



Año de elaboración 2026

Título:

Optimización de la respuesta ante alarmas en plantas fotovoltaicas: integración de sistemas UAS autónomos para la protección de infraestructuras energéticas.

Versión:

Versión 2.0

Autor:

Alberto José Galdón Carreño

Área:

Formación para piloto profesional de drones (STS)

Resumen:

El presente artículo analiza la viabilidad jurídico-operativa de la integración de Sistemas de Aeronaves No Tripuladas (UAS) totalmente autónomos, basados en el modelo *Drone-in-a-Box*, como mecanismo para optimizar la verificación de alarmas en infraestructuras fotovoltaicas.

Frente a las limitaciones inherentes a la protección perimetral estática, caracterizada por un elevado índice de falsas alarmas, esta tecnología disruptiva permite a las centrales receptoras de alarmas (CCRRAA) reducir drásticamente los tiempos de respuesta y mejorar su consciencia situacional.

A través de una revisión sistemática cualitativa, se examina la convergencia entre la normativa aeronáutica vigente (el Real Decreto 517/2024 y la aplicación de la metodología SORA), la legislación de seguridad privada (Ley 5/2014) y el marco de protección de datos (LOPDGDD).

Los hallazgos evidencian que, si bien el sistema autónomo justificaría su operación en categoría específica al ofrecer una confirmación videográfica superior, su naturaleza jurídica quedaría estrictamente relegada a la de un medio técnico de apoyo avanzado. En consecuencia, aunque la tecnología optimizaría el despliegue de la inteligencia táctica, resultaría jurídicamente incapaz de sustituir la intervención física, la cual permanece como competencia indelegable del personal de seguridad privada habilitado.

Palabras clave: UAS autónomos, *Drone-in-a-Box*, Seguridad privada, central receptora de alarmas, metodología SORA, video verificación, plantas fotovoltaicas.

Abstract:

This paper analyzes the legal and operational feasibility of integrating fully autonomous Unmanned Aircraft Systems (UAS), based on the *Drone-in-a-Box* model, to optimize alarm verification in photovoltaic plants. Faced with the inherent limitations of static perimeter protection—often characterized by a high volume of false alarms—autonomous drones emerge as a disruptive technological solution capable of drastically reducing the response times of Alarm Receiving Centres (ARC). Through a qualitative systematic review, the study evaluates the convergence of current aeronautical regulations (Royal Decree 517/2024 and SORA methodology), private security legislation (Law 5/2014), and data protection frameworks (LOPDGDD). The findings demonstrate that, although the autonomous system provides superior videographic confirmation that justifies operations within the Specific Category, its legal status is strictly relegated to that of an advanced technical support tool. Consequently, while the technology optimizes tactical intelligence, it is legally incapable of replacing physical intervention, which remains the exclusive and non-delegable competence of the security guard.

Keywords: Autonomous UAS, *Drone-in-a-Box*, Private security, Alarm Receiving Centre, SORA methodology, Videographic verification, Solar power plant.

Acrónimos y siglas:

- **AEPD:** Agencia Española de Protección de Datos.
- **AESA:** Agencia Estatal de Seguridad Aérea.
- **ARC:** *Air Risk Class* (Clase de Riesgo Aéreo).
- **BVLOS:** *Beyond Visual Line of Sight* (Más allá del alcance visual).
- **C2:** *Command and Control* (Enlace de Mando y Control).
- **CCTV:** Circuito Cerrado de Televisión.
- **CCRRAAUP:** Centrales Receptoras de Alarmas de Uso Propio.
- **CNP:** Cuerpo Nacional de Policía.
- **ConOps:** *Concept of Operations* (Concepto de Operaciones).
- **CRAA:** Central Receptora de Alarmas.
- **DiaB:** *Drone-in-a-Box* (Estación Base Automatizada).
- **EASA:** *European Union Aviation Safety Agency* (Agencia de la Unión Europea para la Seguridad Aérea).
- **EIPD:** Evaluación de Impacto en la Protección de Datos.
- **FFCCSE:** Fuerzas y Cuerpos de Seguridad del Estado.
- **GNSS:** *Global Navigation Satellite System* (Sistema Global de Navegación por Satélite).
- **GPS:** *Global Positioning System* (Sistema de Posicionamiento Global).
- **GRC:** *Ground Risk Class* (Clase de Riesgo en Tierra).
- **IA:** Inteligencia Artificial.
- **JARUS:** *Joint Authorities for Rulemaking on Unmanned Systems* (Autoridades Conjuntas para la Reglamentación de Sistemas No Tripulados).
- **LOPDGDD:** Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- **OSO:** *Operational Safety Objectives* (Objetivos de Seguridad Operacional).
- **RD:** Real Decreto.
- **RGPD:** Reglamento General de Protección de Datos.
- **RPAS:** *Remotely Piloted Aircraft System* (Sistema de Aeronave Pilotada a Distancia).
- **SAIL:** *Specific Assurance and Integrity Level* (Nivel Específico de Garantía e Integridad).

- **SORA:** *Specific Operations Risk Assessment* (Evaluación de Riesgos de Operaciones Específicas).
- **STS:** *Standard Scenarios* (Escenarios Estándar).
- **TFG:** Trabajo Fin de Grado.
- **TFM:** Trabajo Fin de Máster.
- **UAS:** *Unmanned Aircraft System* (Sistema de Aeronave No Tripulada).

Índice

1. Introducción	8
2. Marco Teórico	11
2.1. Marco legislativo de la seguridad privada: atipicidad normativa e innovación tecnológica	11
2.2. Centrales receptoras de alarmas y protocolos de verificación	11
2.3. Regulación española sobre el empleo de drones en seguridad	15
2.3.1. Marcado de clase (C0-C6) e identificación remota.....	16
2.3.2. Autorizaciones en Categoría Específica: STS, PDRA y SORA	17
2.3.3. Procedimientos de autorización: escenario estándar, PDRA y SORA.....	17
2.3.4. Operaciones automáticas <i>drone-in-a-box</i> : autonomía versus supervisión.....	18
2.4. Privacidad: requisitos de protección de datos	23
2.5. Sistemas de seguridad perimetral en plantas fotovoltaicas. Medios tecnológicos y humanos.	24
3. Objetivos	26
3.1. Objetivo General	26
3.2. Objetivos Específicos	26
4. Metodología	27
4.1. Enfoque metodológico	27
4.2. Diseño de la investigación: revisión sistemática.....	27
4.2.1. Fase de Identificación y búsqueda	27
4.2.2. Fase de cribado y criterios de elegibilidad	28
4.2.3. Fase de análisis cualitativo y extracción de datos	28
5. Resultados de la investigación	29

5.1. Agilidad y movilidad aérea: optimización de la respuesta a alarmas	29
5.2. Limite jurídico de la autonomía: complementariedad con la intervención humana .	29
5.3. Cumplimiento en materia de seguridad aérea (AESAs)	30
5.4. Encaje operativo en la seguridad privada.....	31
5.5. Cumplimiento en materia de protección de datos	31
6. Discusión.....	32
7. Conclusiones	35
8. Futuras líneas de investigación	36
Referencias bibliográficas	38

1. Introducción

La transición energética ha consolidado a España como líder en capacidad de generación de energía solar fotovoltaica. Sin embargo, estas infraestructuras —caracterizadas por su gran extensión, aislamiento geográfico y alto valor patrimonial— enfrentan vulnerabilidades significativas frente al robo y el sabotaje.

En un entorno de seguridad corporativa complejo e incierto, la protección perimetral tradicional basada en cámaras termográficas y barreras físicas resulta insuficiente. La interacción constante de estos sistemas con el medio natural genera un volumen inasumible de falsas alarmas, saturando la capacidad de respuesta de las centrales receptoras de alarmas (CCRRAA) e incrementando los riesgos operativos para los servicios de verificación presencial de alarmas.

Frente a esta respuesta reactiva e ineficiente, los sistemas de aeronaves no tripuladas (UAS¹) con autonomía plena emergen como una solución tecnológica disruptiva. Integrados en estaciones base automatizadas (*Drone-in-a-Box*²), estos sistemas podrían despegar automáticamente ante una señal de alarma, verificar el evento transmitiendo vídeo en tiempo real sin intervención humana directa *in situ* (aunque bajo supervisión remota), y regresar a su base de forma autónoma.

¹ **UAS (*Unmanned Aircraft System* - sistema de aeronave no tripulada):** término normativo adoptado por la Agencia de la Unión Europea para la Seguridad Aérea (EASA) y AESA. Engloba no solo la propia aeronave (UA), sino todos los elementos técnicos necesarios para su operación, como la estación de control y los enlaces de mando y control (C2). En el contexto de este estudio, resulta el acrónimo jurídicamente preciso frente a RPAS (*Remotely Piloted Aircraft System*), ya que el concepto UAS incluye a los sistemas con capacidad de vuelo completamente autónomo sin intervención humana directa a los mandos.

² **Drone-in-a-Box (DiaB) o estación base automatizada:** Término técnico e industrial que define a un sistema compuesto por una aeronave no tripulada y una estación terrestre (nido o caja) encargada de su despliegue, refugio, recarga de baterías y descarga de datos de forma automática. Desde una perspectiva jurídica, el Reglamento de Ejecución (UE) 2019/947 no utiliza este nombre comercial, sino que regula su uso bajo el concepto de «operación autónoma». En su artículo 2, punto 17, el Reglamento lo define expresamente como «una operación en la que una aeronave no tripulada opera sin que el piloto a distancia pueda intervenir». Debido a esta falta de intervención humana en tiempo real y a su vuelo más allá del alcance visual (BVLOS), la norma exige que el despliegue de tecnología DiaB en seguridad privada se encuadre dentro de la Categoría Específica, requiriendo complejas autorizaciones operacionales (Diario Oficial de la Unión Europea, 2019, L 152/45).

No obstante, la incorporación operativa de UAS altamente automatizados exige resolver una complicada convergencia legislativa. En el ámbito aeronáutico, regulado principalmente por el Reglamento de Ejecución (UE) 2019/947 y por el Real Decreto 517/2024, la autonomía total para vuelos más allá del alcance visual (BVLOS) está expresamente excluida de la Categoría Abierta.

Además, incluso en la Categoría Específica —única vía legal para estas operaciones— se impone la presencia de un piloto remoto con capacidad de supervisión y control en todo momento, ya que las operaciones totalmente autónomas sin supervisión activa no se encuentran contempladas aún en la normativa vigente.

En consecuencia, los Escenarios Estándar (STS) actuales no permiten prescindir por completo de la intervención humana, al exigir habitualmente observadores visuales desplegadas en campo.

Para implementar estas patrullas aéreas automatizadas es indispensable inscribir el servicio en la Categoría Específica, obteniendo una autorización operacional de la Agencia Estatal de Seguridad Aérea (AESA) basada en la metodología de evaluación de riesgos SORA³ (*Specific Operations Risk Assessment*).

Esta evaluación, adaptada al contexto particular de las plantas fotovoltaicas, implica desarrollar un Concepto de Operaciones (ConOps) robusto que mitigue eficazmente los riesgos tanto en tierra (GRC) como en aire (ARC) de la operación.

Simultáneamente, la dimensión de la privacidad requiere un cumplimiento estricto de la normativa de protección de datos personales vigente, especialmente el RGPD (Reglamento General de Protección de Datos, Reglamento (UE) 2016/679) y la LOPDGDD (Ley Orgánica 3/2018). Al operar como sistemas de videovigilancia móviles, los UAS deben aplicar el

³ **SORA (*Specific Operations Risk Assessment* - Evaluación de Riesgos de Operaciones Específicas):** Metodología desarrollada por el grupo internacional de expertos JARUS (*Joint Authorities for Rulemaking on Unmanned Systems*) y adoptada oficialmente por la Agencia de la Unión Europea para la Seguridad Aérea (EASA) y AESA en España. Proporciona un marco analítico estructurado para identificar, evaluar y mitigar los riesgos terrestres (GRC) y aéreos (ARC) inherentes a las operaciones de UAS en la Categoría Específica. Su aplicación determina el Nivel Específico de Garantía e Integridad (SAIL) de la operación, el cual dicta los Objetivos de Seguridad Operacional (OSO) que el operador debe acreditar documental y técnicamente para obtener la autorización de vuelo. Constituye la herramienta jurídica ineludible para validar el uso de drones con autonomía plena (*Drone-in-a-Box*) en infraestructuras críticas.

principio de minimización de datos mediante tecnologías de geo-vallado (*geofencing*⁴) y enmascaramiento dinámico de imágenes, de modo que se evite la captación de información personal fuera del perímetro autorizado. Estas medidas, diseñadas bajo el paradigma de la «privacidad desde el diseño», garantizan que la vigilancia aérea se limite estrictamente al recinto protegido, respetando la proporcionalidad y la intimidad de la ciudadanía.

Por último, en el ámbito de la seguridad privada, ni la Ley 5/2014, de 4 de abril, de Seguridad Privada ni el vigente Reglamento de Seguridad Privada (Real Decreto 2364/1994) tipifican aún a los UAS entre los medios de seguridad previstos.

No obstante, operativamente pueden asimilarse a medios técnicos de apoyo idóneos para la video verificación de alarmas que exige la Orden INT/316/2011 a las CCRRAA. Desde una perspectiva jurídica, el dron ha de operar estrictamente como un sensor avanzado de detección, sin atribuciones propias de intervención, ya que estas siguen siendo competencia indelegable del personal de seguridad privada habilitado.

En este contexto, el presente trabajo tiene como objetivo principal analizar la viabilidad jurídica y los requerimientos operativos para integrar UAS autónomos en la verificación de alarmas perimetrales en plantas fotovoltaicas en España, en el marco del nuevo Real Decreto 517/2024. En particular, se identifican las principales barreras regulatorias y técnicas impuestas por la normativa aeronáutica (AESA/EASA), se examina la aplicación práctica de la metodología SORA al entorno fotovoltaico y se establecen protocolos de mitigación para garantizar la seguridad de la operación y la protección de datos personales.

A partir de ello, se propone un marco procedimental que integre coherentemente la seguridad aérea, la seguridad privada y la privacidad, asegurando eficacia operativa sin menoscabar las garantías legales ni la necesaria supervisión humana.

⁴ **Geofencing (Geovallado):** Tecnología geoespacial que utiliza sistemas de posicionamiento (GPS/GNSS) para establecer perímetros virtuales definidos por coordenadas geográficas. En la operativa de UAS autónomos, esta herramienta actúa como una barrera lógica y automatizada que restringe el vuelo de la aeronave al área autorizada. Su implementación es una medida de mitigación técnica crítica para el cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), ya que garantiza que los sensores del dron no capten imágenes de la vía pública ni de propiedades colindantes, asegurando que la vigilancia se limite estrictamente al recinto de la planta fotovoltaica y respetando el principio de proporcionalidad y minimización de datos.

2. Marco Teórico

2.1. Marco legislativo de la seguridad privada: atipicidad normativa e innovación tecnológica

El sector de la seguridad privada en España se rige por un marco jurídico complejo que, pese a intentos de modernización, presenta disonancias entre la legislación de base y sus normas de desarrollo.

La piedra angular es la Ley 5/2014, de 4 de abril, de Seguridad Privada, que supuso un cambio de paradigma al reconocer a la seguridad privada como parte importante de la arquitectura general de seguridad pública (Rodríguez, 2020).

No obstante, la aplicación de esta ley se ve obstaculizada por la atipicidad normativa: a falta de un reglamento actualizado, sigue vigente el Reglamento de Seguridad Privada de 1994 (Real Decreto 2364/1994), una norma concebida hace casi tres décadas.

Esta coexistencia de una ley moderna con un reglamento obsoleto genera inseguridad jurídica ante la integración de tecnologías emergentes como los UAS autónomos, que no cuentan con reconocimiento expreso en el marco actual.

Como advierten los expertos Rodríguez (2020), operar solo con interpretaciones analógicas de normas desfasadas puede propiciar zonas grises legales, donde proliferan criterios dispares e incluso potenciales prácticos de intrusismo.

Los profesionales de la seguridad privada se ven obligados a cubrir lagunas legales mediante pautas internas, lo que subraya la necesidad de actualizaciones normativas que otorguen certidumbre y unifiquen la integración de nuevas tecnologías.

2.2. Centrales receptoras de alarmas y protocolos de verificación

Dentro de la arquitectura de seguridad privada, las centrales receptoras de alarmas (CCRRAA) se han consolidado como centros neurálgicos para la gestión de incidentes. La Ley 5/2014 establece dos modelos de CCRRAA: (1) CCRRAA operadas por empresas de seguridad, que prestan servicio a múltiples clientes, y (2) CCRRAA de uso propio, gestionadas por el titular de las instalaciones (frecuentes en sectores estratégicos como el energético, donde se busca control directo).

Optar por una CCRRAA de uso propio responde al interés en la confidencialidad y el control estratégico: la empresa titular monitoriza y gestiona sus propios sistemas de seguridad sin intermediarios.

Como señala Galdón (2025), en la protección de activos críticos dispersos, una central corporativa juega un rol de mando integral, convirtiéndose en el núcleo operativo capaz de transformar una señal de alarma en una respuesta de seguridad alineada con los objetivos del negocio.

Sea cual fuere el tipo de CCRRAA, la normativa impone un control técnico y operativo riguroso. Un aspecto central es la responsabilidad de filtro frente a las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE): la legislación prohíbe comunicar a la policía cualquier alarma no verificada previamente conforme a la Orden INT/316/2011.

Esta norma impone cuatro métodos de verificación de alarmas que las CCRRAA deben aplicar:

- a) **Verificación secuencial:** recepción de tres o más señales de distintos detectores en un intervalo breve, de modo que se descarte la casualidad.
- b) **Verificación por vídeo:** captura de imágenes asociadas al evento. Cada alarma debe vincularse a una cámara de vigilancia cuya cobertura abarque la zona controlada por el detector. Se exige obtener una imagen en el instante del salto de alarma y al menos dos imágenes posteriores (en unos 5 segundos) para confirmar visualmente la intrusión. Si las imágenes no son concluyentes, la alarma sigue sin confirmarse hasta obtener evidencia adicional.
- c) **Verificación por audio:** grabación de un mínimo de diez segundos de audio antes y después del disparo de alarma, con posibilidad de escucha en directo. La alarma se considerará confirmada únicamente si el audio revela sin duda indicios de intrusión (ruidos humanos, roturas, etc.).
- d) **Verificación personal (servicio de «acuda»):** desplazamiento de personal de seguridad al lugar para comprobar in situ lo ocurrido. Ante alarmas no confirmadas por medios técnicos o en casos de indicios graves, la CCRRAA moviliza vigilantes de seguridad habilitados que se trasladan a la instalación. La normativa exige que cualquier acceso al interior se realice con un binomio de vigilantes, lo que garantiza mayor seguridad y cobertura mutua durante la inspección.

Tabla 1.

Tipos de verificación. Fuente. Taxonomía para la evaluación del peligro: hacia la búsqueda de una metodología específica de evaluación del riesgo en centrales receptoras de alarmas. (Galdón 2025).

Tipo de verificación	Tipo de subsistema	Método
Secuencial.	Subsistema de alarma contra intrusión y atraco.	Activación de señales de detección.
Mediante video.	Subsistema de video en combinación con subsistema de alarma contra intrusión y atraco.	Activación de la señal de video previo a la activación de un detector o video sensor.
Mediante audio.	Subsistema de audio en combinación con subsistema de alarma contra intrusión y atraco.	Señal de audio tras activación de un detector o del propio dispositivo.
Mediante personal.	Subsistema de alarma contra intrusión y atraco en combinación con la verificación personal.	Tras la activación de una o más señales de detección se desplazará personal habilitado para realizar la verificación <i>in situ</i> .

Tabla 2.

Tipos de verificación: verificación secuencial. Fuente. Taxonomía para la evaluación del peligro: hacia la búsqueda de una metodología específica de evaluación del riesgo en centrales receptoras de alarmas. (Galdón 2025).

Requisitos de la verificación secuencial	
Número de señales.	De forma sucesiva tres o más señales.
Tipo de detectores.	Elementos de detección diferentes dependiendo de las características arquitectónicas de los inmuebles.
Periodo máximo de activación.	No se deberán superar los 30 minutos entre la activación secuencial de los diferentes detectores.
Alarma sin confirmar.	Activación del primer detector y del segundo detector.
Alarma confirmada.	Activación del segundo detector y el tercer detector, corte de la línea o señal de sabotaje, dentro del periodo máximo de activación.

Tabla 3.

Tipos de verificación: verificación mediante video. Fuente. Taxonomía para la evaluación del peligro: hacia la búsqueda de una metodología específica de evaluación del riesgo en centrales receptoras de alarmas. (Galdón 2025).

Requisitos de la verificación mediante vídeo	
Número de señales	Una señal de alarma mediante una la visualización de una imagen.
Tipo de cámara	La cámara debe estar asociada a un detector, la cobertura de la cámara debe ser superior o igual a la del detector. También puede tratarse de un video sensor que integre cámara y detección.
Registro de vídeo	Registrar una imagen del momento exacto de la alarma y dos imágenes posteriores a ella, en una ventana de 5 segundos.
Alarma sin confirmar	No se dispone de detección asociada a la imagen.
Alarma confirmada	Señal de detección asociada a tres imágenes de video.

Tabla 4.

Tipos de verificación: verificación mediante audio. Fuente. Taxonomía para la evaluación del peligro: hacia la búsqueda de una metodología específica de evaluación del riesgo en centrales receptoras de alarmas. (Galdón 2025).

Requisitos de la verificación mediante audio	
Requisitos técnicos.	Almacenar al menos 10 segundos de audio previos a la señal de alarma.
	Almacenar audio después de producirse la alarma, al menos hasta la que central receptora pueda acceder en directo a la instalación.
	Poder transmitir audio en directo si la central receptora lo demanda.
Alarma confirmada.	Cuando pueda verificarse mediante audio y cumpliendo los requisitos anteriores la intrusión.

Tabla 5.

Tipos de verificación: verificación mediante personal. Fuente. Taxonomía para la evaluación del peligro: hacia la búsqueda de una metodología específica de evaluación del riesgo en centrales receptoras de alarmas. (Galdón 2025).

Requisitos de la verificación mediante personal	
Requisitos.	Ante la alarma confirmada por cualquiera de las verificaciones anteriormente vistas, se podrá enviar al lugar personal para facilitar las llaves de acceso a la instalación a la policía.
	Ante una alarma no confirmada la central receptora podrá desplazar un servicio de verificación personal para realizar las comprobaciones oportunas y facilitar la información a la policía.
Verificación exterior.	Se realizará por un vigilante uniformado con un vehículo rotulado con el anagrama de la empresa.
Verificación interior.	Se realizará por dos vigilantes uniformados con un vehículo rotulado con el anagrama de la empresa.
Alarma confirmada.	Cuando la intrusión pueda ser confirmada por el o los vigilantes desplazados.

Estos métodos de verificación aseguran que la transmisión de una alarma a las FFCCSE nunca sea automática ni precipitada, sino resultado de un juicio humano cualificado que confirma la realidad de la intrusión o emergencia.

Antes de alertar a la policía, la CCRRAA debe descartar cualquier origen accidental, técnico o ambiental de la alarma, asegurando que solo se movilicen recursos públicos ante amenazas reales.

En instalaciones de gran extensión como los parques fotovoltaicos, la eficacia del filtrado depende de evidencias claras y en tiempo real que permitan la identificación de intrusos o indicios de riesgo dentro del perímetro.

En suma, la CCRRAA actúa como un centro de validación operativa y jurídica, responsable de filtrar exhaustivamente los eventos y evitar la activación innecesaria de la respuesta pública, garantizando que la intervención policial sea siempre última ratio ante una situación confirmada.

2.3. Regulación española sobre el empleo de drones en seguridad

La transición hacia un modelo de vigilancia basado en la autonomía plena de los UAS representa la vanguardia en la protección de infraestructuras críticas. A diferencia de los sistemas pilotados a distancia (RPAS), donde la figura del piloto controla manualmente la aeronave, un UAS autónomo se caracteriza por su capacidad de ejecutar misiones complejas de vigilancia y verificación sin intervención humana activa durante el vuelo. Sin embargo, este salto tecnológico tropieza con un intrincado entramado normativo que abarca seguridad aérea, salvaguarda de datos personales y seguridad privada.

Desde la perspectiva aeronáutica, la implantación de soluciones autónomas —materializadas generalmente bajo el modelo industrial *Drone-in-a-Box* (DiaB)— debe conjugarse con el cumplimiento de la normativa europea y española.

En virtud del Reglamento de Ejecución (UE) 2019/947 y del Real Decreto 517/2024, las operaciones de drones de vigilancia en entornos industriales se encuadran necesariamente en la Categoría Específica (STS) al implicar vuelos BVLOS y funciones automatizadas (muchas veces en horarios nocturnos). La operativa *DiaB* supera los límites de los STS existentes (por ejemplo, *STS-02* exige observadores visuales para vuelos BVLOS), por lo que solo puede autorizarse mediante un procedimiento de autorización basado en una evaluación de riesgos SORA. Este análisis debe acreditar ante AESA que los riesgos inherentes se han mitigado a niveles tolerables, demostrando la eficacia de medidas adaptadas al contexto de la planta fotovoltaica.

El régimen europeo de UAS, unificado bajo el Reglamento (UE) 2018/1139 (Reglamento básico EASA) y sus normas de desarrollo, clasifica las operaciones de drones según su riesgo en tres categorías: abierta, específica y certificada. Cada categoría establece condiciones de operación estrictas, proporcionales al nivel de riesgo, y considera variables como las características del UAS y el entorno:

- a) **Categoría Abierta:** operaciones de muy bajo riesgo, sin necesidad de autorización previa, siempre que se cumplan condiciones específicas: drones de ≤ 25 kg con marcado CE de clase C0–C4, vuelos a la vista del piloto (VLOS), altitud ≤ 120 m sobre el terreno, alejados de aglomeraciones y sin sobrevolar personas no involucradas. Esta categoría prohíbe expresamente cualquier operación plenamente autónoma sin supervisión de un piloto remoto, por lo que excluye patrullas automáticas de drones de seguridad en entornos industriales, que incumplirían el requisito de VLOS y supervisión continua.

- b) **Categoría Certificada:** operaciones de alto riesgo, equiparables a la aviación tripulada (ej. drones de gran tamaño para transporte de personas o cargas peligrosas). Exige certificación de la aeronave (según Reglamento Delegado (UE) 2019/945), licencia de piloto equivalente a la aviación tripulada y certificado de operador aéreo similar a un *Air Operator Certificate (AOC)*. Esta categoría, por su complejidad, no resulta aplicable al caso de drones de vigilancia perimetral, reservándose a supuestos de máxima exigencia (transporte de pasajeros, vuelos urbanos, etc.).
- c) **Categoría Específica:** operaciones de riesgo medio que exceden los límites de la categoría abierta sin alcanzar la complejidad de la certificada. Aquí se encuadran las operaciones de drones de vigilancia autónomos en plantas fotovoltaicas, ya que implican vuelos BVLOS, frecuentemente nocturnos, y sin personal presente en el lugar. Todas las operaciones en categoría específica requieren autorización previa de la autoridad aeronáutica (AESA) tras la evaluación de riesgos SORA correspondiente.

2.3.1. Marcado de clase (C0-C6) e identificación remota

El Reglamento Delegado (UE) 2019/945 establece seis clases de drones (C0 a C6) con requisitos técnicos y de seguridad concretos.

Las clases C0–C4 permiten volar en categoría abierta, mientras que las clases C5 y C6 (introducidas en el Reglamento Delegado (UE) 2020/1058) se destinan a operaciones en categoría específica bajo STS (Escenarios Estándar) y exigen prestaciones avanzadas: limitadores de altura configurables, sistemas de *geofencing* integrados, identificación electrónica remota, etc.

En la práctica, los drones de vigilancia autónomos requerirán certificación en clase C5 o C6, particularmente a medida que los STS europeos reemplacen a los escenarios nacionales.

Por otra parte, desde 2024 es obligatoria la identificación electrónica remota (*Remote ID*) en todos los drones de más de 250 g que carezcan de marcado de clase Cx. Los operadores deben equipar sus drones más antiguos con balizas electrónicas que emitan la identidad y posición de la aeronave en tiempo real, permitiendo su seguimiento por las autoridades.

Esto refuerza la trazabilidad de las operaciones y facilita la integración con el futuro espacio aéreo digitalizado (*U-Space*). En paralelo, el Real Decreto 517/2024 ha incorporado al ordenamiento español el Reglamento (UE) 2021/664 sobre despliegue de servicios *U-Space*, que prevé la designación de zonas geográficas UAS con servicios obligatorios de gestión de tráfico, facilitando así las operaciones automatizadas de drones a gran escala.

2.3.2. Autorizaciones en Categoría Específica: STS, PDRA y SORA

El Reglamento Delegado (UE) 2019/945 establece clases técnicas de drones (C0 a C6) con requisitos de diseño y sistemas de seguridad incorporados. Las clases C0–C4 permiten volar en categoría abierta; las clases C5 y C6 (introducidas por el Reglamento Delegado 2020/1058) se destinan a operaciones en categoría específica bajo escenarios estándar STS-01 y STS-02, e incluyen funciones avanzadas de seguridad (p. ej., limitador de altura preconfigurable, *geofencing*, identificación electrónica).

En la práctica, los drones de vigilancia autónomos suelen requerir certificación de clase C5/C6, sobre todo para los escenarios europeos STS (que en un futuro próximo sustituirán a los antiguos estándares nacionales).

Además, desde 2024 es obligatoria la identificación electrónica remota (Remote ID) de todos los drones > 250g sin marcado de clase. Esto impone a los operadores equipar o actualizar los drones antiguos (pre-2023) con balizas de emisión de identidad y posición para su seguimiento en tiempo real por las autoridades, reforzando la trazabilidad y permitiendo la integración con el sistema U-space (espacio aéreo digitalizado).

España, a través del RD 517/2024, ha adaptado la aplicación del Reglamento U-SPACE (UE 2021/664): se prevé la designación de áreas geográficas con servicios U-SPACE obligatorios para facilitar operaciones autónomas seguras a gran escala.

2.3.3. Procedimientos de autorización: escenario estándar, PDRA y SORA.

Para obtener permiso en categoría específica existen tres vías procedimentales, según el riesgo predefinido de la operación:

- a) **Escenarios Estándar (STS):** supuestos típicos de riesgo medio definidos normativamente (en la UE: STS-01 y STS-02). Si la operación encaja exactamente en uno de estos escenarios preaprobados, el operador puede presentar una declaración de cumplimiento (acompañando el ConOps, manuales, etc.) y comenzar los vuelos sin esperar una aprobación formal. España aprobó en 2023 Escenarios Estándar Nacionales (STS-ES), vigentes hasta su sustitución por los STS europeos en 2024. Sin embargo, las verificaciones autónomas ante activaciones de alarmas perimetrales con drones no encajan bien en STS-02 (BVLOS con observadores), ya que operan sin observadores humanos *in situ*, por lo que no pueden acogerse a esta vía simplificada sin adaptaciones adicionales.

- b) **PDRA (*Pre-Defined Risk Assessment*)**: evaluaciones predefinidas para ciertos tipos de operación repetitivos, pensadas para agilizar autorizaciones. Por ejemplo, el PDRA-G02 define mitigaciones estándar para vuelos BVLOS en áreas rurales poco pobladas. AESA ha adoptado guías basadas en PDRA específicos (como PDRA-S01 para fumigación agrícola, PDRA-S02 para inspección de infraestructuras lineales). A fecha de este estudio (2026), no existe un PDRA específico para verificación de alarmas en plantas fotovoltaicas, por lo que es necesario realizar una evaluación SORA individualizada.
- c) **SORA (*Evaluación Específica de Riesgos de la Operación*)**: es el proceso estándar para autorizar casos no cubiertos por STS ni PDRA. El operador realiza un análisis detallado siguiendo la metodología SORA (v2.0 de JARUS, adoptada por EASA), que evalúa por separado el riesgo en aire (ARC) y en tierra (GRC). De la combinación de estos factores se deriva un SAIL (nivel específico de garantía e integridad) entre I y VI. Cada nivel SAIL conlleva una lista de Objetivos de Seguridad Operacional (OSO) que el operador debe cumplir con un grado de robustez determinado, mediante mitigaciones adecuadas (vigilancia del espacio aéreo, rutas segregadas, sistemas de seguridad redundantes, procedimientos de emergencia, seguros ampliados, etc.). Una vez presentada toda la documentación (análisis SORA, ConOps, manual de operaciones), AESA evalúa si los riesgos están mitigados a niveles aceptables y, de ser así, otorga la autorización operacional correspondiente. Cabe mencionar que AESA publica Medios de Cumplimiento Aceptables (AMC) y guías operativas para facilitar a los operadores el cumplimiento de estos requisitos, también pudiendo aceptar soluciones innovadoras mediante medios alternativos de cumplimiento (AltMoC).

En España, AESA gestiona las autorizaciones en categoría específica conforme a los criterios comunes de EASA. El Real Decreto 517/2024 ha actualizado este marco, facilitando trámites (registro electrónico, formación unificada de pilotos) y otorgando mayor seguridad jurídica al sector UAS.

2.3.4. Operaciones automáticas *drone-in-a-box*: autonomía versus supervisión

La operación propuesta implica emplear drones de vigilancia de forma automática, gestionados remotamente desde una central receptora de alarmas (CCRRRAA), para la verificación de alarmas en una planta fotovoltaica. Esto plantea cuestiones sobre el grado de autonomía admisible:

- a) **Autonomía plena vs. supervisión remota**: actualmente la normativa no permite operaciones sin ningún piloto remoto. Solo es viable la semiautónoma: el dron realiza

despegues, navegación programada y aterrizajes de forma autónoma, pero siempre debe haber un piloto remoto responsable supervisando la misión, listo para tomar el control manual ante cualquier incidencia. Es importante destacar que la normativa sí contempla que un mismo piloto remoto pueda supervisar varios drones simultáneamente, siempre que se demuestre que la carga de trabajo es asumible sin menoscabo de la seguridad operacional (mediante el ConOps y el análisis SORA). En el modelo propuesto de CCRRAA con drones integrados, la central funcionaría también como estación de piloto remoto. La CRAA recibiría el vídeo en directo de los drones y podría ordenar su despegue ante alarmas, siempre asignando a cada dron un piloto remoto debidamente certificado, ya sea presente en la sala de control o conectado de forma telemática, en todo momento de la operación.

- b) **Planes de Operación (ConOps) y limitaciones técnicas:** para implementar un sistema *Drone-in-a-Box* en una planta fotovoltaica se requiere un ConOps minucioso que describa cómo se integrará la vigilancia del dron con el sistema de seguridad existente y a la vez cumplirá con los requerimientos de seguridad aérea. Entre otros puntos, el ConOps debe especificar la zona de operación: se definirá un espacio aéreo controlado alrededor de la planta, dentro del cual el dron realizará sus misiones, programándose electrónicamente dicho perímetro en el sistema de navegación del dron para prevenir salidas involuntarias fuera del área autorizada. Asimismo, se detallarán los perfiles de vuelo (p. ej., rutas perimetrales predeterminadas a una altura y velocidad seguras) y la frecuencia de las rondas (despegues *ad hoc* ante alarmas). Si se planean operaciones 24/7, el ConOps debe contemplar vuelos nocturnos (permitidos en categoría específica con autorización), exigiendo iluminación anticollisión en el dron y rutas adaptadas para minimizar molestias acústicas. Se debe explicar cómo la estación *Drone-in-a-Box* ejecuta automáticamente despegues y aterrizajes y qué procedimientos de emergencia están programados (por ejemplo, retorno autónomo a la base o aterrizaje seguro en un punto designado ante pérdida de comunicación). También es fundamental describir la integración con la CCRRAA: qué personal supervisará los drones (operadores de central habilitados como pilotos remotos), cómo se ordena el despegue cuando salta una alarma, y cuáles son los protocolos de video verificación a seguir con las imágenes obtenidas.
- c) **Coordinación del espacio aéreo:** debido a que las operaciones BVLOS se realizan sin supervisión visual local, es imprescindible evitar conflictos con otras aeronaves. AESA puede imponer condiciones de segregación del espacio aéreo para garantizar la seguridad de la operación. En general, se plantean dos escenarios:

- a. **La planta fotovoltaica está en una zona rural fuera de espacios aéreos controlados:** el riesgo de tráfico tripulado es bajo; puede bastar entonces con mantener altitudes reducidas de vuelo (p. ej., ≤ 60 m) y equipar el dron con sistemas de identificación electrónica (ADS-B, balizas) para alertar a posibles aeronaves en la zona.
- b. **La planta se sitúa cerca de un aeródromo o en espacio aéreo controlado:** será necesario establecer coordinación con los servicios de control de tráfico aéreo (ATC) y/o limitar altitudes y horarios de operación del dron para evitar interferir con tráfico tripulado. Cabe señalar que el RD 517/2024 ha eliminado la necesidad de coordinar con ATC ciertas operaciones BVLOS en espacio controlado por debajo de 60 m de altura y fuera de entorno de aeródromo, lo cual ha agilizado algunas vigilancias BVLOS. No obstante, si la operación supera esos límites, AESA exigirá un plan específico de coordinación (por ejemplo, emisión de NOTAM⁵ o integración en un espacio *U-Space*) para mitigar los riesgos aéreos.
- d) **Medidas de mitigación de riesgos (SORA):** el análisis SORA aplicable a una planta fotovoltaica recomendará diversas medidas de seguridad. Para reducir el riesgo en tierra (GRC), la mitigación principal consiste en mantener una zona controlada sin personas bajo la trayectoria del dron, de forma que cualquier caída ocurra en un área sin terceros. Los perfiles de vuelo deben limitar altitud y velocidad para reducir la energía de impacto potencial, y en algunos casos se podría exigir equipar el dron con paracaídas u otros dispositivos que atenúen daños en caso de caída. En cuanto al riesgo en aire (ARC), es clave limitar la altura de vuelo (p. ej., ≤ 90 m) para reducir la probabilidad de conflicto con aviación tripulada, e idealmente dotar al dron de sistemas de detección y evitación (DAA) activos para identificar aeronaves próximas y maniobrar si es necesario. Adicionalmente, para aumentar la visibilidad electrónica, se pueden usar transpondedores ADS-B u otros dispositivos de señalización. Otro aspecto crítico es la continuidad de

⁵ Organización de Aviación Civil Internacional (OACI), Anexo 15 al Convenio sobre Aviación Civil Internacional: Servicios de Información Aeronáutica, 16.^a ed. (Montreal: OACI, 2018), cap. 1. La normativa define el NOTAM (por sus siglas en inglés, *Notice to Airmen* o Aviso a los Aviadores) como un «aviso distribuido por medios de telecomunicaciones que contiene información relativa al establecimiento, condición o modificación de cualquier instalación aeronáutica, servicio, procedimiento o peligro, cuyo conocimiento oportuno es esencial para el personal encargado de las operaciones de vuelo».

enlace C2: la operación debe tener protocolos claros para pérdida de la comunicación entre el dron y la CRA o el piloto remoto. Es imprescindible programar a la aeronave para ejecutar automáticamente un procedimiento de contingencia si el enlace se corta: por ejemplo, mantener vuelo estacionario un tiempo breve y luego efectuar un retorno autónomo al punto de despegue. Si se pierde la señal GNSS⁶ y el dron no puede navegar de vuelta, debe preverse un aterrizaje automático controlado en una zona segura dentro de la planta. Todas estas respuestas de contingencia deben documentarse en el ConOps y los manuales operativos. El ConOps debe incluir también los umbrales meteorológicos que determinan la suspensión de vuelos (velocidad máxima de viento, lluvia intensa, tormentas eléctricas, etc.), para no comprometer la seguridad. Asimismo, el análisis SORA debe contemplar medidas de protección de datos. La operación de drones con cámaras requiere acreditar el cumplimiento del RGPD y la LOPDGDD. Deben adoptarse medidas como carteles de aviso de videovigilancia con drones, limitar el ángulo de visión de las cámaras, restringir el campo visual del dron al interior del recinto y aplicar técnicas para garantizar la minimización de datos personales (por ejemplo, difuminado de áreas externas). Igualmente, la solicitud de autorización a AESA debe identificar a los puntos de contacto del operador, asegurar su disponibilidad 24/7 para coordinación con autoridades en caso necesario, e incorporar la CCRRAA como estación de control remoto en su Manual de Operaciones, detallando cómo se gestionan los drones desde la central, incluyendo cómo se recibe y analiza el vídeo y cómo se comunicará con las FFCCSE en caso de intrusión confirmada. Si la operación considera la gestión simultánea de varios drones (multi-UAS), el SORA debe demostrar claramente la viabilidad de que un único piloto supervise múltiples aeronaves a la vez. Se requiere justificar que la carga de trabajo es asumible, que se cuenta con medios técnicos adecuados (como interfaces que integren las señales de varios drones) y que existen procedimientos de emergencia para garantizar la seguridad en todo momento.

⁶ Organización de Aviación Civil Internacional (OACI), Anexo 10 al Convenio sobre Aviación Civil Internacional: Telecomunicaciones Aeronáuticas, Volumen I (Radioayudas para la navegación), 7.ª ed. (Montreal: OACI, 2018), cap. 2. La normativa define el Sistema Mundial de Navegación por Satélite (GNSS) como un «sistema mundial de determinación de la posición y de la hora, que incluye una o más constelaciones de satélites, receptores de aeronave y supervisión de la integridad del sistema». En consecuencia, la señal GNSS es la emisión de radiofrecuencia continua transmitida por dichas constelaciones (como GPS o Galileo), que proporciona los datos de temporización y orbitales necesarios para que los receptores, incluidos los de los sistemas de aeronaves no tripuladas (UAS), calculen su posición tridimensional con exactitud.

- e) **Obligaciones del operador UAS:** la explotación de UAS en el ámbito de la seguridad privada conlleva obligaciones organizativas y regulatorias. El operador UAS —que puede ser la empresa de seguridad contratada o la propia empresa titular de la planta si asume directamente la operación— debe cumplir con los requisitos de AESA y coordinarse con otros organismos competentes. Entre las principales exigencias se encuentran:
- a. **Registro del operador y aeronaves:** el operador debe inscribirse en AESA (consiguiendo un número de registro de operador con prefijo ESP que ha de figurar en todas sus aeronaves) y asegurar que cada dron lleva una placa identificativa y, de ser necesario, un sistema de Remote ID activo. La ausencia de registro o identificación adecuada se considera infracción grave en seguridad aérea, con posibles sanciones administrativas.
 - b. **Competencia del personal:** los pilotos a distancia a cargo deben estar cualificados para vuelos en categoría específica (formación avanzada, examen práctico y certificaciones específicas, como la de radiofonista UAS si la operación prevé interacción con el tráfico controlado). Dado que los operadores de CCRRAA que gestionen drones cumplirán un doble rol, de piloto remoto y de operador de seguridad privada, se hace recomendable una doble formación: certificación como piloto UAS y familiarización con protocolos de video verificación, normativa de seguridad privada y coordinación con fuerzas de seguridad.
 - c. **Manual de operaciones:** es imprescindible disponer de un Manual de Operaciones coherente con el ConOps y la evaluación SORA, donde se describan todas las fases de la operación y los procedimientos ante posibles contingencias. Este manual debe integrar las responsabilidades de la CCRRAA, detallar quién asume la posición de piloto al mando en cada misión, los chequeos pre-vuelo del dron, la gestión de las comunicaciones seguras y las respuestas previstas ante emergencias (pérdida de enlace, intrusión de otra aeronave, accidentabilidad). AESA puede auditar e inspeccionar la operación para verificar el cumplimiento de esta documentación en la práctica.
 - d. **Seguro de responsabilidad civil:** tanto la normativa europea como la nacional exigen un seguro de responsabilidad reservado a riesgos asociados al uso de UAS en categoría específica, que cubra los posibles daños a terceros y a la instalación. Aunque las pólizas mínimas obligatorias varían según la masa del dron y el tipo de operación, en este contexto industrial es fundamental contar con coberturas amplias por potenciales contingencias (por ejemplo, daños a infraestructuras críticas, lesiones a personal,

violación de privacidad). La falta de seguro o la insuficiencia de la cobertura puede acarrear sanciones y una exposición directa a reclamaciones civiles.

- e. **Mantenimiento y ciberseguridad:** el operador debe implementar un plan riguroso de mantenimiento preventivo y correctivo que asegure la aeronavegabilidad continuada de los drones, incluyendo revisiones periódicas de motores, hélices, baterías y sensores críticos. Por otra parte, la dependencia de redes y enlaces remotos hace indispensable adoptar sólidas medidas de ciberseguridad: uso de comunicaciones cifradas, control de acceso, autenticación multifactor, protocolos para prevenir *jamming* y *spoofing* (interferencias y suplantaciones), y planes de continuidad operativa en caso de ciber incidente, especialmente si la planta se considera infraestructura crítica.

2.4. Privacidad: requisitos de protección de datos

La incorporación de UAS para la verificación de alarmas conlleva un tratamiento de imágenes potencialmente identificativas de personas, lo que implica cumplir estrictamente la legislación de privacidad: RGPD y LOPDGDD, además de las directrices de la Agencia Española de Protección de Datos (AEPD) en materia de sistemas de captación de imágenes. Es necesario adaptar los principios de protección de datos a esta tecnología:

- a) **Legitimación y finalidad:** el tratamiento de imágenes mediante drones puede estar legitimado en la medida en que responda a la necesidad de garantizar la seguridad de personas y bienes (misión de interés público). Debe limitarse la finalidad a la verificación de alarmas de la instalación, sin utilizaciones posteriores incompatibles.
- b) **Privacidad desde el diseño y minimización de datos:** el ConOps de los UAS debe aplicar el principio de «privacidad desde el diseño y por defecto». Como sistemas de captación de imágenes móviles, es imprescindible implementar salvaguardas que aseguren la minimización de datos. Para ello, se deben emplear medidas técnicas como el geo-vallado (que impide al dron salir del espacio autorizado) y máscaras dinámicas de privacidad (que difuminan o bloquean imágenes captadas fuera del perímetro protegido), de modo que la recolección de información se limite estrictamente al entorno autorizado.
- c) **Evaluación de impacto en la protección de datos (EIPD):** conforme al RGPD, antes de iniciar el tratamiento debe realizarse una EIPD cuando se utilizan tecnologías susceptibles de alto riesgo para los derechos fundamentales. La captación de imágenes móvil mediante drones encaja en este supuesto, por lo que es obligado evaluar exhaustivamente su impacto: analizar la tecnología empleada, justificar la necesidad de

su uso y detallar las medidas para mitigar riesgos (encriptación de transmisiones, limitación en el ángulo de las cámaras, rutinas automáticas de borrado de imágenes no relevantes, etc.). Esta evaluación, a cargo del delegado de protección de datos, permitirá calibrar los riesgos residuales y establecer controles adicionales si fuera necesario.

- d) **Obligaciones de transparencia y minimización temporal:** la empresa responsable del tratamiento (el titular de la planta o la empresa de seguridad encargada) debe cumplir con la información a los afectados: colocar carteles visibles en todos los accesos al recinto, informando sobre la existencia de videovigilancia con drones y el modo de ejercer derechos (acceso, rectificación, supresión, etc.). En cuanto a la conservación de imágenes, la normativa obliga a eliminar las grabaciones en un plazo máximo de un mes desde su captación, salvo que sea necesario conservarlas para ponerlas a disposición de las autoridades (por ejemplo, si registran un delito). Estas pautas se aplican igualmente a las imágenes transmitidas por el dron, que deben considerarse parte del subsistema de seguridad de la planta. Si una empresa de seguridad externa opera los drones y accede a las imágenes, actúa como encargado del tratamiento, relación que debe formalizarse mediante contrato conforme al artículo 28 RGPD y controlarse por el delegado de protección de datos (obligatorio en empresas de seguridad privada). Cumpliendo estas directrices, el uso de drones como herramienta de seguridad queda legitimado sin vulnerar derechos fundamentales ni incurrir en infracciones de protección de datos, fortaleciendo la aceptación social de la tecnología.

2.5. Sistemas de seguridad perimetral en plantas fotovoltaicas. Medios tecnológicos y humanos.

La protección de una planta fotovoltaica exige un diseño de seguridad integral, orientado a mitigar y controlar los riesgos de intrusión, robo y vandalismo. La arquitectura de seguridad combina múltiples subsistemas tecnológicos con protocolos operativos estrictos, buscando una respuesta eficaz y ajustada a la normativa:

- a) **Subsistema perimetral fijo (sensores y cámaras):** la protección del perímetro es prioritaria. Se despliega una red de cámaras termográficas repartidas estratégicamente según la orografía y la disposición de los paneles solares. Estas cámaras detectan la firma térmica de intrusos potenciales incluso en ausencia de luz, y transmiten la señal a un sistema central con analítica de vídeo (inteligencia artificial) capaz de discriminar entre un ser humano y la de un animal. Solo cuando el algoritmo identifica un patrón compatible con una presencia intrusa, el sistema genera una alarma de intrusión hacia la

CRAA. Todas las cámaras funcionan en un circuito supervisado: cualquier pérdida de señal o intento de sabotaje produce una alarma técnica inmediata en la CRAA, garantizando la vigilancia continua. En paralelo, la planta está equipada con un sistema de alarma anti-intrusión con detectores volumétricos y magnéticos en recintos sensibles (centros de control, subestaciones, etc.), centralizados en un subsistema anti-intrusión que envía las señales a la CRAA. El subsistema visual podría complementarse con cámaras domo motorizadas PTZ, configuradas con preposiciones para apuntar automáticamente a puntos críticos ante activaciones de alarma, enriqueciendo la información disponible para la verificación.

- b) **Verificación personal y servicio de «acuda»:** la verificación personal es el tercer pilar del sistema de seguridad, complementando la verificación técnica. Consiste en el desplazamiento de vigilantes de seguridad habilitados al lugar de la alarma para confirmar presencialmente la situación (Orden INT/316/2011). Este procedimiento está estrictamente reglado: ante una alarma no confirmada por vídeo o audio, la CRAA contacta de inmediato tanto con las FFCCSE como con el servicio de «acuda» para que se dirijan al lugar. Los vigilantes acuden uniformados y equipados, y para acceder al interior de la instalación han de hacerlo siempre en binomio (dos vigilantes), conforme a la normativa, lo que les permite actuar con mayor seguridad cubriéndose mutuamente. La custodia de llaves de la instalación suele gestionarse en la CRAA, de manera que los vigilantes tengan acceso a recintos cerrados. La tarea fundamental del equipo de «acuda» es verificar físicamente la intrusión, inspeccionando el perímetro y los puntos sensibles para detectar daños o la presencia de personas. Deben informar en tiempo real a la CRAA de sus hallazgos, para su eventual transmisión a las FFCCSE. Si la CRAA pierde la señal de vídeo o detecta un fallo de comunicación que impide la verificación remota, sería preceptivo activar a un vigilante de «acuda» para asegurar la continuidad de la vigilancia *in situ*.

Desde una perspectiva jurídico-operativa, no cabría sostener que los drones autónomos sustituyan este servicio de verificación personal, sino, más bien, que se integren como medios técnicos de apoyo con una función eminentemente informativa y disuasoria, permaneciendo la resolución última del incidente bajo la esfera de la intervención humana habilitada.

3. Objetivos

3.1. Objetivo General

Analizar la viabilidad jurídica y la coherencia técnico-operativa de la integración de sistemas de aeronaves no tripuladas (UAS) con capacidades autónomas (*Drone-in-a-Box*) como medio de apoyo en la verificación de alarmas perimetrales de plantas fotovoltaicas en España, garantizando el cumplimiento de la normativa aplicable (aeronáutica, seguridad privada y protección de datos).

3.2. Objetivos Específicos

Para alcanzar el objetivo general se plantean los siguientes objetivos específicos:

1. **Analizar el marco normativo aeronáutico aplicable:** examinar las disposiciones del Real Decreto 517/2024 y del Reglamento (UE) 2019/947, identificando las limitaciones legales actuales para la autonomía de los UAS en operaciones BVLOS, y justificando la necesidad de recurrir a la Categoría Específica (con autorización operacional individual) frente a la imposibilidad de encajar en la categoría abierta o en un Escenario Estándar.
2. **Aplicar la metodología SORA a un caso real:** desglosar la metodología **SORA** en un escenario representativo de una planta fotovoltaica aislada, mostrando cómo la delimitación perimetral de la instalación actúa como mitigación clave para reducir la clase de riesgo y alcanzar un Nivel SAIL moderado (II o III), y cómo el cumplimiento de los OSO correspondientes permite obtener la autorización de AESA.
3. **Determinar el encaje en la seguridad privada:** evaluar la integración de UAS autónomos en el marco de la Ley 5/2014 de Seguridad Privada y la Orden INT/316/2011, precisando su rol como sensor avanzado de video verificación en las centrales receptoras de alarmas y su coordinación con el servicio de verificación personal, sin menoscabar las competencias exclusivas de intervención asignadas al personal de seguridad privada.
4. **Establecer protocolos de privacidad y protección de datos:** definir los requerimientos de «privacidad desde el diseño» (geo-vallado, enmascaramiento de imágenes, encriptación de comunicaciones) necesarios para garantizar el cumplimiento de la LOPDGDD en las operaciones de video verificación aérea, evitando vulnerar derechos fundamentales y asegurando la legitimidad del uso de drones para seguridad.

4. Metodología

4.1. Enfoque metodológico

La presente investigación adopta un diseño metodológico de naturaleza estrictamente cualitativa, descriptiva y analítica. El núcleo del estudio se fundamenta en una revisión sistemática de carácter normativo y bibliográfico, orientada a diseccionar la convergencia legal y operativa necesaria para la integración de Sistemas de Aeronaves No Tripuladas (UAS) autónomos en la seguridad privada.

Este enfoque cualitativo resulta especialmente idóneo para abordar fenómenos emergentes y de alta complejidad regulatoria donde no se persigue la cuantificación de variables estadísticas, sino la interpretación, el contraste y el análisis crítico de los distintos marcos jurídicos (seguridad aérea, seguridad privada y protección de datos) que condicionan el despliegue de estas tecnologías en infraestructuras críticas.

4.2. Diseño de la investigación: revisión sistemática

Para garantizar la exhaustividad, transparencia y replicabilidad del proceso de búsqueda y selección de fuentes, el diseño de la investigación adapta los principios metodológicos de las revisiones sistemáticas (inspirándose en la trazabilidad de estándares como el modelo PRISMA) al ámbito del análisis jurídico y técnico. Este proceso se ha estructurado en tres fases secuenciales:

4.2.1. Fase de Identificación y búsqueda

La recolección del corpus documental se ha llevado a cabo mediante la consulta directa de fuentes primarias en repositorios institucionales y bases de datos académicas de impacto. La estrategia de búsqueda se ha dividido en dos ejes:

- a) **Eje Normativo e Institucional:** Consulta exhaustiva en el Boletín Oficial del Estado (BOE), el Diario Oficial de la Unión Europea (DOUE), y los repositorios técnicos de la Agencia Estatal de Seguridad Aérea (AESA), la Agencia de la Unión Europea para la Seguridad Aérea (EASA) y la Agencia Española de Protección de Datos (AEPD).
- b) **Eje Doctrinal y Académico:** Búsqueda de literatura científica en bases de datos como Dialnet, Scopus y Web of Science, empleando cadenas de búsqueda booleanas específicas que relacionan términos clave como: «UAS autónomos» y «metodología SORA», o «videovigilancia aérea» y «seguridad privada».

4.2.2. Fase de cribado y criterios de elegibilidad

Para depurar la información obtenida y asegurar la máxima calidad y pertinencia del corpus final, se han aplicado de forma acumulativa los siguientes criterios de selección:

a) Criterios de inclusión:

- I. Documentos normativos de obligado cumplimiento vigentes en el ordenamiento español y europeo (ej. Real Decreto 517/2024, Reglamento de Ejecución (UE) 2019/947, Ley 5/2014, LOPDGDD).
- II. Guías técnicas, directrices y material de orientación (AMC/GM) elaborados por organismos reguladores oficiales (AESA, EASA, AEPD) relativos a la evaluación de riesgos (SORA) y la privacidad desde el diseño.
- III. Artículos científicos, tesis doctorales y manuales técnicos sujetos a revisión por pares, publicados en los últimos 10 años, que aborden la integración tecnológica en la seguridad corporativa.

b) Criterios de exclusión:

- I. Normativa derogada o extemporánea, a excepción de aquella que resulte imprescindible para contextualizar la evolución histórica o comprender el actual anacronismo reglamentario, artículos de opinión, notas de prensa corporativas, publicaciones en foros no oficiales o literatura divulgativa carente de evidencia empírica, soporte institucional o rigor jurídico.
- II. Documentos que aborden la tecnología de los drones desde una perspectiva puramente recreativa, sin traslación directa al ámbito de la seguridad privada corporativa.

4.2.3. Fase de análisis cualitativo y extracción de datos

Una vez configurado el corpus documental definitivo, se procedió a la fase de análisis temático de contenido. La información extraída no se analizó de forma aislada, sino que fue sometida a un proceso de triangulación normativa. Esto implica que las directrices operacionales de la metodología SORA se contrastaron directamente con las exigencias de minimización de datos de la AEPD y con las competencias de las centrales receptoras de alarmas (CCRRAA) estipuladas por el Ministerio del Interior.

Este análisis transversal ha permitido identificar los vacíos legales «zonas grises», las barreras operativas impuestas por los actuales Escenarios Estándar (STS), y fundamentar el

diseño de una propuesta procedimental sólida para el desarrollo de un Concepto de Operaciones (ConOps) y un manual de operaciones viable y legalmente garantista.

5. Resultados de la investigación

El análisis revelaría transformaciones significativas en la concepción de la seguridad perimetral a partir de la integración de drones autónomos, pero también destacaría la persistencia de límites normativos que condicionan su plena implementación. A continuación, se sintetizan los resultados principales:

5.1. Agilidad y movilidad aérea: optimización de la respuesta a alarmas

La integración de un sistema UAS autónomo sincronizado con la CRAA permitiría reducir notablemente los tiempos de verificación respecto a la verificación personal. Mientras que el desplazamiento de un vigilante a un punto remoto de una planta de 100 hectáreas puede requerir varios minutos e incluso alguna hora (dada la orografía y la distancia), un UAS podría sobrevolar el punto en cuestión en segundos desde la activación de la alarma.

Esta extraordinaria movilidad tridimensional confiere a la CRAA una conciencia situacional sin precedentes: el dron, con visión cenital, elimina las «zonas ciegas» de los sensores fijos al poder reposicionarse continuamente, incluso enfocando desde múltiples ángulos. Así, facilita la identificación precoz de intrusos, su seguimiento en tiempo real y la evaluación rápida de las circunstancias.

La información en vivo transmitida por el dron permitiría al operador de la CRAA guiar de forma más detallada a los vigilantes o a las fuerzas policiales hacia el objetivo, mejorando la eficacia y seguridad de la respuesta. En definitiva, el dron, al integrarse con los sensores perimetrales, agregaría agilidad e inmediatez a la respuesta operativa ante amenazas.

5.2. Limite jurídico de la autonomía: complementariedad con la intervención humana

Un hallazgo crucial es la existencia de un «techo jurídico» a la utilidad independiente de esta tecnología. A pesar de la agilidad y precisión que ofrecería un dron autónomo para confirmar una intrusión, legalmente no puede prescindirse de la supervisión humana.

La normativa actual impone que siempre haya un piloto remoto supervisando la misión, y además el dron no tiene capacidad legal ni operativa para sustituir la intervención del personal de seguridad.

La verificación personal de alarmas sigue siendo imprescindible: la Orden INT/316/2011 reserva estrictamente al vigilante habilitado las funciones de verificación personal de alarmas.

Por tanto, el UAS se definiría jurídicamente como un medio técnico de video verificación, que proporciona evidencias videográficas validadas de la intrusión, pero no conllevaría por sí solo la resolución del incidente.

Su auténtica eficacia radicaría en la relación simbiótica con el componente humano: gracias a la inteligencia táctica que aporta el dron, la intervención del vigilante o de las FFCCSE podría ejecutarse con mayor seguridad y efectividad.

El dron optimizaría y complementaría la labor del personal humano, pero no la sustituiría, dado que la presencia humana sigue siendo indispensable como garante de la legalidad y de la toma de decisiones bajo criterios de proporcionalidad, necesidad y responsabilidad.

5.3. Cumplimiento en materia de seguridad aérea (AESA)

La incorporación de drones autónomos en plantas fotovoltaicas exigiría un grado elevado de cumplimiento en materia de seguridad aérea. Bajo el Real Decreto 517/2024, la operativa *DiaB (drone-in-a-box)* se sitúa invariablemente en la Categoría Específica con autorización de AESA, lo que conllevaría una serie de requisitos técnicos y procedimentales superiores a los aplicables en operaciones con drones convencionales.

La aplicación de la metodología SORA en una planta fotovoltaica perimetrada indicaría que el nivel SAIL resultante suele ser II o III, dada la mitigación del riesgo en tierra al mantener ausencia de terceros en la zona de sobrevuelo, así como el limitado riesgo en aire por la baja altura de operación.

Aun así, la AESA exige al operador demostrar el cumplimiento riguroso de los OSO correspondientes a ese SAIL. En la práctica, esto implicaría incorporar mitigaciones robustas en varios frentes: gestión estricta del volumen operacional (geo-cercas para impedir la salida del dron de la zona autorizada, un sistema independiente de finalización de vuelo —*kill switch*— que garantice la caída del dron dentro del recinto en caso de emergencia), redundancias en las comunicaciones (doble enlace radio y redes móviles) y procedimientos específicos para detectar y evitar otras aeronaves (vigilancia del espacio aéreo, DAA o altitud limitada).

De esta forma, se podría conseguir que la operación sea evaluada y declarada segura, obteniendo la autorización de AESA. De no cumplirse alguno de estos requisitos, la autorización sería denegada y la operación no sería legalmente viable.

5.4. Encaje operativo en la seguridad privada

Desde la perspectiva de la seguridad privada, estos drones deberían integrarse plenamente en la operativa del servicio de seguridad de la planta, figurando en los procedimientos de la CRAA y en el Plan de Seguridad del recinto.

El UAS autónomo se equipararía al método de verificación por vídeo definido en la Orden INT/316/2011: las alarmas confirmadas mediante vídeo emitido por el dron serían jurídicamente válidas para su comunicación a las FFCCSE.

En consecuencia, el servicio de verificación personal se beneficiaría de una drástica reducción de falsas alarmas, y la activación de recursos policiales se fundamentaría en evidencias sólidas.

Ahora bien, para asegurar una implementación adecuada, es necesario que el personal implicado cumpla las dos facetas: piloto de UAS habilitado y operador de central receptora de alarmas conocedor de la normativa sectorial.

Así se garantiza que la CRAA gestione los drones dentro de un marco de cumplimiento dual, a la vez técnico-aeronáutico y de seguridad privada. Cabría apuntar que a medio plazo será deseable una actualización del Reglamento de Seguridad Privada que reconozca explícitamente estos medios aéreos.

La falta de mención específica de los UAS en la regulación actual es un factor de incertidumbre interpretativa, que podría generar criterios dispares en la práctica si no se resolviese; por ello es prudente mantener un nivel de crítica constructiva y abogar por un ajuste normativo que disipase estas divergencias.

5.5. Cumplimiento en materia de protección de datos

La salvaguardia de la privacidad aparece como un eje crítico de legitimación de esta tecnología. En la evaluación de impacto en protección de datos (EIPD) que se realice, sería preceptivo la necesidad de implementar con rigor el principio de «privacidad desde el diseño».

En primer lugar, sería imperativo la minimización de datos: la configuración técnica de los UAS debería asegurar que la captación de imágenes se limite a la zona objeto de vigilancia. El

uso de barreras geográficas virtuales y máscaras de privacidad garantiza la estricta focalización de la vigilancia en la planta fotovoltaica.

Asimismo, para cumplir con la transparencia exigida por la LOPDGDD, deberían situarse en los accesos al recinto carteles informativos sobre la videovigilancia con drones, de modo que cualquier persona pueda conocer que su imagen puede ser captada y tratada en ese perímetro.

Además, los flujos de vídeo en tiempo real del dron hacia la CRAA deberían tratarse como datos personales sensibles, aplicando medidas de ciberseguridad —cifrado de datos, canales seguros— y almacenando las grabaciones solo el tiempo indispensable para su finalidad de seguridad (con supresión automática a los 30 días, salvo incidencia).

Cumplidas estas condiciones, el sistema UAS se adecuaría a la normativa de protección de datos, asegurando un equilibrio entre la innovación en seguridad y el respeto a la privacidad de terceros.

6. Discusión

Del análisis integral realizado se desprende que las operaciones de verificación de alarmas mediante video autónoma con drones en plantas fotovoltaicas estarían técnicamente al alcance y ofrecerían una mejora sustancial en la capacidad de detección y respuesta, pero a la vez se moverían en los límites del marco regulatorio vigente.

Si bien la tecnología *Drone-in-a-Box* proporcionaría una vigilancia proactiva y ubicua del perímetro, su despliegue hoy en día no eliminaría la necesidad del factor humano: antes bien, instauraría un modelo híbrido de seguridad donde la intervención humana continúa siendo esencial.

En este sentido, la convergencia entre tecnología y legalidad se lograría en la práctica no prescindiendo del servicio de verificación personal de alarmas, sino haciéndolo más eficiente y seguro mediante la información privilegiada que aportaría el dron.

La CRAA asumiría así un papel ampliado: no solo gestionaría alarmas y coordinaría los servicios de acuda, sino que supervisaría y controlaría drones que actúan como sistemas de captación de imágenes móviles.

No obstante, persistirían retos normativos que delinean el contorno práctico de la solución. En primer término, destacaría la frontera legal de la autonomía: mientras la tecnología

permitiría operaciones cada vez más autónomas e incluso la supervisión de múltiples drones por un único operador, el ordenamiento actual sigue exigiendo, con prudencia, una supervisión humana continua, lo cual impone una dimensión organizativa significativa en la operación (turnos permanentes de pilotos remotos certificados, sistemas de redundancia humana).

Esta restricción normativa, aunque pueda ser percibida como un freno al ideal de automatización 24/7, responde a un principio de cautela necesario para garantizar responsabilidad y seguridad en las fases iniciales de adopción de estas tecnologías.

No es descartable que futuras actualizaciones normativas permitan relajaciones graduales conforme se demuestre estadísticamente la fiabilidad de los sistemas autónomos, pero en la coyuntura actual la supervisión humana es ineludible.

Otro aspecto de debate es la categoría jurídica del dron en la seguridad privada. Si bien se ha argumentado que su función entra en la video verificación técnica, su empleo efectivo aún se sostiene en interpretaciones analógicas de la normativa vigente.

La ausencia de un reconocimiento explícito de estos sistemas crea incertidumbres interpretativas: diferentes actores podrían tener criterios divergentes sobre hasta dónde pueden llegar las capacidades autónomas del dron, o sobre quién debe asumir la responsabilidad en caso de incidentes.

Esta zona gris normativa evidenciada por el estudio subraya la importancia de que el legislador aborde la cuestión en una futura reforma del Reglamento de Seguridad Privada, para dotar de plena seguridad jurídica a estos dispositivos y homologar su uso en las prácticas profesionales.

El análisis ha mostrado asimismo la idoneidad de aplicar la metodología SORA al contexto de las plantas fotovoltaicas. Estas instalaciones, al hallarse en entornos aislados y estar valladas, permitirían mitigar significativamente gran parte de los riesgos, lo que facilitaría la calificación de las operaciones en niveles SAIL manejables para los operadores privados.

Este aspecto es crucial, pues haría viable la obtención de autorizaciones por parte de AESA sin exigir inversiones prohibitivas. Con todo, la implementación de los OSO implicaría a las empresas energéticas asumir nuevos roles, equiparables en algunos aspectos a los de pequeñas organizaciones aeronáuticas (por ejemplo, instaurar un sistema de gestión de la seguridad, planes de mantenimiento, control de cumplimiento normativo, etc.).

En este punto se atisba una brecha de capacidades: compañías habituadas a implantar sistemas de alarma tradicionales se enfrentan al reto de absorber competencias aeronáuticas avanzadas, lo que podría requerir la colaboración con empresas especializadas en operaciones UAS y la formación intensiva de su personal.

Otra cuestión discutida es el régimen de las operaciones continuas con drones. Aunque técnicamente es posible mantener patrullaje constante si se dispone de drones redundantes y estaciones de carga automatizadas, surgen obstáculos prácticos: la fatiga operativa del personal (un único piloto no puede supervisar indefinidamente sin descanso), la necesidad de rotación de drones para recarga y mantenimiento, y las limitaciones actuales en lo relativo a multi-UAS (gestionar más de un dron simultáneamente requiere interfaces y protocolos avanzados, aún en desarrollo).

Además, se advirtió de los límites en caso de pérdida de objetivo: si un intruso sale del perímetro, el dron no podría seguirlo fuera del área autorizada por las restricciones legales de privacidad, lo que obligaría a que la continuidad de la intervención recaiga en las FFCCSE o en el servicio de verificación personal.

Este escenario marca un umbral operativo: la tecnología del dron, aunque potente, tendría un alcance geográfico jurídicamente acotado, por lo que las transiciones entre la fase de video verificación aérea y la de persecución o intervención requieren un protocolo claro de transferencia de la información y la responsabilidad a los agentes humanos.

En suma, la adopción de drones autónomos para la video verificación de las plantas fotovoltaicas representa un salto cualitativo en términos de eficacia y cobertura, pero simultáneamente evidenciaría la necesidad de flexibilizar y adaptar la normativa.

La convergencia final de estos sistemas con la legalidad vigente implicaría tanto aprovechar al máximo sus capacidades de detección y verificación rápida, como reconocer y preservar el papel insustituible de la intervención humana en la protección de personas y bienes. Este equilibrio normativo-tecnológico es fundamental para no comprometer la seguridad jurídica ni la operativa, asegurando así la legitimidad y sostenibilidad de esta innovación en la práctica.

Conclusiones

La presente investigación confirmaría la viabilidad operativa y jurídica (bajo ciertas condiciones) de los sistemas UAS autónomos como vectores para la video verificación, sin perjuicio de los límites que impone el marco normativo vigente. De las secciones anteriores se desprenden las siguientes conclusiones principales:

Consolidación de un marco aeronáutico habilitador: el Real Decreto 517/2024 aporta el andamiaje regulatorio necesario para la operativa *Drone-in-a-Box* en España. No obstante, la plena autonomía de los UAS está jurídicamente acotada: las operaciones plenamente autónomas sin supervisión humana no están permitidas ni en categoría abierta ni realizada la autorización individual en categoría específica. Por tanto, cualquier despliegue de drones autónomos en seguridad perimetral requiere actualmente la implicación de personal humano (pilotos remotos en CRAA) y una autorización operacional basada en análisis SORA. En este sentido, la metodología SORA demuestra ser un instrumento eficaz para captar las particularidades de las plantas fotovoltaicas, cuya naturaleza aislada facilita una baja exposición de terceros y, por tanto, niveles SAIL moderados (II–III) que permiten cumplir las exigencias sin incurrir en requisitos inasumibles.

UAS autónomos como complementos, no sustitutos, del servicio e verificación personal de alarmas: desde la óptica de la seguridad privada, el dron autónomo se integra con éxito como medio técnico de video verificación de forma rápida y fiable, pero no reemplaza la intervención humana en la gestión final del incidente. Sigue siendo imprescindible la verificación personal (servicio de «acuda») y la actuación de las FFCCSE; la función del UAS es proporcionar inteligencia táctica en tiempo real que sirva de apoyo a la toma de decisiones y a la respuesta del personal humano. Este modelo híbrido hombre-máquina refuerza la seguridad privada en su papel de filtro, reduciendo drásticamente las falsas alarmas e incrementando la eficacia de las intervenciones policiales al llegar estas sobre incidentes confirmados y con información previa. En línea con la doctrina de la complementariedad subordinada (Rodríguez, 2020), se consolida la visión de la seguridad privada como aliada indispensable de las FFCCSE, aportando una capa tecnológica que mejora el filtrado y la gestión táctica, pero manteniendo siempre la preeminencia de la autoridad pública y del factor humano en la última fase.

Reforzamiento de la privacidad como condición habilitante: la aplicación de medidas de privacidad desde el diseño es un requisito sine qua non para el despliegue legítimo de estos

sistemas. El cumplimiento de la LOPDGDD demanda geo-vallado, enmascaramiento de imágenes, cartelería informativa y estrictos protocolos de gestión de imágenes. Estas medidas no solo protegen derechos fundamentales, sino que legitiman social y jurídicamente la innovación seguridad, previniendo sanciones por violaciones de privacidad y generando confianza entre los actores implicados y la ciudadanía.

Límites operativos y necesidad de actualización normativa: la implementación real de drones autónomos 24/7 conlleva todavía desafíos operativos (mantenimiento constante, supervisión simultánea de múltiples drones, integración segura en el espacio aéreo) que requieren soluciones tecnológicas y organizativas avanzadas. En paralelo, la falta de mención expresa de estos sistemas en la normativa de seguridad privada crea espacios de incertidumbre, por lo que resulta recomendable una actualización del Reglamento de Seguridad Privada para acomodar formalmente estos medios. De esta forma, se eliminarían riesgos interpretativos y se garantizaría un encaje normativo claro de los drones en la operativa legal de la seguridad privada, homogenizando criterios en todo el sector.

Hacia un modelo consolidado de seguridad inteligente: la integración de UAS autónomos impulsa la evolución de las centrales de alarmas tradicionales hacia auténticos centros de gestión integral de seguridad. Un ConOps bien diseñado y una organización adecuada permiten convertir los datos recogidos por los drones en conocimiento táctico en tiempo real, incrementando la capacidad de anticipación y respuesta ante amenazas. Esta transición hacia una seguridad inteligente representa un salto cualitativo en la protección de activos críticos: la inclusión de drones como recurso proactivo reduce la dependencia de la reacción tardía, aporta ubicuidad de la vigilancia y permite una gestión de incidentes en tiempo real, protegiendo mejor la continuidad del negocio y los activos estratégicos. Sin embargo, esta evolución conlleva la asunción de estándares organizativos más elevados, equiparables a los de las operaciones aéreas, y demanda una constante formación y adaptación de los profesionales de seguridad privada a nuevos roles y responsabilidades.

8. Futuras líneas de investigación

El presente trabajo, al situarse en la intersección de normativas y tecnologías emergentes, sugiere diversas direcciones para explorar en futuras investigaciones:

- a) **Actualización del marco normativo de seguridad privada:** se identifica la necesidad de análisis específicos sobre cómo un nuevo Reglamento de Seguridad Privada podría

integrar expresamente los sistemas UAS. Una línea de investigación consiste en formular propuestas concretas de reforma normativa, estableciendo estándares y responsabilidades claras para la instalación, operación y control de drones de seguridad. Incluiría aspectos como la habilitación del personal que los opera, la supervisión de la autoridad competente, o la clarificación de la responsabilidad ante incidentes.

- b) **Inteligencia artificial y automatización en videovigilancia:** explorar cómo la inteligencia artificial (IA) puede mejorar aún más la detección y clasificación de amenazas en los flujos de vídeo de drones, manteniendo el requisito de supervisión humana para las decisiones críticas. Esto abarca el desarrollo de algoritmos de aprendizaje automático capaces de identificar comportamientos sospechosos de forma autónoma, y el análisis ético y legal de la toma de decisiones asistida por IA en seguridad privada.
- c) **Operaciones multi-UAS a gran escala:** investigar la viabilidad de desplegar flotas coordinadas de drones autónomos en la protección de extensas infraestructuras, con un único centro de control. Esto implica estudiar la carga de trabajo de un piloto remoto supervisando varios drones, el diseño de interfaces hombre-máquina eficientes que integren múltiples flujos de vídeo, y los límites operativos en contextos de intrusiones múltiples simultáneas.
- d) **Resiliencia y ciberseguridad en sistemas *Drone-in-a-Box*:** dada la dependencia de la conectividad en estos sistemas, es fundamental investigar cómo reforzar la ciberseguridad y la resiliencia frente a intentos de *hacking* o sabotaje digital. Otra línea de investigación es el estudio de redundancias técnicas (*backups* de comunicaciones, sistemas anti-interferencias) que permitan sostener operaciones seguras incluso en escenarios de fallo o ataques cibernéticos, dado que la confiabilidad de las comunicaciones es crucial para la seguridad de la operación.

Referencias bibliográficas

- Fernández Chiclano, R. (2024). *Utilización de sistemas RPAS en labores de protección de seguridad ciudadana en la Guardia Civil*. [Tesis doctoral, Universidad Católica de Murcia]. Repositorio Institucional UCAM.
- Galdón Carreño, A. J. (2025). *Taxonomía para la evaluación del peligro: hacia la búsqueda de una metodología específica de evaluación del riesgo en centrales receptoras de alarmas*. [Trabajo Fin de Grado, Universidad Isabel I].
- González Puente, C., y González Botija, F. (2018). *Los drones y los derechos fundamentales en la UE*. Revista Universitaria Europea, (29), 143-162.
- Instituto Español de Estudios Estratégicos. (2026). *Geopolítica del espacio (Cuadernos de Estrategia 235)*. Ministerio de Defensa, Secretaría General Técnica.
- Ley 5/2014, de 4 de abril, de Seguridad Privada. (2014, 5 de abril). Boletín Oficial del Estado, núm. 83, pp. 28951-29002. <https://www.boe.es/eli/es/l/2014/04/04/5/con>
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018, 6 de diciembre). Boletín Oficial del Estado, núm. 294, pp. 119788-119857. <https://www.boe.es/eli/es/lo/2018/12/05/3/con>
- Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada. (2011, 18 de febrero). Boletín Oficial del Estado, núm. 42, pp. 18274-18288. <https://www.boe.es/eli/es/o/2011/02/01/int316/con>
- Organización de Aviación Civil Internacional. (2018). *Anexo 10 al Convenio sobre Aviación Civil Internacional: Telecomunicaciones aeronáuticas*. Volumen I: Radioayudas para la navegación (7.ª ed.).
- Organización de Aviación Civil Internacional. (2018). *Anexo 15 al Convenio sobre Aviación Civil Internacional: Servicios de información aeronáutica* (16.ª ed.).
- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada. (1995, 11 de enero). Boletín Oficial del Estado, núm. 10, pp. 917-943. <https://www.boe.es/eli/es/rd/1994/12/09/2364/con>

- Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas (UAS). (2024, 5 de junio). Boletín Oficial del Estado, núm. 136, pp. 65613-65691.
<https://www.boe.es/eli/es/rd/2024/06/04/517>
- Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas. (2019, 11 de junio). Diario Oficial de la Unión Europea, L 152, pp. 45-71.
http://data.europa.eu/eli/reg_impl/2019/947/oj
- Rodríguez Rodríguez, J. F. (2020). *Análisis de la Legislación Española en materia de Seguridad Privada* [Tesis doctoral, Universidad Católica de Murcia]. Repositorio Institucional UCAM.
- Savall Ibiza, V. (2022). *Ciber-tecnologías de la vigilancia: Un estudio comparativo a escala nacional sobre la aplicación de las nuevas técnicas de control en la seguridad pública y privada* [Trabajo Fin de Grado, Universidad Miguel Hernández].
- Soria Fernández, A. (2020). *Normativa de drones (RPAS) civiles en España: Análisis de su creación y evolución* [Trabajo Fin de Grado, Universitat Autònoma de Barcelona]. Dipòsit Digital de Documents de la UAB.
- Torres Gomis, S. (2025). *Drones en Operaciones no EASA Directas: Marco Normativo y Prácticas Policiales* [Trabajo Fin de Grado, Universidad Miguel Hernández de Elche].