *hash* de la muestra y el del fichero imagen. La obtención de valores *hash* se emplea para demostrar que el fichero imagen es idéntico al contenido de la muestra. En ciencia forense digital se emplean diversos algoritmos para la obtención de valores *hash*, por ejemplo *Sha-256*. La mayoría de las máquinas y aplicaciones forenses tienen una opción para generar este tipo de códigos.

El examen y el análisis solo se aplicarán a la copia forense de la evidencia original, a no ser que las circunstancias lo impidan. Este requisito es fundamental para preservar la integridad de la evidencia. La copia forense de las evidencias electrónicas nunca debe almacenarse en la propia muestra, sino en otro soporte. Además, debe estar claramente etiquetada, para no confundirla con la evidencia electrónica original o con copias forenses correspondientes a otros casos. Por consiguiente, antes de aceptar un caso, el laboratorio forense digital debe disponer de los soportes necesarios.

En los siguientes apartados se describe el proceso de extracción de datos a partir de drones. El método de extracción es muy similar al utilizado con teléfonos móviles, ya que hay puntos comunes entre unos y otros dispositivos.

5.2.1 Tipos de extracción de datos

Antes de iniciar el examen forense, hay que consultar la documentación del caso aportada por la entidad solicitante, a fin de determinar el tipo de datos que es necesario extraer de la muestra. De este modo, se podrá decidir el método de extracción más adecuado para el caso.

Existen cuatro niveles de extracción de datos aplicables a los drones. Se describen a continuación, empezando por el que permite extraer mayor cantidad de datos y terminando por el que menos datos produce.

Figura 31 - Dron en proceso de examen

a) Extracción física

La extracción física es la adquisición de datos binarios en bruto a partir del soporte de almacenamiento del dispositivo. En una etapa posterior, estos datos en bruto deben tratarse con aplicaciones de análisis forense específicas. Normalmente, este método permite acceder a los datos en vivo y los datos borrados, a los ficheros del sistema operativo y a zonas del dispositivo a las que el usuario no suele tener acceso.

b) Volcado del sistema de archivos

El volcado del sistema de archivos es un híbrido entre la extracción física y la extracción lógica. Esta técnica permite recuperar el sistema de archivos del dispositivo e interpretar los datos en la fase de tratamiento. De este modo, es posible recuperar, por ejemplo, bases de datos con información telemática o de comunicación que tal vez no serían accesibles con la extracción lógica o física. Una de las limitaciones del volcado del sistema de archivos es que no permite recuperar todos los datos borrados, lo sí se puede hacer con la extracción física.

c) Extracción lógica

La extracción lógica implica recibir información del dron y permitir que el dispositivo presente los datos para el análisis. Normalmente, equivale a acceder a los datos en el propio dispositivo. Con este método solo pueden obtenerse datos en vivo. La mayoría de las aplicaciones de análisis forense de drones ofrecen esta opción, siempre que los datos no estén almacenados en una tarjeta extraíble. El problema de la extracción lógica es que no hay manera de verificar los datos en el propio dron, ya que muchos no disponen de pantalla para visualizar su contenido.

d) Chip-off

En los drones estropeados o que solo tengan memoria interna, se puede recurrir al *chip-off* (retirada del chip) para obtener los datos necesarios. Este método permite además extraer datos binarios en bruto desde el almacenamiento del dispositivo, pero requiere retirar de manera permanente el microprocesador de la placa de memoria. La aplicación de la técnica del *chip-off* puede estropear el dispositivo y dejarlo inutilizable. Además, las expectativas son moderadas en el caso de drones, ya que algunos modelos recientes encriptan la información que almacenan en el chip de memoria.

En el caso de los dispositivos de control remoto, es preciso localizar el chip en la placa de memoria del control remoto y adquirir los datos mediante una conexión USB, los puertos JTAG o un *chip-off*. Además, cuando el dispositivo de control contiene tarjetas de memoria extraíbles, estas deben tratarse como cualquier tipo de soporte extraíble.

El orden de aplicación de los diferentes métodos de extracción es importante. Hay que procurar utilizar el método de examen que resulte menos destructivo y al mismo tiempo ofrezca el máximo de información. De este modo se puede acceder a zonas que podrían quedar sobrescritas o dañadas en etapas posteriores. Los métodos invasivos deberían reservarse como último recurso, sobre todo el *chip-off*, ya que el proceso puede destruir la muestra y dejarla sin posibilidad de recuperación.

Se ha comprobado que el uso de los puertos JTAG para recuperar datos puede causar problemas en algunos modelos populares de drones. Este método debería experimentarse con un dispositivo de prueba antes de utilizarlo con la muestra, ya que se podría alterar el microcontrolador, lo que impediría recuperar más datos de ese módulo en el futuro.

5.2.2 Herramientas de extracción

Normalmente, el análisis de drones requiere el empleo de aplicaciones, cables de alimentación y cables de datos específicos. Las técnicas más avanzadas, como el *chip-off*, precisan herramientas adicionales. Por ejemplo, pueden necesitarse útiles de desoldado y reboleado y dispositivos específicos para leer datos en bruto a partir de chips de memoria. A veces, puede ser necesario recurrir a *suites* de *software* del fabricante, aunque no sean específicas de informática forense, como única vía para obtener los datos buscados en el examen.

5.2.3 Formato del fichero de extracción

Debido a la necesidad de utilizar herramientas especializadas en la extracción de datos de drones, a menudo se obtienen ficheros en formatos exclusivos. Muchas veces es posible convertir esos formatos a los de otras herramientas, para aprovechar todas las posibilidades de descodificación disponibles. Otros formatos no exclusivos son los de ficheros BIN y ficheros RAW.

5.2.4 Secuencia del proceso

Figura 32 -Proceso de extracción de datos válido para drones y dispositivos de control remoto

a) Identificar la muestra y los soportes de información

Antes de pasar a la etapa siguiente, es necesario observar la muestra disponible.

i) Drones

La etiqueta de la muestra estará adherida al interior del dron o estampada en su parte trasera. Debe incluir datos como el fabricante, el número de modelo, el número de serie y los identificadores de conexión (por ejemplo, dirección WiFi Mac).

ii) Dispositivos de control remoto

La etiqueta de la muestra estará adherida en la parte trasera del control remoto o en el interior del compartimento de las baterías. Debe incluir la marca y el modelo, el número de serie y el identificador de emparejamiento. Además, puede ser que el control remoto funcione con un sistema operativo conocido, como Android. En ese caso, se utilizarán las pautas generales para el análisis de dispositivos móviles.

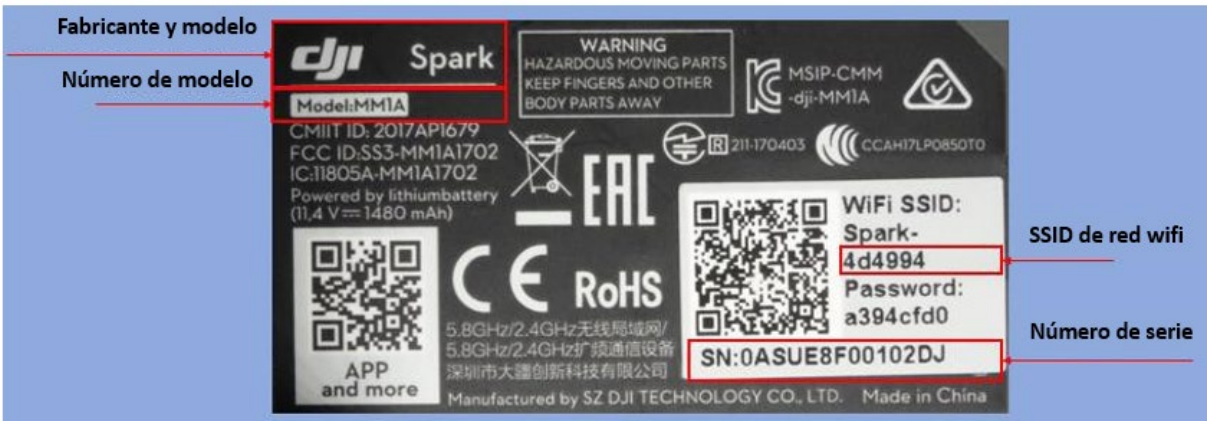


Figura 33 - Etiqueta de identificación de un dron

El siguiente paso consiste en preparar un soporte para almacenar los datos extraídos.

b) Aislar la muestra de la red

Al llevar a cabo la extracción, el dispositivo debe estar encendido.

i) Drones

Para evitar que el dispositivo trate de conectarse a la red, con el consiguiente riesgo de modificación de los datos, hay que aislar la muestra de la red y de los dispositivos asociados, como el teléfono móvil que se empleaba junto con la muestra.

ii) Dispositivos de control remoto

Para evitar cualquier intento de conexión a satélites GPS o a dispositivos emparejados, como el dron o el terminal móvil asociado, con el consiguiente riesgo de que se alteren los datos, es preciso aislar la muestra para que no capte señales de red, inalámbricas o de GPS y no se creen datos o ficheros nuevos que puedan revelar la ubicación del laboratorio forense digital.

En función del presupuesto, este aislamiento puede conseguirse con diferentes métodos.

Métodos de aislamiento de drones o controles remotos	
Blindaje de sala	Se puede instalar un blindaje de Faraday en una sala del laboratorio para evitar la entrada de señales de red. Sin embargo, se trata de una solución muy cara, por lo que, como alternativa eficaz, podrían utilizarse bolsas de Faraday individuales.
Equipos de interferencia inalámbrica	Este tipo de equipos bloquean las señales de entrada de las redes WiFi, GPS o de telefonía móvil. En algunas jurisdicciones, es ilegal utilizarlos. Además, pueden interferir en otros equipos que se conectan a redes de telefonía, WiFi o GPS para enviar o recibir datos.
Método manual	Es la solución más barata y fácil de aplicar. Consiste en cubrir las antenas del dron o del control remoto con papel de aluminio, para limitar la recepción de señales de satélite. No es un método a toda prueba, y hay que asegurarse de que las antenas y la zona que rodea al dron o al control remoto quedan totalmente cubiertas. Hay que señalar que, al poner en marcha un dron, este tratará de captar una señal GPS para verificar su posición, la fecha y la hora. Estos detalles pueden utilizarse posteriormente para verificar la autenticidad de bases de datos contenidas en el dron, como la de zonas de exclusión de vuelo. Por ello, cada vez que se pone en marcha un dron, en su sistema de archivos podría generarse un nuevo fichero de datos que aparecería en cualquier examen posterior.

Cuadro 21 - Métodos de aislamiento de drones y controles remotos

c) Extracción de datos pertinentes

Dado que algunas técnicas de extracción o de *rooting* (acceso al directorio raíz) y algunos drones o dispositivos de control remoto se basan en programas similares a los sistemas operativos móviles más conocidos (sobre todo, Android), el bloqueo de escritura no siempre funciona. En todo caso, el bloqueo de escritura debe emplearse siempre que sea posible; por ejemplo, al analizar tarjetas de memoria. No obstante, es sabido que este método no siempre es aplicable al análisis de drones o dispositivos de control remoto. Por ello, es imprescindible prever las consecuencias de cada actuación realizada al manejar drones o controles remotos y ser capaz de explicar y justificar cada paso.

Los drones y los dispositivos de control pueden emplear dos tipos de almacenamiento muy diferentes que deben tratarse con técnicas específicas, según se describe en el cuadro siguiente.

Soportes de almacenamiento de drones y dispositivos de control remoto	
Soporte	**Descripción**
Tarjetas de memoria	Pueden examinarse como el disco duro de un ordenador. Se puede emplear tanto la extracción lógica como la extracción física, siempre que se disponga de una aplicación forense que permita esas opciones. Es preciso acceder a la tarjeta, extraer los datos y volver a colocar la tarjeta en el dispositivo, antes de conectarlo. Algunos dispositivos almacenan información en la tarjeta de memoria y, si detectan que esta no está disponible, se puede producir una pérdida de datos. Si se dispone del tiempo y los recursos necesarios, debe crearse un clon bit a bit de la tarjeta de memoria e introducir la tarjeta clonada en el terminal.

Memoria interna	Esta situación requiere el empleo de herramientas forenses o del fabricante, compatibles con el dron o dispositivo de control remoto. Algunos dispositivos admiten la extracción física de datos. Las herramientas forenses reiniciarán el dispositivo de una manera específica y llevarán a cabo una extracción física de la información sin modificar ni alterar los datos de usuario presentes en el dispositivo.

Cuadro 22 - Soportes de información en drones y controles remotos

Posibles trazas de datos presentes en un dron o control remoto	
Elementos que se almacenan de manera predeterminada en el dron o dispositivo de control remoto. La probabilidad de hallar estas trazas es elevada, aunque el sospechoso haya intentado ocultar su rastro. Algunas de las trazas que pueden descubrirse son:	
Elementos presentes en muestras generales: • Espacio sobrante (*slack space*) • Espacio sin asignar • Caché de miniaturas • Ficheros de registro	Elementos específicos de los drones: • Historial de actualizaciones • Registros de diagnóstico • Cuentas de correo registradas • Dispositivos emparejados • Ficheros multimedia • Registros telemáticos o de vuelo • Caché de miniaturas de ficheros multimedia • Elementos cartográficos (geocoordenadas, puntos de referencia, posiciones de base) • Aplicaciones específicas (por ejemplo, las incluidas por el fabricante del dron) • Correos electrónicos con nuevos registros de drones o actualizaciones del fabricante • Ficheros CSV con datos telemáticos, diagnósticos o coordenadas GPS

Cuadro 23 - Trazas que pueden estar presentes en un dron o dispositivo de control remoto

El proceso de extracción variará en función de la herramienta utilizada. La mayoría de las aplicaciones forenses incluyen un tutorial donde se explica el procedimiento aplicable para efectuar una extracción fructífera. En algunos casos, el examen y el análisis del dron o el control remoto requieren modificar los ficheros de sistema o el propio sistema operativo para extraer los datos, lo que puede causar una pérdida irreparable de información. Sin embargo, esto solo afecta a los ficheros de sistema, con escaso valor probatorio. Para saber qué se altera con estos procesos, es necesario haber seguido la formación proporcionada por los fabricantes del dron o de la aplicación forense, o tener experiencia práctica con la verificación o extracción de información de drones y otros dispositivos móviles.

Otra fuente muy interesante de evidencias forenses son los ficheros de respaldo, telemetría o diagnóstico del dron. Algunos drones y sus dispositivos asociados crean copias de respaldo en otros dispositivos, como un ordenador de sobremesa o un portátil, o en plataformas en la nube. Estos respaldos pueden ser útiles para establecer una cronología de las evidencias, y también pueden servir para acceder a datos históricos que no están presente en el propio dron. Además, algunas copias de respaldo pueden analizarse como si fueran dispositivos físicos.

Debido a las características de los drones y sus dispositivos de control, es posible que las herramientas forenses habituales no permitan extraer y analizar los datos. En ese caso, puede ser necesario emplear otras aplicaciones comerciales para extraer y analizar información. Cuando se recurra a ello, es conveniente realizar controles y aseguramientos de calidad para cerciorarse de que se verifican los datos recuperados y evaluar el impacto en la muestra antes de emplear la solución escogida. Además, si se emplea *software* específico del fabricante, hay que tener en cuenta si la aplicación podría enviar como referencia a los servidores del fabricante datos o copias de los ficheros recuperados.

d) Verificación de la muestra y de los datos extraídos

Una vez se han extraído los datos, hay que verificarlos, comparándolos con los datos presentes en la muestra. El responsable del examen debe cotejar fechas y horas, coordenadas geográficas e información del sistema o los usuarios, que a veces se convierten a otro formato durante el proceso de extracción. Dado que los drones no disponen de una interfaz que permita verificar esos datos en el propio dispositivo, es conveniente utilizar cuando sea posible al menos dos aplicaciones forenses distintas para adquirir y analizar los datos extraídos. Esto se conoce como *dual tooling* (doble utillaje).

e) Documentar todas las actuaciones

El último paso en el proceso de adquisición de datos de un dron o un dispositivo de control remoto es asegurar la documentación de todos los pasos. Durante la adquisición hay que tomar notas, consignando la fecha y hora de cada actuación, las aplicaciones forenses o complementarias que se hayan empleado, y cualquier error o anormalidad que surja durante el proceso. Esto es imprescindible para la cadena de custodia, y además se deberá aportar si la evidencia se utiliza en un tribunal. No hay que olvidar que puede haber un desfase temporal importante entre la adquisición, el examen, el análisis y la actuación judicial, por lo que las anotaciones deben ser tan completas como sea posible.

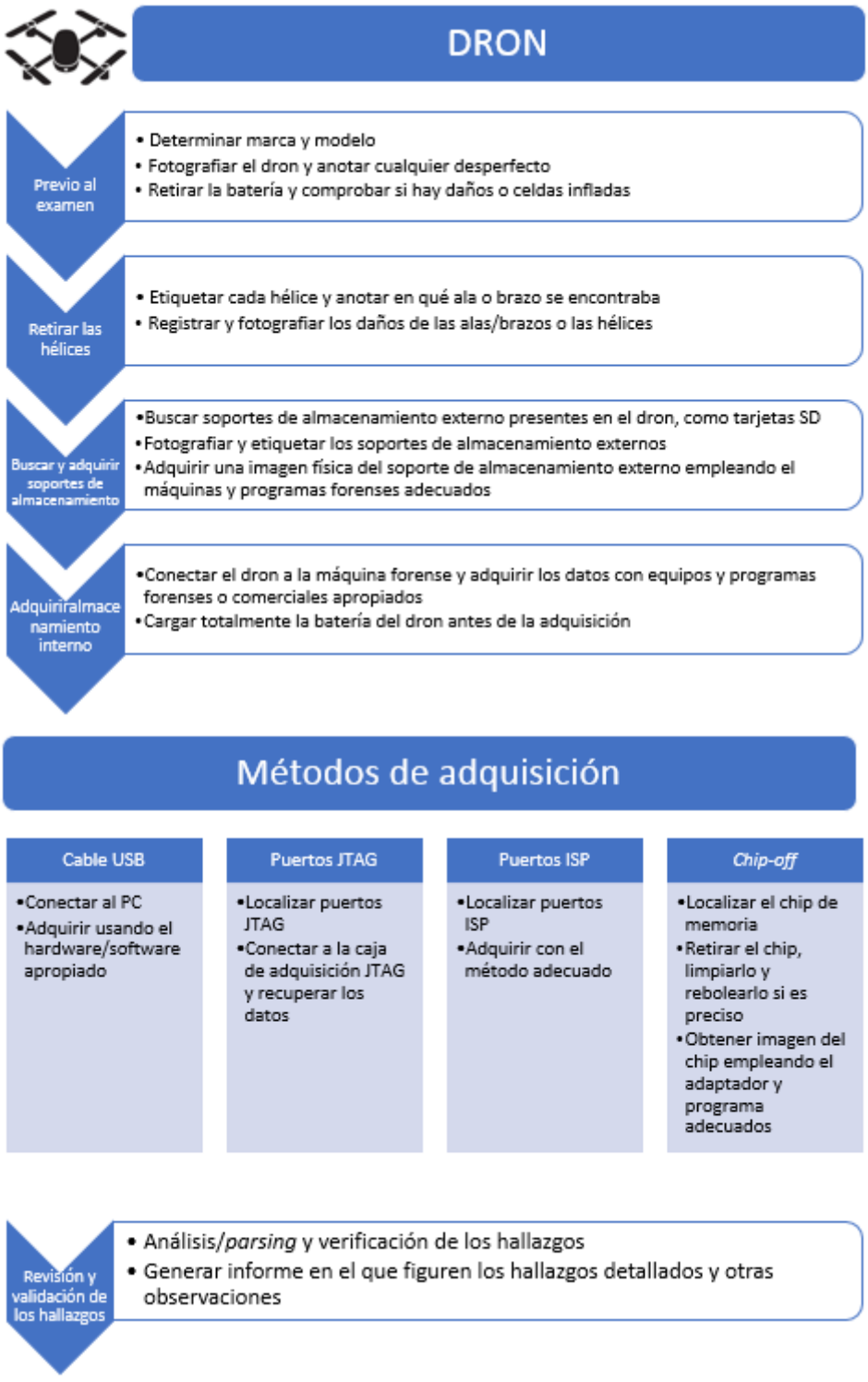


Figura 34 - Organigrama del examen de un dron

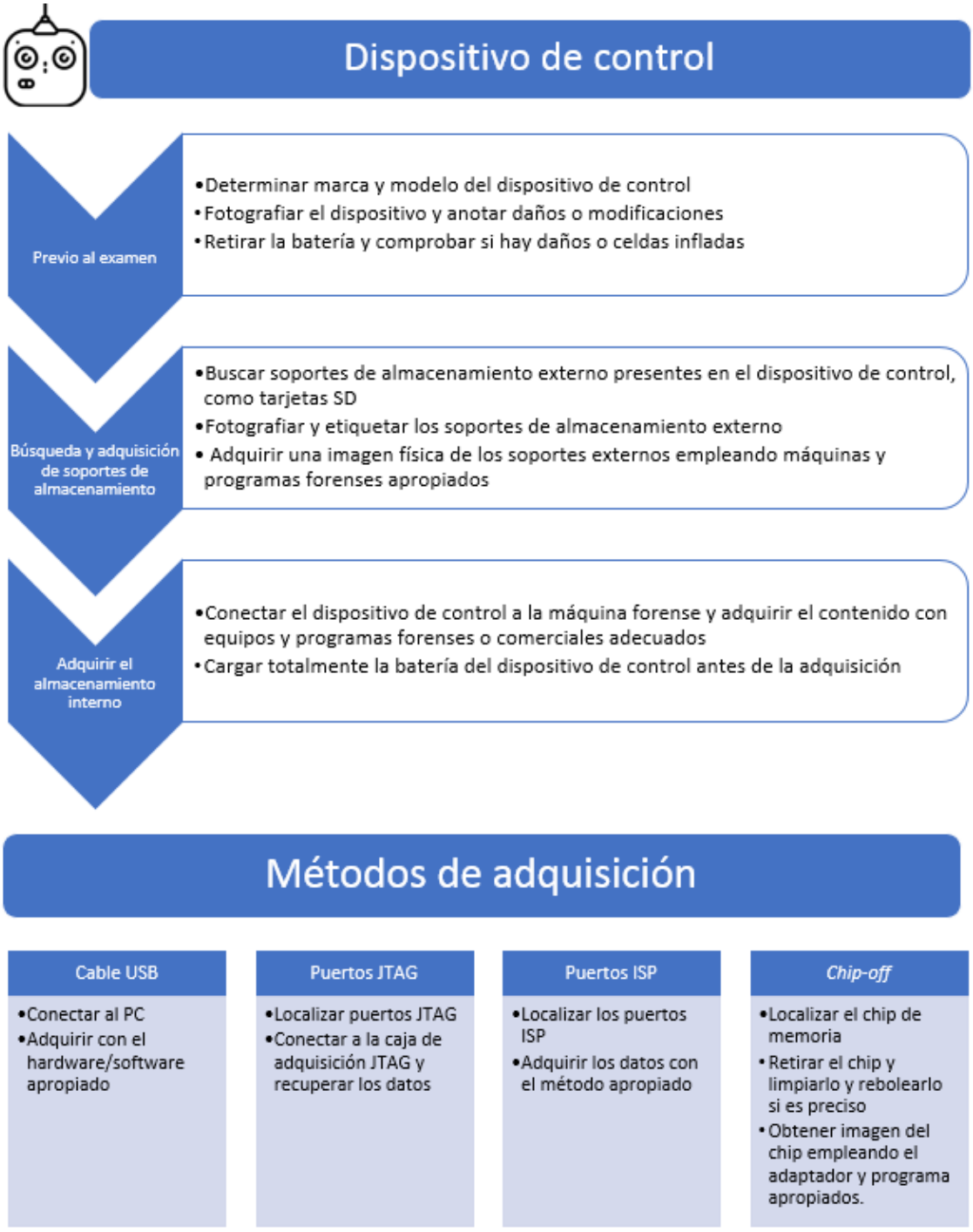


Figura 35 - Organigrama del examen de un control remoto

5.2.5 Otras fuentes de evidencias

Un dron puede tener muchos otros dispositivos asociados, como cargas útiles, complementos electrónicos o gafas de visión en primera persona, y además puede haber sido objeto de añadidos o modificaciones. Los encargados del examen forense deben tener una actitud abierta a la hora de considerar qué muestras pueden ser pertinentes o útiles para la investigación del caso.

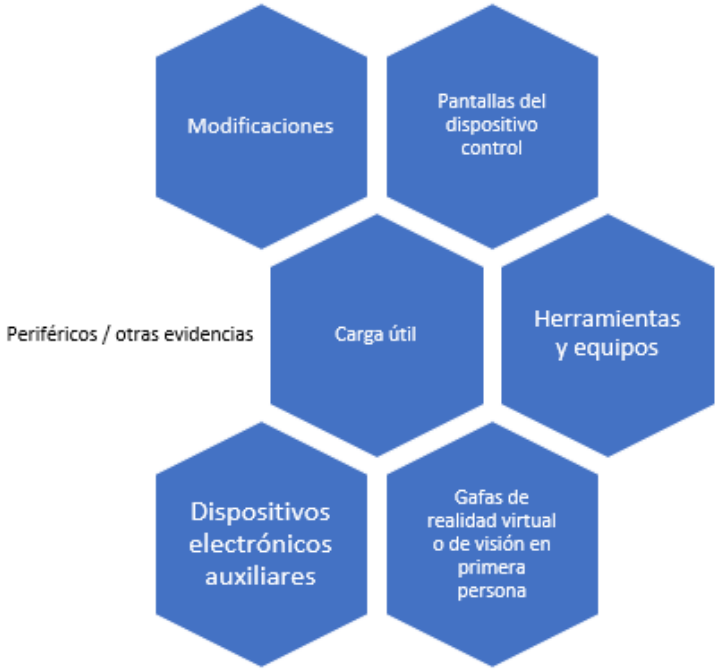


Figura 36. Otras fuentes de evidencias

A veces sucede que datos electrónicos fundamentales para la investigación se encuentran en un dispositivo asociado, como un ordenador portátil o un teléfono móvil. Si no es posible examinar exhaustivamente esos dispositivos, es conveniente realizar y documentar un *triage* de los dispositivos y de los datos almacenados.

5.3 Examen

Siempre que sea posible, hay que evitar examinar las evidencias originales. Siempre hay que trabajar con la copia forense (fichero imagen) de la evidencia. Cuando sea imprescindible acceder a la muestra original, hay que proteger los datos con un bloqueador de escritura.

En algunos casos, es necesario llevar a cabo el examen en un entorno aislado o preestablecido. Por ejemplo, realizando una simulación en un sistema de bases de datos o en un programa de juegos. Para ello, se puede usar tecnología de virtualización y encapsular el caso en un continente de trabajo. Al finalizar el examen, se podrá revertir la estación de trabajo a su estado anterior utilizando una imagen conocida o las opciones que ofrezca el sistema operativo.

Para más información sobre los métodos de examen de evidencias digitales, véase el apartado 5.2 de la guía general para laboratorios forenses digitales elaborada por INTERPOL.

5.4 Análisis

5.4.1 Procedimientos para el análisis de trazas digitales

Del mismo modo que los delincuentes dejan trazas físicas en el lugar de los hechos, cuando se utiliza un dron para cometer una infracción, quedan trazas e indicios de las ubicaciones y las acciones que se sucedieron hasta el momento en que se embargó el dron o el dispositivo asociado.

Los datos o la información que es necesario extraer de un dron o un control remoto dependen del tipo de caso.

a) Imágenes y vídeos

Para analizar fotografías o vídeos, hay que tener una idea clara de lo que interesa a la entidad solicitante. ¿Se están buscando los propios ficheros multimedia creados por el dispositivo, o los indicios que estos puedan aportar sobre la comisión de un acto delictivo? La revisión de las imágenes y los vídeos almacenados puede ayudar a entender cómo se usaba el dron y las zonas que este recorrió.

Normalmente, el análisis de las fotografías comienza con el análisis de las firmas digitales. El siguiente paso consiste en recorrer las imágenes de la galería mediante la vista de miniaturas.

En el caso del análisis de vídeo, existen aplicaciones que permiten extraer imágenes fijas a partir de vídeos (por ejemplo, X imágenes cada Y segundos o minutos). Las imágenes extraídas pueden revisarse posteriormente en una galería. Este proceso otorga gran eficiencia a la previsualización de ficheros de vídeo.

En aquellos casos en los que es importante conocer la ubicación o los detalles de producción de las imágenes o vídeos, es conveniente extraer los metadatos de los ficheros. Los metadatos son conjuntos de datos que aportan información sobre otros datos; por ejemplo, las coordenadas GPS del lugar donde se obtuvo la imagen, la fecha y la hora de su creación o el dispositivo utilizado para captar la imagen. Si el fichero multimedia se obtuvo desde el dron, habrá geoetiquetas generadas automáticamente por el sistema, a no ser que el usuario hubiera modificado la configuración.

Algunas muestras pueden contener miles de fotografías y vídeos, y resulta imposible recorrerlas todas y localizar una imagen específica. En ese caso, lo mejor es extraer todas las imágenes y enviarlas en conjunto a la entidad solicitante. Además, en el dron puede haber múltiples copias de una misma fotografía o vídeo, ya que a partir de las grabaciones originales se crean miniaturas o vídeos comprimidos para facilitar la experiencia del usuario.

La tarea de visualizar el contenido de los ficheros de fotografía o vídeo es sencilla y no requiere experiencia en análisis forense digital, por lo que puede encargarse de ella la propia entidad solicitante. Una vez se hayan identificado las fotografías o vídeos pertinentes, se podrá llevar a cabo un nuevo examen para extraer información más significativa, como las coordenadas GPS o los datos de creación y modificación.

b) Registros de vuelo

Los registros de vuelo de los drones tienen valor probatorio en muchos casos. Por lo general, contienen los siguientes elementos:

- Posiciones GPS
- Fechas y horas
- Parámetros específicos (velocidad del rotor, altitud y dirección)
- Datos telemáticos
- Códigos de fallos de diagnóstico
- Registros de soportes asociados

El análisis de los registros de vuelo puede ser útil para determinar el presunto objetivo o finalidad del dron. Un ejemplo es la posición del dron en un momento concreto, lo que podría indicar la intención del piloto de acceder a una zona de exclusión de vuelo o a un espacio restringido.

La mayoría de las aplicaciones de análisis forense incluyen una opción de *parsing* (análisis de la estructura), útil para analizar los registros de vuelo. Sin embargo, dado que la tecnología evoluciona y algunos modelos de dron se actualizan con frecuencia, las aplicaciones de análisis forense pueden requerir tiempo para actualizar su base de datos. Por ello, es fundamental entender la estructura subyacente a los registros de vuelo. La mayor parte de los drones emplean bases de datos SQLite o ficheros CSV, por lo que puede ser recomendable efectuar manualmente un *parsing* con la aplicación adecuada para visualizar los datos.

De este modo, no se depende de una aplicación en concreto y además es posible cotejar los resultados obtenidos por la aplicación con los de los registros de vuelo.

c) Aplicaciones y programas informáticos

Si bien no hay ningún procedimiento normalizado que sirva para analizar todo tipo de dispositivos, dada su diversidad, por lo general el análisis se inicia recopilando en fuentes fiables información sobre los programas o aplicaciones instalados. A continuación, pueden verificarse los hallazgos por medio de una simulación o instalando la aplicación en un dispositivo de prueba para experimentar su funcionalidad y las posibilidades de obtención de datos. De este modo, se puede tener una idea más clara sobre los derechos de usuario de la aplicación y los datos de registro necesarios para utilizarla.

d) Actividad de usuario

El sistema operativo del dron rastrea la actividad de los usuarios y la almacena en diferentes lugres. Entre otros datos, recoge:

- Horas de encendido y apagado del dron
- Ajustes de configuración del dron
- Uso del dispositivo
- Identificadores y cuentas de usuario
- Conexiones a redes inalámbricas y a otros dispositivos
- Registros telemáticos

Analizar esta información ayuda a entender el comportamiento de los usuarios e incluso puede demostrar actividades ilícitas. En función del sistema operativo, estos elementos se almacenan en diferentes ficheros y ubicaciones.

e) Espacio sin asignar

Las zonas sin asignar pueden contener evidencias de todos los tipos mencionados. Las aplicaciones de *carving* (extracción de conjuntos de datos inmersos en otros conjuntos de datos) permiten buscar y extraer ciertos tipos de ficheros situados en zonas sin asignar. Debido a que el *carving* es lento y laborioso, hay que tener claro previamente qué tipo de ficheros se están buscando. Este proceso no funciona bien con ficheros fragmentados. Por lo general, los datos situados en zonas sin asignar no pueden asociarse a usuarios concretos, marcas temporales o ubicaciones en una estructura de carpetas.

f) Almacenamiento remoto y en la nube

Cuando al examinar un dron se descubren trazas de utilización de servicios en la nube, puede suceder lo siguiente:

- Los datos están almacenados localmente en el dron y remotamente en la nube;
- Los datos están almacenados exclusivamente en la nube, y puede que no haya ningún tipo de información en el dron.

De hecho, los datos almacenados de manera remota podrían estar en más de un servidor, no en uno solo. Muchas veces, ni siquiera el proveedor del servicio en la nube puede saber exactamente en qué servidor, centro de datos o país se encuentran algunos de los datos.

Aunque técnicamente no es difícil crear una copia forense de la máquina virtual situada en la nube, deben tenerse en cuenta algunos aspectos jurídicos. En función de la legislación aplicable, puede ser necesario obtener una autorización judicial para interceptar este tipo de datos. Además, puede resultar complicado demostrar que los datos se adquirieron de conformidad con la normativa legal vigente en el país solicitante.

Otro inconveniente es que probablemente se podrán extraer pocos datos recuperables. De hecho, si el sospechoso creó una máquina virtual temporal para cometer un delito y después la borró, es posible que no pueda recuperarse ninguna evidencia.

La posibilidad de adquirir y analizar datos almacenados en una ubicación remota depende de la normativa aplicable. Por ejemplo, algunas jurisdicciones permiten que, si se dan determinadas circunstancias, se puedan adquirir los datos conectándose al almacenamiento remoto con el nombre de usuario y contraseña presentes en el dron. En otras jurisdicciones, esto no es posible. En ese caso puede recurrirse a los canales oficiales para solicitar al proveedor que conserve y acceda a los datos.

5.5 Presentación

En la fase de presentación es necesario agrupar los hallazgos de una manera comprensible para las partes interesadas. Al finalizar el análisis, se elabora un informe forense con los resultados de la investigación. En este caso hay que explicar e ilustrar las cuestiones técnicas complicadas, para facilitar la comprensión de los jueces, fiscales y otros profesionales implicados. Es posible que además sea necesario interpretar los datos y expresar una opinión sobre los mismos. En algunos casos, cuando se haya analizado un gran número de muestras, puede ser difícil presentar los resultados al equipo de investigación. Se recomienda utilizar alguna aplicación de análisis para facilitar el cotejo de las evidencias digitales con otros datos obtenidos en las investigaciones. Este tipo de herramientas pueden usarse también para indexar y hacer búsquedas en las muestras, de manera que el equipo de investigación pueda tener una visión general del caso.

5.5.1 Admisibilidad de las evidencias electrónicas

Los criterios sobre la admisibilidad de evidencias electrónicas difieren según la jurisdicción. Por lo general, para valorar la idoneidad de las evidencias digitales para una actuación judicial, hay que tener en cuenta los criterios siguientes:

Criterios de admisibilidad de evidencias electrónicas	
Autenticidad	La evidencia debe establecer los hechos de una manera que no arroje dudas y que sea representativa de su estado original.
Exhaustividad	El análisis de las evidencias y cualquier opinión basada en el mismo deben reflejar la situación en su totalidad, sin modificarla para que encaje con el punto de vista favorable o deseado.
Fiabilidad	En el proceso seguido para obtener y manejar las evidencias no debe haber ningún paso que pueda plantear dudas sobre su autenticidad o veracidad.
Capacidad persuasiva	Las evidencias deben reflejar los hechos de una manera que resulte convincente para las partes que intervengan en el tribunal.

Proporcionalidad	Los métodos empleados para obtener las evidencias deben ser legítimos y proporcionales al interés de la justicia: el prejuicio (esto es, el grado de intrusión o coerción) causado a los derechos de cualquiera de las partes no debe pesar más que el valor probatorio de la evidencia (esto es, su utilidad como prueba).

Cuadro 24 - Criterios generales de admisibilidad de evidencias digitales

5.5.2 Redacción del informe

El informe forense debe estar redactado de manera clara y comprensible. Los resultados deben figurar adecuadamente resumidos, ofreciendo una respuesta concisa a la petición sobre el caso planteada por la entidad solicitante.

En lugar de incluir los conceptos técnicos en el texto general, es conveniente detallarlos en un anexo. De este modo, se facilita la lectura del informe por parte de personas que no sean especialistas en la materia.

Además, no deben incluirse afirmaciones que no puedan demostrarse. Por ejemplo, una frase como "el sospechoso alteró el fichero A" debería sustituirse por: "el fichero A hallado en el ordenador B había sido alterado".

A veces, debido a la complejidad del caso, es difícil resumir los hallazgos en un informe. Para facilitar la comprensión, resulta útil incluir gráficos y otras ayudas visuales, como animaciones, fotografías o demostraciones en directo.

5.5.3 Testimonios periciales

En algunas jurisdicciones basta con presentar un informe forense y no es necesario que el responsable del examen esté presente en el juicio. En otras, es preciso que comparezca para presentar un testimonio pericial en relación con el caso.

Un perito es una persona que, gracias a su formación, experiencia o especialización, es experta en un ámbito concreto que resulta desconocido para el ciudadano medio. Se considera que los conocimientos del perito son garantía suficiente para aceptar oficial o judicialmente su dictamen (científico o técnico) sobre unas evidencias o unos hechos situados en el ámbito de su especialización, lo que se conoce como testimonio pericial.

En algunas jurisdicciones, la admisión de un profesional como perito en un juicio dependerá de la decisión del juez, y su asesoramiento solo se considerará válido para el caso concreto en el que intervenga. En otras, la categoría de perito se concede oficialmente, y quienes la obtienen pueden prestar asesoramiento en cualquier caso que entre en su ámbito de especialización.

Los derechos y deberes de los peritos varían en cada país. Es importante que los analistas forenses conozcan bien la legislación aplicable en su zona y los procedimientos seguidos en los tribunales, así como su papel y sus derechos y obligaciones como peritos.

Para más información sobre la manera de asegurar la calidad y la admisibilidad de las evidencias electrónicas obtenidas en laboratorios forenses digitales, véanse los apartados 6.1 y 6.2 de la Guía general de INTERPOL para laboratorios forenses digitales.

6. EJEMPLOS DE DATOS DE DRONES

En la siguiente tabla se muestran las ubicaciones habituales de los registros de vuelo y los ficheros multimedia en algunos modelos de dron existentes en el mercado.

6.1 Registros de vuelo

Modelo/marca del dron	Ubicación de los datos	Tipo de fichero	Nombre predeterminado
DJI Phantom 3	Memoria SD interna	.dat	FLYXXX
DJI Phantom 4 Pro	Memoria SD interna	.dat Se generan dos registros adicionales: PHARM.LOG y USER.LOG	FLYXXX
DJI MAVIC 2	Memoria eMMC interna	.dat	
YNEEX Q500 4K	Tarjeta SD (cuando se guardan en el dispositivo de control)	.csv	Conexiones remotas / GPS / telemetría
Parrot ANAFI	Tarjeta SD externa (o iPhone combinado con dispositivo de control)	.bin (.json)	Log.bin (XXDate&TImeXX.json)

Cuadro 25 - Ubicación de registros de vuelo en algunos modelos de dron

6.2 Ubicación de ficheros multimedia

Marca/modelo del dron	Ubicación	Ruta del fichero	Tipo de fichero	Nombre predeterminado
 **DJI Phantom 3**				
Fotografías	Memoria SD externa	\DCIM\	.jpg/.dng	FLYXXX
Vídeo	Memoria SD externa	\DJI\dji.pilot\DJI_REC ORD\	.mp4/.mov	FLYXXX
 **DJI Phantom 4**				
Fotografías	Memoria SD externa	\DCIM\	.jpg/.dng	FLYXXX
Vídeo	Memoria SD externa	\DCIM\	.mov/.mp4	FLYXXX
 **DJI MAVIC 2**				
Fotografía	Memoria eMMC interna / memoria SD externa	\DCIM\	.jpg/.dng	FLYXXX
Vídeo	Memoria SD externa	\DCIM\	.mov/.mp4	FLYXXX

 **YUNEEC Q500 4K**			
Fotografía	SD de la cámara	\DCIM\	.jpg/.dng
Vídeo	SD de la cámara	\DCIM\	.mp4
 **Parrot ANAFI**			
Fotografía	SD externa	\DCIM\100MEDIA	.jpg/.dng
Vídeo	SD externa	\DCIM\100MEDIA	.mp4
*** Puede haber grabaciones de vídeo adicionales en la tarjeta micro-SD del dispositivo de control, en el directorio: \FPV-Video\Local\, con la extensión ".avc".**			

Cuadro 26 - Ubicaciones de ficheros multimedia en algunos modelos de dron

6.3 Aplicaciones móviles asociadas

La mayoría de los drones se acompañan de aplicaciones de teléfono móvil para pilotar el dron, visualizar las imágenes de la cámara o ubicar la trayectoria en un mapa. Por lo general, estas aplicaciones requieren que el usuario se registre con una cuenta de correo electrónico válida o que acceda con su perfil de Facebook, Google, Apple o Outlook. Todas estas aplicaciones se descargan desde plataformas como Google Play Store o Apple Store y requieren permisos de acceso para utilizar determinadas funciones del terminal móvil. En las tablas siguientes se detallan las aplicaciones asociadas a los drones DJI, Parrot y Yuneec.

Hay que tener en cuenta la posibilidad de que se hayan utilizado aplicaciones de terceros para controlar o supervisar el dron, por lo que, al examinar un teléfono móvil, ordenador portátil o tableta, se debe verificar la funcionalidad de las aplicaciones instaladas y descartar que estén asociadas al dron analizado. Además, estas aplicaciones podrían contener información relativa a otros drones registrados.

Para más información sobre el análisis forense de teléfonos móviles, consúltese la guía general de INTERPOL para laboratorios forenses digitales.

6.3.1 Aplicación móvil DJI

El fabricante DJI ofrece aplicaciones móviles para todos sus drones. La más utilizada es la versión DJI Go 4.

Nombre de la aplicación	DJI Go 4
Icono de la aplicación	
Fabricante	DJI Technology
Plataformas soportadas	iOS, Android

Descripción del fabricante

Capta el mundo desde el aire. La aplicación DJI GO 4.0 ha sido optimizada para los productos más recientes de DJI, como Phantom 4, Mavic Pro, Phantom 4 Pro e Inspire 2. Esta versión ofrece la posibilidad de transmitir imágenes casi en tiempo real y de ajustar la configuración de la cámara, así como opciones para el montaje y la difusión de las imágenes aéreas.

Características:

- Página de inicio e interfaz de usuario totalmente renovadas
- Transmisión de imágenes HD casi en tiempo real
- Ajustes de configuración de la cámara
- Interfaz de reproducción actualizada
- Área de montaje actualizada, con interfaz de usuario mejorada
- Más plantillas y pistas de música en el área de montaje
- Facilidad para la descarga, montaje y difusión de vídeo
- *Streaming* en directo integrado
- Grabación de datos de vuelo casi en tiempo real

Capturas de pantalla

Página de inicio de la aplicación	Controles de vuelo
	

Cuadro 27 - Aplicación móvil DJI Go 4

6.3.2 Aplicación móvil Parrot

Nombre de la aplicación	Free Flight Pro
Icono de la aplicación	
Fabricante	Parrot SA
Plataformas soportadas	iOS, Android

Descripción del fabricante

La aplicación de pilotaje oficial de los drones Parrot.

PILOTA TU DRON DESDE TU TABLETA O TELÉFONO INTELIGENTE

Descarga FreeFlight Pro, la aplicación gratuita que te ofrece opciones avanzadas de configuración de vuelo para pilotar tu dron Parrot Bebop, Bebop 2 o Disco.

Para el modelo ANAFI, utiliza la nueva aplicación Freeflight 6.
Aviso: la aplicación Freeflight 6 no puede usarse con el Parrot Bebop 2 y con la gama Parrot Disco.

PILOTAJE INTUITIVO
Los controles táctiles de FreeFlight Pro facilitan el manejo de los drones Parrot sea cual sea la experiencia del piloto. Es posible personalizar la interfaz de la aplicación según los conocimientos del usuario, sea principiante o avanzado. Si buscas una experiencia de pilotaje más precisa, conecta tu teléfono o tableta a la aplicación Parrot Skycontroller 2.

VUELO INMERSIVO

¡Sube a bordo con las nuevas gafas de visión en primera persona Parrot Cockpit! Ahora, FreeFlight Pro incluye un modo de vuelo inmersivo que se combina con las gafas Parrot Cockpit para garantizar una experiencia inaudita y emocionante. Para activarlo, inserta tu teléfono inteligente en las gafas, despega y experimenta la magia de volar. Cuando está activado el vuelo inmersivo, los datos de telemetría se muestran en directo en la pantalla para ofrecerte la mejor sesión.

FOTOGRAFÍA Y VÍDEO AVANZADOS

FreeFlight Pro incluye ajustes avanzados de fotografía y vídeo. Con el modo Photo podrás captar imágenes de alta calidad en formatos profesionales como RAW y DNG. Además, puedes grabar vídeos Full HD en 1080p a 30Mb/s y personalizar el balance de blancos, la exposición y la tasa de refresco. El modo Time-lapse te permite obtener imágenes a intervalos fijos para obtener impresionantes vídeos acelerados. Finalmente, durante el vuelo podrás disfrutar de *streaming* de vídeo en tiempo real desde tu teléfono o tableta.

PARROT CLOUD

Al hacerte miembro de Parrot Cloud podrás seguir todas tus aventuras y entrar en contacto con otros pilotos de drones. Comparte tus sesiones de fotos, vídeos y datos con otros pilotos y cárgalas al instante en YouTube, Google Photos o Twitter. Además, tendrás un respaldo gratuito de todos los datos compartidos en Parrot Cloud.

FLIGHT PLAN (compra desde la aplicación)

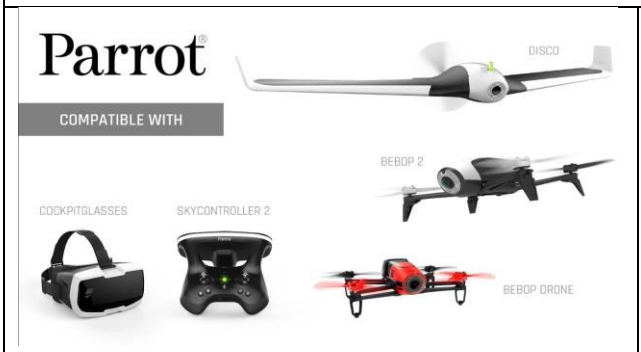
Programa con antelación vuelos autónomos desde tu teléfono o tableta con la opción Flight Plan (se adquiere desde la aplicación). Crea trayectorias personalizadas para tu dron, seleccionando puntos de referencia GPS en la pantalla. ¡Pulsa el botón de despegue y contempla cómo tu dron hace el resto! El dron capturará vídeos increíbles con su modo de vuelo inteligente, con opción de establecer puntos de interés, lo que te permite centrar la sesión de vuelo en torno a un objeto determinado.

ACROBACIAS, RIZOS Y VIRAJES

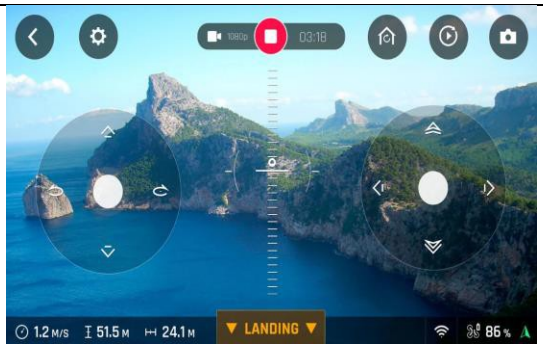
La aplicación FreeFlight Pro incluye otras opciones divertidas, como el botón táctil de vuelta mortal. Haz que tu dron Bebop voltee, vire y haga rizos con un solo toque en la pantalla de pilotaje.

Para consultar otros trucos, consejos y tutoriales de vuelo, visita la web Parrot.com antes de despegar. ¡Que disfrutes del viaje!

Capturas de pantalla



Compatibilidad de la aplicación



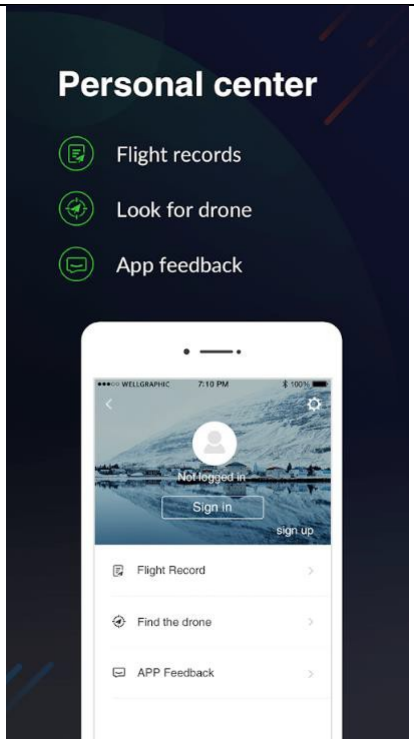
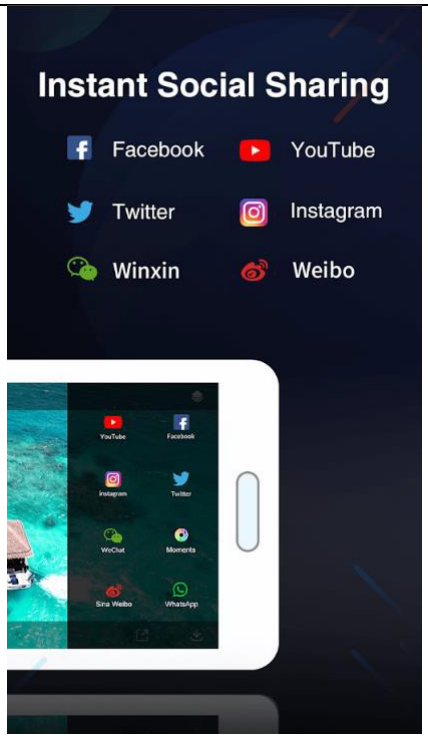
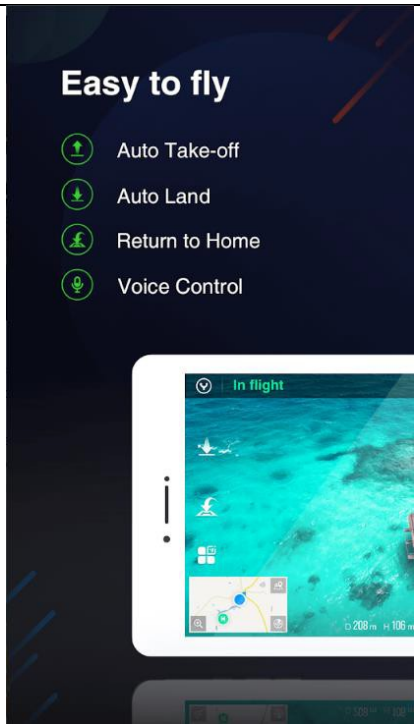
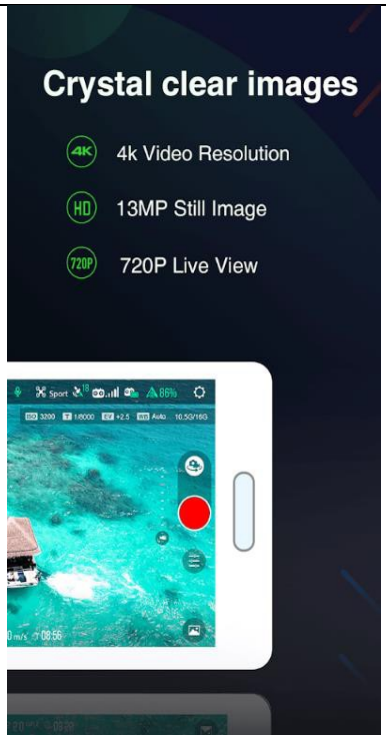
Aplicación usada como controlador de vuelo

	
Visión con las gafas Cockpit	

Cuadro 28 - Características de la aplicación Freeflight de Parrot

6.3.3 Aplicación móvil Yuneec

Nombre de la aplicación	Yuneec Pilot
Icono de la aplicación	
Fabricante	**Yuneec International Co., ltd**
Plataformas soportadas	iOS, Android
Descripción del fabricante La aplicación Yuneec Pilot se ha desarrollado específicamente para el dron Mantis Q, un modelo compacto y robusto con el que puedes hacer mucho más que captar momentos especiales con fotografías y vídeos 4K. El Mantis Q asegura la diversión gracias a su innovador control por voz, su modo deportivo rápido, sus modos de gran autonomía y vuelo automático, el práctico reconocimiento facial y la integración de redes sociales. Diseñado como un práctico compañero de viaje que puedes llevarte a cualquier lugar, es perfecto para los amantes de la naturaleza, los aficionados a la electrónica y los adictos a la adrenalina.	
Capturas de pantalla	

	
Pantalla de cuenta de usuario	Integración de redes sociales
	
Opciones de la aplicación	Opciones de la aplicación

Cuadro 29 - Características de la aplicación móvil Yuneec

6.3.4 Aplicación móvil Yuneec para la cámara del dron

Nombre de la aplicación	CG03
Icono de la aplicación	
Fabricante	**Yuneec International Co., ltd**
Plataformas soportadas	iOS, Android
Descripción del fabricante La aplicación CGO es una estación de control desde tierra para dispositivos Android y ofrece las siguientes funciones: regulación de exposición, ajuste de sensibilidad, balance de blancos, tiempo de obturación, etc. La aplicación CGO se encuentra en desarrollo. Para más información, visita nuestro sitio web: http://www.yuneec.com.	
Capturas de pantalla	
	
Pantalla principal de la aplicación	
	
Pantalla de ajustes de vídeo	

Cuadro 30 - Características de la aplicación para cámara Yuneec

Además, Yuneec permite acceder a la plataforma Android desde el visor del control remoto.

Figura 37 - Control remoto Yuneec

6.4 Nota sobre las ubicaciones del almacenamiento en los drones

Yuneec permite que el usuario almacene los datos generados en tres ubicaciones:

- Cardán de la cámara
- Dron
- Control remoto

Figura 38 - Ubicaciones de datos en el Yuneec Typhoon Q500 4K

En el ejemplo anterior, el dron podría incluir una tarjeta SD en la propia aeronave, en la cámara o en el control remoto. Por eso es fundamental comenzar inspeccionando detalladamente el dron y los dispositivos asociados, para asegurarse de que se localizan y analizan todos los soportes de información en la medida necesaria.

Además, cuando haya algún teléfono o tableta emparejado con el dron, podría haber datos en la aplicación asociada instalada en el terminal móvil.

7. HERRAMIENTAS HABITUALES EN EL ANÁLISIS FORENSE DE DRONES

El mercado de las herramientas para el análisis forense de drones está en pañales, y la mayoría de las aplicaciones comerciales forman parte de *suites* para el análisis general de evidencias móviles o informáticas. Las capacidades de esas herramientas pueden variar de un mes a otro, por lo que antes de elegir la aplicación idónea para extraer datos de un dron hay que buscar información sobre los fabricantes, los dispositivos soportados y los tipos de datos que pueden extraerse en cada caso.

7.1 Cellebrite/MSAB XRY/Oxygen/CFID

- Permite montar y efectuar un *parsing* de los datos de drones. Solo es apta para una selección limitada de modelos, pero es interesante utilizarla cuando sea posible, ya que simplifica el tratamiento de los drones y de los datos asociados. Se recomienda emplear como mínimo dos herramientas distintas para cerciorarse de verificar los datos extraídos.

7.2 CsvView y DatCon (http://datfile.net/)

- DatCon es una herramienta de código abierto que permite el *parsing* y la conversión de ficheros .dat de drones DJI a otros formatos, como .kml o .csv. Además permite traspasar ciertos datos, como los detalles de configuración y registros de sucesos, a un fichero de registro independiente.

- CsvView es una herramienta similar del mismo desarrollador, interesante para el *parsing* de registros. A pesar de su nombre, no se limita a los ficheros CSV y acepta registros .dat originales. Aunque estas dos aplicaciones son parecidas, tienen distintas características y opciones.

7.3 DRone Open source Parser (DROP) (https://github.com/unhcfreg/)

- La aplicación DROP ha sido desarrollada por Devon Clark y el Grupo de Formación e Investigación Forense sobre Drones de la Universidad de New Hampshire. Esta herramienta de código abierto puede emplearse para el *parsing* y la conversión de registros de vuelo procedentes de drones Phantom 3 de DJI. Además, ofrece un desglose parcial de la estructura de datos de los ficheros, gracias a una herramienta de ingeniería inversa de DatCon.

7.4 Google Earth Pro (https://www.google.co.uk/earth/versions/#download-pro)

- Permite transmitir datos en línea. Esta herramienta de cartografía puede utilizarse para visualizar datos de vuelo extraídos de registros. Se ha experimentado con éxito con ficheros CSV y KML.

7.5 ST2Dash y Dashware (https://github.com/ajpierson/st2dash; http://www.dashware.net/)

- Permite transmitir datos en línea.

- ST2Dash es una herramienta de código abierto pensada para convertir registros de vuelo y de controlador ST10+ y Q500 a un formato utilizable por Dashware. Dashware es una *suite* de edición gratuita que superpone datos de telemetría en grabaciones de vídeo. Las pruebas indican que es poco práctica para el uso forense, ya que la sincronización es laboriosa y no aporta información que no estuviera previamente disponible. Sin embargo, puede ser útil en algunas circunstancias.

7.6 DJI Assistant

- Esta herramienta puede utilizarse para adquirir datos de un dron DJI y para el *parsing* de registros de vuelo recuperados y su conversión a ficheros CSV.

7.7 FTK Imager

- Es útil para crear imágenes de tarjetas SD con fines de análisis. Nota: es preciso utilizar un bloqueador de escritura.

7.8 VLC Player

- Reproductor multimedia multifuncional que soporta diferentes *codecs* y formatos de vídeo. Puede utilizarse para visualizar los ficheros multimedia generados por el dron examinado.
- Dado que las tarjetas SD, tanto externas como internas, pueden estar en formato FAT32 o exFAT, es fácil analizarlas con *suites* de análisis forense, como FTK o Autopsy.

8. SITIOS WEB ÚTILES

Existen numerosos sitios web centrados en las características de los drones y en el análisis forense aplicado a los mismos. A continuación se indican algunas referencias que pueden ayudar a entender las peculiaridades de los drones:

Drone Forensics (https://www.droneforensics.com/)

El programa Drone Forensics tiene como objetivo identificar datos de utilidad forense presentes en drones comerciales o profesionales, como ayuda para investigaciones policiales y oficiales. El programa está a cargo de la compañía estadounidense VTO Inc., de Broomfield (Colorado).

Forensic Focus (https://www.forensicfocus.com/)

Este sitio web incluye foros muy activos sobre ciencia forense digital, así como información sobre las últimas novedades en este ámbito.

RPAS Forensic Validation Analysis Towards a Technical Investigation Process: A Case Study of Yuneec Typhoon H (Análisis forense de validación de aeronaves no tripuladas, orientado a la investigación técnica: Estudio de un Yuneec Typhoon H)

(https://www.mdpi.com/1424-8220/19/15/3246)

En este artículo se analizan imágenes de drones con ayuda de bases de datos de referencia para análisis forense (Computer Forensics Reference Datasets, CFReDS) y se presentan los resultados en el caso de un vehículo aéreo Typhoon H fabricado por la compañía Yuneec. Además se estudia la disponibilidad y la utilidad de las evidencias digitales para efectuar un tipo de investigación más práctico y capaz de evolucionar a partir de la experiencia.

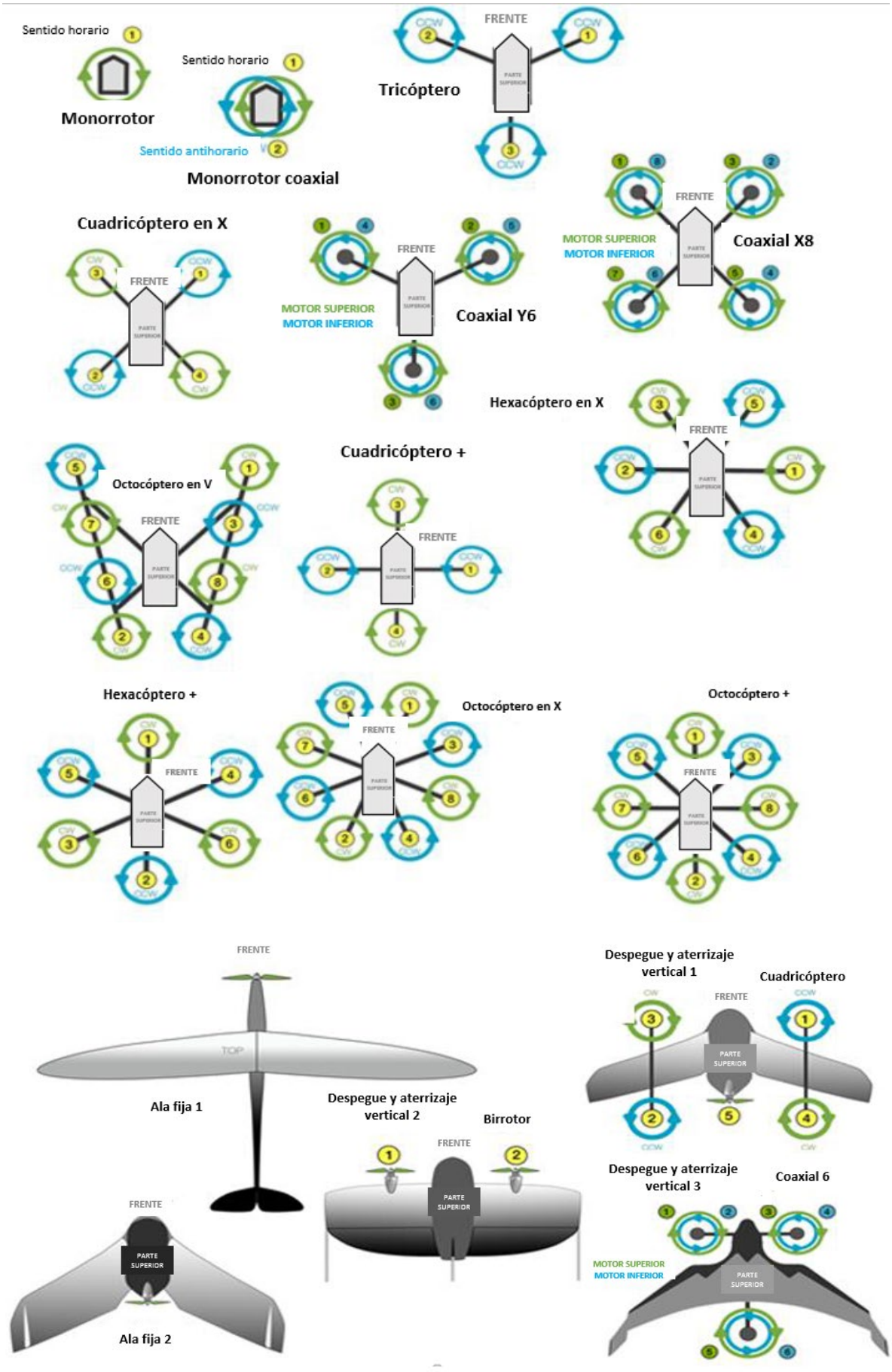
Organismos nacionales de aviación civil (https://www.icao.int/pages/links.aspx)

Directorio con detalles de todos los organismos nacionales de aviación. Puede ser interesante consultarlo cuando se deba investigar un incidente en el que haya un dron implicado.

Anexos

Anexo A: Tipos de drones

Tipo de dron	Ventajas	Inconvenientes	Uso habitual
Multirrotor 	• Accesibilidad • Facilidad de uso • Despegue y aterrizaje vertical y planeo • Buen control de cámara • Puede volar en espacios cerrados	• Duración de vuelo corta • Pequeña capacidad de carga útil	Inspección mediante fotografía y vídeo aéreos
Ala fija 	• Gran autonomía • Abarca zonas amplias • Rapidez de vuelo	• Precisa mucho espacio para el despegue y el aterrizaje • No admite despegue y aterrizaje vertical ni planeo • Para manejar los modelos no autónomos se requiere formación específica • Son caros	Entregas, cartografía aérea, inspección de oleoductos y tendidos eléctricos
Monorrotor 	• Despegue y aterrizaje vertical y planeo • Gran autonomía (alimentado con combustible) • Mayor capacidad de carga útil	• Más peligrosos • Manejo difícil, se requiere formación • Son caros	Exploración mediante láser (sistema LIDAR)
Híbrido de ala fija 	• Despegue y aterrizaje vertical y gran autonomía	• Imperfectos en el planeo y el vuelo hacia adelante • Aún en desarrollo	Entregas
Elios 	• Resistente a colisiones • Diseñado para interiores y espacios cerrados • Resistente al polvo y salpicaduras	• Caro	Inspección de espacios interiores o cerrados y acceso a zonas difíciles


Sentido horario
Monorrotor
Sentido horario
Sentido antihorario
Monorrotor coaxial
Tricóptero
FRENTE
Cuadricóptero en X
FRENTE
MOTOR SUPERIOR
MOTOR INFERIOR
Coaxial Y6
Coaxial X8
Hexacóptero en X
Octocóptero en V
Cuadricóptero +
Hexacóptero +
Octocóptero en X
Octocóptero +
Ala fija 1
Despegue y aterrizaje vertical 2
Birrotor
Despegue y aterrizaje vertical 1
Cuadricóptero
Despegue y aterrizaje vertical 3
Coaxial 6
Ala fija 2
PARTE SUPERIOR

Tipos de baterías usadas en los drones	
	
Baterías LiPo selladas	**Hobby**

Tipos de dispositivos de control		
		
Específico	**Mando acompañante**	**Mando acompañante perfeccionado**

Anexo B: Registro de actuaciones del equipo de primera intervención ante un incidente con drones

Actuaciones de los agentes

Registrar el incidente

Tomar vídeos o fotografías del vehículo en vuelo, incluidos los alrededores (p.ej., aglomeración de personas, zona construida, etc.).

Cualquier incursión en la zona restringida o de exclusión de vuelo de un aeropuerto, base militar, central nuclear, cárcel o área reservada debe considerarse una amenaza contra la seguridad pública.

Localizar al piloto

Lo más probable es que el piloto se encuentre en un lugar que le ofrezca una buena visibilidad y le permita mantener el control del dron. Por lo general manejará algún dispositivo con las dos manos (un mando convencional, una tableta o un teléfono inteligente) y estará pendiente de la aeronave; es decir, mirará hacia la aeronave, sin modificar su orientación. Puede estar quieto o caminar lentamente. Este tipo de actitudes pueden ayudar a diferenciarlo entre las personas que haya a su alrededor.

Abordar al piloto para averiguar lo siguiente:

¿Qué está haciendo?

¿Qué está grabando?

¿Dispone de la licencia necesaria para manejar el dron?

Determinar el tipo de infracción

Por ejemplo, puede tratarse de:

Alteración del orden público

Agresión

Daños criminales

Terrorismo

Obstrucción

Si considera que se está cometiendo algún delito, solicite al departamento responsable que se lleve al piloto fuera de la zona concurrida y hable con él.

Investigación preliminar
Determinar el punto desde el que despegó el dron y el punto donde aterrizó.
Cerrar el lugar de los hechos para evitar que el dron pueda causar daños a las personas.
Acceder al lugar del incidente y valorar los motivos de la presencia del dron.
Dron
¿De qué tipo es el dron? (multirrotor, ala fija...)
¿Aterrizó o cayó a tierra por accidente?
¿Está todavía en marcha?
¿Hay alguna carga útil?
¿Existen riesgos evidentes? (p. ej., peligro de explosión, hélices girando, carga útil no identificada...)
Operador / piloto
¿Se puede localizar al piloto del dron?
¿Sigue habiendo comunicación entre el control remoto y el dron?
¿El piloto obedece las indicaciones?
¿Se muestra cooperador?
¿Cuál es la utilización prevista del dron?

Cierre del lugar de los hechos

Fecha		
Hora		
Ubicación		
Coordenadas GPS	**Longitud**	**Latitud**
Verifique indicios de daños en el dron o señales de colisión en la zona circundante		
Notas		

Anexo C: Hoja de registro de incidente con dron

Hoja de registro de incidente con dron

Agente que interviene							
Tipo de dron							
Multirrotor		**Ala fija**		**Monorrotor**			
Otro							
Marca				**Modelo**			
¿Está en marcha el dron?	Sí		No				
Si desconecta el dron, indique el método utilizado							
Botón de apagado		**Retirada de batería**		**Otro**			
Fecha		**Hora**					
Condiciones climáticas (tiempo soleado, nublado, lluvia, viento...)							
Notas							

Esbozo del lugar de los hechos

(Indique dos puntos de referencia fijos y mantenga la escala)

¿Se han tomado fotografías del dron y de la zona circundante?					
Sí		**No**			
¿Se ha localizado al operador del dron?					
Sí		**No**			
¿Se ha localizado y recuperado equipamiento asociado al dron?					
Sí		**No**			
Equipamiento asociado					
Control remoto		**Teléfono móvil**		**Tableta**	
Baterías		**Tarjetas de memoria**		**Otros**	
Si "otros", detállese:					
Formulario cumplimentado por:		**Número de contacto**			
Firma					
Fecha		**Hora**			

Anexo D: Registro de examen de dron

Registro de examen de dron

Consideraciones para examinar un dron en un laboratorio forense digital
1. Los drones pueden almacenar información tanto en soportes internos como en tarjetas SD externas • La tarjeta SD interna puede contener registros de vuelo y puede requerir desmontaje de la aeronave • Para acceder a la memoria interna, en algunos casos puede crearse una imagen del dron mediante conexión USB. No obstante, en algunos drones no es posible usar bloqueo de escritura para obtener los datos de la memoria interna.
2. Los drones contienen datos de diferentes tipos en el propio dispositivo y en otros dispositivos conectados en red (control remoto, portátil, teléfono móvil, tableta, etc.) • Siga el procedimiento de adquisición adecuado para los dispositivos conectados en red • Recuerde los procedimientos forenses básicos para la adquisición de datos de dispositivos conectados a una red.
3. Al examinar drones o dispositivos conectados, siga los procedimientos necesarios para aislarlos de la red
4. Si no hay soportes extraíbles internos o externos, puede ser necesario acceder al chip de memoria *flash* del dispositivo.

Obtención inicial de evidencias / detalles del caso

Nombre e identificación del investigador	
Número de caso	
Organismo encargado de la investigación	

Estrategia del examen forense

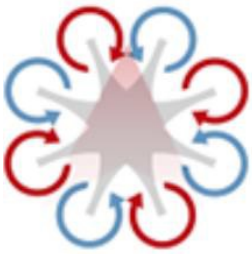
(Explique brevemente las pruebas que se realizarán con las evidencias recibidas en el laboratorio)

* Incluya una sinopsis de las actuaciones previstas, sin necesidad de detallar todos los pasos.

Evaluación inicial y descripción física de la muestra

Tipo de dispositivo examinado			
◯ **Aeronave no tripulada**	◯ **Dispositivo de control**	◯ **Teléfono**	◯ **Ordenador / otros**
Si “otros”, descríbalo.			
¿Se han obtenido los indicios biológicos? (material biológico, ADN, huellas dactilares, riesgos biológicos, etc.)	◯ **SÍ**	◯ **NO**	◯ **No aplicable**
¿En qué estado se encuentra el dispositivo examinado?	◯ **Dañado**	◯ **Modificado**	◯ **No se observan daños**
Si hay daños o modificaciones, descríbalos.			
¿Se ha fotografiado el dispositivo?	◯ **SÍ**	◯ **NO**	◯ **No aplicable**
Notas del responsable del examen (Use este apartado para registrar información no prevista en el cuadro)			

Notas de examen del dispositivo

Fabricante	
Tipo de dron (rodee con un círculo la imagen que corresponda)	 ☐  ☐  ☐  ☐  ☐  ☐  ☐ Otro: incluya dibujo
Nombre del modelo	
Color	
Número de serie o de pieza	

	Especifique la ubicación (cámara, dron, interior, visor, otro)	
¿Existe almacenamiento extraíble? (p. ej., tarjetas de memoria, unidades USB, discos duros)	Tipo de almacenamiento extraíble (micro-SD, SD, otro)	
	Capacidad tarjeta de memoria	
	Marca y número de serie	
¿Existen otros componentes con etiquetas o números de serie? (indíquelos más abajo, indicando los números de serie o de pieza)		

¿Se han fotografiado los componentes extraíbles?	☐ Sí	☐ No	☐ No aplicable
	Indique su ubicación (cámara, dron, interior, visor, otro)		
¿Existe almacenamiento extraíble? (tarjetas de memoria, unidades USB, discos duros)	Tipo almacenamiento extraíble (micro-SD, SD, otro)		
	Capacidad tarjeta memoria		
	Marca / número de serie		
¿Existen otros componentes con etiquetas o números de serie? (Indíquelos, junto con el número de serie o de pieza)			

¿Se han fotografiado los componentes extraíbles?	☐ Sí	☐ No	☐ No aplicable

Notas del responsable del examen

¿Qué tipos de herramientas forenses se usaron para la adquisición de datos? (Indique nombre y versión)		
¿Cómo se conectó el dispositivo a la herramienta forense para la adquisición de datos?	Cable ☐ Wi-Fi ☐	*Chip-off* ☐ JTAG/ISP ☐ Otro ☐
Fuente de la adquisición (tarjeta SD, memoria interna, microprocesador...)		
¿Cuánto duró la adquisición de datos?		

Notas de examen (Anote todos los valores obtenidos y los comportamientos observados durante la extracción)

Fecha de finalización del examen	
Hora de finalización del examen	
Firma	

Anexo E: Tarjeta de seguridad de las baterías LiPo

Seguridad de las baterías LiPo

- **Las baterías de litio deben manejarse con precaución porque un golpe o cortocircuito puede hacer que se incendien.**
- **Cuando no estén en uso o al cargarlas, introdúzcalas en una bolsa especial y mantenga la bolsa en un lugar protegido del fuego.**
- **Si una batería LiPo aumenta de volumen (se infla) o si no se cargan todas las celdas, descártela.**
- **Antes de deshacerse de una batería LiPo, hay que descargarla por completo conectándola a una carga resistiva (bombilla o función de carga y descarga).**
- **Es recomendable tener a mano un cubo de metal con arena por si se prende fuego en la batería.**
- **NO vierta agua sobre una batería LiPo en llamas, ya que el litio extraería oxígeno del agua y alimentaría el fuego.**
- **Las baterías de litio pueden tener un comportamiento imprevisible en caso de caída o durante la carga y descarga.**

Anexo F: Lista de comprobación del equipamiento básico para actuar ante un incidente con drones

En la siguiente lista se detalla el equipamiento básico del que debería disponer un laboratorio de análisis forense. Téngase en cuenta que esta lista no es exhaustiva y que algunos casos pueden requerir equipamiento adicional.

Nº	Artículo	
1	Ordenador portátil	☐
2	Aplicaciones de análisis y recuperación de datos de drones	☐
3	Aplicaciones de recuperación de datos	☐
4	Aplicaciones de análisis de dispositivos móviles	☐
5	Aplicaciones de obtención y análisis de imágenes	☐
6	Bolsa o caja de Faraday	☐
7	Cámara	☐
8	Precinto policial y materiales asociados	☐
9	Bloqueador de escritura	☐
10	Soportes vacíos para conservar los datos extraídos de las evidencias electrónicas analizadas, tanto a corto como a largo plazo: • Lápiz de memoria • Disco duro externo • Disco duro	☐
11	Conjunto de herramientas eléctricas y electrónicas	☐
12	Cable alargador	☐
13	Bolsa para baterías LiPo	☐

Anexo G: Competencias básicas de los equipos de primera intervención y los especialistas en análisis forense digital

A continuación se indican las competencias básicas recomendables para los agentes de la primera intervención encargados de tareas técnicas

1. Finalidad

Este apartado tiene como finalidad describir las competencias deseables para los agentes encargados de efectuar una intervención de nivel básico, de nivel técnico o de nivel técnico avanzado en el lugar de los hechos y para los profesionales de laboratorios forenses digitales que deban gestionar un incidente con drones.

Nivel de competencia	
BÁSICO	Agente de primera intervención no especializado
INTERMEDIO	Agente de primera intervención de nivel técnico
AVANZADO	Agente de primera intervención de nivel técnico avanzado
	Especialista en análisis forense de drones

2. Ámbito

Los destinatarios son los equipos de primera intervención sobre el terreno que deban manejar drones o dispositivos asociados. En el caso de que se emplee *hardware* o *software* para recuperar datos de drones, es recomendable seguir las buenas prácticas indicadas. Esta sección puede no ser aplicable al personal de laboratorio encargado de efectuar la recuperación forense del contenido del dron.

3. Definición

El análisis forense de drones es el empleo de metodología científica para recuperar los datos almacenados en un dron o en sus dispositivos asociados, como el control remoto o los móviles emparejados, con una finalidad policial.

4. Limitaciones

Los drones suponen un desafío importante para las fuerzas del orden porque se basan en una tecnología en rápida evolución. Actualmente existen innumerables modelos, y se calcula que cada tres o seis meses aparecen nuevas familias de drones. En muchos se utilizan sistemas operativos cerrados e interfaces exclusivas, lo que dificulta la extracción forense de evidencias digitales.

Los drones funcionan junto con otros dispositivos asociados, como un control remoto o un visor instalado en un móvil o una tableta. También pueden ser de interés las baterías o las tarjetas de memoria que se hayan utilizado con el dron.

Algunas de las dificultades que pueden presentarse:

Señales de entrada y salida: Hay que tratar de bloquear las señales de entrada y salida de los drones y los dispositivos asociados. Algunos de los métodos habituales son las cajas de bloqueo de radiofrecuencia o los equipos de interferencia. El bloqueo de las señales de radiofrecuencia puede agotar la batería, resulta caro y no siempre funciona, ya que podría alterar los datos del dron. Además, hay que cerciorarse de que el sospechoso no pueda borrar información a distancia.

Cables: Los cables de comunicación de datos suelen ser específicos para cada modelo de dron. Además, a menudo las herramientas forenses requieren un cable específico. Los cables de datos pueden incluir diferentes conexiones (RJ-45, USB, RS-232). Todo ello implica que el análisis forense de drones requiera un gran número de cables distintos.

Destrucción de los datos: Existen sistemas que permiten destruir los datos de un dron tanto localmente como a distancia.

Drivers (controladores): Puede haber conflictos entre *drivers* del sistema operativo, *drivers* exclusivos del fabricante y versiones de distintos comercializadores, por lo que puede ser difícil elegir el adecuado. Los *drivers* pueden estar incluidos en la herramienta utilizada o descargarse desde un sitio web. Cuando se utiliza más de una herramienta de análisis forense, puede haber competencia entre los *drivers* aplicados a un mismo recurso.

Carácter dinámico de los datos: Los datos contenidos en un dron en activo (conectado) varían constantemente, y en este caso no funcionan los métodos de bloqueo de escritura convencionales.

Cifrado: Puede ser que los datos se almacenen en forma cifrada para impedir que sean analizados.

Equipamiento: Es posible que el equipamiento disponible no sea la versión más reciente, por los requisitos de verificación previa de *hardware*, *firmware* y *software* vigentes en el organismo encargado del examen.

Análisis sobre el terreno: Los equipos de primera intervención deben ser conscientes de los riesgos asociados al *triage* de drones. El *triage* no se considera un examen completo, y es preciso proteger el dron para asegurar el examen posterior.

Estado de la evidencia: Las herramientas comerciales pueden no ser útiles para manejar drones que hayan sufrido un daño físico.

Valores *hash*: Normalmente, en objetos digitales (ficheros gráficos, de audio o vídeo) debe haber una coherencia entre la estación de trabajo forense y el valor *hash* obtenido por la aplicación del dron. Dada la inestabilidad de los sistemas operativos de los drones, por lo general no hay coherencia entre los valores *hash* de los ficheros del caso, debido a la optimización de los ficheros de sistema.

Estándares industriales: Los fabricantes de drones no emplean un método normalizado para el almacenamiento de datos (pueden usar sistemas operativos cerrados o conexiones exclusivas).

Pérdida de potencia: Muchos drones pueden perder datos o alterarlos o iniciar medidas de seguridad adicionales cuando su batería se descarga o se apaga.

Tarjetas extraíbles: Es arriesgado tratar este tipo de tarjetas dentro del propio dron (puede que no se obtenga la totalidad de los datos, incluidos los datos borrados, o que se alteren las marcas de fecha y hora).

Formación: Los profesionales encargados de copiar la información de un dron o los dispositivos asociados deben haber recibido formación específica para asegurar la integridad de los datos.

Datos sin asignar o borrados: Muchas herramientas de análisis forense de drones solamente permiten efectuar una adquisición lógica. En cambio, para obtener los datos borrados puede ser necesaria una adquisición física.

Dispositivos asociados: Para utilizar las funciones de un dron se requiere un dispositivo de control o un visor remoto, y estos dispositivos no siempre están presentes en el lugar de los hechos. Además, el dron podría haber llevado baterías y tarjetas de memoria que quizá no aparezcan en las inmediaciones.

Anexo H: Competencias básicas de los agentes de primera intervención

A continuación se indican las competencias básicas recomendables para los agentes de primera intervención encargados de efectuar tareas técnicas

Los agentes encargados de la primera intervención pueden tener la responsabilidad de recopilar y efectuar un examen básico de los drones. Existen tres niveles de capacitación:

Nivel 1: Agentes de primera intervención no especializados, que recopilan y/o examinan manualmente drones y dispositivos asociados.

Nivel 2: Agentes de primera intervención de nivel técnico, que utilizan una herramienta o aplicación para extraer datos del dron o el dispositivo asociado. Para emplear herramientas básicas de descarga o extracción de datos de drones y dispositivos asociados se requiere haber cursado una formación específica.

Nivel 3: Agentes de primera intervención de nivel técnico avanzado, que utilizan herramientas o aplicaciones avanzadas para extraer datos del dron y los dispositivos asociados. Para emplear herramientas avanzadas de descarga o extracción de datos de drones y dispositivos asociados se requiere haber cursado una formación específica.

La rama de la ciencia forense aplicada a los drones y dispositivos asociados está aún en evolución y presenta algunos elementos en común con la informática forense tradicional.

El profesional encargado debe tener nociones generales de análisis forense digital y mantenerse al día mediante la lectura de revistas especializadas, la asistencia a cursos, la participación en asociaciones, la formación continuada o en el lugar de trabajo y la experiencia práctica.

Los profesionales encargados de examinar drones deben respetar las pautas y los procedimientos operativos normalizados, así como un código deontológico que asegure la neutralidad del proceso.

Los casos asignados pueden requerir diferentes niveles de especialización, y las personas encargadas del examen deben disponer del nivel de formación adecuado.

Niveles de análisis: El nivel del análisis depende de la petición y de las características específicas de la investigación. Los niveles de análisis más elevados requieren un tipo de examen más exhaustivo.

Anexo I: Competencias básicas de los agentes de primera intervención no especializados

A continuación se indican las competencias básicas recomendables para los agentes de primera intervención no especializados

1. Capacidad para identificar las configuraciones básicas de los drones
    a. Saber identificar tipos de drones y aeronaves no tripuladas
    b. Conocer los procedimientos de desconexión apropiados para los drones y los dispositivos asociados
2. Aplicar precauciones de seguridad en el lugar del incidente: saber cómo cerrar la zona
    a. Lugar de los hechos
3. Interrogar a testigos y sospechosos
4. Procedimientos de neutralización
5. Entender cómo proteger las evidencias: recopilar, manejar y embalar
    a. Tomar fotografías del lugar de los hechos
    b. Asignar números a las evidencias y etiquetarlas
    c. Embalar adecuadamente las evidencias
6. Mantener la cadena de custodia
7. Conocer el marco jurídico aplicable

Anexo J: Competencias básicas de los agentes de primera intervención de nivel técnico

A continuación se indican las competencias básicas recomendables para los agentes de primera intervención de nivel técnico

En la siguiente lista se detallan las competencias mínimas que debe tener un agente de primera intervención de nivel técnico, encargado de analizar manualmente un dron sobre el terreno con ayuda de herramientas específicas.

- Todas las competencias indicadas para los agentes de primera intervención no especializados, y además:

1. Conocer la manera adecuada de recopilar, etiquetar, preservar y embargar preventivamente evidencias.
2. Entender las consecuencias y los riesgos asociados al contacto con el dron.
3. Entender que colocar una tarjeta de memoria en diferentes ordenadores, móviles o drones puede modificar los datos contenidos.
4. Entender que la retirada o sustitución de una batería pude causar un reinicio del dron.
5. Conocer la jurisprudencia y las autoridades competentes.
6. Identificar los siguientes tipos de drones: multirrotor y ala fija.
7. Entender la importancia de documentar adecuadamente el lugar de los hechos.
8. Conocer el procedimiento de embargo preventivo adecuado para drones y dispositivos asociados.
9. Entender la necesidad y la importancia de verificar los datos extraídos del dron y los dispositivos asociados.
10. Conocer las posibilidades de los dispositivos asociados, como el control remoto o el móvil empleado para visualizar las grabaciones del dron.
11. Manejar adecuadamente las baterías del dron para conservarlas en condiciones de seguridad, sin riesgo de explosión o fuga de líquido.
12. Conocer los riesgos biológicos que pueden presentar los drones y los dispositivos asociados.
13. Determinar si es necesario tomar indicios biológicos, tales como huellas dactilares, ADN, etc.

Anexo K: Competencias básicas de los agentes de primera intervención de nivel técnico avanzado

A continuación se indican las competencias básicas recomendadas para los agentes de primera intervención de nivel técnico avanzado

En la siguiente lista se indican las competencias mínimas requeridas para los agentes de primera intervención que utilicen herramientas de análisis avanzado para examinar un dron o un dispositivo asociado. Un ejemplo del nivel 2 sería un agente u oficial de patrulla que disponga de la debida formación y utilice una aplicación o un dispositivo de *hardware* para descargar datos de un dron o un dispositivo asociado.

Entre otras tareas, estos agentes pueden ocuparse de efectuar un examen lógico o de los ficheros de sistema mediante aplicaciones o dispositivos específicos para la adquisición de datos contenidos en el dron y accesibles para el sistema o el usuario: registros de vuelo, posiciones de base, telemetría, credenciales de usuario, fotografías, vídeos, audios, datos de aplicaciones, información del dispositivo.

Todas las competencias recomendadas para los agentes de primera intervención no especializados y para los agentes de primera intervención de nivel técnico, y además:

1. Conocer los principales acrónimos utilizados para describir los componentes y las funciones de los drones.
2. Identificar los siguientes tipos de drones: multirrotor y ala fija.
3. Identificar qué información puede estar almacenada en un dron o dispositivo asociado.
4. Identificar qué información puede estar almacenada en una tarjeta de memoria.
5. Identificar otras ubicaciones donde pueda haber información almacenada.
6. Entender las cuestiones legales relacionadas con los drones (alcance de la orden de actuación, consentimiento, jurisprudencia, licencias, requisitos de certificación...)
7. Capacidad para aislar el dron de la señal de mando mediante una desconexión del dron, utilizando blindaje de radiofrecuencias o desactivando las comunicaciones de radio.
8. Capacidad para explicar las ventajas e inconvenientes de desconectar el dron.
9. Describir los métodos y las herramientas necesarios para tratar un dron o un dispositivo asociado.
10. Conocer las funcionalidades de las herramientas, sus limitaciones y la posible necesidad de exámenes adicionales (p. ej., el volcado lógico de datos podría no ser suficiente para recuperar datos borrados en el dron, el controlador o la tarjeta de memoria).
11. Entender la necesidad de experimentar, mantener y validar las herramientas empleadas.
12. Conocer las buenas prácticas aplicables al examen de drones.
13. Entender que algunas aplicaciones o dispositivos de extracción podrían no ser útiles para obtener los datos de tarjetas de memoria.
14. Capacidad para defender en un tribunal la utilización de las herramientas escogidas.

Glosarios

Perspectiva general

1.1 Téngase en cuenta que la terminología relativa a las aeronaves no tripuladas está aún en evolución, por lo que el presente Glosario no es exhaustivo ni definitivo. En la lista indicada a continuación se combinan definiciones de la Organización de la Aviación Civil Internacional (OACI), expresiones de "uso habitual" que se consideran alternativas aceptables y una serie de términos obsoletos. Aunque los términos obsoletos todavía son reconocibles, para asegurar un vocabulario común se recomienda ceñirse a la terminología aceptada.

1.2 En la lista también se incluyen algunos términos de uso militar, recogidos en las publicaciones normativas de la Autoridad de Aviación Militar. Estos términos (señalados con un asterisco*) no son necesariamente aplicables a las aeronaves no tripuladas que se rigen por la normativa civil.

NOTA: Los términos "piloto" y "piloto remoto" se están utilizando cada vez más en todo el mundo (incluso en la OACI) para referirse a la persona que controla directamente una aeronave no tripulada, y esta tendencia se refleja en el presente documento. No obstante, cabe señalar que, en el caso del Reino Unido, la Orden de navegación aérea de 2016 estipula una serie de requisitos jurídicos aplicables a un "piloto". De acuerdo con ello, el término solo se aplica a pilotos en el sentido tradicional: esto es, personas que se encuentren a bordo de la aeronave. En estos momentos, la ley no establece ningún requisito específico para controlar una aeronave no tripulada; es una labor pendiente.

Glosario I: Abreviaciones de aviación generales

Abreviaciones habituales aplicables a drones

AAIB	Air Accidents Investigation Branch	dependencia de investigación de accidentes aéreos
ACAS	Airborne Collision Avoidance System	sistema anticolisión de a bordo
AIP	Aeronautical Information Publication	publicación de información aeronáutica
ANO	Air Navigation Order	orden de navegación aérea
ANSP	Air Navigation Service Provider	proveedor de servicios de navegación aérea
AOA	Aircraft Operating Authority*	autoridad de operación de aeronaves*
ATC	Air Traffic Control	control del tránsito aéreo
ATM	Air Traffic Management	gestión del tránsito aéreo
ATS	Air Traffic Service	servicios de tránsito aéreo
ATSU	Air Traffic Service Unit	unidad de servicios de tránsito aéreo
BRS	Ballistic Recovery Systems	sistemas de recuperación balística
BVLOS	Beyond Visual Line of Sight	más allá del alcance visual
CAA	Civil Aviation Authority	autoridad de aviación civil
CFT	Certificate for Flight Trials	certificado para vuelos de prueba
CPL	Commercial Pilot Licence	licencia de piloto comercial
CRM	Crew Resource Management	gestión de recursos de la tripulación
C-UAV (C-UAS)	Counter Unmanned Aircraft Vehicle (System)	contra vehículos (sistemas) aéreos no tripulados
DA	Danger Area	zona de peligro
DAP	Directorate of Airspace Policy	Dirección de políticas sobre espacio aéreo
EASA	European Aviation Safety Agency	Agencia Europea de Seguridad Aérea (AESA)
ERF	Emergency Restriction of Flying	restricción de vuelos por emergencia
EVLOS	Extended Visual Line of Sight	alcance visual ampliado
FAA	Federal Aviation Administration	Administración Federal de Aviación
FIR	Flight Information Region	región de información de vuelo
FISO	Flight Information Service Officer	oficial de servicios de información de vuelo
FMC	Flight Management Computer	ordenador de gestión de vuelo
FOP	Flight Operations Policy	política de operaciones de vuelo

FRTOL	Flight Radio Telephony Operators' Licence	licencia de operador de radiotelefonía de vuelos
GCS	Ground Control Station	estación de control terrestre
HALE	High Altitude Long Endurance	gran altitud y gran autonomía
HMI	Human-Machine Interface	interfaz persona-máquina
ICAO	International Civil Aviation Organization	Organización de la Aviación Civil Internacional (OACI)
IFR	Instrument Flight Rules	reglas de vuelo por instrumentos
JAA	Joint Aviation Authority	autoridades conjuntas de aviación
MAA	Military Aviation Authority	autoridad de aviación militar
MALE	Medium Altitude Long Endurance	altitud media y gran autonomía
MoD	Ministry of Defence	Ministerio de Defensa
MOR	Mandatory Occurrence Reporting	sistema de notificación obligatoria de sucesos
MRP	MAA Regulatory Publication(s)	publicaciones reguladoras de la autoridad de aviación militar
MTOM	Maximum Take-off Mass	masa máxima al despegue
NAA	National Aviation Authority	autoridad aeronáutica nacional (AAN)
NAS	National Airspace	espacio aéreo nacional
NOTAM	NOtice To AirMen	aviso para aviadores
RA(T)	Restricted Area (Temporary)	zona (temporalmente) restringida
RCS	Radar Cross Section	sección equivalente de radar
RPA	Remotely Piloted Aircraft	aeronave pilotada a distancia
RPAS	Remotely Piloted Aircraft System Remotely Piloted Air System*	sistema de aeronave pilotada a distancia sistema aéreo pilotado a distancia*
RPAS Cdr	Remotely Piloted Air System Commander*	comandante de sistema aéreo pilotado a distancia*
RPS	Remote Pilot Station	estación de pilotaje a distancia
RTF	Radiotelephony	radiotelefonía
RTS	Release to Service	aptitud para el servicio
SARPs	Standards and Recommended Practices	normas y métodos recomendados
SRG	Safety Regulation Group	grupo de reguladores de seguridad
SSR	Secondary Surveillance Radar	radar secundario de vigilancia
SUA	Small Unmanned Aircraft	pequeña aeronave no tripulada
SUAS	Small Unmanned Aircraft System	pequeño sistema de aeronave no tripulada

SUSA	Small Unmanned Surveillance Aircraft	pequeña aeronave de vigilancia no tripulada
TCAS	Traffic Collision Avoidance System	sistema anticolisión y de vigilancia del tránsito
TDA	Temporary Danger Area	zona de peligro temporal
UA	Unmanned Aircraft	aeronave no tripulada
UAS	Unmanned Aircraft System(s)	sistema de aeronave no tripulada
UAS-p	UAS Pilot (legacy term)	piloto de aeronave no tripulada (término obsoleto)
UAV	Unmanned Aerial Vehicle(s) (legacy term)	vehículo aéreo no tripulado (término obsoleto)
UAV-p	UAV Pilot (legacy term)	piloto de vehículo aéreo no tripulado (término obsoleto)
UIR	Upper Flight Information Region	región superior de informaciones de vuelo
VFR	Visual Flight Rules	reglas de vuelo visual
VLOS	Visual Line of Sight	alcance visual

En las páginas siguientes figuran explicaciones más detalladas de estos términos.

Glosario II: Abreviaciones técnicas

Abreviaciones técnicas habituales

ACC	Accelerometer	acelerómetro
AUW	All Up Weight	peso total en carga
ARTF	Almost Ready to Fly	casi listo para volar
AH	Altitude Hold	mantenimiento de altura
mAh	milliamp Hours.	miliamperio-hora
Rx	Receive (as in receive radio signal)	recepción (de señal de radio)
Tx	Transmit (as in transmit radio signal)	transmisión (de señal de radio)

Glosario III: Glosario de análisis forense de drones

Terminología habitual en ciencia forense digital

A		
Acquisition	adquisición	Véase "imagen"
Archive Copy	copia de archivo	Copia de los datos ubicados en un soporte apto para el almacenamiento a largo plazo, a partir de la cual pueden obtenerse sucesivas copias de trabajo.
Archive Image	imagen de archivo	Cualquier imagen ubicada en un soporte apto para el almacenamiento a largo plazo, obtenida duplicando bit a bit los datos originales contenidos en un soporte de almacenamiento a largo plazo.
Authentication	autenticación	Proceso por el que se verifica que unos datos constituyen una representación exacta de lo que pretenden reflejar.
C		
Capture	captura	Proceso de grabación de datos tales como imágenes, secuencias de vídeo o detalles de vuelo.
Chain of Custody / Continuity	cadena de custodia / continuidad	Documentación cronológica de los movimientos, ubicaciones y posesión de las evidencias.
Copy	copia	Reproducción precisa de información.
D		
Data	datos	Información en formato analógico o digital que puede ser transmitida o tratada.
Data Analysis	análisis de datos	Evaluación de la información contenida en un soporte.
Data Extraction	extracción de datos	Proceso que identifica y recupera información que podría no ser visible de manera inmediata.
Data Smear	emborronamiento de datos	Modificación de los datos mediante un sistema en activo durante el proceso de adquisición.
Digital Evidence	evidencia digital	Información de valor probatorio que está almacenada o transmitida en forma binaria.

Directory Listing	lista de directorio	Lista de los ficheros contenidos en un objeto. Puede contener otra información, como el tamaño o la fecha de los ficheros.
Downloading / Exporting	descarga / exportación	Proceso de recuperación de datos digitales, audios, vídeos e imágenes fijas y datos de transacciones. Puede ser en formato nativo o exclusivo o en formato abierto.
E		
Erased File Recovery	recuperación de borrados	Proceso de recuperación de ficheros borrados
Extraction	extracción	Método de exportación de datos desde una fuente (p. ej., copiar datos de una previsualización EnCase, volcado de datos de un teléfono móvil). Véase “extracción de datos”.
F		
File Format	formato de fichero	Estructura en la que se organizan los datos de un fichero
File Slack	espacio sobrante	Espacio situado entre el final lógico de un fichero y el final de la última unidad de almacenamiento del fichero. En el sistema FAT, espacio situado entre el final lógico del fichero y el final del clúster.
Forensic	ciencia forense	Aplicación del conocimiento forense a una cuestión jurídica, en especial en relación con la investigación de un delito.
Forensic Cloning	clonación forense	Proceso de creación de un duplicado bit a bit de los datos disponibles, de un soporte físico a otro.
G		
GeoTag	geoetiqueta	Coordenadas GPS añadidas como metadatos a los ficheros
GPX	GPX	Formato de intercambio GPS. Esquema XML diseñado como formato GPS común para aplicaciones informáticas.
H		
Hash or Hash Value	*hash* o valor *hash*	Valores numéricos generados mediante funciones específicas, para certificar la integridad de evidencias digitales y/o efectuar comparaciones de inclusión o exclusión con conjuntos de valores conocidos.
I		
Integrity Verification	verificación de la integridad	Proceso empleado para confirmar que los datos presentados son completos y no se han alterado desde el momento de la adquisición.

L		
Log File	fichero de registro	Registro de actuaciones, sucesos y datos relacionados.
Logical Acquisition / Copy	copia / adquisición lógica	Reproducción exacta de la información contenida en un volumen lógico (volumen montado, asignación de unidad lógica, etc.).
M		
Media	soporte	Objeto en el que pueden almacenarse datos
Meta Data	metadatos	Datos, usualmente integrados en un fichero, que describen un fichero o directorio; pueden incluir las ubicaciones del almacenamiento de contenidos, marcas de fecha y hora, datos de aplicaciones y permisos.
Mobile Device	dispositivo móvil	Dispositivo portátil con una determinada estructura de sistemas, capacidad de procesamiento y memoria incorporada, que también puede tener capacidades de telefonía
Mobile Phone Forensics	análisis forense de teléfonos móviles	Utilización con fines jurídicos de metodología científica para recuperar los datos almacenados en un teléfono móvil.
Multimedia Evidence	evidencia multimedia	Soporte analógico o digital, que puede consistir en película, cinta, soporte magnético u óptico, y/o la información que contiene.
N		
Native File Format	formato nativo	Formato original de un fichero. Un fichero creado con una aplicación puede ser leído con otras aplicaciones, pero el formato nativo es el que le adjudicó la aplicación con la que se creó. En muchos casos, los atributos específicos de un fichero (por ejemplo, las fuentes de un documento) solo pueden modificarse cuando el fichero se abre con el programa utilizado para su creación.
P		
Password Recovery	recuperación de contraseñas	Proceso de localización e identificación de una serie de caracteres empleada para restringir el acceso a la información.
PCB	PCI	Placa de circuito impreso. En electrónica, puede referirse a la placa sola o acompañada de componentes.
Peer Review / Technical Review	revisión por pares / revisión técnica	Evaluación de informes, notas, datos, conclusiones y otros documentos, realizada por un segundo profesional cualificado.
Physical Copy	copia física	(c) Reproducción exacta de la información contenida en un dispositivo físico.

Physical Image/Acquisition	imagen / adquisición física	(c) Duplicado bit a bit de los datos contenidos en un dispositivo.
Pixel	píxel	Elemento visual, componente mínimo de una imagen que puede ser tratado individualmente en un sistema de imágenes electrónicas [*The Focal Encyclopedia of Photography*, 4ª edición, 2007].
Playback	reproducción	Visualización y escucha de material registrado por medio de una cámara, casete u otro dispositivo.
Preview	previsualización	(c) Subproceso de *triage* en el que se revisan elementos para evaluar la necesidad de obtener o seguir examinando imágenes.
Primary Image	imagen primaria	Se refiere a la primera vez en la que se registra una imagen en un soporte que constituye un objeto identificable e independiente. Por ejemplo, imagen digital registrada en una tarjeta *flash* o descargada de Internet.
Processed Image	imagen tratada	Cualquier imagen que haya pasado por un proceso de mejoramiento, restauración u otra operación.
Proficiency test	prueba de aptitud	Prueba para evaluar a los analistas, el personal técnico de apoyo o el rendimiento general de un organismo (*se incluyen cuatro ejemplos*): 1. **Prueba abierta**: los analistas o el personal técnico saben que están siendo evaluados. 2. **Prueba ciega**: los analistas o el personal técnico no saben que están siendo evaluados. 3. **Prueba interna**: realizada por el propio organismo. 4. **Prueba externa**: realizada por un organismo independiente del organismo evaluado.
Proprietary File Format	formato propietario	Cualquier formato de fichero que sea exclusivo de un fabricante o producto concretos.
Q		
Quality Assurance	aseguramiento de calidad	Actuaciones sistemáticas y planificadas, necesarias para tener la seguridad de que el producto o servicio de un laboratorio u organismo satisface los requisitos de calidad establecidos.
R		
Reconstruction	reconstrucción	Proceso de reparación de soportes dañados, con miras a recuperar los datos.
Reference Materials	materiales de referencia	Elementos tales como documentación publicada, manuales de *hardware* o *software*,

		conjuntos de valores *hash*, series de encabezamientos, etc.
Reliability	fiabilidad	Grado en que se puede confiar en la información.
Reproducibility	reproducibilidad	Grado en el que un proceso puede arrojar los mismos resultados en pruebas repetidas.
Residue	residuo	(c) Datos contenidos en el espacio sin asignar o en el espacio sobrante. (a) El residuo de una señal filtrada es la diferencia algebraica entre la salida del filtro y la entrada [*Diamond Cut Users Manual*].
Resolution	resolución	Acción, proceso o capacidad de distinguir entre dos partes o estímulos separados pero adyacentes, tales como elementos de detalle de una imagen o colores similares [tomado de *Encyclopedia of Photography,* 3ª edición].
S		
Source Code	código fuente	Lista de instrucciones escritas en un lenguaje de programación y utilizadas para construir un programa de *software*.
Storage Media	soporte de almacenamiento	Cualquier objeto en el que se conservan datos.
T		
Technical/Peer Review	revisión técnica/por pares	Evaluación de informes, notas, datos, conclusiones u otros documentos, realizada por un segundo profesional cualificado
Timeline Sequence Reconstruction	reconstrucción de secuencia cronológica	Proceso de relacionar entre sí imágenes, audios u otros datos, en una sucesión ordenada cronológicamente.
Track Log	registro de seguimiento	Lista completa de los puntos de seguimiento creados por un dispositivo GPS.
Triage	*triage* o muestreo	Proceso por el que se determinan prioridades o se ordenan los elementos susceptibles de recopilación o análisis.
U		
Unallocated Space	espacio sin asignar	En un ordenador, zonas disponibles para el almacenamiento de datos. Puede haber contenido previamente almacenado. También se conoce como “espacio libre”.
V		
Validation	validación	Proceso de realización de una serie de experimentos para establecer la eficacia y fiabilidad de una herramienta, una técnica o un procedimiento y su posible modificación.

Validation Testing	experimento de validación	Evaluación para determinar si una herramienta, técnica o procedimiento funcionan correctamente y cumplen lo previsto
Verification	verificación	1. Proceso de confirmación de la exactitud con que un elemento refleja el original. 2. Confirmación de que una herramienta, técnica o procedimiento funcionan como se espera.
Video	vídeo	Representación electrónica de una secuencia de imágenes que reflejan escenas fijas o en movimiento. Puede incluir audio.
W		
Waypoint	punto de referencia	Ubicación almacenada por un dispositivo GPS a partir de la interacción con el usuario.
Work Copy	copia de trabajo	Copia o duplicado de una grabación o de datos, que pude utilizarse para el ulterior tratamiento o análisis.
Write Block / Write Protect	bloqueo / protección contra escritura	Métodos de *hardware* o *software* que impiden la modificación del contenido de un soporte.

Nota: Las definiciones anteriores proceden de la versión 3.0 (23 de junio de 2016) del glosario sobre evidencias digitales y multimedia elaborado por el Grupo de Trabajo Científico sobre Evidencias Digitales.

Glosario IV: Glosario de aeronaves no tripuladas

Terminología habitual sobre aeronaves no tripuladas

0-9		
2.4GHz	2,4 GHz	Frecuencia utilizada en las comunicaciones de radio digitales (espectro ensanchado) de nuestras aplicaciones, que incluyen radiocomunicación en 2,4 Ghz, Bluetooth y algunos equipos de transmisión de vídeo. Se trata de una banda distinta de la de 72 Mhz empleada tradicionalmente para las comunicaciones de radio analógicas. Para evitar un conflicto de frecuencias, es conveniente emplear equipos de radio de 72 Mhz cuando se empleen transmisores de vídeo de 2,4 GHz a bordo, o emplear vídeo de 900 Mhz cuando se empleen equipos de radio RC de 2,4 GHz. La transmisión en 2,4 GHz es habitual en la franja de frecuencias sin licencia.
3D Mapping	cartografía 3D	Paquete de *software* que permite crear mapas en 3D desde el dron y cartografiar zonas extensas de manera rápida y eficaz. Lo utilizan agricultores para mejorar la rotación de cultivos y compañías de seguros para valorar daños en edificios sin correr riesgos directos. Las empresas forestales pueden usarlo para supervisar la distribución de la cúpula arbórea, y los arquitectos para cartografiar en 3D la topografía de un emplazamiento de obra.
5.8GHz	5,8 GHz	La franja de 2,4 GHz se usa habitualmente en microondas, Bluetooth, drones, etc. Por ello, situar un dron en esta franja puede implicar distorsiones por otros dispositivos inalámbricos o drones. La transmisión en 5,8 GHz suele es habitual en la franja sin licencia.
A		
Accelerometer (ACC)	acelerómetro	Dispositivo que mide las fuerzas de aceleración en una dirección concreta. Se usa para estabilizar cuadricópteros en condiciones de viento.
ACRO Mode	modo ACRO	También conocido como modo acrobático o “Rate”, cuando el control remoto se emplea para controlar la velocidad angular del dron. Se usa sobre todo para llevar a cabo vueltas mortales y alabeos.
Ascent Speed	velocidad ascendente	Velocidad con la que el dron asciende en el aire. Por ejemplo, el Wind 4 tiene una velocidad ascendente de 4 metros por segundo (m/s).
ATTI Mode	modo ATTI	Modo de posición de vuelo: En este modo, el dron mantiene su altitud gracias a la presión barométrica, sin emplear GPS o Glonass para estabilizar la posición. Por ello, si el dron es arrastrado por el viento, probablemente no podrá mantener la misma posición y habrá que reajustar la trayectoria de vuelo.

Aircraft ***(ICAO)***	aeronave (OACI)	Toda máquina que puede sustentarse en la atmósfera por reacciones del aire que no sean las reacciones del mismo contra la superficie de la tierra.
Airframe	fuselaje	El fuselaje es la estructura física de la aeronave no tripulada, necesaria para lograr un vuelo controlado.
All Up Weight (AUW)	peso total en carga	Peso total de la aeronave, incluidas las baterías y otras piezas.
Almost Ready to Fly (ARTF)	casi listo para volar	También conocido como ARA: conjunto que contiene todos los componentes necesarios pero puede requerir el montaje del dron. Normalmente, no está incluido el receptor.
Altitude Hold (AH)	mantenimiento de altitud	Mantenimiento de la altitud del dron, por medio de un sensor-altímetro barométrico.
Auto Levelling	autonivelado	Modo de vuelo que permite que la aeronave se mantenga nivelada, gracias al acelerómetro o giroscopio.
Autonomous Aircraft	aeronave autónoma	Aeronave no tripulada que no requiere la intervención del piloto para gestionar el vuelo. Es una subcategoría de las aeronaves no tripuladas.
Autonomous Flight	vuelo autónomo	Trayectoria de vuelo orientada mediante puntos de referencia de GPS.
Autonomous Operation	operación autónoma	Operación en la cual una aeronave no tripulada funciona sin que el piloto intervenga directamente en el manejo.
B		
Barometric Altimeter (BARO)	altímetro barométrico	Sensor medidor de altitud que utiliza la presión barométrica, al igual que el transmisor: controla el vuelo del dron o cuadricóptero desde tierra.
Battery	batería	En los drones se utilizan diversos tipos de baterías. Puede usarse una batería integrada o una batería de tipo cartucho para alimentar el controlador de vuelo, el receptor o el transmisor de vídeo.
BeiDou	BeiDou	Sistema chino de navegación basado en dos constelaciones de satélites.
Bind	enlace	Procedimiento para asociar el dispositivo de control al dron.
Bind aNd Fly (BNF)	enlazar y volar	Los productos *Bind-N-Fly* llevan todo lo necesario para controlar el dron, excepto el transmisor. Se puede usar un transmisor propio y enlazarlo al receptor incorporado al dron.

Brushless Motor	motor *brushless* (o motor sin escobillas)	Estos motores llevan imanes permanentes que giran alrededor de un armazón fijo para eliminar los problemas asociados a la conducción de corriente a la pieza móvil. Los motores sin escobillas son mucho más eficientes y duraderos que los motores con escobillas, porque no hay fricción y por lo tanto hay menos distorsión.
BVLoS	operación más allá del alcance visual	Se refiere al manejo de drones más allá del alcance visual del piloto. En la mayoría de los países, este tipo de vuelo no está permitido o está muy limitado. Según la normativa vigente en el Reino Unido, los drones solo pueden manejarse dentro del alcance visual del piloto: hasta 122 m de altura y en un radio de 500 m en cualquier dirección.
C		
Centre of Gravity (CG or CoG)	centro de gravedad	El punto central de equilibrio de un dron.
Channel	canal	Puede ser la frecuencia que emplean el transmisor de vídeo o la función de enlace entre el controlador-transmisor y el dron. Por ejemplo, se puede asignar un canal para controlar el acelerador o para encender o apagar las luces de navegación. La mayoría de los drones emplean como mínimo 6 canales.
Controlled Airspace	espacio aéreo controlado	Espacio aéreo de dimensiones específicas en el que se aseguran servicios de control del tránsito aéreo para los vuelos IFR y VFR según la clasificación establecida.
Controlled Zone (CTR)	zona controlada	Zona controlada que ocupa una superficie y una altitud predeterminadas.
Controller	dispositivo de control	Dispositivo utilizado por el piloto del dron para controlar el cuadricóptero. También se conoce como “transmisor”.
Command and Control Link (C2) *(ICAO)*	enlace de mando y control C2 (OAIC)	Enlace de datos entre la aeronave pilotada a distancia y la estación de piloto remoto para fines de dirigir el vuelo.
Counter UAV (C-UAV)	contra aeronaves no tripuladas	La tecnología contra drones, también conocida como “contra aeronaves no tripuladas”, se refiere a los sistemas empleados para detectar o interceptar aeronaves no tripuladas. Véase también "DTI".
D		
Descent Speed	velocidad de descenso	La velocidad con la que el dron desciende desde el aire. Por ejemplo, un dron puede tener una velocidad de descenso de 3 metros por segundo (m/s).

Detect and Avoid *(ICAO)*	detectar y evitar (OACI)	Capacidad de ver, captar o detectar tránsito en conflicto u otros peligros y adoptar las medidas apropiadas para cumplir con las reglas de vuelo aplicables. Esta tecnología ofrece funciones de autoseparación y evitación de colisiones, para conseguir una capacidad análoga a la de "ver y evitar" requerida en las aeronaves tripuladas.
Detect, Track and Identify (DTI)	detectar, seguir e identificar	Tecnología que detecta y sigue en tiempo real objetos en movimiento, como aeronaves no tripuladas, mediante un sensor o un conjunto de sensores.
DJI Aeroscope	Aeroscope	Aeroscope es la tecnología contra drones DJI. Al interceptar los enlaces de comunicación entre un dron DJI y un control remoto, Aeroscope puede enviar datos de identificación en tiempo real, como el código de serie de la aeronave no tripulada, la marca y el modelo, posición, velocidad, latitud y ubicación del control terrestre.
Drone	dron	Término utilizado habitualmente para referirse a las aeronaves no tripuladas. Se aplica a aeronaves no tripuladas de diferentes tamaños y fabricadas con diferentes fines, desde su utilización por las fuerzas armadas hasta la práctica de fotografía digital por parte de aficionados. Otra denominación es la de "aeronave pilotada a distancia".
DSM / DSM2 / DSMX	**DSM / DSM2 / DSMX**	El fabricante de equipos de radiocomunicación Spektrum ha dado a su tecnología exclusiva el nombre de "Digital Spectrum Modulation" (modulación del espectro digital). Cada transmisor tiene un identificador único (*globally unique identifier*, GUID) al que puede enlazarse el receptor, de manera que no haya interferencias con otros sistemas DSM de Spektrum. El sistema DSM se basa en la tecnología de espectro ensanchado de secuencia directa (DSSS).
DSSS	espectro ensanchado de secuencia directa	La tecnología de espectro ensanchado de secuencia directa (Direct-Sequence Spread Spectrum) se basa en la modulación. Como sucede en otras tecnologías de espectro ensanchado, la señal transmitida ocupa más ancho de banda que la señal de información que modula la frecuencia portadora o de difusión. El concepto de "espectro ensanchado" se refiere a que la señal portadora se produce en todo el ancho de banda (espectro) de la frecuencia de transmisión del dispositivo.
E		
Electromagnetic Interference (EMI)	interferencia electromagnética	Interferencia eléctrica, a veces procedente de fuentes externas.
Electronic Speed Control (ESC)	regulador electrónico de la velocidad	Dispositivo que controla el motor de una aeronave eléctrica y traslada las señales del controlador de vuelo a los motores que rigen la velocidad y la dirección de rotación. Suele incluir un circuito eliminador de batería (Battery Elimination Circuit, BEC), que alimenta el sistema de radiocomunicación y otros elementos electrónicos de la aeronave, como el piloto automático.

Electronically Erasable Programmable Read Only Memory (EEPROM)	ROM programable y borrable eléctricamente (EEPROM)	La memoria de solo lectura (ROM) programable y borrable eléctricamente es un tipo de memoria no volátil empleada en ordenadores y otros dispositivos electrónicos para almacenar pequeñas cantidades de datos que se precisan cuando se corta la alimentación, p. ej., las tablas de referencia o calibración estática. A diferencia de lo que sucede en la mayoría de las memorias no volátiles, en la memoria EEPROM es posible leer, borrar o sobrescribir los bytes de manera independiente.
Elevator (ELEV)	timón de cabeceo	También conocido como “pitch” (véase la definición).
EVLOS	alcance visual ampliado	Tipo de operación que supera los parámetros básicos, en la que por lo general se emplea a un observador situado al extremo del alcance visual marcado por la normativa de cada jurisdicción. Por ejemplo, si el límite del alcance visual del dron son 500 m de distancia del piloto, el observador se sitúa a 500 m del piloto en la dirección de vuelo del dron y, cuando el dron alcanza los 500 m, el observador amplia el alcance visual otros 500 m más, lo que da un margen de operación de 1 kilómetro. Generalmente el observador se comunica con el piloto para indicarle el comportamiento del dron, y a veces emplea un dispositivo de control remoto para asumir el manejo del dron. De este modo, se puede llevar el dron hasta 500 metros de distancia del observador, y así sucesivamente.
F		
Field of View (FOV)	campo de visión	Medida del espacio que se puede ver a través de la lente de una cámara. Por lo general se indica en grados.
First Person View (FPV)	visión en primera persona (FPV)	Conexión inalámbrica entre la cámara del dron y una pantalla situada en el dispositivo de control o en una pantalla asociada (teléfono o tableta) y que permite ver lo mismo que se ve desde el dron. Hay cierta polémica sobre si esta opción permitiría que un piloto experimentado llevase una aeronave no tripulada más allá de su alcance de visión, si bien se recomienda precaución en todo caso.
Flight Controller	controlador de vuelo	Microprocesador encargado del control del vuelo, que actúa como el “cerebro” del dron.
Flight Envelope	envolvente de vuelo	Rango de maniobrabilidad, en el que se establecen los límites de alabeo, elevación y guiñada para asegurar la estabilidad de la aeronave.

Fly Away	*fly-away* o escape	Se refiere al movimiento de una aeronave no tripulada que pierde el control del operador. Generalmente está causado por interferencias electromagnéticas externas. Algunos drones se construyen con sistemas de protección contra *fly-away*. En caso de pérdida de control, el sistema de posicionamiento GPS del dron puede llevarlo hasta la posición inicial.
Frame	chasis	Véase "fuselaje".
Frequency Hopping	salto de frecuencia	Modificación de las frecuencias de la señal transmitida, de acuerdo con una pauta determinada, para evitar posibles fallos de comunicación en una frecuencia concreta.
G		
Geofence	geocerca	Barrera geográfica virtual, definida por GPS, que desencadena una repuesta de la aeronave cuando se accede a una zona determinada.
Gimbal	cardán	Suspensión especial de la cámara, dotada de servomotores que le permiten oscilar e inclinarse. De este modo, la cámara puede mantener la misma posición independientemente del movimiento del dron, lo que permite obtener una imagen estable, sin pérdida de calidad.
Global Positioning System (GPS)	sistema de posicionamiento global (GPS)	Conjunto de satélites situados en una órbita cercana a la Tierra, cuyas señales permiten que el dron determine su posición respecto de tierra.
GLONASS	GLONASS	Acrónimo de "Globalnaya Navigazionnaya Sputnikovaya" (sistema mundial de navegación orbital por satélite), versión rusa del sistema GPS.
Ground Control Station (GCS)	estación de control terrestre	Véase "estación de control remoto". *Nota: Se prefiere el término "estación de control remoto" por ser independiente del lugar donde se emplee (por ejemplo, un buque u otra aeronave).*
Gyroscope	giroscopio	Proporciona una velocidad angular en torno a 3 ejes espaciales para mantener la orientación de un cuadricóptero.
H		
Handover	traspaso	Acción de trasladar el control de las operaciones de una estación de control remoto a otra.
Heads Up Display (HUD)	visualización frontal (HUD)	Visualización mostrada directamente frente al operador del dron. La visualización frontal puede incluir datos de telemetría, como la altitud, velocidad, ángulo de vuelo, lectura de brújula y coordenadas GPS. Véase también "visualización en pantalla".

Hexacopter (Hexa)	hexacóptero	Aeronave multirrotor que emplea seis rotores para volar.
Home Location	posición de base	La posición de base es la ubicación de despegue almacenada en el dron, o bien otra ubicación establecida por el usuario. Se utiliza al activar el comando de retorno a la base (RTH) debido a un agotamiento de la batería, una maniobra de seguridad si se ha perdido la señal durante 3 segundos o una maniobra automática al pulsar el botón "Home" en el controlador o en la aplicación.
Hovering Time	autonomía en vuelo estacionario	Se refiere al tiempo durante el cual el dron puede permanecer en vuelo estacionario cuando no está en movimiento. Varía en función de la carga útil: cuando más pesada, menos autonomía de vuelo estacionario.
I		
IP Rating	calificación de estanqueidad (IP)	La calificación IP se emplea para definir el grado en que las cajas de componentes eléctricos protegen contra la humedad o elementos externos (herramientas, polvo...). Por ejemplo: "IP65" significa que la caja es estanca contra el polvo y contra la aspersión de agua.
Inertial Measurement Unit (IMU)	unidad inercial	Por lo general, el sistema de control de la estabilización y orientación está equipado con un mínimo de 3 acelerómetros (que miden el vector de gravedad en las dimensiones x, y y z) y 2 giroscopios (que miden la rotación en torno al eje de vuelco y el eje de cabeceo). Ninguno de estos mecanismos sería suficiente por sí solo, porque los acelerómetros se desconectan con el movimiento (esto es, funcionan durante períodos cortos) y los giroscopios se desvían con el tiempo. El *software* utilizado combina los datos de ambos tipos de sensores para determinar la posición de vuelo y el movimiento de la aeronave.
L		
Landing Gear	tren de aterrizaje	La mayoría de los drones llevan un tren de aterrizaje fijo, que también puede ser retráctil para permitir la visión de 360º durante el vuelo. Los drones de ala fija no llevan tren de aterrizaje, ya que pueden tomar tierra sobre su base.
Lithium Polymer Battery (LIPO)	batería de polímeros de litio (LIPO)	Una variante son las baterías de ion-litio (Li-Ion). Los componentes químicos de estas baterías ofrecen más potencia con menor peso, en comparación con las baterías de níquel-hidruro metálico (NiMh) o de níquel-cadmio (NiCad).
Line of Sight (LOS)	alcance visual	Campo de visibilidad, que debe ajustarse a la normativa al operar una aeronave no tripulada. Si se pierde el alcance visual de la aeronave se puede perder el control de la misma, con la posibilidad de causar daños en personas o bienes.

Lost Link *(ICAO)*	enlace perdido (OACI)	Pérdida de contacto del enlace de mando y control con la aeronave pilotada a distancia que impide al piloto remoto dirigir el vuelo de la aeronave.
M		
Magnometer	magnetómetro	Brújula electrónica utilizada para determinar la dirección a la que apunta la aeronave no tripulada.
Multirrotor	multirrotor	Término general aplicable a los drones que emplean más de un motor y más de una hélice para conseguir la elevación y la propulsión del vehículo. Los drones más utilizados tienen 4 rotores, pero su número puede llegar hasta 12.
N		
Nano	nanodrón o nano	Dron en miniatura, de menos de 8 gramos, utilizado por lo general como juguete.
No Fly Zone (NFZ)	zona de exclusión aérea	Se refiere a las zonas donde rigen restricciones de vuelo (véase "geocerca") y donde está prohibido el acceso de aeronaves no tripuladas.
O		
Octocopter	octocóptero	Dron multirrotor que emplea seis rotores para volar.
Operator *(ICAO)*	operador (OACI)	Persona, organización o compañía que asegura la operación de aeronaves. *Nota: En el contexto de los vehículos aéreos no tripulados, la operación se refiere al manejo a distancia del vehículo.*
On Screen Display (OSD)	visualización en pantalla	Integración de datos (por lo general, información de telemetría) en las imágenes de vídeo en tiempo real que la aeronave envía a la estación terrestre.
P		
Payload	carga útil	Elemento que el dron puede cargar, elevar, soltar o entregar.
PIC	piloto al mando	Persona que tienen la responsabilidad legal de controlar el dron en un momento determinado.
Pilot	piloto	Persona que controla directamente la aeronave no tripulada (véase "piloto remoto").
Pitch	*pitch* o cabeceo	Ángulo que adquiere el dron durante el vuelo: indica qué brazo está por encima de los demás.
Point Of Interest (POI)	punto de interés	Lugar que debe alcanzar la aeronave no tripulada. Una definición alternativa es cualquier zona que deba captar la cámara del dron.

Power Distribution Board	placa de distribución de potencia	Pequeña placa de circuitos impresos que organiza las conexiones eléctricas y distribuye la potencia entre baterías, reguladores de velocidad y otros componentes del sistema. No se utiliza en todos los drones, pero es habitual en los vehículos de aficionado, para simplificar el cableado.
Propellers	hélices	Son los elementos que aseguran la elevación del dron y su permanencia en el aire. Funcionan según las instrucciones ingresadas por el piloto y la intensidad de giro es la que causa el movimiento del dron.
Proportional, Integral, Derivative Control (PID)	regulador de acción proporcional, integral y derivada	Algoritmo matemático empleado por el controlador de vuelo para asegurar una ratio estable de respuesta y potencia en los motores del dron. Su ajuste puede ampliar la capacidad de respuesta del dron, pero también su inestabilidad.
Q		
QUAD / Quadcopter	cuadricóptero	Dron multirrotor, también conocido como helicóptero de cuatro hélices. Estas aeronaves tienen un diseño más sencillo que el de otros drones de tamaño similar y utilizan 4 palas en lugar de 2.
R		
Radio Line-Of-Sight (RLOS)	radio de visibilidad directa	Contacto electrónico punto a punto y sin obstrucciones entre un transmisor y un receptor.
Radio Controlled (RC)	radiocontrolado	Se aplica a los drones que reciben las instrucciones de vuelo por medio de señales de radio. El piloto situado en tierra utiliza un terminal similar a un mando de videojuegos o también, cuando el dron tiene conexión wifi, una tableta o un ordenador.
Ready To Fly (RTF)	listo para volar	Se refiere a los drones o cuadricópteros que se venden con todo lo necesario para iniciar el vuelo. El conjunto puede incluir el dron, las baterías, el manual de instrucciones, los controladores y cualquier otro elemento necesario para operar el dron.
Receiver	receptor	En términos generales, la radio incluida en el dron para recibir las instrucciones que el operador envía desde el transmisor. El receptor puede ser también una configuración de cámara o gafas de visión en primera persona utilizada por el operador para recibir imágenes en tiempo real enviadas por el dron.
Received Signal Strength Indicator (RSSI)	indicador de intensidad de señal recibida	Intensidad de la señal de radio enviada al dron desde el dispositivo de control.
Return to Home (RTH)	retorno a la base	Retorno del dron a la posición de base después de despegar.

Revolutions Per Minute (RPM)	revoluciones por minuto (rpm)	Número de veces que gira el timón del dron en un ciclo de 60 segundos.
Remote Pilot *(ICAO)*	piloto remoto (OACI)	Persona que manipula los controles de vuelo de una aeronave pilotada a distancia durante el tiempo de vuelo.
Remote Pilot Station (RPS)	estación de pilotaje remoto	Componente del vehículo aéreo pilotado a distancia que contiene el equipo empleado por el operador de la aeronave.
Remotely Piloted Air System*	sistema aéreo pilotado a distancia*	Sistema aéreo no tripulado formado por una serie de dispositivos, tales como la unidad de control terrestre, el sistema de despegue y el vehículo aéreo pilotado a distancia, junto con los elementos de seguridad necesarios.
Remotely-Piloted Aircraft (RPA) *(ICAO)*	aeronave pilotada a distancia (RPA) (OACI)	Aeronave que no lleva a bordo un piloto a los mandos.
Remotely-Piloted Aircraft System (RPAS). *(ICAO)*	sistema de aeronave pilotada a distancia (RPAS)	Aeronave pilotada a distancia, junto con la estación de control remoto, el mando y los sistemas de enlace, además de los componentes específicos de cada diseño.
Roll	alabeo	Término de aviación referido a la rotación en torno a un eje. Permite el movimiento lateral del dron.
Rotorcraft	giroplano	Vehículo aéreo que consigue la elevación y la propulsión mediante palas de rotor, sin necesidad de las alas típicas de los aviones. Cuando la propulsión del giroplano se asegura con dos o más palas de hélice, se conoce como multirrotor.
RPA Observer *(ICAO*)	observador de RPA (OACI)	Persona que dispone de la formación necesaria y que, mediante observación visual de la aeronave pilotada a distancia, ayuda al piloto remoto en la realización segura del vuelo.
RPAS Commander*	comandante de RPAS*	El comandante de aeronave no tripulada es la persona encargada de garantizar la seguridad de un vuelo y de supervisar a la persona que controla directamente la aeronave. Sus deberes equivalen a los de un comandante de aeronave tripulada.
RTK	navegación cinética en tiempo real (RTK)	Técnica de navegación basada en datos de posición más precisos gracias a sistemas satelitales como el GPS.
Rudder	timón	Elemento que asegura la dirección del vuelo.

S		
Sense and Avoid (SAA)	sistema de detección y evitación	Véase “detectar y evitar”.
Servo	servomotor	Elemento mecánico presente en algunos drones para asegurar el movimiento de algunos componentes o superficies. La mayoría de los drones no requieren servomotores porque su movimiento se controla modificando la velocidad de cada rotor. Los servomotores son más habituales en los drones de ala fija o en los cardanes.
Small Unmanned Aircraft (SUA)	pequeño vehículo aéreo no tripulado	Cualquier vehículo aéreo no tripulado, distinto de un globo o cometa, cuya masa sin combustible, pero incluyendo cualquier elemento o equipo instalado a añadido a la aeronave al comienzo del vuelo, no supere el límite especificado en cada país.
Small Unmanned Surveillance Aircraft (SUSA)	Pequeño vehículo aéreo de vigilancia no tripulado	Aeronave no tripulada de tamaño pequeño que incorpora algún elemento para la vigilancia o la obtención de información.
Swarm	enjambre	Término técnico referido a un grupo de aeronaves no tripuladas manejadas mediante inteligencia artificial. Los drones en enjambre pueden comunicarse entre sí durante el vuelo y responder de manera autónoma a condiciones cambiantes. Se podría comparar a una bandada de estorninos que reacciona a un peligro súbito, como la presencia de un halcón, moviéndose en conjunto como un solo organismo. No debe confundirse un enjambre con un grupo de aeronaves que vuelen en formación y actúen por separado de manera autónoma.
T		
Telemetry	telemetría	Datos relativos a todos los aspectos del vuelo de un dron: velocidad, altitud, balanceo, alabeo, guiñada, duración de batería, posición, etc.
Thermal	térmico	Las cámaras térmicas permiten obtener imágenes y datos térmicos, útiles para la inspección de edificios industriales, control de cultivos y otras finalidades más tradicionales, como la búsqueda de huellas de vida en situaciones de emergencia.
Throttle	acelerador	Controla la velocidad (en revoluciones por minuto o rpm) de las hélices o motores. A su vez, esto puede servir para que el controlador de vuelo modifique la altitud o la dirección del dron.
Transmitter	transmisor	Sinónimo del dispositivo de control: permite controlar desde tierra el vuelo del dron.

Trim	compensación	Ajuste realizado para modificar el valor de base de la palanca de control del transmisor. Si el dron tiene tendencia a desviarse en una dirección cuando no se toca la palanca, el operador puede compensar la palanca para que el vehículo se mantenga en posición en todo momento, aunque el operador no toque el dispositivo de control.
Tripod mode	modo de trípode	Modo de movimiento muy lento y estable, ideal para captar fotografías o vídeos a poca distancia de tierra. Es un estilo de filmación muy preciso, utilizado con frecuencia por fotógrafos y cineastas.
U		
UAS-p ***(legacy term)***	piloto de aeronave no tripulada (*término obsoleto*)	Véase “piloto”.
UAV Pilot/UAV-p ***(legacy term)***	piloto de vehículo aéreo no tripulado (*término obsoleto*)	Véase “piloto”.
Unmanned Aircraft (UA)	Vehículo aéreo no tripulado	Vehículo aéreo que está previsto para funcionar sin la presencia de un piloto humano a bordo, como parte de un sistema de vehículo aéreo no tripulado. Presenta las siguientes características: - capacidad para mantener un vuelo sostenido por medios aerodinámicos; - puede ser pilotado a distancia o funcionar de manera autónoma; - es reutilizable; - no está clasificado como arma guiada u otro tipo de dispositivo diseñado para disparar municiones. *Nota: Se consideran un subconjunto de las aeronaves no tripuladas.*
Unmanned Aircraft System	Sistema de vehículo aéreo no tripulado	Sistema formado por diversos elementos, como la propia aeronave no tripulada y los demás dispositivos necesarios para asegurar el vuelo: estación de pilotaje remoto, enlace de comunicaciones y elemento de despegue y recuperación. Cada uno de estos componentes puede ser múltiple.

V		
VLoS	operación dentro del alcance visual	También conocido como “línea de alcance visual”. Concepto opuesto al de “operación fuera del alcance visual”. Es la manera en la que deberían manejarse los drones, siempre dentro del alcance visual del operador.
Vertical Take-off and Landing (VTOL)	despegue y aterrizaje vertical	Característica útil en los cuadricópteros y otras aeronaves no tripuladas de tipo multirrotor. Estos vehículos pueden despegar verticalmente, utilizando menos espacio. Las aeronaves de ala fija necesitan un tramo de pista para despegar y aterrizar.
Visual Line-Of-Sight (VLOS) Operation *(ICAO)*	operación con visibilidad directa visual (OACI)	Operación en la cual el piloto remoto o el observador mantienen contacto visual directo con la aeronave no tripulada.
W		
Waypoint	punto de referencia	Conjunto de tres o más coordenadas empleado para orientar la ruta de vuelo preestablecida para un dron durante una misión autónoma.
Wide Open Throttle (WOT)	acelerador a tope	Cuando se empuja completamente la palanca del acelerador del dispositivo de control remoto (a todo gas).
Y		
Yaw	guiñada	Término de aviación que describe la rotación del dron en torno a su eje central. Controla la dirección hacia la que se dirige el cuadricóptero.

- - - - - - -

INTERPOL

Mayor comunicación policial
para un mundo más seguro

WWW.INTERPOL.INT

INTERPOL_HQ

@INTERPOL_HQ

INTERPOLHQ

INTERPOLHQ