

EMERGENCIAS

Revista oficial
del SPPME-A
Año 2026
Nº 001



092





SINDICATO PROFESIONAL DE POLICÍAS MUNICIPALES DE ESPAÑA - ANDALUCÍA

EDICIÓN: La revista EMERGENCIAS 092 es una publicación periódica, de ámbito autonómico, del Sindicato Profesional de Policías Municipales de España-Andalucía (SPPME-A).

ARTÍCULOS: Como revista divulgativa en el ámbito competencial y de interés para la Policía Local de Andalucía, los artículos publicados han pasado una revisión para evaluar su actualidad, originalidad, calidad y rigor profesional.

PERMISO DE REPRODUCCIÓN: Se autoriza la impresión y difusión de esta revista por cualquier tipo de medio. Quedan reservados todos los derechos del Autor, prohibiéndose cualquier copia total o parcial de los artículos contenidos en esta obra, para su inclusión en otras publicaciones, salvo autorización expresa de sus autores.

Revista EMERGENCIAS 092 del
Sindicato Profesional de Policías
Municipales de España-Andalucía
(SPPME-A) ®
Fundada en 2025
Primera época. Año I. Nº 001. 2026

Edición, dirección y administración
Sindicato Profesional de Policías
Municipales de España-Andalucía
(SPPME-A)

Avda. Málaga nº 12, bajo izquierda
41004 Sevilla. Tel: 646 136 645
sppme-a@sppme-a.es
www.sppme-a.es

Maquetación
ANURA DIGITAL, S.C.

ISSN 3101-2701
Título clave: Emergencias 092

EJEMPLAR DE DISTRIBUCIÓN GRATUITA

Esta publicación electrónica se divulga y distribuye con la colaboración del Sindicato Profesional de Policías Municipales de España-Sección Andalucía.

Se publicará en la Revista online del SPPME-A, con la finalidad de actualizar y perfeccionar sobre esta temática a los interesados en ella.

Siendo de interés policial, su visualización, así como su impresión, estará disponible para cualquier Policía Local que esté interesado en formarse y mejorar profesionalmente.

© Reservados todos los derechos del Autor, queda prohibida cualquier copia total o parcial de esta obra para su inclusión en otras publicaciones, salvo autorización expresa de sus autores. Queda autorizada su impresión y difusión por cualquier tipo de medio.

ÍNDICE

- 1. SISTEMAS DE RETENCIÓN INFANTIL EN AUTOMÓVILES.
ACTUACIÓN POLICIAL: CONTROL, PREVENCIÓN Y EDUCACIÓN.**
AUTOR: MIGUEL ÁNGEL RODRÍGUEZ OCHOA
Páginas: 4 - 27
- 2. ACTUALIZACIÓN DRONES REAL DECRETO 517/2024.
ACTUACIÓN POLICIAL LOCAL OPERACIONES NO EASA**
AUTOR: MIGUEL ÁNGEL RODRÍGUEZ OCHOA
Páginas: 28 - 55
- 3. INTRODUCCIÓN A LA CIBERSEGURIDAD I**
AUTOR: FRANCISCO DE BORJA VIEJO ARENAL
Páginas: 56 - 72



SISTEMAS DE RETENCIÓN INFANTIL EN AUTOMÓVILES. ACTUACIÓN POLICIAL: CONTROL, PREVENCIÓN Y EDUCACIÓN.

AUTOR: MIGUEL ÁNGEL RODRÍGUEZ OCHOA

Nº 04/ 2025/ 3041 INSCRIPCIÓN EN EL REGISTRO DE
PROPIEDAD DE LA JUNTA DE ANDALUCÍA (NINF@)

ÍNDICE DE CONTENIDOS

Prólogo

Introducción

Objetivos

- . Analizar la normativa legal imperante en el tema de sistemas de retención infantil (SRI).
- . Clasificar y definir las distintas clases de SRI homologados.
- . Desarrollar pautas técnicas y operativas para la supervisión del uso correcto de los SRI.
- . Impulsar un enfoque preventivo y educativo en la labor policial.
- . Potenciar la formación específica del policía.
- . Fomentar cooperación entre instituciones para una protección integral en el transporte infantil.

Marco Legal Vigente

- . Reglamento UNECE R44/04
- . Reglamento UNECE R129 (i-Size)

Clasificación de los Sistemas de Retención Infantil

Intervención Policial: Control, Prevención y Educación

1. Control en Vía Pública, Supervisión y Vigilancia
2. Prevención y Educación Vial
3. Coordinación Interinstitucional
4. Propuestas Operativas de Mejora
5. Medición del Impacto de la Intervención Policial

Criterios Técnicos para la Inspección del SRI

Transcendencia Científica del uso correcto de los SRI y la contramarcha (ACM)

Conclusión

Bibliografía

PRÓLOGO

Introducción, Objetivos, Desarrollo, Conclusión: La seguridad vial infantil establece un eje prioritario dentro de los estudios públicos para protección de la infancia. La Policía Local Andaluza, por su cercanía a la ciudadanía y su función educativa y sancionadora, desempeña un papel fundamental en el control del uso correcto de los Sistemas de Retención Infantil (SRI). En la presente publicación profundizaremos en los aspectos técnicos, normativos y operativos de dicha supervisión, basándose en el marco legal vigente y en los estudios científicos internacionales.

Nuestra finalidad será analizar la normativa legal aplicable a los SRI, clasificar las clases existentes en el marco vigente, establecer criterios técnicos para la inspección policial, promover una perspectiva educativa en la actuación policial, engrosar la formación técnica de los policías y promover la cooperación interinstitucional para un plan general de seguridad infantil en el tráfico.

Se expone un estudio exhaustivo de las normativas europeas R44/04 y R129, donde se describe los sistemas de retención según peso, estatura y orientación o ubicación. Se definirán las pautas de inspección que deben seguir los agentes de Policía Local, incluyendo características técnicas claves como homologación, anclaje y uso del sistema. Asimismo, se estudian tácticas de prevención, campañas educativas y coordinación con entidades sociales y educativas. Los conocimientos o experiencia del trabajo se extraen de obras científicas recientes que respaldan la operatividad de los SRI en la reducción de la mortalidad y lesiones infantiles.

La Policía Local en Andalucía debe llevar a cabo su trabajo poniendo el foco en la prevención y el trato humano, mezclando el rigor técnico con vocación profesional. Su arbitraje en el uso de SRI es clave con los menores, ya que su intervención es una herramienta decisiva en la salvaguarda y protección de la infancia, en tanto convierte el conocimiento específico en acciones cotidianas de gran efecto en la sociedad.

Los sistemas de retención infantil (S.R.I.) son imprescindibles y deben utilizarse siempre, en cada viaje o en cada trayecto por muy corto que sea, sin excepción. No hay que confiarse ni bajar la guardia en los trayectos habituales y cotidianos. Suelen ser los desplazamientos más cortos, como por ejemplo de casa al cole o a casa de los abuelos, en los que se suelen correr y concentrar más riesgos.

Sistemas de retención infantil, Policía Local, seguridad vial, contramarcha, prevención, vigilancia, serán las palabras que organicen y nos muestren las pautas a seguir para encontrar el equilibrio perfecto para la prevención y protección infantil en el tráfico.

INTRODUCCIÓN

El cuidado de la infancia juega un papel determinante en nuestra sociedad y en la de cualquier país que se precie, especialmente cuando hablamos desde la perspectiva de su bienestar e integridad física. En el entorno que se mueven, los más pequeños representan un grupo de

alto riesgo de vulnerabilidad por sus características físicas y mentales propias de su edad. A diferencia de los adultos, el niño no posee la capacidad de sujetarse bien por sí solo ni de entender los peligros resultantes al viajar en un vehículo. Por eso, las leyes europeas y españolas han enfocado sus esfuerzos en establecer y crear unas reglas que obliguen al uso de asientos especiales para niños, los sistemas de retención infantil (SRI), pensados concretamente para mitigar los efectos de un impacto, asegurando a los niños a bordo ante un frenazo brusco viajando, estos dispositivos, comúnmente conocidas como sillitas de niños para el coche, son sistemas obligatorios y se adecuan dependiendo de la edad, peso y altura los menores.

En este escenario, la Policía Local Andaluza juega un papel de especial relevancia. Dada su cercanía al ciudadano, su labor preventiva y su poder sancionador como agente de la autoridad, le convierten en una pieza esencial para concienciar e impulsar una cultura de seguridad vial infantil. Sin embargo, esta tarea no se puede simplificar en aplicar normas al pie de la letra, requiere de una perspectiva global que mezcle, supervisión, formación, educación, comunicación y trabajo conjunto entre instituciones. La intervención policial en temas de SRI no debe verse solo como una reacción a las infracciones, sino como una medida de protección estructural a largo plazo que abarque la capacitación del actuante, la sensibilización de las familias y la mejora constante de los sistemas de vigilancia.

La realidad estadística actual deja muy claro la urgencia de esta cuestión. Según datos de la Dirección General de Tráfico (DGT, 2024), un 46% de los menores fallecidos en siniestros viales durante el año 2023 no utilizaban un sistema de retención adecuado. Esta cifra evidencia no solo el incumplimiento normativo, sino también una carencia estructural en la concienciación de la población sobre los riesgos que conlleva una instalación o elección incorrecta del sistema. El problema se agrava si se considera que muchos progenitores o tutores desconocen la existencia de diferentes normativas (R44/04 y R129), los criterios de uso por altura o peso, o la importancia de mantener la contramarcha hasta los 15 meses como mínimo.

Diversos estudios han demostrado que la probabilidad de supervivencia de un niño adecuadamente sujeto puede multiplicarse por cinco, especialmente cuando se emplean sistemas en sentido contrario a la marcha (Henary et al., 2007). Esta protección es particularmente relevante en los traumatismos cervicales y craneoencefálicos, principales responsables de la mortalidad infantil por accidente de tráfico. La biomecánica del impacto ha demostrado que los menores que viajan en sentido de la marcha antes de que su estructura ósea esté completamente desarrollada presentan un riesgo significativamente mayor de lesiones irreversibles (BMJ Injury Prevention, 2019).

El presente documento analiza en profundidad el marco legal, técnico y operativo en el que se desarrolla la actuación de la Policía Local en Andalucía respecto al uso de SRI. El enfoque parte

de una perspectiva integradora que combina la base normativa, los conocimientos científicos actualizados, la formación del agente y el desarrollo de estrategias colaborativas con otros actores sociales. Solo así podrá alcanzarse un modelo de movilidad infantil verdaderamente seguro, donde cada intervención policial contribuya de forma directa a la reducción de la siniestralidad y al fortalecimiento de la conciencia colectiva sobre la seguridad vial infantil.

OBJETIVOS

Analizar la normativa legal imperante en el tema de sistemas de retención infantil (SRI)

Este estudio tiene como objetivo principal, realizar un examen a fondo y de manera ordenada de las leyes actuales en relación los Sistemas de Retención Infantil (SRI). Esto implica tanto la legislación a nivel nacional como las propias de cada comunidad autónoma, prestando particular atención a la Comunidad Autónoma de Andalucía. El análisis se centrará en las normas que establecen la obligatoriedad del uso de los SRI para todos, así como las características técnicas y exigencias que deben cumplir estos sistemas para garantizar la seguridad y protección de los menores en los vehículos.

Con ese objetivo, examinaremos con atención las normas fundamentales como como la Ley de Tráfico, Circulación de Vehículos a Motor y la de Seguridad Vial, el Reglamento General de Circulación, así como también las directivas de europea y normas UNE que tiene que ver con la homologación de los sistemas de retención para niños. Asimismo, consideraremos cualquier cambio por actualizaciones en la normativa y las campañas promovidas e impulsadas por la Dirección General de Tráfico (DGT) y otras entidades competentes en la materia.

Un apartado fundamental de este artículo, consistirá en precisar y delimitar las competencias o facultades que tiene la Policía Local en materia de supervisión, control y el fomento del uso idóneo de los SRI. En esta línea, se evaluará la función que desempeña este cuerpo de seguridad en la ejecución efectiva de las leyes y normas, incluyendo su capacidad para llevar a cabo inspecciones, establecer sanciones por infracciones y poner en marcha acciones preventivas y de concienciación dirigidas a la población.

Para concluir este apartado, el estudio examinará como la Policía Local contribuye a evitar o previene de riesgos en las carreteras que afectan directamente en la prevención de riesgos viales que afectan de forma directa a la comunidad infantil, analizando su función no únicamente como policía sancionador, sino también como actor esencial en la enseñanza sobre la seguridad vial y en la defensa del derecho de los más jóvenes a una movilidad segura.

Clasificar y definir las distintas clases de SRI homologados:

Examinar las especificaciones técnicas de las sillas de seguridad infantil que cumplen con las normativas europeas ECE R44/04 y ECE R129 (i-Size), diferenciando como su uso varía en función a los parámetros de peso, estatura y edad del niño. También se explicará la forma correcta de instalarlas en los vehículos, prestando especial atención en el empleo de los sistemas ISOFIX, arneses y cinturones de seguridad, así como a los errores más comunes al colocarlas y usarlas.

Desarrollar pautas técnicas y operativas para la supervisión del uso correcto de los SRI:

Crear una guía práctica de actuación dirigida a los agentes de Policía Local con criterios claros y actualizados para confirmar que los sistemas de retención infantil se emplean como es debido. Durante los controles preventivos de tráfico. Estas directrices cubrirán una correcta y eficaz revisión de la homologación de los dispositivos, su correcta orientación (contramarcha o en sentido de la circulación), su idoneidad para el menor y la comprobación visual de su correcta sujeción en el coche.

Impulsar un enfoque preventivo y educativo en la labor policial:

Resulta crucial que la intervención policial vaya más allá del mero cumplimiento de la ley o dedicarse solo a castigar infracciones. Los Agentes deben asumir un rol más completo y constructivo, priorizando la prevención y formación como pilares fundamentales en su trabajo. Esto implica que los agentes no solo respondan a las infracciones o situaciones de riesgo, sino que también actúen como agentes de cambio social, fomentando una cultura de respeto y responsabilidad ciudadana.

Para alcanzar este objetivo, se promoverán diversas estrategias dirigidas a la sensibilización y formación de la comunidad. Dentro de estas tácticas destacan campañas informativas que empleen diferentes canales de comunicación para llegar a la máxima cantidad de personas posibles, transmitiendo mensajes directos y entendibles sobre normas y ventajas relacionadas con el uso correcto de los Sistemas de Retención Infantil (SRI).

También, se llevarán a cabo talleres interactivos y días de concienciación que comprometan directamente a los diferentes implicados de la sociedad, como son los padres, madres, tutores legales, profesores y cuidadores. Estos eventos servirán para explicar a fondo la relevancia de los SRI, cómo emplearlos correctamente y los posibles peligros asociados a su mal uso o inexistencia. Así, la meta no solo será informar, sino también buscar un compromiso real y un cambio de actitud que mejore la protección de los menores en el transporte.

La formación que reciben los agentes de policía incluye la cooperación con instituciones educativas y organizaciones comunitarias tales como asociaciones vecinales para integrar estos conocimientos dentro de los programas de capacitación y actividades comunitarias. El objetivo es forjar un panorama donde la prevención sea una responsabilidad de todos y la

seguridad vial se considere una prioridad fundamental, aminorando así los siniestros y sus consecuencias negativas que pueden dimanar por no usar bien los sistemas de protección. En resumen, cuando se fomenta una estrategia que prioriza la prevención y la educación ciudadana, la función de la policía se ve mejorada y fortalecida, dejando su rol meramente de control para convertirse en un pilar clave en la construcción de una comunidad más segura, consciente y responsable.

Potenciar la formación específica del policía:

Resulta indispensable fortalecer la capacitación técnica y especializada de los funcionarios policiales, para asegurar una actuación más eficiente en materia de seguridad vial infantil. Con este propósito, se han de concebir e implementar proyectos formativos que aborden de forma comprensiva y exhaustiva las variadas vertientes relacionados con la protección de los menores en su movilidad.

Estos cursos profundizarán en la biomecánica del impacto, permitiendo a los agentes entender el funcionamiento de los sistemas de retención infantil, así como las consecuencias y los efectos que las colisiones puedan tener en el de los pequeños. Gracias a este conocimiento, los agentes del orden podrán evaluar de forma más efectiva las situaciones de peligro e identificar posibles fallos en el uso o colocación de estos sistemas.

Además, la formación deberá abarcar un estudio detallado de las normativas europeas vigentes relativas a la seguridad vial infantil, con el fin de que los agentes estén plenamente familiarizados con las regulaciones y estándares que rigen el uso adecuado de los sistemas de retención y las obligaciones legales asociadas. Este conocimiento les permitirá aplicar la ley con mayor precisión y fundamento.

También es crucial capacitar a los policías en estrategias de comunicación eficaces, de manera que sepan interactuar correctamente con los padres, tutores o con los propios niños. Enseñarles trucos de persuasión y pedagogía permitirá que en las intervenciones policiales no solo se enfoque en sancionar, sino que también ayuden a crear un cambio de actitud positivo y duradero en la comunidad, impulsando que se respeten voluntariamente las normas de seguridad vial.

En resumen, esta formación especializada asegurará que los agentes de policía estén mejor formados para prevenir accidentes, actuar en modo educativo y colaborar para reducir los accidentes y por consiguiente los heridos graves y mortales en la población infantil, promoviendo un entorno vial más seguro en las carreteras para todos.

Fomentar la cooperación entre instituciones para una protección integral en el transporte infantil:

Establecer lazos de cooperación entre la Policía Local y distintas organizaciones o entidades tanto del sector público y como privado, incluyendo centros educativos, centros sanitarios, servicios sociales, ayuntamientos y organismos autonómicos y estatales. Esta concurrencia permitirá diseñar e implementar estrategias conjuntas que fortalezcan la cultura de la seguridad vial desde una perspectiva integral y transversal, con el foco puesto en la protección de los menores como colectivo vulnerable en el entorno del tráfico rodado.

MARCO LEGAL VIGENTE

El uso obligatorio de sistemas de retención infantil (SRI) en vehículos está regulado en España por una combinación de normas nacionales y reglamentación internacional, en particular por la adaptación del Reglamento General de Circulación a través del Real Decreto 667/2015 (BOE, 2015). Esta modificación introdujo criterios más exigentes y alineados con las recomendaciones de seguridad vial de la Unión Europea y de organismos como la Comisión Económica para Europa de las Naciones Unidas (UNECE).

La legislación española establece que los menores de edad de estatura igual o inferior a 135 centímetros deben viajar en vehículos utilizando un sistema de retención infantil homologado y adaptado a su talla y peso, situado preferentemente en los asientos traseros. Esta obligación es de carácter imperativo, y su incumplimiento constituye una infracción grave, sancionada con 200 euros y la pérdida de 4 puntos del permiso de conducir (Dirección General de Tráfico, 2024).

En el plano internacional, existen dos normativas vigentes para la homologación de los SRI:

Reglamento UNECE R44/04: clasifica los sistemas en función del peso del menor (grupos 0, 0+, I, II y III) y permite orientaciones tanto a favor como en contra de la marcha. Dicha normativa ECE R44/04 ha dejado de estar en vigor para la venta de sistemas de retención infantil en el ámbito de la Unión Europea. A partir del 1 de septiembre de 2024, solo se pueden vender sillas con la homologación ECE R129 (i-Size). Sin embargo, las sillas de coche homologadas bajo la normativa ECE R44/04 que ya están en circulación pueden continuar utilizándose, pues mantienen su validez legal y garantizan un nivel adecuado de seguridad.

Reglamento UNECE R129 (i-Size): progresivamente obligatorio desde 2013, es una normativa europea que comenzó a implementarse con el objetivo de mejorar significativamente la seguridad de los niños en los vehículos. A diferencia de regulaciones anteriores que clasificaban los sistemas de retención infantil únicamente por peso, esta regulación establece criterios basados en la altura del niño, lo que permite una mejor adaptación del sistema de seguridad a las características físicas del menor.

Uno de los avances más importantes introducidos por el reglamento i-Size es el refuerzo de los requisitos de protección lateral. Esto pone de manifiesto que los sistemas de retención deben ofrecer un mayor volumen de protección a los niños frente a impactos laterales, bastantes comunes y especialmente peligrosos en los accidentes. Por eso, los estudios de choque con arreglo a esta normativa, son más rigurosos y específicos referente a la simulación de golpes desde distintos ángulos.

Además, la normativa actual exige el uso obligatorio de las sillas orientadas en sentido contrario a la marcha como mínimo durante los primeros 15 meses de vida del bebé. Esta regla se basa en investigaciones que demuestran que colocar a los niños en esta posición disminuye notablemente el riesgo de lesiones graves en la cabeza, cuello y espalda en caso de accidente, ya que la energía de impacto se reparte de forma más gradual y por tanto más segura, por todo el respaldo del dispositivo de retención.

Otra innovación clave que ha impulsado el reglamento UNECE R129 es la apuesta por el sistema Isofix como método estándar para anclar las sillitas en el coche. El sistema Isofix garantiza una fijación más infalible, ágil y sencilla, evitando las equivocaciones más comunes a la hora de instalarlas pudiendo comprometer la eficiencia del SRI. Con esta normalización, los padres más seguros y tienen más confianza en que la sillita está correctamente instalada, aumentando así la seguridad de los niños.

Por lo tanto, la normativa i-Size aporta una mejora notable en la protección infantil en los desplazamientos en vehículos, amoldándose a las últimas investigaciones en seguridad vial y fomentando tecnologías que faciliten el uso perfecto de los sistemas de retención infantil, tal como ha sido distinguido por el Consejo Europeo de Seguridad en el Transporte (ETSC) en 2022.

Ambos reglamentos concurren legalmente, pero las autoridades aconsejan priorizan el uso de SRI bajo la norma R129 por presentar niveles superiores de seguridad. Según la Fundación Mapfre (2023), los sistemas homologados con R129 han demostrado mejores resultados en pruebas dinámicas de impacto lateral y frontal.

COMPARATIVA ENTRE LAS NORMATIVAS R44/04 Y R129 (I-SIZE)

R44/04		R 129	
POR PESO		POR ALTURA	
			
ORIENTACIÓN			
GRUPO 0+	GRUPO 0+ up 13 kg	 0-4 AÑOS	
GRUPO 1	GRUPO 1 9-18 kg	 3,5-12 AÑOS	
GRUPO 2	GRUPO 2 15-25 kg	 2,4-36 cm	
GRUPO 3	GRUPO 3 22-36 kg		

Sistemas de Retención Infantil



Más allá de lo que establece la normativa, la DGT y los expertos en seguridad vial infantil recomiendan utilizar un sistema de retención infantil (SRI) hasta que el niño alcance una altura de 150 cm.

La Policía Local, como autoridad competente en materia de tráfico dentro del ámbito urbano, debe conocer en profundidad ambos marcos regulatorios, ya que durante los controles rutinarios o las campañas específicas de vigilancia (como las promovidas por la DGT) tiene la responsabilidad de identificar y verificar el cumplimiento de los requisitos técnicos y legales del sistema de retención empleado.

Una correcta intervención policial implica la evaluación de varios aspectos:

- Que el SRI esté homologado conforme a alguna de las normativas vigentes (R44/04 o R129), visible mediante etiqueta con código ECE.
- Que el sistema sea adecuado a la edad, peso o altura del menor.
- Que esté correctamente instalado y fijado (preferiblemente mediante Isofix).
- Que se haya desactivado el airbag frontal si el menor viaja en el asiento delantero en sentido contrario a la marcha.

Es importante destacar que, aunque la legislación vigente permite que los menores cuya estatura no supere los 135 centímetros puedan viajar en el asiento delantero del vehículo bajo ciertas circunstancias específicas por ejemplo, cuando el automóvil no cuenta con asientos traseros disponibles o estos están ocupados, desde una perspectiva preventiva y orientada

a la reducción del riesgo de lesiones en caso de accidente, todas las campañas y programas de seguridad vial insisten en que la opción más segura es que los niños viajen siempre en los asientos traseros. Esta recomendación se basa en estudios y estadísticas que demuestran que la protección que ofrecen los asientos traseros es significativamente mayor para los menores, ya que en el asiento delantero existe un mayor riesgo debido a la proximidad del airbag y la estructura del vehículo en caso de impacto frontal. Por tanto, a pesar de que la normativa contempla excepciones, la práctica más aconsejable para garantizar la seguridad de los niños durante los desplazamientos es ubicarlos en la parte trasera del vehículo siempre que sea posible. Esto ayuda a reducir las lesiones y proteger su integridad física en un accidente o siniestro.

La aplicación de esta normativa no solo se ajusta al ámbito sancionador. La Policía Local está facultada para intervenir como agente educador y conciliador entre la norma y la sociedad, difundiendo el conocimiento de la normativa y solventando dudas e inquietudes técnicas que puedan aparecer durante las supervisiones, jornadas educativas o los planes de formación. Este trabajo educativo, alimentado en el conocimiento estricto de la norma, es primordial para el cambio de costumbres y la consolidación de una educación vial protectora de la niñez.

CLASIFICACIÓN DE SISTEMAS DE RETENCIÓN INFANTIL

Entender y tener claro cómo se clasifican los de los sistemas de retención infantil (SRI) es fundamental para una intervención policial eficiente. Ayuda a los agentes de la Policía a saber con precisión si el sistema que se está usando es el correcto, considerando las características de talla y peso del menor. La clasificación de los SRI no solo hace más fácil el trabajo de inspección, sino que también es vital para crear campañas de concienciación usando datos reales.

Actualmente concurren dos reglamentos de homologación vigentes: la UNECE R44/04, absorto en el peso del menor, y la UNECE R129 (conocida como normativa i-Size), basada en la estatura. Esta coexistencia genera cierta controversia entre la ciudadanía, por lo que la tarea educativa de los policías locales es agentes se vuelve fundamental.

Según la normativa europea UNECE R44/04 (por la masa o peso)

Esta normativa, aun en vigor, clasifica los Sistemas de retención infantil en categorías según el peso del niño:

Grupo	Peso del niño	Edad aproximada	Tipo de sistema
0	Hasta 10 kg	0 a 9 meses	Capazo o silla en sentido contrario a la marcha
0+	Hasta 13 kg	0 a 18 meses	Silla en sentido contrario a la marcha
I	9 a 18 kg	9 meses a 4 años	Silla con arneses propios
II	15 a 25 kg	4 a 6 años	Cojín elevador con respaldo
III	22 a 36 kg	6 a 12 años	Cojín elevador (con o sin respaldo)

Esta clasificación, si bien resulta útil, presenta sus fallos, dado que el peso por sí solo no muestra aspectos como el tamaño del tronco o como está el desarrollo óseo, factores clave en la protección ante traumatismos (BMJ Injury Prevention, 2019).

Según la normativa UNECE R129 (i-Size, por altura)

Desde que se implantó gradualmente desde 2013, la normativa R129, representa un progreso sustancial en la protección vial infantil. Se basa en criterios de altura y exige pruebas de impacto lateral. Introduce además la obligación de mantener a los menores en sentido contrario a la marcha hasta al menos los 15 meses, algo ampliamente avalado por la evidencia científica (Henary et al., 2007).

Altura del niño	Edad estimada	Tipo de sistema
40 a 75 cm	0 a 12 meses	Silla en sentido contrario
75 a 105 cm	1 a 4 años	Silla con arneses propios
> 100 cm	> 4 años	Silla con respaldo, uso de cinturón del vehículo

La normativa i-Size también fomenta el uso del sistema Isofix, lo que reduce considerablemente los errores de instalación. Según estudios de la Fundación Mapfre (2023), más del 60% de los errores detectados en la instalación de SRI corresponden a dispositivos anclados con cinturón mal ajustado o con arneses incorrectamente colocados.

Por tanto, se recomienda a las familias optar, siempre que sea posible, por dispositivos homologados bajo R129 y con anclaje Isofix. Esta elección no solo garantiza un mayor nivel de protección, sino que facilita el trabajo de supervisión por parte de los agentes de policía, al ser sistemas con indicadores visuales y auditivos de instalación correcta.

INTERVENCIÓN POLICIAL: CONTROL, PREVENCIÓN Y EDUCACIÓN

La actuación policial no debe basarse solo en verificar del uso adecuado de los sistemas de retención infantil, debe ir mucho más allá. Es importante entender que los agentes de Policía Local en Andalucía, cercanos a la población y desempeñando su función, que debe ir más allá de la mera vigilancia, tiene la responsabilidad de obrar como un verdadero educador social. Su labor no se limita exclusivamente a observar y sancionar infracciones, sino que también deben ser partícipes activos en la transformación de las costumbres y comportamientos de los ciudadanos, fomentando una cultura de seguridad vial ajustada a la protección de los niños.

Por lo expuesto, una acertada intervención policial debe estar sustentada en una visión completa que abarque muchos aspectos. Esto implica no basta la supervisión activa y afanosa en las vías públicas para asegurar que los dispositivos de seguridad infantil se utilicen bien y según las normas vigentes, sino también es necesario poner en marcha campañas preventivas bien estructuradas. Dentro de estos planes o estrategias se harán campañas informativas, talleres de concienciación y trabajar de la mano con colegios y asociaciones vecinales, con el objetivo de sensibilizar a las familias sobre la importancia vital de estos sistemas para salvar vidas y reducir lesiones en caso de siniestros viales.

Por otro lado, la formación continua y el trato frecuente con la población constituyen pilares fundamentales en esta tarea. La Policía Local debe tomar la iniciativa, manteniendo charlas de forma abierta y cercano con la comunidad, resolviendo dudas, dando consejos a medida y adaptando su trabajo a las circunstancias y necesidades específicas de cada barrio o municipio. Así, se ayuda a construir una cultura de respeto y responsabilidad mutua que no solo incrementará la seguridad vial, sino que también consolida la relación de confianza entre los habitantes y las policías locales.

En resumen, la actuación policial en relación de los dispositivos de seguridad infantil debe ser mucho más que un control esporádico de tráfico, debe ser una actividad continua de formación y prevención que impulse una transformación real y permanente en los comportamientos de los ciudadanos, con el objetivo último de salvaguardar la vida y la integridad de los niños durante su movilidad en vehículos.



1.-CONTROL EN VÍA PÚBLICA, SUPERVISIÓN Y VIGILANCIA

Las tareas de control representan la esencia tradicional de la actuación policial, erigiéndose como una herramienta indispensable. Esta supervisión proactiva implica la ejecución de controles específicos y campañas regulares dirigidas a garantizar el empleo apropiado de los SRI. La Policía Local deberá verificar

la disponibilidad del sistema, así como su correcta instalación, la adecuación según el peso y la edad del menor, así como la sensibilización de los conductores respecto su transcendencia. Sin embargo, su eficacia depende en gran medida de la capacitación técnica del agente, de su criterio a la hora de evaluar situaciones diversas y de su habilidad para comunicar de manera clara y empática.

Los puntos de control deben implementarse en ubicaciones estratégicas: accesos a centros educativos, áreas de estacionamiento de centros de salud, entornos urbanos con elevada densidad de tráfico infantil, y durante campañas especiales coordinadas con la DGT o los ayuntamientos.

Durante la inspección, el agente debe:

- Identificar el tipo de sistema de retención utilizado y verificar su homologación (R44/04 o R129).
- Comprobar que el sistema es adecuado a las características del menor (estatura, peso, edad).
- Verificar la instalación y el uso correcto del anclaje (Isofix o cinturón).
- Supervisar el ajuste del arnés, el ángulo de inclinación y la ausencia de objetos sueltos que puedan multiplicar los efectos de una desaceleración brusca.
- Informar al conductor de manera pedagógica en caso de uso inadecuado, entregando material informativo si procede.

La actuación debe ser especialmente rigurosa en caso de reincidencia o situaciones de riesgo manifiesto (ej. menor sin retención alguna), procediendo entonces a la sanción administrativa conforme al artículo 65.4.c de la Ley de Seguridad Vial. El cumplimiento de esta normativa recae sobre el conductor, quien, en caso de incumplimiento, puede enfrentarse a una multa de 200 euros y la retirada de cuatro puntos del permiso de conducir, si es el responsable del menor. Según la Ley de Tráfico y Seguridad Vial en vigor, podrán llegar a inmovilizar el vehículo por no llevar a los niños correctamente sentados.

Podemos decir que los errores más comunes que cometemos los padres a la hora de colocar a nuestros menores los sistemas de retención infantil y por tanto hacer un mal uso de los mismos son:

Colocar al niño sin ajustar bien el arnés:

- Arnés demasiado suelto o demasiado apretado, lo que compromete la seguridad.
- No pasar correctamente las correas por los hombros o no abrochar bien el clip del pecho.

Usar ropa voluminosa en el niño:

- Abrigos o chaquetas gruesas que hacen que el arnés no quede ajustado adecuadamente, aumentando el riesgo en caso de accidente.

No elegir el sistema adecuado según la edad, peso y altura:

- Pasar demasiado rápido a una silla para niños mayores o a un elevador.
- Mantener al niño en un sistema para bebés cuando ya ha superado las especificaciones.

Colocar al niño en la posición incorrecta:

- Orientar la silla hacia adelante cuando el niño debería ir mirando hacia atrás.
- Poner la silla en el asiento delantero cuando es más seguro y recomendable que esté en el asiento trasero.

No asegurarse de que la silla esté bien instalada:

- La silla se mueve o no está bien anclada, lo que puede ser peligroso en un frenazo o choque.
- Uso incorrecto del cinturón de seguridad o del sistema ISOFIX.

No usar el arnés cuando usan sillas elevadoras:

- Algunos padres solo colocan al niño en la silla elevadora sin asegurar el cinturón de seguridad correctamente.

Colocar objetos o juguetes dentro del sistema de retención:

- Esto puede interferir con la correcta colocación del arnés y la comodidad del niño.

Permitir que el niño se quite el cinturón o arnés durante el viaje:

- No supervisar que el niño mantenga bien puesto el sistema.

Ignorar las instrucciones del fabricante:

- No leer o no seguir las recomendaciones específicas para el modelo de silla.

2.- PREVENCIÓN Y EDUCACIÓN VIAL

La prevención estructurada se basa en detectar factores de riesgo antes de que se traduzcan en infracciones o accidentes. Esto incluye identificar patrones de comportamiento inseguros, zonas de riesgo en entornos escolares o residenciales, y establecer planes de acción orientados a reducir la siniestralidad infantil en vehículos. La recopilación de datos, el análisis estadístico y la colaboración con otras instituciones permiten anticiparse a problemas recurrentes y diseñar medidas específicas para evitarlos.

La correcta intervención policial debe contemplar estos tres ejes (control, prevención y educación) como partes interdependientes de una misma estrategia. No se trata únicamente de sancionar, sino de generar conciencia, fomentar hábitos responsables y proteger la vida de los menores como prioridad absoluta. La prevención es el principal instrumento para lograr una movilidad infantil segura. Una de las funciones más transformadoras de la Policía Local es la educación. Esta se concreta en actividades formativas, charlas en colegios, campañas de sensibilización dirigidas a padres y madres, y la distribución de materiales informativos. La educación vial no solo debe estar dirigida a los niños, sino también a los adultos responsables de su transporte. A través de un enfoque pedagógico adaptado y accesible, se puede lograr una mayor implicación social en el uso correcto de los sistemas de retención infantil.

Dentro del abanico de acciones formativas y de divulgación dirigidas a diferentes colectivos, que podría desarrollar la Policía Local, se podrían encontrar:

- **Talleres en centros educativos:** dirigidos tanto a escolares como a familias, con demostraciones prácticas sobre la correcta instalación de SRI.
- **Colaboración con centros de salud:** entrega de folletos y charlas informativas en revisiones pediátricas.
- **Campañas municipales:** mediante redes sociales institucionales, medios de comunicación locales y señalética urbana que refuerce el mensaje preventivo.
- **Convenios con asociaciones profesionales:** de pediatras, autoescuelas, fabricantes de SRI o fundaciones de seguridad vial, para unificar criterios técnicos y mensajes divulgativos.

Estas acciones deben estar sustentadas en la evidencia científica más actual y ajustadas a las particularidades socioculturales del municipio o distrito en el que se desarrollan.

3. COORDINACIÓN INSTITUCIONAL

La seguridad vial infantil requiere una estrategia multisectorial. La Policía Local debe asumir una posición activa en las redes locales de prevención de riesgos infantiles, colaborando con:

- **Direcciones de centros escolares y AMPAs:** para organizar charlas, simulacros y campañas.
- **Servicios Sociales y de Salud:** para detectar situaciones de vulnerabilidad social que puedan limitar el acceso a SRI adecuados.
- **Áreas de movilidad urbana:** para incorporar la perspectiva de infancia en los planes de movilidad sostenible.
- **Otros cuerpos de seguridad:** especialmente Guardia Civil de Tráfico y policías autonómicas, con quienes se pueden compartir buenas prácticas y datos de siniestralidad.

Esta coordinación debe estar formalizada mediante convenios, protocolos o mesas de trabajo locales que aseguren la continuidad y evaluación de las acciones implementadas.

4. PROPUESTAS OPERATIVAS DE MEJORA.

Además de los procedimientos ya establecidos, la Policía Local puede implementar actuaciones específicas de gran impacto social y preventivo, tales como:

- **Puntos de revisión preventiva itinerantes:** unidades móviles en zonas escolares, mercadillos o ferias donde se ofrezcan inspecciones voluntarias y asesoramiento gratuito sobre el uso correcto de SRI.
- **Incorporación de SRI demostrativos en vehículos policiales:** para facilitar la formación práctica durante charlas o controles, y mejorar la capacidad pedagógica del agente.
- **Creación de una base de datos de incidencias:** en colaboración con los servicios sociales, para identificar patrones de riesgo y familias que requieran intervención preventiva personalizada.
- **Protocolos de actuación ante menores no sujetos en vehículos:** estableciendo procedimientos de notificación urgente a servicios sociales o centros educativos si se detecta una situación de riesgo grave o negligencia reiterada.

5. MEDICIÓN EN LA INTERVENCIÓN POLICIAL

Para que una política de seguridad vial sea eficaz, debe incluir mecanismos claros y sistemáticos de evaluación. Sin ellos, las acciones no podrán justificarse ni modificarse adecuadamente. La Policía Local debe consolidar estos datos en informes periódicos que apoyen la continuidad de campañas, la capacitación del personal y la inversión en equipamiento. Se recomienda a las unidades de Policía Local que implementen indicadores para valorar la eficacia de sus actuaciones, tales como:

- Número de controles realizados y número de infracciones detectadas.
- Porcentaje de uso correcto de SRI antes y después de campañas educativas.
- Grado de satisfacción de la población tras acciones divulgativas.
- Evolución de la siniestralidad infantil en el municipio.

Estos datos pueden integrarse en informes periódicos de evaluación que justifiquen la continuidad de las campañas, así como la necesidad de inversión en formación o equipamiento.

CRITERIOS TÉCNICOS PARA LA REVISIÓN DE LOS SRI.

Para una inspección eficiente de los sistemas de retención infantil, no basta solo con conocer la normativa vigente, también se necesita una formación técnica y biomecánica del funcionamiento de estos dispositivos de seguridad. La complejidad de los SRI precisa una formación específica y actualizada que les ayude actuar con precisión, profesionalidad y perspectiva preventiva.

Seguidamente, se exponen los principales criterios técnicos a tener en cuenta por los agentes en un control de tráfico:

- **Homologación del sistema:** el agente debe verificar la presencia de la etiqueta de homologación ECE. Esta puede corresponder a la normativa R44/04 (etiqueta con grupo de peso y código ECE) o a la R129 (con referencia a i-Size y estatura del menor). La ausencia de esta etiqueta invalida el dispositivo como legal.
- **Adecuación del SRI al menor:** es imprescindible evaluar si el sistema está correctamente dimensionado. En la normativa R44/04, el criterio es el peso; en la R129, la estatura. El agente puede solicitar al conductor la edad aproximada del menor, pero deberá guiarse principalmente por la observación física.
- **Sistema de fijación:** se debe comprobar si el SRI está anclado mediante Isofix (más seguro y con indicadores de correcta instalación) o con cinturón de seguridad. En el segundo caso, es más frecuente detectar errores de montaje, holguras o desplazamientos.
- **Sentido de la marcha:** se revisará si el menor viaja en sentido contrario cuando corresponde. En menores de 15 meses, es obligatorio; en muchos casos, es recomendable hasta los 4 años. Viajar en sentido de la marcha antes de tiempo incrementa el riesgo de lesiones cervicales graves (Henary et al., 2007).
- **Arnés y cinturones:** se verificará que el arnés esté bien ajustado (sin holguras, a la altura adecuada de los hombros) y que no presente torsiones. En el caso de elevadores sin respaldo, se comprobará que el cinturón de seguridad del vehículo pase correctamente por el hombro y no por el cuello.
- **Reposacabezas y posición del respaldo:** la altura del respaldo debe adaptarse a la altura del menor, permitiendo una sujeción óptima de cabeza y cuello. El respaldo no debe ir reclinado en exceso, ni el menor debe ir dormido con la cabeza caída hacia delante.
- **Elementos adicionales:** el agente debe observar si existen objetos sueltos (juguetes, mochilas, tabletas) en el habitáculo, ya que en caso de colisión pueden convertirse en proyectiles peligrosos. También puede advertir sobre el uso inadecuado de fundas, reductores no homologados o accesorios comerciales que interfieran con la eficacia del sistema.

Una actuación profesional en el ámbito policial no solo implica el cumplimiento estricto de la normativa y procedimientos, sino que también requiere la aplicación cuidadosa de criterios pedagógicos que permitan un enfoque más humano y formativo en el trato con los ciudadanos. Así, cuando se detectan fallos sin importancia que no revistan gravedad o infracciones leves, el policía podrá optar por una advertencia verbal, intentando dar una explicación técnica y aclaratoria acerca de la índole del error y como poder corregirlo. Esta forma de proceder busca concienciar y fomentar una mejora voluntaria, evitando denunciar siempre que sea posible.

No obstante, en aquellos escenarios en que presenten situaciones de alto riesgo, donde se pueda poner en peligro la seguridad o el orden público, o si alguien es reincidente cometiendo infracciones, resulta imprescindible sancionar estrictamente y de acuerdo con lo estipulado en la normativa legal vigente. Esta acción es clave para disuadir y mantener el orden, garantizando que cada cual asuma las consecuencias derivadas de sus acciones en proporción a su gravedad. Es decir, una intervención profesional debe mezclar la contundencia con una perspectiva pedagógica que fomente la responsabilidad y el respeto a las reglas, ajustando nuestro modo de actuar a la situación para conseguir los mejores resultados tanto para la institución como para todos los ciudadanos.

Finalmente, es muy aconsejable que cada jefatura de Policía Local ponga en marcha y desarrollen sus propios protocolos específicos, junto con unas listas de control que sirvan de guía a la hora de llevar a cabo inspecciones de los Sistema de Retención infantil (SRI). El simple hecho de crear y adoptar estas herramientas ayuda significativamente a la homogeneidad y coherencia a la hora de la intervención, garantizando que todas las inspecciones sigan unas pautas claras y sin fisuras. Aparte, estos protocolos hacen más fácil un registro metódico y ordenado de los datos recopilados en las inspecciones, algo que resulta fundamental para obtener datos fiables y comparables. Esta formación permite realizar valoraciones de las medidas adoptadas con más precisión y más base, lo que ayuda a identificar áreas de mejora, optimizar recursos y que las acciones de la policía sean más eficaces. En resumen, si estos procesos se normalizan y quedan sistematizados, contribuirán a una gestión más transparente, eficaz y enfocada a mejoras en los resultados dentro de las jefaturas policiales.

TRANSCENDENCIA CIENTÍFICA DEL USO CORRECTO DE LOS SRI Y LA CONTRAMARCHA (ACM).

Esta ampliamente documentado, gracias a estudios a nivel internacional, la importancia del uso correcto de los sistemas de retención infantil (SRI). Su efectividad para aminorar lesiones y muertes de menores en siniestros viales ha sido reafirmada por investigaciones biomecánicas y estadísticas a lo largo de los últimos años. Este apartado se integran todos los hallazgos más importantes y se llega a la conclusión de como traducirlas en prácticas policiales más eficientes.

Diversos estudios han establecido que los SRI correctamente instalados y utilizados reducen en un 70-80% el riesgo de lesiones mortales en niños de corta edad implicados en colisiones (Durbin et al., 2003; Arbogast et al., 2004). Según la DGT el uso de los sistemas de retención infantil (S.R.I.) reduce en un 75% las muertes. un 90% las lesiones.

Las lesiones más comunes en menores no sujetos adecuadamente incluyen traumatismos craneoencefálicos, lesiones cervicales y hemorragias internas, todas ellas con alto potencial de letalidad o secuelas permanentes. Se ha demostrado que las lesiones más frecuentes que se producen en niños de hasta 2 años son de cuello generadas por el tamaño de la cabeza y lo fragilidad de la columna vertebral a esta edad. Entre niños 2 y hasta 4 años las lesiones frecuentes son de cabeza ya que la estructura vertebral no es lo suficientemente robusta como para resistir las fuerzas generadas por una desaceleración repentina, mientras que las lesiones en niños de entre 4 a 10 años se concentran en el abdomen, existiendo un riesgo elevado de hemorragias internas o traumatismos abdominales debido a que los órganos aún no están firmemente anclados a la cavidad abdominal.

Uno de los hallazgos más significativos lo ofrece el estudio de Henary et al. (2007), que demuestra que los niños menores de dos años que viajan en sentido contrario a la marcha tienen cinco veces menos probabilidades de sufrir lesiones graves o mortales en comparación con los que lo hacen en sentido de la marcha. Este dato es consistente con estudios más recientes como los realizados por Sherwood et al. (2016) y Zuby (2019), que insisten en la necesidad de prolongar el uso de contramarcha más allá del mínimo legal de 15 meses, idealmente hasta los 4 años.

Está científicamente demostrado que los impactos recibidos en sentido contrario a la marcha son significativamente menos letales que aquellos a favor de la marcha, especialmente en colisiones frontales o desaceleraciones bruscas, bajo condiciones de fuerza equivalentes. No solo lo avalan múltiples estudios y ensayos, sino también la evidencia científica y médica al analizar las lesiones en niños que viajaban a favor de la marcha (AFM), junto con las

ineludibles leyes de la física. Las estadísticas de los países nórdicos como Suecia, Finlandia y Noruega, donde el uso de sillas a contramarcha (ACM) está ampliamente extendido, confirman su eficacia ya que tienen las tasas de mortalidad infantil en carretera más bajas del mundo.

Las sillitas instaladas en sentido contrario a la marcha ofrecen hasta cinco veces más protección que las orientadas hacia delante. Por esta razón, se aconseja mantener a los menores viajando a contramarcha todo el tiempo que sea viable, preferiblemente hasta los 4 años, siempre que sus características físicas lo permitan. La eficacia de una silla a contramarcha no solo depende de su orientación, sino también de que su instalación y uso sean correctos.

Asimismo, los errores de instalación representan una causa común de fallo del sistema. Un metaanálisis de Koppel et al. (2008) concluyó que entre el 40% y el 70% de los SRI revisados presentaban al menos un error de instalación significativo, lo que compromete seriamente su eficacia. Según Ramsey et al. (2021), muchos de estos errores se derivan del desconocimiento de las instrucciones del fabricante, del uso inadecuado del cinturón de seguridad o del empleo de accesorios no homologados. Además, investigaciones recientes han incorporado datos biomecánicos obtenidos mediante simuladores de impacto. Jermakian et al. (2020) destacan que una mala orientación del SRI o un anclaje deficiente puede incrementar hasta un 300% la carga cervical durante una colisión, especialmente en menores de tres años.

Por tanto, la vigilancia de los agentes de policía se presenta como un instrumento clave para la salud ciudadana. La supervisión constante ayuda a identificar peligros potenciales antes que se produzca un accidente, añadiendo una ventaja preventiva esencial. De acuerdo con una investigación llevada a cabo en Noruega por Bentsen et al. (2021), los municipios con revisiones frecuentes de SRI registraron un nivel de cumplimiento del 96%, en contraste con el 73% en zonas sin supervisión continua. A su vez, la implementación de auditorías públicas y campañas informativas constantes mejora el grado de cumplimiento de las normativas en hasta un 20% anual (Johansson & Stigson, 2018).

La implicación policial no debe entenderse solo como mecanismo sancionador, sino como puente entre la ciencia y la ciudadanía. Informar, formar, advertir y acompañar son verbos que deben guiar cada intervención policial, en especial cuando se trata de colectivos vulnerables como la infancia. Para ello, es imprescindible que los agentes dispongan de formación continua basada en evidencia y accedan a materiales actualizados sobre avances en seguridad pasiva. En conclusión, la ciencia ha demostrado de forma inequívoca que el uso correcto de los sistemas de retención infantil salva vidas. La Policía Local, velando por la ley y la seguridad ciudadana, debe aplicar su experiencia en práctica día a día, mediante una vigilancia técnica, humanizada y dinámica que ayude a proteger a los jóvenes y a construir una verdadera cultura de la preventiva.

CONCLUSIÓN

El trabajo de la Policía Local en Andalucía con respecto de sistemas de retención infantil (SRI) constituye mucho más que una formación legal: encarna un compromiso de responsabilidad institucional profundo con la protección del tesoro más valioso de toda nuestra sociedad, la vida de nuestros. Su implicación constante en este ámbito demuestra la evolución del cuerpo policial hasta convertirse en herramienta clave no solo en la vigilancia y sanción, sino también en el fomento de una conciencia preventiva sólida, basada en la ciencia y humanista.

Garantizar un transporte infantil seguro exige adoptar una perspectiva global que abarque desde la formación técnica de los policías y fomentar la cooperación entre instituciones. La seguridad en las carreteras deja de ser una cuestión aislada sino un elemento central, un eje articulador de políticas públicas, donde la Policía Local puede liderar un cambio mediante intervenciones o acciones educativas, controles rigurosos y campañas de sensibilización que los ciudadanos entiendan fácilmente.

En esta coyuntura, el manejo del marco legal jurídico, la percepción de la biomecánica o factor humano en el siniestro, el análisis de las pruebas científicas y la cercanía en el trato con las familias son instrumentos fundamentales. Cada intervención policial debe entenderse como una ocasión única para salvar una vida, para reconducir un hábito peligroso o para plantar una semilla que genere conciencia social.

Las acciones desarrolladas durante este estudio dejan claro que la labor policía se ha basado en criterios técnicos y de prevención, nada de tarea puntual, requiere constancia, actualización permanente y un fuerte compromiso con la comunidad como servicio público. Capacitar, revisar, respaldar y proteger no son funciones secundarias, son la esencia de la identidad profesional del policía actual.

En resumen, apostar por una actuación especializada, integra y comprometida en el uso adecuado de los sistemas de seguridad infantil no solo evita sufrimientos innecesarios, sino que legitima la figura del policía como defensor de derechos, guía para ciudadanía y promotor proactivo del bienestar infantil.

“Cada menor correctamente protegido es una vida que sigue, un futuro que avanza y una sociedad que respeta”.

BIBLIOGRAFÍA Y FUENTES UTILIZADAS

- Arbogast, K. B., Durbin, D. R., Kallan, M. J., & Winston, F. K. (2004). Evaluation of pediatric use patterns of automotive restraint systems. *Accident Analysis & Prevention*, 36(3), 369–375. [https://doi.org/10.1016/S0001-4575\(03\)00032-2](https://doi.org/10.1016/S0001-4575(03)00032-2)
- Bentsen, T., Fosmark, D. S., & Høye, A. (2021). Impact of child restraint enforcement and awareness campaigns on usage rates in Norway. *Accident Analysis & Prevention*, 150, 105906. <https://doi.org/10.1016/j.aap.2020.105906>
- BMJ Injury Prevention. (2019). Effectiveness of child safety restraints in preventing injury. <https://injuryprevention.bmj.com/>
- Dirección General de Tráfico. (2024). Informe anual de siniestralidad vial infantil. Madrid: Ministerio del Interior.
- Durbin, D. R., Elliott, M. R., & Winston, F. K. (2003). Belt-positioning booster seats and reduction in risk of injury among children in vehicle crashes. *Journal of the American Medical Association*, 289(21), 2835–2840. <https://doi.org/10.1001/jama.289.21.2835>
- European Transport Safety Council. (2022). Reducing Child Deaths on European Roads. <https://etsc.eu/>
- Henary, B., Sherwood, C. P., Crandall, J. R., Kent, R. W., Vaca, F. E., Arbogast, K. B., & Bull, M. J. (2007). Car safety seats for children: rear facing for best protection. *Injury Prevention*, 13(6), 398–402. <https://doi.org/10.1136/ip.2006.015115>
- Jermakian, J. S., Zuby, D. S., & Wells, J. K. (2020). Biomechanical performance of child restraint systems in side-impact crash simulations. *Traffic Injury Prevention*, 21(sup1), S41–S48. <https://doi.org/10.1080/15389588.2020.1720452>
- Johansson, R., & Stigson, H. (2018). Evaluating the effect of child safety campaigns and law enforcement in Sweden. *Safety Science*, 110, 301–307. <https://doi.org/10.1016/j.ssci.2018.03.007>
- Koppel, S., Charlton, J., Fitzharris, M., & Fildes, B. (2008). How important is child restraint misuse? *Traffic Injury Prevention*, 9(6), 561–566. <https://doi.org/10.1080/15389580802335191>
- Ramsey, A., Hill, D., & Norman, J. (2021). Common misuse patterns in the installation of child restraint systems. *International Journal of Injury Control and Safety Promotion*, 28(3), 284–290. <https://doi.org/10.1080/17457300.2021.1877401>
- Reglamento General de Circulación. (2015). Real Decreto 667/2015, de 17 de julio, por el que se modifica el Reglamento General de Circulación. BOE n.º 173.
- Reglamento UNECE R44/04 y UNECE R129. (2020). Comisión Económica para Europa de las Naciones Unidas.
- Sherwood, C. P., Ferguson, S. A., & Crandall, J. R. (2016). Observed misuse of child restraints and booster seats. *Accident Analysis & Prevention*, 94, 93–100. <https://doi.org/10.1016/j.aap.2016.05.013>
- Zuby, D. S. (2019). Child seat orientation and its impact on injury risk: A review. *Journal of Safety Research*, 70, 87–93. <https://doi.org/10.1016/j.jsr.2019.05.006>



ACTUALIZACIÓN DRONES REAL DECRETO 517/2024. ACTUACIÓN POLICÍA LOCAL OPERACIONES NO EASA.

AUTOR: MIGUEL ÁNGEL RODRÍGUEZ OCHOA
POLICÍA LOCAL DE LA RINCONADA. (SEVILLA)

Nº 04/2025/3021 REGISTRO DE PROPIEDAD
DE LA JUNTA DE ANDALUCÍA (NINF@)

ÍNDICE DE CONTENIDOS

Prólogo.

Contexto Histórico.

Uas, Piloto y Operador

Edad mínima piloto a distancia.

Edad mínima operadores.

Clases de Uas y Categorías operacionales. Requisitos.

Actividades o servicios No Easa. Régimen Jurídico.

Actividades No Easa Directas.

Actividades No Easa Indirectas.

Diferencias entre operaciones Easa y No Easa.

Nuevos requisitos para zonas geográficas Uas.

Obligaciones en materia de registro de operadores Uas.

La Exención del requisito de identificación a distancia para Uas.

Como saber donde volar tu Uas.

Régimen Sancionador.

Epílogo.

Bibliografía y webgrafía.

PRÓLOGO

Sabido es que la Agencia de Seguridad Aérea de la Unión Europea, conocida por sus siglas en inglés EASA (European Aviation Safety Agency), es la entidad responsable de velar por la seguridad en la aviación y la protección del medio ambiente dentro del espacio aéreo de la Unión Europea. Sus funciones incluyen la supervisión e inspección de las operaciones del transporte aéreo y sus sistemas, así como la aprobación y certificación de equipos y productos relacionados con la aeronáutica. Pero su función principal se encuentra en establecer criterios y unificar procedimientos o estándares que se apliquen comúnmente entre países miembros, con el fin de asegurar operaciones aéreas seguras y coordinadas.

Por su parte, la AESA, la Entidad Estatal de Supervisión de la Seguridad Aérea, es la autoridad española responsable de supervisar que se respeten las normativas en el ámbito de la aviación civil en todo el territorio español. Tiene cierta potestad para añadir algunas normas sobre la normativa general que pone EASA. También impulsa la puesta en funcionamiento de la normativa aérea, tanto a nivel nacional como internacional, buscando fortalecer la seguridad, calidad y sostenibilidad del sistema aeronáutico español.

Para lograr esta armonización, se crean regulaciones comunes que deben aplicarse en todos los países miembros. En lo que respecta a los sistemas de aeronaves no tripuladas (UAS), se han elaborado el Reglamento de Ejecución (UE) 2019/947 y el Reglamento Delegado (UE) 2019/945.

En caso de que se infrinjan las normas de aviación civil dentro de España, AESA es la entidad que tiene la autoridad para imponer sanciones.

Y es el Real Decreto 517/2024, de 4 de junio el que desarrolla el régimen jurídico para actuación policial en las operaciones NO EASA, objetivo de esta publicación.

CONTEXTO HISTÓRICO

Hasta el año 2014, en España no existía una regulación específica para el uso de aeronaves pilotadas por control remoto, también conocidas como RPAS (Remotely Piloted Aircraft Systems). Esto generaba un vacío legal que dificultaba tanto el desarrollo de operaciones con drones como la definición de responsabilidades para sus operadores. Fue precisamente en 2014 cuando se estableció el primer marco normativo en este ámbito mediante la aprobación de la Ley 18/2014. En esta ley, concretamente en su artículo 50, se establecían por primera vez los requisitos legales necesarios para llevar a cabo operaciones con RPAS, así como las condiciones que debían cumplir los pilotos remotos encargados de su manejo.

Sin embargo, esta primera normativa era provisional y bastante limitada, por lo que fue necesario desarrollar una regulación más detallada y acorde con la rápida evolución del sector. En respuesta a ello, a finales del año 2017 entró en vigor el Real Decreto 1036/2017. Esta norma nacional supuso un avance importante, ya que regulaba de forma más completa el uso civil de los RPAS en el territorio español. Con la entrada en vigor de este real decreto, quedó derogado el artículo 50 de la Ley 18/2014, que había servido como base temporal. El nuevo real decreto introducía aspectos técnicos, operacionales y administrativos más desarrollados, abarcando desde los tipos de operaciones permitidas hasta los requisitos para las aeronaves, los pilotos y las condiciones del espacio aéreo.

A nivel europeo, la regulación también evolucionó. En junio de 2019, la Agencia de la Unión Europea para la Seguridad Aérea (EASA) promovió la implementación de un marco común en todos los Estados miembros mediante la publicación de dos reglamentos fundamentales: el Reglamento de Ejecución (UE) 2019/947 y el Reglamento Delegado (UE) 2019/945. Estos reglamentos, de aplicación directa en todos los países de la Unión Europea, establecían tanto las normas operativas para el uso de UAS (Unmanned Aircraft Systems) como los requisitos que debían cumplir los propios aparatos, dependiendo de su categoría de uso, peso y nivel de riesgo de las operaciones.

Finalmente, el 25 de junio de 2024 entró en vigor el Real Decreto 517/2024, que representa la normativa nacional más reciente en esta materia. Esta nueva disposición legal sustituye al anterior Real Decreto 1036/2017, al tiempo que lo deroga oficialmente. Su objetivo es desarrollar de manera más precisa el régimen jurídico aplicable al uso civil de los sistemas de aeronaves no tripuladas, integrando de forma plena la normativa europea ya vigente y adaptándose a las nuevas necesidades tecnológicas y operativas del sector. Con ello, se consolida un marco legal más robusto, moderno y coordinado a nivel europeo para garantizar un uso seguro y eficiente de los drones en el espacio aéreo español.

UAS, PILOTO Y OPERADOR

Nos podemos referir a las aeronaves no tripuladas con diferentes nombres. El más común y actual para definir una aeronave no tripulada en el territorio español podría ser el Dron, pero será el termino genérico UAS quien englobe todos los tipos y el término utilizado en los reglamentos de la comisión para referirnos a ellas.

Sus pilotos, denominados a distancia, serán personas físicas encargadas de la operación segura de los UAS, ya sea controlando manualmente los mandos de vuelo o supervisando el vuelo automático. En el caso de este último, el piloto tiene la capacidad de modificar parámetros como la velocidad, rumbo o altura del dron en cualquier momento, garantizando su buen funcionamiento durante el vuelo.

Por otro lado, un operador de UAS puede ser un individuo o una entidad jurídica, quien es el propietario o arrendador del dron. El operador es la persona responsable de la gestión del dron, ya sea en términos legales o administrativos.

Aunque el piloto a distancia y el operador pueden ser la misma persona, esto no es obligatorio. Un piloto puede trabajar para una empresa que opera drones, sin necesidad de ser el propietario. De manera similar, cuando alguien usa su dron en su tiempo libre, se considera tanto piloto como operador.

EDAD MÍNIMA PILOTO A DISTANCIA

La edad mínima para ejercer como piloto a distancia (la persona que controla un dron durante el vuelo), depende del tipo de operación que se vaya a realizar y de la categoría a la que pertenezca dicha operación, según la normativa europea recogida en el Reglamento de Ejecución (UE) 2019/947 y la legislación nacional en vigor; el Real Decreto 517/2024.

En el caso de las operaciones incluidas dentro de la categoría abierta, que son aquellas de bajo riesgo y que no requieren autorización previa por parte de la autoridad aeronáutica, la normativa europea establece una edad mínima de 16 años para los pilotos a distancia. No obstante, los Estados miembros tienen la posibilidad de reducir esta edad en determinadas subcategorías de esta categoría abierta. En el caso de España, la Agencia Estatal de Seguridad Aérea (AESA) ha establecido que se permite operar drones en las subcategorías A1 y A3 desde los 14 años, siempre que el piloto cumpla con los requisitos de formación y obtenga el correspondiente certificado.

Para las operaciones encuadradas en la categoría específica, que implican un nivel de riesgo superior y requieren una autorización operativa individual o una declaración por parte del operador, la edad mínima para los pilotos a distancia se mantiene en los 16 años. En este caso, los Estados miembros no pueden modificar ni reducir este límite, por lo que se aplica de forma uniforme en toda la Unión Europea.

En cuanto a la categoría certificada, que está destinada a operaciones de alto riesgo similares a las de la aviación tripulada, la normativa aún está en desarrollo y no se ha fijado una edad mínima concreta. Sin embargo, dado el nivel de complejidad y riesgo asociado a este tipo de operaciones, se prevé que los requisitos para los pilotos sean más estrictos y que probablemente incluyan una edad mínima de 18 años, al igual que ocurre con los pilotos de aviación convencional.

En resumen, en España, un joven puede comenzar a volar drones desde los 14 años en ciertos casos de bajo riesgo dentro de la categoría abierta, siempre que cumpla con la formación exigida. Para vuelos más complejos, a partir de los 16 años ya se puede operar en categorías abiertas generales y en la específica, mientras que las operaciones de mayor riesgo requerirán, con toda probabilidad, una edad superior una vez se definan completamente los requisitos para esa categoría.

EDAD MÍNIMA OPERADORES

En 2025, la edad mínima para operar drones en España, tanto para uso recreativo como profesional, es de 16 años, aunque existen excepciones en la categoría abierta para ciertos tipos de drones. Para drones de clase C0 (generalmente de juguete o de menos de 250 gramos), la edad mínima es de 12 años, siempre y cuando se opere bajo supervisión de un piloto remoto mayor de 16 años.

Categoría Abierta (A1) con drones C0: Se permite a menores de 16 años, específicamente de 12 años, operar drones de clase C0, que suelen ser drones de juguete o de bajo peso, bajo supervisión.

Operaciones en la categoría abierta: En general, para operar drones en la categoría abierta, la edad mínima es de 16 años, aunque existen excepciones para ciertas subcategorías y tipos de drones como los mencionados anteriormente.

Operaciones en categorías específica y certificada: Para operaciones más complejas, como las que se realizan en la categoría específica o certificada, se requiere la mayoría de edad (18 años).

CLASES DE UAS Y CATEGORIAS OPERACIONALES. REQUISITOS

El Reglamento delegado (UE) 2019/945 hace referencia al diseño y fabricación de los UAS y que tenemos diferentes clases de UAS que irán desde los C0 los más sencillos hasta los C6, los UAS de mayor envergadura.

En cuanto al reglamento de ejecución (UE) 2019/947 nos dice como debemos ejecutar los vuelos. Es donde se establece las diferentes categorías de operación y los últimos escenarios estándar. Tendremos la categoría abierta A1/A3, en otro nivel dentro de la categoría abierta el A2 y luego tendríamos la categoría específica donde están los dos escenarios estándar en los que podremos operar en STS y por último la categoría certificada.

Las categorías de operación las diferenciamos en función del riesgo que estas implican. La de riesgo más bajito es la categoría abierta que no se requiere ninguna autorización ni declaración hacia AESA de que vamos a volar en dicha categoría.

En la categoría específica hay mayor riesgo y dentro de esta categoría nos encontramos con los escenarios estándar o con la posibilidad de solicitar alguna autorización operacional en caso no nos podamos acoger a ninguno de los dos escenarios que están establecidos.

La de más de alto riesgo es en categoría certificada y que sigue un régimen regulatorio similar a la aviación tripulada.

Dentro de la categoría abierta tenemos tres subcategorías; la A1 la A2 y A3. Las condiciones comunes para las tres subcategorías son:

1.- Que siempre volaremos en VLOS, es decir, dentro del alcance visual, el UAS siempre estará en línea de vista para nosotros, excepto para drones FPV, que son unos UAS pilotados a través de unas gafas que tendrán la misma visión que la cámara de nuestro dron y como no tenemos línea directa de vista con el UAS, nos tendremos que ayudar de un observador que estará continuamente mirando el dron por si en algún momento estamos en peligro o vamos a realizar una maniobra que podamos poner en riesgo la seguridad del vuelo.

2.- La altura máxima de vuelo será de 120 metros con la pequeña excepción de que si estamos a menos de 50 metros de un obstáculo que sea superior en altura a 105 metros podríamos incrementar nuestra altura de vuelo en 15 metros por encima de los 105. No sobrepasaremos nunca los 150 metros de altura ya que ahí empieza la aviación tripulada.

3.- En un encuentro con una nave tripulada, ella tendría prioridad teniendo nosotros que practicar una maniobra evasiva bajando la altura del vuelo incluso aterrizar si es necesario.

- 4.- No se permite el vuelo sobre concentraciones de personas.
- 5.- Como pilotos podemos ayudarnos de un observador, aunque no es obligatorio.
- 6.- Se prohíbe transportar mercancías peligrosas ni dejar caer ningún objeto.

En la subcategoría A1 además de los requisitos anteriormente mencionados, tendremos otros requisitos particulares. Las condiciones particulares de operación dentro de la subcategoría A1 podremos sobrevolar personas no participantes en la operación excepto cuando volemos con UAS de clase C1, es decir podremos volar personas no participantes con UAS de clase C0 o similar. Los requisitos para los pilotos a distancia en esta subcategoría sería superar el examen en la página web de AESA para la categoría abierta A1 A3.

Los requisitos que tienen que tener los UAS para volar en la subcategoría A1; tener etiqueta de identificación clase C0, debiendo pesar menos de 250 gramos, tener una velocidad de menos de 19 m/s y altura máxima de vuelo limitada a 120 metros. Además, otras condiciones como que sea comercializado con las instrucciones del fabricante, que sean eléctricos, que estén diseñados para evitar dañar a personas y que sean controlables y manejables de forma segura.

Las características de los UAS de la clase C1 seguimos imitando la altura de vuelo a 120 mts, seguimos con los 19 m/s y seguimos con unos requisitos diseñados para evitar dañar a personas, eléctrico deberá tener sistema de geoconsciencia, siendo lo más importante que ya nos vamos a un tamaño superior. Pudiendo llegar a UAS de hasta 900gr o que tengan una energía de impacto inferior a 80 julios.

En la subcategoría A2, donde tendremos las mismas condiciones que en la A1/A3 pero añadimos una más ya que vamos a volar con UAS de mayor envergadura, deberemos dejar una distancia horizontal segura de personas no participantes de al menos 30 metros. Esta distancia vendrá marcada por una altura de 30 metros para arriba, y vamos a intentar actuar siempre siguiendo la regla 1:1, es decir, tanta altura de vuelo, tanta distancia horizontal de una persona no participante.

Si volamos a 30 metros o menos de altura, en este caso como mínimo siempre dejaremos 5 metros de distancia horizontal, una vez ese mínimo va depender de si tenemos o no activado el modo baja velocidad, haciendo que el UAS vuele como máximo a 3 m/s. Teniendo ese modo activo podemos mantener la regla 1:1, en caso de no tenerlo activado el modo baja velocidad, siempre estaremos obligados a dejar 30 metros de distancia horizontal.

Dentro de los requisitos de los pilotos a distancia en la subcategoría A2 tenemos haber aprobado la teoría del A1/A3, aprobar la teoría del examen A2 y tendríamos que hacernos un examen práctico a nosotros mismos.

Los UAS que podrán volar en esta categoría serán los de la clase C2, con una notables diferenciará de los anteriores, pues tiene la función de baja velocidad con un límite de 3 m/s y que nos podremos ir hasta 4 kg de peso. Además, tendrán que estar equipados con luces de controlabilidad y visibles de noche, ser eléctricos, sistema de geoconsciencia y N.º de serie físico y único.

En la subcategoría A3, como requisito extra además de la condiciones ya conocidas para categoría abierta, es que tendremos que volar siempre a una distancia horizontal mínima de 150 m de cualquier zona residencial, comercial, industrial o recreativa, es decir, prácticamente se nos limita el vuelo a un entorno rural, pensad que ya vamos a ir con drones de mayor envergadura llegando hasta los 25 kg, con lo cual sin haber superado ningún examen práctico deberemos alejarnos de todas aquellas zonas donde podamos hacerle daño a alguien.

Los requisitos de los pilotos a distancia serán iguales a los de la A1, haber superado el examen teórico para A1/A3.

En esta subcategoría del A3, nos podremos ir a UAS de la clase C3 cuya diferencia principal es la máxima dimensión permitida que son 3 metros y nos vamos ya a 25 kg de peso. También podríamos utilizar los de la clase C2 o si son de construcción privada que pesen menos de 25 kg o UAS introducidos en el mercado antes del 1 de enero de 2024 y pesen menos de los 25 kg. Además, en esta subcategoría, tenemos la clase C4 que es una clase más pensada en el aeromodelismo y no dispone de modo automático de vuelo.

UAS	DRI**	MTOM	Operación	Formación
Clase			Subcategoría	Requisitos a pilotos
Construcción privada	NO X			
Legacy <250 g	NO X	< 250 g	A1	Familiarización con el manual de usuario facilitado por el fabricante del UAS
C0	NO X			
C1	SI ✓	< 900 g		- Familiarización con el manual de usuario facilitado por el fabricante del UAS. - Prueba de superación de formación en línea.
C1	SI ✓	< 4 kg	A1	- Familiarización con el manual de usuario facilitado por el fabricante del UAS. - Prueba de superación de formación en línea, y - Declaración de formación autopráctica, y - Certificado de Competencia de Piloto a Distancia
C3	NO X			
Construcción privada	NO X	< 25 kg	A3	- No volar en encima de ninguna persona no participante - No esta permitido el vuelo sobre reuniones de personas - No volar por encima de ninguna persona no participante 30 m de permitido el vuelo sobre reuniones de personas 30 m de cualquier persona no participantes 5 m de distancia si dispona de modo de baja velocidad - No volar cierras de pestestro a distancia de - Zonas residenciales - Zonas comerciales - Zonas industriales - Zonas recreativas
Legacy >250 g	NO X			

<https://www.seguridadaerea.gob.es/>

En la categoría específica, que como ya dijimos anteriormente era la categoría con riesgo medio. En ella tenemos diferentes modos para operar, la más habitual es dentro de los escenarios estándar, los famosos STS 01 y STS 02 que son dos tipos de escenarios definidos por EASA y en el caso de España con alguna modificación efectuada por AESA en el que nos marcan ciertas características de vuelo y ciertas condiciones para poder operar en estos escenarios, algo que veremos más adelante (RD 517/2024).

Hay mil opciones en las que nos podemos ver envueltos a la hora de realizar un vuelo, como es imposible con todos los pilotos que hay y todas las operaciones que hay día a día en el estado, que para cada vez que queramos volar le enviemos a AESA una solicitud de vuelo, lo que hicieron es crear dos tipos de escenarios más comunes y poner una normativa y de esta forma cada vez que un piloto quiera volar en estos escenarios únicamente tendrán que haber aprobado el carné de los STS y notificar a AESA que va realizar este tipo de vuelos. Entonces, si nos acogemos alguno de los dos escenarios, con hacer una primera notificación a AESA de que vamos a realizar vuelos en estos escenarios es suficiente.

Que nos permite estos escenarios, pues el STS 01 nos permite volar en entorno urbano y el STS 02, nos permite llevar el UAS fuera del alcance visual, es decir, volar en BVLOS.

Si no nos pudiéramos acoger a ninguno de estos dos escenarios, aunque sea un caso extraño podría darse, en ese caso tendríamos que solicitar a AESA una autorización operacional, es decir, enviar una notificación en la que digamos que queremos realizar este tipo de vuelo, somos pilotos certificados en categoría abierta y en escenario estándar y queremos realizar este vuelo con esta seguridad y AESA nos podrá decir si sí, si no o si sí, pero haciendo alguna rectificación.

Por último, tenemos la categoría certificada, que es la de operación de mayor riesgo, siendo similares sus procedimientos a la de aviación tripulada.

En esta categoría tenemos 3 principales tipos de vuelos, UAS de dimensiones mayores a 3 metros, realizar el transporte de personas o el transporte de mercancía peligrosa que tiene un alto riesgo para terceras partes en caso de accidente.

Destacar que el certificado tiene una validez de 5 años y, se deberá iniciar el proceso de renovación ante AESA previamente a la fecha de expiración.

ACTIVIDADES O SERVICIOS NO EASA. RÉGIMEN JURÍDICO.

Una vez conocido las diferentes categorías operacionales y sus requisitos, vamos a centrarnos en el principal objeto de esta publicación, que es la divulgación de los conocimientos obtenidos en relación a las actividades NO EASA, ya que, En España, las operaciones con drones realizadas por la Policía Local no estarían dentro del ámbito de aplicación de la normativa EASA, clasificándose como operaciones NO EASA.

El RD 517/2024, de 4 junio, que desarrolla el régimen jurídico para la utilización de UAS, ha impulsado cambios significativos en la normativa aplicable a las actividades o servicios **NO EASA**, en el que los operadores que realizan actividades o servicios No EASA han tenido un periodo transitorio para adaptarse íntegramente hasta 25 de junio de 2025, excepto en lo relativo al uso del espacio aéreo y las áreas geográficas de UAS, que se les aplica desde el momento en que entró en vigor.

Tras investigar su origen, sus objetivos y las últimas actualizaciones que nos trae El RD, podemos decir que las actividades **NO EASA** son aquellas que están excluidas de la aplicación del reglamento Europeo UE 2018/1139 y entre las que se encuentra las actividades o servicios de aduanas, policía, servicios militares, búsqueda y salvamento, lucha contra incendios, control fronterizo, vigilancia costera o similares, entre las que se incluyen las de vigilancia y disciplina del tráfico en todo el territorio nacional, bajo el control y la responsabilidad de un Estado miembro, emprendidas en el interés general por un organismo investido de autoridad pública o en nombre de este.

El RD 517/2024 deroga lo dispuesto en el Real Decreto 1036/2017, y es la Resolución del 10 de noviembre de 2024, emitida por la Dirección de la Agencia Estatal de Seguridad Aérea, la que aprueba los escenarios estándar nacionales (STS-ES-NE) para el uso de sistemas de aeronaves no tripuladas (UAS) en la categoría «Específica», dentro de actividades o servicios que no están bajo el ámbito de EASA. Esta resolución se adopta conforme al Real Decreto 517/2024, de 4 de junio, donde se establece el marco legal para el uso civil de los UAS. Los escenarios estándar nacionales aprobados mediante esta resolución se aplican en el territorio y el espacio aéreo español al uso de aeronaves no tripuladas que estén sujetas al Real Decreto 517/2024, siempre que realicen actividades o presten servicios que no estén regulados por EASA. No es necesario que las aeronaves cuenten con marcado de clase para operar bajo estos escenarios estándar nacionales.

Los escenarios estándar nacionales no EASA publicados hasta la fecha son los siguientes:

- **STS-ES-01NE:** Operaciones VLOS (línea visual directa) sobre una zona terrestre controlada en un entorno urbano o con presencia de población.
- **STS-ES-02NE:** Operaciones BVLOS (más allá de la línea visual), con observadores del espacio aéreo, sobre una zona terrestre controlada en un entorno escasamente poblado.

Se entiende por “zona terrestre controlada” aquel espacio en tierra donde se lleva a cabo la operación con UAS y en el que el operador puede asegurar que únicamente se encuentran personas implicadas directamente en dicha operación.

Como venimos diciendo, el Real Decreto 517/2024 es el marco legal aplicable a las actividades o servicios que no están bajo la normativa EASA y que son llevados a cabo directamente por una entidad con autoridad pública responsable de dicha actividad o servicio (actividades NO EASA directas), así como a aquellas que se realizan en representación de una entidad con autoridad pública (actividades NO EASA indirectas). Las actividades o servicios no EASA regulados en la resolución del 10 de noviembre de 2024, cuando sean llevados a cabo directamente por un organismo con autoridad pública, no requieren la presentación de una declaración operacional.

Sin embargo, los operadores de UAS que no sean un organismo con autoridad pública, pero actúen en su nombre, sí deberán realizar estas actividades o servicios no EASA mediante una declaración operacional.

Estas declaraciones deberán presentarse utilizando el formulario que la AESA pondrá a disposición en su sede electrónica.

Por tanto, las actividades o servicios NO EASA directas se rigen tanto por lo dispuesto en el Real Decreto 517/2024 como por la normativa europea, aunque con ciertas excepciones. En cuanto a las actividades NO EASA indirectas, estas se encuentran bajo el ámbito del Real Decreto 517/2024 y de la normativa europea aplicable a los UAS.

ACTIVIDADES NO EASA DIRECTAS

Aplicable exclusivamente a los operadores de UAS que lleven a cabo actividades o servicios no regulados por EASA, siempre que estos sean ejecutados directamente por una entidad con autoridad pública.

La categoría abierta abarca todas aquellas operaciones con UAS que implican un bajo nivel de riesgo operativo. Para las operaciones que se encuadren dentro de esta categoría conforme al artículo 4 del Reglamento de Ejecución (UE) 2019/947, el operador de UAS debe cumplir con los requisitos vistos anteriormente:

- Estar registrado como operador e identificar sus aeronaves con el número correspondiente. Para más detalles y posibles excepciones.
- Asegurar que los pilotos a distancia cuenten con la formación adecuada para la subcategoría en la que se va a operar.
- Verificar los requisitos específicos aplicables en función del área de operación o la naturaleza de la actividad.
- Contar con un seguro de responsabilidad civil frente a terceros.

Las operaciones con UAS que se lleven a cabo bajo un escenario estándar aprobado en el marco del Reglamento de Ejecución, o bajo un escenario estándar nacional aprobado por la Agencia Estatal de Seguridad Aérea, no requieren la presentación de una declaración operacional.

Sin embargo, el organismo competente deberá asegurarse de que dichas operaciones se ajustan estrictamente al escenario estándar correspondiente.

Como apoyo a los operadores directos No EASA que operen bajo escenarios estándar nacionales No EASA (STS-ES-NE), se pone a disposición material orientativo para la elaboración del Manual de Operaciones general, así como Conceptos de Operación (ConOps) específicos para cada escenario.

En los casos, en el que las operaciones incluidas en la categoría específica que no puedan realizarse conforme escenario estándar y por tanto no requerirán una autorización operacional emitida por AESA, el organismo investido de autoridad pública que tenga la responsabilidad sobre la actividad o el servicio correspondiente deberá asegurarse de que la operación se lleve a cabo cumpliendo los siguientes requisitos:

- Que se haya realizado previamente una evaluación del riesgo operacional, conforme a los estándares técnicos publicados por EASA, adoptados por AESA, o utilizando la metodología SORA (Specific Operation Risk Assessment).
- Que el operador cuente con la capacidad técnica y profesional suficiente.
- Que se apliquen medidas de mitigación adecuadas para garantizar la seguridad de la operación.

Por tanto, corresponde al organismo responsable de la actividad:

- Autorizar la ejecución de las operaciones;
- Verificar que se desarrollan conforme a la normativa aplicable según su categoría operacional;
- Establecer los procedimientos necesarios que definan las medidas de mitigación a aplicar.

En cualquier caso, debe asegurarse que la operación mantenga un nivel de seguridad equivalente, en línea con los objetivos de seguridad establecidos en el Reglamento Base, así como en sus actos delegados y de ejecución.

ACTIVIDADES NO EASA INDIRECTAS

Los UAS, así como el personal y las empresas que lleven a cabo actividades o presten servicios NO EASA en representación de un organismo público, deben ajustarse a lo dispuesto en el Real Decreto y en los reglamentos europeos correspondientes, siendo los requisitos aplicables los mismos que para las actividades EASA, con adaptaciones específicas en lo referente a la zonificación.

En categoría abierta operaciones con UAS que implican un bajo riesgo operacional, para realizar operaciones dentro de esta categoría, el operador de UAS deberá cumplir con los siguientes requisitos:

- Registrarse como operador e incorporar su número de registro en todas las aeronaves utilizadas.
- Asegurar que los pilotos a distancia estén debidamente formados, conforme a la subcategoría de operación en la que se encuadre la actividad.
- Verificar los requisitos adicionales aplicables según la localización de la operación o la naturaleza de la actividad a desarrollar.
- Contar con un seguro de responsabilidad civil frente a terceros, conforme normativa.

En Categoría específica, la operación de UAS bajo un escenario estándar, ya sea adoptado en el marco del Reglamento de Ejecución (UE) 2019/947 o reconocido como escenario estándar nacional por la Agencia Estatal de Seguridad Aérea (AESA), requiere la presentación de una declaración operacional, siguiendo el mismo procedimiento establecido para las declaraciones de conformidad con los escenarios estándar nacionales.

El operador de UAS será responsable de garantizar que la operación se ajuste estrictamente al escenario estándar declarado.

Contenido de la declaración operacional:

La declaración correspondiente a un escenario estándar debe incluir:

- Información administrativa del operador de UAS.
- Declaración de que la operación cumple con los requisitos operacionales definidos en el escenario estándar aplicable.
- Compromiso del operador de aplicar todas las medidas de mitigación necesarias para garantizar la seguridad de la operación.
- Confirmación de que se dispone de un seguro adecuado para cada vuelo realizado bajo el marco de la declaración.

Presentación de la declaración:

Las declaraciones operacionales deberán presentarse telemáticamente a través de la sede electrónica de AESA. Para ello, es imprescindible que el operador esté previamente registrado como operador de UAS no EASA.

DIFERENCIA ENTRE OPERACIONES EASA Y NO EASA

La diferencia fundamental entre operaciones EASA y no EASA radica en la jurisdicción, regulación y supervisión aplicable a las operaciones aéreas, especialmente dentro del contexto europeo.

Las operaciones EASA están reguladas por la Agencia de la Unión Europea para la Seguridad Aérea (EASA) y se aplican a todos los operadores y aeronaves registrados en países miembros de la Unión Europea o en países que han adoptado el marco EASA. Estas operaciones deben cumplir con una normativa común y armonizada, como el Reglamento (UE) 965/2012, que garantiza estándares uniformes de seguridad, mantenimiento, licencias, operaciones

comerciales y técnicas en toda Europa.

Por otro lado, las operaciones no EASA (también conocidas como nacionales o bajo autoridad estatal) están reguladas directamente por las autoridades aeronáuticas de cada país, fuera del marco normativo de EASA. Estas incluyen aeronaves registradas en países no pertenecientes a la UE o aquellas excluidas explícitamente del reglamento EASA, como aviones históricos, militares, de construcción por aficionados o ciertas operaciones especializadas.

Podemos decir, que la diferencia fundamental está en que las operaciones EASA están sujetas a una regulación europea común y centralizada, mientras que las operaciones no EASA dependen de la normativa local de cada Estado miembro o de terceros países, lo que implica diferencias en los requisitos técnicos, operativos y de supervisión.

La principal diferencia o novedad, introducida por el RD 517/2024 para la formación de pilotos a distancia, respecto a lo anterior se encuentra en la formación en escenarios estándar nacionales («STS-ES») para actividades No EASA, que de acuerdo lo establecido en el artículo 20, para la realización de operaciones de UAS en los escenarios estándar nacionales («STS-ES») los pilotos a distancia deberán:

- Estar en posesión de un certificado de conocimientos teóricos de piloto a distancia, de conformidad con lo establecido en la definición de los correspondientes escenarios estándar, por la Agencia Estatal de Seguridad Aérea y que hemos visto anteriormente.
- Estar en posesión de una acreditación que certifique una formación completa de aptitudes prácticas para el escenario estándar correspondiente tal y como lo establecido en su definición según los escenarios e impartidas por entidades facultadas.

En resumen;

Los escenarios STS-ES-NE (tanto el STS-ES-01NE como el STS-ES-02NE) solo son válidos dentro del espacio aéreo bajo soberanía española. Esto significa que no tienen validez ni reconocimiento en otros países miembros de EASA ni en terceros países.

Los escenarios STS-ES-01NE y STS-ES-02NE son operacionales exclusivamente en España y aplicables únicamente a vuelos bajo la categoría “específica” No EASA.

El examen teórico que necesitas para acceder a estos dos escenarios es exactamente el mismo que el de los escenarios estándar EASA (tanto los europeos como los nacionales).

NUEVOS REQUISITOS PARA ZONAS GEOGRÁFICAS UAS.

El Real Decreto 517/2024 introduce mejora en la regulación de las zonas geográficas UAS en España, que, además de las normas operacionales por categorías (abierta, específica, certificada), define restricciones adicionales según el espacio donde se vuela.

Tipos de zonas geográficas

- Generales: incorporan diversas áreas delimitadas por ley, como:
 - Espacios en torno a aeródromos y helipuertos (civil o militar).
 - Espacio aéreo controlado y zonas FIZ.
 - Áreas protegidas ambiental o culturalmente.
 - Zonas urbanas con implicaciones de seguridad.
 - Áreas restringidas militarmente o por defensa nacional.
- Particulares: creadas por CIDETRA (Comisión Interministerial de Defensa y Transportes) por razones específicas con carácter permanente, aunque pueden activarse temporalmente según las necesidades.

Clasificación operacional

Dentro de estas zonas hay áreas que:

- Prohíben el vuelo de UAS.
- Permiten vuelo siempre que se cumplan ciertas condiciones.
- Exigen autorización previa a través del sistema ENAIRE.
- Requieren equipo específico (como sistemas de identificación o geoconsciencia)

Aplicación ENAIRE Drones

ENAIRE ofrece una herramienta interactiva (web y app móvil) que permite a los operadores:

- Visualizar en el mapa España con diferentes capas (espacio controlado, zonas protegidas, zonas urbanas, etc.).
- Consultar limitaciones actuales mediante NOTAM, AIP y datos técnicos.
- Prepararse para vuelos, identificando si es necesario plan de vuelo, coordinación o equipo extra

Zonas geográficas temporales

Pueden establecerse zonas UAS de forma temporal, por un plazo máximo de 6 meses, para actividades específicas (eventos, emergencias...).

- Se activan mediante coordinación “táctica o pre-táctica” entre autoridades aeronáuticas y militares.
- Se notifican vía ENAIRE Drones, NOTAM o suplementos AIP
- Superposición de zonas y jerarquía normativa
- Cuando conviven varias zonas en un mismo espacio, se deben cumplir todas las condiciones operacionales.
- Si hay conflicto, la norma más restrictiva prevalece, especialmente si una zona particular contradice una general.

Equipamiento obligatorio

Según el artículo 35 del RD 517/2024, los UAS deben estar equipados adecuadamente según tipo de zona:

- -En CTR/FIZ: sistemas de identificación, transpondedores, luces de navegación/anticolisión, enlace C2 por radio aeronáutica.
- -En otras zonas, puede requerirse: geoconsciencia, sistemas DRI u otros según la normativa.

OBLIGACIONES EN MATERIA DE REGISTRO DE OPERADORES UAS.

En España los operadores de drones que realicen actividades o servicios no regulados por la Agencia de la Unión Europea para la Seguridad Aérea (EASA), No EASA realizados indirectamente, en nombre de un organismo investido de autoridad pública, están obligados a la inscripción digital en el Registro de operadores de UAS.

Igualmente, los operadores de actividades o servicios No EASA realizados directamente están obligados a la inscripción en el Registro, salvo que se trate de las Fuerzas y Cuerpos de Seguridad regulados por la Ley Orgánica 2/1986, de 13 de marzo, el Centro Nacional de Inteligencia (CNI), la Dirección Adjunta de Vigilancia Aduanera (Aduanas) o la Dirección General de Tráfico (DGT). En dicha salvedad, la inscripción es voluntaria.

¿Quiénes deben registrarse?

Deben inscribirse en el Registro de operadores de UAS aquellos que:

- Realicen actividades o servicios no EASA directamente.
- Realicen actividades o servicios no EASA indirectamente, en nombre de un organismo investido de autoridad pública.

Están exentos de esta obligación, aunque pueden inscribirse voluntariamente:

- Las Fuerzas y Cuerpos de Seguridad regulados por la Ley Orgánica 2/1986, de 13 de marzo.
- El Centro Nacional de Inteligencia (CNI).
- La Dirección Adjunta de Vigilancia Aduanera (Aduanas).
- La Dirección General de Tráfico (DGT).

¿Cómo realizar la inscripción?

La inscripción se realiza de forma digital a través de la sede electrónica de AESA. Es recomendable utilizar un certificado digital para agilizar el proceso. Los pasos generales son:

- Alta de usuario: Acceder a la aplicación de UAS y darse de alta como usuario.
- Registro como operador: Una vez aprobado el alta, proceder al registro como operador de UAS.

Es importante completar el registro como operador en un plazo máximo de 90 días tras el alta de usuario; de lo contrario, el sistema eliminará el usuario, debiendo realizar nuevamente este trámite.

Documentación necesaria

Durante el proceso de inscripción, se solicitará la siguiente información y documentación:

- Datos personales o de la entidad operadora.
- Información sobre el dron: marca, modelo, peso y características técnicas.
- Seguro de responsabilidad civil que cubra los daños a terceros.
- Manual de operaciones o procedimientos, si aplica.

Recursos adicionales

Para obtener más información y acceder a la aplicación de registro, puedes visitar los siguientes enlaces:

- Registro de operador de drones/UAS - AESA
- Guía de registro como operador de UAS

Además, AESA ha publicado una guía detallada que explica paso a paso cómo realizar el registro como operador de UAS.

¿A quién se aplica la obligación de registro?

Operadores NO EASA

Están sujetos a inscripción en el Registro de operadores UAS de AESA (de manera obligatoria) aquellos que realicen:

- Actividades o servicios no EASA directamente, o
- Actividades o servicios no EASA indirectamente, en nombre de un organismo investido de autoridad pública.

Exenciones (registro voluntario)

No están obligados, aunque sí pueden registrarse voluntariamente, los siguientes operadores públicos:

- Fuerzas y Cuerpos de Seguridad regulados por la Ley Orgánica 2/1986
- Centro Nacional de Inteligencia (CNI)
- Dirección Adjunta de Vigilancia Aduanera (Aduanas)
- Dirección General de Tráfico (DGT)

Marco legal y normativa aplicable

- El Real Decreto 517/2024, publicado el 4 de junio de 2024, regula específicamente las actividades no EASA y establece las obligaciones de registro.
- Las operaciones de UAS (abierta, específica o certificada) están también reguladas por los Reglamentos (UE) 2019/947 y 2019/945, y su regulación nacional complementaria.

¿Cómo registrarse? Paso a paso

Alta de usuario

1. Accede a la sede electrónica de AESA.
2. Identifícate con un certificado digital, DNle o Cl@ve PIN (para residentes). Los extranjeros deben usar e4F.
3. Crea una cuenta en la aplicación de UAS (opción “Alta de usuario”).

Inscripción como operador

1. Una vez aprobado el alta, accede al módulo “Registro de operador de drones/UAS”.
2. Completa el formulario con:
 - Datos personales o de la entidad
 - Información del dron: marca, modelo, peso, características técnicas
 - Seguro de responsabilidad civil
 - Manual de operaciones o procedimientos (si aplica).
3. Envía la solicitud. El sistema genera un número de registro único, que debe colocarse de forma visible en cada dron.
4. Importante: tras el alta, tienes un plazo máximo de 90 días para completar el registro de operador, o la cuenta será eliminada.

Confirmación y uso

- Recibirás acuse de recibo y, si está todo correcto, el certificado en pocos días.
- En caso de modificaciones (p. ej. cambio de datos, drones operados), se debe actualizar el registro. Cada actualización extiende la validez 3 años más.

Requisitos técnicos y software

- Utiliza los navegadores compatibles recomendados por AESA.
- Asegúrate de tener actualizadas las versiones de Java y del programa Autofirma.
- El certificado digital debe estar correctamente instalado en el navegador

Seguro obligatorio

Todos los operadores deben contar con una póliza de responsabilidad civil que cubra daños a terceros derivados de la actividad de vuelo. Se aplican los límites previstos en la Ley de Navegación Aérea y su actualización mediante Real Decreto (artículos 126 y 127).

Operaciones: categorías y declaraciones

- Categoría abierta: de bajo riesgo. Solo es necesario el registro de operador y seguro.
- Categoría específica: requiere añadir el dron al perfil y presentar una declaración operacional o autorización dependiendo del caso.
- En categoría certificada (p. ej. lucha contra incendios, SAR) puede requerirse certificación adicional como operador o cumplimiento de estándares.

Obligaciones continuas

- Mantener los datos del registro actualizados: datos de contacto, drones operados, situación legal.
- Notificar cualquier cese o suspensión: importa para dar de baja temporal o definitiva el registro, lo que afecta también las autorizaciones asociadas.

LA EXENCIÓN DEL REQUISITO DE IDENTIFICACIÓN A DISTANCIA PARA UAS

Por motivos de seguridad pública, los Unmanned Aircraft Systems (UAS) que realicen actividades o servicios fuera del ámbito de la Agencia Europea de la Seguridad Aérea (EASA) podrán operar sin cumplir con el requisito de estar equipados con un sistema o accesorio de identificación a distancia, o sin verificar la veracidad de la información suministrada, siempre que se apliquen medidas de atenuación complementarias que garanticen niveles de seguridad equivalentes.

Estas exenciones son aplicables a UAS que realicen actividades relacionadas con:

- Operaciones contra el crimen organizado, terrorismo o amenazas muy graves a la seguridad ciudadana.
- Prevención y evitación de peligros, amenazas o agresiones contra la independencia o integridad territorial de España.
- Protección de los intereses nacionales y la estabilidad del Estado de Derecho o sus instituciones.

Las entidades autorizadas para realizar estas operaciones sin el requisito de identificación a distancia son:

- Las Fuerzas y Cuerpos de Seguridad del Estado dependientes del Gobierno de la Nación.
- Los Cuerpos de Policía dependientes de las Comunidades Autónomas.
- La Dirección Adjunta de Vigilancia Aduanera.
- El Centro Nacional de Inteligencia.

Es importante destacar que estas exenciones están sujetas a la aplicación de medidas de seguridad que garanticen niveles equivalentes de protección y control, en consonancia con los objetivos de seguridad pública y defensa nacional.

COMO SABER DONDE VOLAR TU UAS

ENAIRE Drones es la plataforma oficial del Ministerio de Transportes, Movilidad y Agenda Urbana de España que proporciona información esencial para planificar vuelos de drones (UAS) de forma segura y conforme a la normativa vigente. Esta herramienta es útil tanto para operadores recreativos como profesionales.

Dentro de sus funcionalidades principales tenemos:

- **Mapa interactivo personalizado:** A partir de un cuestionario previo (tipo de dron, finalidad, localización), la plataforma genera un mapa adaptado a cada caso, indicando zonas restringidas, áreas concretas de control aéreo, aeropuertos, helipuertos o bases militares, en base a la AIP España y datos AIRAC enaire.es.
- **Consulta de NOTAM y avisos aeronáuticos:** Permite acceder a avisos actualizados que puedan afectar al vuelo, asegurando que el piloto esté al tanto de restricciones temporales enaire.es.
- **Planificación de ruta y mediciones:** Facilita herramientas para dibujar la ruta de vuelo, medir distancias y zonificar áreas específicas dentro del mapa.
- **Integración con ENAIRE:** Planea En operaciones más complejas o en espacio aéreo controlado, permite gestionar solicitudes de permiso de vuelo desde la misma plataforma.

RÉGIMEN SANCIONADOR

Por incumplimiento de la normativa de Seguridad Aérea ante la Agencia Estatal de Seguridad Aérea (AESA).

La Agencia Estatal de Seguridad Aérea (AESA) es el organismo competente en España para supervisar, regular y sancionar las actividades relacionadas con la navegación aérea civil. En caso de incumplimiento de la normativa vigente, AESA puede imponer sanciones económicas, clasificadas según su gravedad en leves, graves y muy graves. Estas sanciones se regulan por lo dispuesto en la Ley 21/2003, de Seguridad Aérea, y normativa complementaria.

Clasificación y cuantía de las sanciones

Infracciones Leves

Cuantía: de 60 € a 45.000 € Se consideran infracciones leves aquellas que, sin implicar un

riesgo directo o grave para la seguridad aérea, suponen un incumplimiento de obligaciones administrativas, técnicas o de coordinación.

Ejemplos de infracciones leves:

- Volar un dron en una zona autorizada, pero sin llevar consigo la documentación exigida (manual de operaciones, seguro, registro del operador).
- No comunicar a tiempo un cambio en los datos del operador de drones.
- Realizar vuelos recreativos sin mantener la distancia mínima con personas, pero sin poner en riesgo su integridad.

Infracciones Graves

Cuantía: de 45.001 € a 90.000 € Estas infracciones implican un riesgo significativo para la seguridad aérea, las personas o los bienes, o suponen un incumplimiento relevante de las condiciones establecidas para las operaciones aéreas.

Ejemplos de infracciones graves:

- Volar un dron dentro del espacio aéreo controlado sin permiso de ENAIRE o sin coordinación previa con la torre de control.
- No disponer del seguro obligatorio de responsabilidad civil durante una operación comercial.
- Realizar vuelos nocturnos sin contar con la habilitación o equipos exigidos.

Infracciones Muy Graves

Cuantía: de 90.001 € a 225.000 € Son aquellas que suponen un grave riesgo para la seguridad aérea, la vida humana o el medio ambiente, o que reflejan un incumplimiento intencionado, recurrente o de gran impacto de la normativa.

Ejemplos de infracciones muy graves:

- Volar un dron en las inmediaciones de un aeropuerto o espacio aéreo restringido sin autorización, pudiendo interferir con aeronaves tripuladas.
- Incumplir reiteradamente las advertencias o requerimientos de AESA tras inspecciones o informes previos.
- Manipular intencionadamente los sistemas de identificación remota del dron para ocultar su operativa.

Otras sanciones no atribuibles directamente a AESA

Además de las sanciones mencionadas, existen otras infracciones sancionadas por otras

autoridades competentes, que también pueden derivarse del uso indebido de aeronaves no tripuladas o tripuladas:

1. Vuelos en entornos Protegidos por Zonas de Especial Protección para las Aves (ZEPA)

Sancionado por: Gerencia de Medio Ambiente de la Junta de una comunidad autónoma.

Motivo: Sobrevolar espacios naturales protegidos sin autorización puede alterar la fauna silvestre, especialmente en periodos de cría o nidificación.

Ejemplo: Volar un dron en un Parque Natural (Zona ZEPA) sin permiso ambiental, perturbando a especies en peligro como el buitre leonado.

2. Falta de registro previo según la Ley Orgánica de Protección de la Seguridad Ciudadana.

Sancionado por: Subdelegación del Gobierno Motivo: Realizar actividades con drones en zonas urbanas o sensibles sin haber hecho el registro previo ante la autoridad gubernativa.

Ejemplo: Grabar con un dron en una manifestación en una ciudad sin notificar previamente a la Subdelegación del Gobierno, incumpliendo las obligaciones de seguridad ciudadana.

Como evitar sanciones

- Consultar siempre la normativa actualizada de AESA antes de operar.
- Utilizar herramientas oficiales como Enaire Drones para verificar si una zona es volable.
- Obtener las autorizaciones necesarias para vuelos en espacio aéreo controlado, entorno urbano o zonas ZEPA.
- Mantener la documentación técnica y legal del dron actualizada y disponible en cada operación.
- Cumplir con las obligaciones de registro tanto ante AESA como ante la Subdelegación del Gobierno cuando sea necesario.

EPÍLOGO

Muchos Ayuntamientos andaluces están adquiriendo un compromiso con la innovación tecnológica y su aplicación en la seguridad pública. Para ello están creando unidades de drones en sus Policías Locales, una nueva herramienta que puede ser clave para la vigilancia y la seguridad pública, así como para la obtención de información. Es una ocasión para aplicar y complementar la labor de la Policía Local mediante el uso de nuevas tecnologías.

Dentro de las inversiones están adquiriendo diferentes drones en función a las pretensiones a cubrir como puedan ser drones de distintos tamaños y capacidades, igualmente se están

formando Agentes al más alto nivel que les permite operarlos con plena eficacia. Los Agentes de las unidades de dron están recibiendo la formación necesaria y cuentan con la máxima certificación como pilotos de drones (NO EASA), lo que garantiza un uso profesional y seguro de estos dispositivos al servicio de la ciudadanía.

Los drones permitirán llevar a cabo muchas tareas útiles para nuestra ciudad, entre ellas:

Búsqueda y rescate: Los drones con cámaras térmicas aportan múltiples ventajas en diversos ámbitos. Gracias a la detección de calor corporal, estos drones pueden localizar personas desaparecidas en la oscuridad, entre maleza o en condiciones de visibilidad reducida. Pueden cubrir grandes áreas rápidamente y suministrar datos en tiempo real para agilizar operaciones de rescate.

Control del tráfico y gestión de accidentes: Proporcionan una visión aérea instantánea para monitorizar atascos, detectar colisiones o bloqueos en las carreteras, mejorando la respuesta de las autoridades y reduciendo tiempos de intervención.

Vigilancia urbana y medioambiental: Permiten detectar actividades ilegales como venta ambulante, como vertidos tóxicos, construcciones no autorizadas o incendios incipientes al identificar puntos calientes o anomalías térmicas, incluso por la noche o bajo humo.

Control de aglomeraciones y seguridad pública: En eventos masivos, su visión desde el aire ayuda a medir la densidad de personas y a anticiparse a situaciones problemáticas, facilitando una intervención precoz y eficiente.

Dentro de las ventajas que puede ofrecernos una unidad de drones dentro de la Policía Local podemos destacar poder ver dentro de una operación nocturna o de poca visibilidad como pueda ser una noche cerrada, con niebla, humo o vegetación densa.

Cobertura rápida de grandes áreas: útiles en entornos extensos, peligrosos o de difícil acceso.

Datos en tiempo real: permiten tomar decisiones inmediatas con información precisa desde el cielo.

Eficiencia y ahorro: reducen riesgos para el personal, minimizan recursos tradicionales (helicópteros, patrullas) y resultan más económicos.

En definitiva, para la Policía Local se trata de una herramienta avanzada que contribuirá al desarrollo de un servicio público más eficiente y adaptado a las necesidades del futuro de nuestra ciudad.

BLIOGRAFÍA Y FUENTES UTILIZADAS

- Agencia Estatal de Seguridad Aérea. (2024, 10 de noviembre). Resolución de 10 de noviembre de 2024, de la Dirección de la Agencia Estatal de Seguridad Aérea, por la que se aprueban los escenarios estándar nacionales para operaciones de UAS en la categoría «específica» en actividades o servicios no EASA, de conformidad con el Real Decreto 517/2024, de 4 de junio.
- Comisión Europea. (2019a). Reglamento Delegado (UE) 2019/945 de la Comisión, de 12 de marzo de 2019, sobre los sistemas de aeronaves no tripuladas y sobre los operadores de terceros países de sistemas de aeronaves no tripuladas.
- Comisión Europea. (2019b). 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 sistemas de aeronaves no tripuladas.
- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia. (Boletín Oficial del Estado, 17 de octubre de 2014).
- Ley 21/2003, de 7 de julio, de Seguridad Aérea. (Boletín Oficial del Estado, 8 de julio de 2003).
- Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. (Boletín Oficial del Estado, 14 de marzo de 1986).
- Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. (Boletín Oficial del Estado, 29 de diciembre de 2017).
- Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de los sistemas de aeronaves no tripuladas (UAS), y se modifican el Real Decreto 1088/2020, de 9 de diciembre, por el que se regula el sistema de notificación de sucesos de la aviación civil (Sistema SNS); el Reglamento de la Circulación Aérea, aprobado por Real Decreto 57/2002, de 18 de enero; y el Real Decreto 931/2010, de 23 de julio, por el que se regula el procedimiento de certificación de proveedores civiles de servicios de navegación aérea y su control normativo. (Boletín Oficial del Estado, 24 de junio de 2024).
- Agencia Estatal de Seguridad Aérea. (s.f.). Registro de operador de drones/UAS. Recuperado de <https://www.seguridadaerea.gob.es/>.
- ENAIRE. (s.f.). ENAIRE Drones. <https://drones.enaire.es>
- <https://www.cursosdrones.com/>



INTRODUCCIÓN A LA CIBERSEGURIDAD I

AUTOR: FRANCISCO DE BORJA VIEJO ARENAL

Nº 2025999010106954 INSCRIPCIÓN EN EL REGISTRO DE PROPIEDAD DE LA JUNTA DE ANDALUCÍA (NINF@)

ÍNDICE DE CONTENIDOS

Prólogo

1 INTRODUCCIÓN

- 1.1 Seguridad informática y seguridad de la información**
Seguridad informática.
Seguridad de la información.
Relación entre ciberseguridad y seguridad de la información.
- 1.2 Concepto de ciberseguridad**
- 1.3 ¿De quién hay que protegerse?**
- 1.4 Cibercriminal Vs Hacker**
- 1.5 Principales características**
Confidencialidad.
Integridad.
Disponibilidad.

2 HISTORIAL DEL HACKING

- 2.1 Hechos más importantes en la historia.**
- 2.2 Ciberdelincuentes más conocidos.**

3 GLOSARIO DE TÉRMINOS

4 TIPOS DE USUARIOS

5 BIBLIOGRAFÍA Y FUENTES UTILIZADAS

PRÓLOGO

La presente publicación es la primera parte de un documento dividido en dos. En esta ocasión presentaremos a los agentes una serie de conceptos básicos y haremos un breve recorrido por la historia del hacking.

El escrito, titulado “INTRODUCCIÓN A LA CIBERSEGURIDAD POLICIAL I”, nace motivado por el creciente número de incidentes de seguridad que afectan cada vez más a los equipos electrónicos, según los datos publicados por el Ministerio del Interior, en el primer trimestre del año 2024, se registraron un total de 606.895 incidentes, de los que 484.467 (79,8% del total), son de tipo convencional, suponiendo un aumento del 0.9% respecto al mismo periodo del año anterior. El resto, 122.428 infracciones penales (20,2% del total) responden a ciberdelitos, suponiendo un aumento del 13.5% respecto al mismo periodo del año anterior. Al comparar, comprobamos como el aumento de la cibercriminalidad es superior a la del resto de delitos.

El mismo organismo publicó los ciberdelitos cometidos en 2016, en el cual, a lo largo de su primer trimestre, solo se registraron 70.178, comparado con el mismo periodo de 2023, donde los incidentes ascendieron hasta 427.448, podemos comprobar cómo, en solo ocho años, el cibercrimen ha sufrido un aumento superior al 509%.

La progresión seguirá en ascenso, hasta el punto que, desde la plataforma Zerod, estiman para 2025 unos costes relacionados con los ciberataques superiores a los 20.000 millones de euros.

En un mundo cada vez más globalizado y digitalizado, donde la tecnología está presente en todos los aspectos de la vida, el ciberespacio ha eliminado la barrera física permitiendo la comisión de delitos con un mayor anonimato y una mayor velocidad, lo que dificulta su persecución.

Por todo esto, es necesario que los miembros de la FFCCSS tomen conciencia de la importancia de este tipo de criminalidad y asuman su responsabilidad preparándose para hacerle frente, siendo esta función fundamental tanto para la prevención como para la detección y persecución de este tipo de delitos.

1 INTRODUCCIÓN

Si en mi equipo solo tengo algunas fotografías, ¿A quién podrían interesar?, ¿Para qué necesito un antivirus?, ¿Por qué debo actualizar mi sistema operativo o mis aplicaciones?

Estas son preguntas que a día de hoy aún se hacen muchos usuarios, tanto en el ámbito personal como profesional. A estos mismos habría que plantearles otra serie de cuestiones como ¿utilizas la banca en línea?, ¿realizas compras y pagas facilitando los datos de una tarjeta bancaria?, ¿tienes acceso a información personal o confidencial de tu familia? Si su respuesta fuera afirmativa, sí que tendrían muchos elementos interesantes para un atacante y, además, les estaría permitiendo obtenerlas con muy poco esfuerzo.

En gran parte de los incidentes de seguridad los afectados afirman desconocer la existencia de su vulnerabilidad. No menos sorprendente resulta que casi ninguna de las prácticas más habituales que constituyen una amenaza es novedosa, pues llevamos ya mucho tiempo inmersos en el mundo online y deberíamos conocer sus riesgos.

1.1 SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

En la mayoría de las ocasiones se utilizan ambos términos como sinónimos, pero, a pesar de estar íntimamente relacionados, son conceptos diferentes. A continuación, vamos a proceder a explicar cada uno de ellos.

Seguridad informática

Hay una serie de vocablos que podemos utilizar indistintamente, estos son seguridad informática, seguridad de las tecnologías de la información o ciberseguridad. Todos hacen referencia a la rama de la informática que se centra en proteger, no solo las infraestructuras, sino también la información que éstas contienen y los datos que circulan por las redes.

Por tanto, comprende el software, el hardware, las redes de computadoras y todo aquello que la Jefatura considere que, si terceras personas no autorizadas tuvieran acceso, supondría un riesgo para la entidad. Además, se encarga de conseguir que los sistemas sean seguros mediante el diseño de las técnicas, métodos, procedimientos y normas necesarias para identificar y eliminar vulnerabilidades.

Seguridad de la información

En esta ocasión nos referimos al conjunto de medidas preventivas y reactivas, tanto de las organizaciones como de cada uno de sus equipos informáticos, que tienen como objetivo proteger y resguardar la información para mantener la confidencialidad, disponibilidad e integridad de los sistemas y los datos que contienen.

Relación entre ciberseguridad y seguridad de la información.

El objetivo de la seguridad informática es proteger los equipos informáticos con el fin de garantizar la integridad y privacidad de los datos que contiene. Por su parte, la seguridad de la información va un poco más lejos, ya que, además, de lo anterior, tratará de proteger la información contenida en otro tipo de formatos como los impresos en papel, discos duros, memorias flash, CDs, etc. Además, implementará medidas de seguridad que afectarán a las personas que conocen la información.

1.2 CONCEPTO DE CIBERSEGURIDAD.

Tras todo lo anterior, podríamos definir la ciberseguridad como la disciplina que protege una infraestructura digital, incluyendo la información que contenga o que circula a través de sus redes de datos. El objetivo principal es garantizar la seguridad en el ciberespacio, respetando la privacidad y la libertad de los usuarios. La evolución tecnológica y el aumento en la sofisticación de los ataques hacen que el nivel de exigencia vaya en aumento.

1.3 ¿DE QUIÉN HAY QUE PROTEGERSE?

En general, los principales creadores de amenazas son:

Ciberdelincuentes: centran sus ataques principalmente en las empresas, sobre todo en bancos y otras entidades financieras, pero también pueden atacar a usuarios particulares.

Hactivistas: término formado por la fusión de las palabras hacker y activista, por tanto, podríamos decir que son personas, o grupos de personas, que utilizan sus conocimientos para ejecutar ataques con una finalidad y una motivación ideológica. Sus acciones van encaminadas a exponer a la luz pública maniobras de gobiernos o corporaciones, reivindicar derechos y libertades, crear conciencia social o fomentar la acción y la desobediencia civil.

Cibervándalos: ejecutan sus acciones para demostrar su capacidad o simplemente por diversión, más que por la obtención de beneficios. En este grupo podemos encontrar jóvenes sin experiencia que utilizan la multitud de herramientas a las que pueden acceder que no exigen altos conocimientos, hasta estudiantes habilidosos o profesionales con grandes capacidades.

Ciberespías: sus principales objetivos son la obtención de información sensible tanto de gobiernos o empresas como de particulares, información que utilizan para obtener una ventaja competitiva o para venderla y obtener así un beneficio económico.

Ciberterroristas: actores que se sirven de medios tecnológicos para realizar ataques terroristas. Utilizan redes sociales, servicios de mensajería o sitios de intercambio de ficheros para comunicarse, financiarse y reclutar adeptos.

Estados: los gobiernos son conscientes de la importancia de la guerra digital, por ello, los países están invirtiendo cada vez más en potenciar tanto sus capacidades de ataque como de defensa. Estos ataques pueden ir dirigidos contra otros estados o contra el sector privado, destinados al sabotaje de procesos críticos, al espionaje, a la difusión de mensajes políticos u operaciones de desinformación. Al disponer de muchos recursos, son ataques muy sofisticados y difíciles de detectar.

Insiders o actores internos: son personas que trabajan dentro de la organización afectada por un ataque siendo partícipes del mismo. Podemos clasificarlos en dos tipos, aquellos que revelan maliciosamente información cuya motivación suele ser de naturaleza personal o aquellos cuyo comportamiento descuidado o inconsciente ha puesto en riesgo la organización.

1.4 CIBERCRIMINAL VS HACKER

Hay un concepto que debemos tener claro, el de hacker. Si consultamos el Diccionario de la Lengua española, observamos que incluye dos acepciones para este término, uno es el de “persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora” y el otro nos lo presenta como “pirata informático”. Esta descripción no corresponde con la realidad, los expertos en ciberseguridad llevan años luchando para que la población entienda que los hackers que utilizan sus conocimientos para delinquir, no son hackers, si no ciberdelincuentes.

Por lo tanto, debemos tener clara la diferencia entre hacker y ciberdelincuente (también conocidos como crackers). En ambos nos encontramos ante personas que utilizan sus conocimientos para explorar aplicaciones, servicios, sitios web y demás herramientas con el objetivo de localizar problemas o fallos de seguridad. La diferencia radica en que la intención del hacker es solucionar, disminuir o comunicar de dichas vulnerabilidades con el fin de que sean solventados, mientras que el ciberdelincuente tratará de obtener un beneficio mediante la explotación de dichas vulnerabilidades.

Entonces, ¿En qué momento el hacking deja de ser un acto legal y se convierte en un delito? La clave para diferenciar ambos conceptos es el consentimiento. Para no cometer ninguna ilegalidad, debemos estar autorizados por la persona o entidad objeto de estudio para acceder a toda aquella información que sea de naturaleza privada o confidencial.

¿Qué análisis legales podemos llevar a cabo sin el consentimiento del propietario de la información? Aún careciendo del citado consentimiento, hay una serie de análisis pasivos que sí podemos realizar, ya que no son más que accesos a registros públicos.

Entre estos análisis podemos destacar:

Whois: este protocolo se utiliza para realizar consultas a una base de datos, la cual devuelve información como propietario de dominio, dirección IP, localización geográfica o datos de contacto entre otros.

Ataques de Fuerza bruta de subdominios mediante consultas de DNS, estos procesos se suelen realizar utilizando herramientas como recon-ng o dnsrecon.

OSINT: son las siglas en inglés de Open Source INTelligence o Recopilación de información mediante fuentes abiertas, estas operaciones se llevan a cabo a través de herramientas como Maltego. A través de estas operaciones podemos recopilar gran variedad de datos que van desde direcciones de correo electrónico hasta datos de filiación pasando por nombres de usuario en redes profesionales, contactos, teléfonos, asistencias físicas de eventos y un gran largo etcétera.

Análisis de metadatos de los elementos publicados por la entidad objeto de estudio, con herramientas como FOCA.

Localización de sistemas expuestos a internet utilizando Shodan, recopilando datos sobre los servicios y protocolos que utilizan.

Hoy en día, según Karspersky, podemos encontrar cuatro tipos de ciberdelincuentes:

Jóvenes sin experiencia: Usuarios que utilizan los numerosos sitios web disponibles en la red, donde se detallan los procesos y herramientas necesarias para crear y desarrollar malware, y cómo configurarlos para eludir el software antivirus.

Estudiantes cualificados: Alumnos que acaban de aprender a utilizar diferentes herramientas o lenguajes de programación, estando ansiosos por probar sus habilidades y demostrar su capacidad e inteligencia.

Desarrolladores profesionales: Programadores con capacidad para crear programas muy sofisticados capaces de acceder a diferentes tipos de sistemas sin el consentimiento de sus propietarios, utilizando para ello procesos innovadores, ingeniería social u otro tipo de métodos.

Investigadores: Usuarios cuyo objetivo es investigar el potencial de la «fauna informática», los cuales poseen unos conocimientos tan elevados que les permiten crear nuevos sistemas de infección resistentes a análisis de antivirus, debido a que son capaces de ocultar la infección.

Una vez visto lo anterior podemos definir la ciberseguridad como la protección de sistemas informáticos, redes, dispositivos y datos de accesos no autorizados, uso malintencionado,

robo o daño. La ciberseguridad también implica la prevención de interrupciones o ataques que puedan comprometer la confidencialidad, integridad y disponibilidad de la información y los sistemas.

La ciberseguridad abarca una amplia gama de medidas de seguridad, incluyendo la autenticación de usuarios, la encriptación de datos, el monitoreo de redes, la detección y prevención de intrusiones, la gestión de vulnerabilidades, la formación en seguridad de los empleados y la respuesta a incidentes.

1.5 PRINCIPALES CARACTERÍSTICAS.

Como se ha mencionado, la ciberseguridad también implica la prevención de interrupciones o ataques que puedan comprometer la confidencialidad, integridad y disponibilidad de la información y los sistemas. Si no podemos garantizar estos tres parámetros, nuestro sistema no se podría catalogar como seguro. Para lograr este objetivo la ISO (Internacional Organization for Standardization o es la Organización Internacional de Normalización) definió un modelo denominado modelo o triada "CIA" ("CID" en español),

esta triada forma un sistema básico para el desarrollo de sistemas seguros, que se utiliza para encontrar vulnerabilidades y generar protocolos para implementar soluciones.

Confidencialidad

La confidencialidad implica los esfuerzos destinados a prevenir una revelación de datos no autorizada, ya sea de forma intencionada o no. Con este parámetro aseguramos que sólo personas autorizadas accedan a dichos datos e impedimos su propagación, permitiendo que aquellos que necesitan tener acceso tengan los privilegios necesarios. Para lograrlo debemos controlar el acceso a la información evitando la salida no autorizada, accidental o intencionada, asegurando, además, su integridad.

Integridad

Este atributo garantiza que la información sea precisa y completa y, por lo tanto, confiable, estando libre de alteraciones, manteniendo dicha información libre de modificaciones no autorizadas. Esto nos permite asegurar que los datos son auténticos, precisos y confiables.

Disponibilidad

Este requisito garantiza que la información sea accesible sin interrupciones, encontrándose disponible para el personal autorizado cuando se requiere y en la forma requerida.

A estos tres parámetros podríamos añadirles la autenticación, formando los requisitos ACID, los cuales forman parte de las cinco dimensiones de la seguridad, que son los cuatro ya comentados y la trazabilidad. Si un sistema de información cumple con estos 5 requisitos, podríamos considerarlo como seguro.

2 HISTORIAL DEL HACKING.

Los ciberdelincuentes y comisión de ciberdelitos, no son hechos recientes, existen desde hace décadas, pero a medida que se ha extendido el uso de la tecnología, se han vuelto más comunes. A continuación, veremos algunos de los hechos más importantes y sus autores.

2.1 HECHOS MÁS IMPORTANTES EN LA HISTORIA.

En la década de los sesenta, se acuña el término “hacker” en el Instituto Tecnológico de Massachusetts (MIT), término que se utilizaba para describir a los programadores y estudiantes que exploraban la tecnología de la computación.

En la década de los setenta se lleva a cabo el primer gran ataque de hacking, concretamente en 1971, cuando un estudiante de la Universidad de Illinois, llamado Robert Tappan Morris, creó el primer gusano informático que se propagó por toda la antigua red ARPANET, causando daños significativos.

En la década de los ochenta, el mismo sujeto crea el gusano Morris, éste fue el primer ejemplar de malware autorreplicable que afectó a la citada ARPANET. En aquella fecha había unos 60.000 servidores conectados a la red, fue tan grande su expansión, que el 2 de noviembre de 1988, resultaron infectados alrededor de 6.000 de todos de ellos. Esto provocó que, para responder a posibles incidentes similares, se creara el CERT (Computer Emergency Response Team o Equipo de Respuesta ante Emergencias Informáticas). Finalmente, el autor del malware fue procesado y condenado, siendo la primera persona condenada por la ley de fraudes informáticos desarrollada en 1986.

En La década de los noventa comenzaron a aparecer grupos de hackers como “L0pht” y “Cult of the Dead Cow”. En estos años, surge la figura de Kevin Mitnick.

En los 2000 surge la figura de Dmitry Sklyarov. En 2002, el virus informático “Code Red” infectó cientos de miles de servidores de Internet. En 2008, el hacker “Mafiaboy” fue arrestado por un ataque de denegación de servicio distribuido contra importantes sitios web, incluyendo Amazon y eBay.

En la década de 2010 surgen grupos de hackers como Anonymous y LulzSec, que llevaron a cabo una serie de ataques cibernéticos contra empresas y gobiernos. En 2013, Edward Snowden filtró información clasificada sobre el programa de vigilancia masiva de la NSA, lo que provocó un gran debate sobre la privacidad y la seguridad en línea.

En la actualidad los ataques cibernéticos siguen siendo un problema importante, con grandes empresas y gobiernos siendo víctimas de ataques de ransomware y otros tipos de ciberataques. La pandemia de COVID-19, ha llevado a un aumento en los ataques de phishing y otros tipos de ataques relacionados con el trabajo remoto y la seguridad en línea.

2.2 CIBERDELINCUENTES MÁS CONOCIDOS.

Como hemos visto, los ataques no surgen de un día para otro, los delincuentes fueron desarrollando técnicas para descubrir vulnerabilidades críticas y exponer debilidades clave. Vamos a presentar varios de los expertos más relevantes de todos los tiempos en el descubrimiento y explotación de vulnerabilidades:

Kevin Mitnick

Conocido con el seudónimo de Cóndor, es, aun en la actualidad, uno de los crackers más famosos de los Estados Unidos y una figura crucial en los ataques estadounidenses. Era conocido por utilizar técnicas de ingeniería social para obtener acceso a sistemas, como el engaño de los usuarios para que le facilitasen sus contraseñas. Comenzó su actividad con 16 años accediendo a archivos protegidos dentro de ordenadores ajenos, concretamente a los de su colegio, con la única intención de husmear. En 1981 eludió los sistemas de seguridad de la compañía Pacific Bell colándose en sus oficinas de COMSOS y les sustrajo los manuales de sus ordenadores. En 1982 atacó el Comando de Defensa Aeroespacial de Norteamérica, lo que, en 1983, inspiró la película dirigida por John Badham, “Juegos de guerra”. En 1989, se infiltró en la red Digital Equipment Corporation consiguiendo hacer copias de su software. Posteriormente, fue detenido, juzgado, condenado y enviado a prisión. Durante su libertad condicional, pirateó los sistemas de correo de voz de Pacific Bell, con esta acción, Mitnik no pretendía conseguir ningún tipo de beneficio, su intención era demostrar que la operación podía llevarse a cabo. Se emitió una orden de arresto por dicho incidente, pero el sujeto huyó y estuvo escondido durante unos tres años. El 15 de febrero de 1995, fue finalmente capturado terminando nuevamente en prisión condenado por varios cargos de fraude electrónico e informático. Tras todo esto, Mitnick, dejó de actuar como un delincuente, convirtiéndose en un auténtico hacker hasta su fallecimiento el pasado año 2023.

Tsutomu Shimomura

Coetáneo con el anterior, es un físico japonés, experto en seguridad informática y alto miembro del Centro de Supercomputación de San Diego. Es conocido por ayudar al FBI a rastrear y arrestar al hacker Kevin Mitnick, tras invadir el sistema de la AT&T, lo que le permitió rastrear y escuchar llamadas, para luego remitírselas al FBI. Por este motivo hay quien lo califica como el mejor hacker de la historia. En los últimos años también ha trabajado en el área de investigación en seguridad informática, ha sido consultor de varias agencias gubernamentales en temas de seguridad y delincuencia informática. Más tarde escribió un libro sobre su participación en los hechos anteriormente narrados, adaptándose a los cines con la película “TrackDown” del año 2000.

Matthew Bevan y Richard Pryce

Conocidos como Kuji y Datastream Cowboy, son duo de británicos que, en 1996, atacaron varias redes y sistemas militares entre las que se incluyen la Base aérea norteamericana Griffiss, la Agencia de Sistemas de Información de Defensa y el Instituto Coreano de Investigación Atómica. Se les ha acusado de estar punto de iniciar la tercera guerra mundial tras copiar las investigaciones del citado Instituto Coreano de Investigación Atómica en los sistemas militares estadounidenses, demostrando que hasta las redes militares presentan vulnerabilidades.

Nicolae Popescu

Conocido por sus alias “Nae” y “Stoichitoiu” se encuentra en paradero desconocido desde el año 2012, siendo uno de los ciberdelincuentes más buscados del mundo por el FBI desde 2013. El gobierno de Estados Unidos ofrece una recompensa de 1 millón de dólares por cualquier información que conduzca a su detención. Popescu lideraba una banda criminal acusada de estafa masiva a consumidores de Estados Unidos en una web de subastas. La banda fue desarticulada a mediados de 2012, pero no se logró detener a todos los integrantes.

Michael Calce

Conocido como “Mafiaboy”, en febrero de 2000, a los 15 años de edad, consiguió hacerse con el control de las redes de ordenadores de la universidad y utilizó sus recursos para modificar Yahoo, el que, en ese momento, era el motor de búsqueda más utilizado. En tan solo una semana fue capaz de tumbar los servidores de otras importantes compañías como Dell, eBay, CNN y Amazon, utilizando un ataque de denegación de servicio para saturar sus servidores corporativos, consiguiendo en consecuencia, bloquear sus correspondiente sitios web. Podríamos decir que el desarrollo de la legislación sobre cibercrimen se convirtió en una prioridad importante del gobierno tras el ataque de Calce.

Alexsey Belan

Es los últimos años se ha convertido uno de los ciberdelincuentes más conocidos. Nació el 27 de junio de 1987 en Riga (Letonia) aunque porta pasaporte ruso. Al igual que Nicolae Popesco, en la actualidad se encuentra busca y captura. Entre los años 2012 y 2013 fue acusado por ataques que afectaron a millones de personas, en 2014 se le acusó del robo de los datos de 500 millones de usuario de Yahoo. Se lucraba vendiendo los datos robados de las más de 600 millones de cuentas a las que tuvo acceso y por asesorar a otros cibercriminales

Kevin Poulsen

Conocido con el alias Dark Dante, con apenas 17 de edad, en 1983, atacó la ya mencionada ARPANET, siendo rápidamente capturado. Al ser menor de edad el gobierno decidió no procesarlo y dejarlo en libertad con una advertencia, a la cual hizo caso omiso, ya que, en 1988, atacó un ordenador federal accediendo a los archivos relacionados con Ferdinand Marcos, décimo presidente de la República de Filipinas, depuesto por la Revolución de EDSA en 1986. Al ser descubierto, Kevin pasó a la clandestinidad, durante este intervalo de tiempo pudo acceder a archivos gubernamentales y reveló secretos, llevándolo a ser el primer hacker acusado de espionaje por las autoridades de los Estados Unidos. En 1990, pirateó un concurso de una estación de radio, ganó un Porsche, unas vacaciones y 20 000 dólares asegurándose de ser la persona 102 que llamaba al programa. Poulsen no tardó mucho en ser detenido, prohibiéndosele, además, utilizar cualquier ordenador durante un periodo de tres años. Tras todo esto logró reinventarse, convirtiéndose en un reconocido periodista divulgador de temas relacionados con la seguridad informática, llegando a ser editor jefe de Wired.

Existe una gran cantidad de sujetos o agrupaciones importantes sobre los que podríamos informarnos, como: Evgeniy Mikhailovich Bogachev, Jonathan James, ASTRA, Jeanson James Ancheta, Albert González, Adrian Lamo o Anonymous

3 GLOSARIO DE TÉRMINOS.

En el siguiente apartado vamos a familiarizarnos con la nomenclatura básica que debemos conocer:

Adware: Es toda aplicación que muestra publicidad al usuario durante la instalación o utilización de cualquier programa, esta herramienta es utilizada por los creadores del software para generar beneficios de forma legítima. Generalmente se suele incluir en las versiones shareware, eliminándose tras adquirir la versión completa del software. Por tanto, en principio, este programa es inocuo, pero se cataloga como malware en el momento que los ciberdelincuentes lo incluyen en algunas herramientas para recopilar información del equipo en el que se instala.

Antimalware: herramienta utilizada para detectar software malintencionado instalado en los equipos.

Antivirus: programa con cierta semejanza al anterior, pero en esta ocasión además de detectar malware informático, sirve para prevenir, detectar y eliminar este código malicioso.

Ataque de fuerza bruta: método utilizado para averiguar contraseñas probando todas las combinaciones posibles de letras mayúsculas y minúsculas, números y signos, hasta encontrar la combinación correcta. Con este tipo de ataques se suele tardar mucho tiempo en encontrar la combinación correcta ya que se utiliza el método de prueba y error, para reducir los tiempos se suele combinar con un ataque de diccionario.

Backdoor (puerta trasera): trozo de código que presenta un programa, el cual crea un punto oculto de acceso al sistema. Este backdoor puede ser introducido en la aplicación por sus desarrolladores para facilitar las funciones de mantenimiento, por tanto, como el adware, no tiene un fin malintencionado. El problema surge cuando un atacante descubre este punto de acceso y consigue explotar esta vulnerabilidad, o bien lo introduce de forma con finalidad malintencionada.

BotNet: conjunto, o red, de dispositivos informáticos infectados mediante malware, denominados bots (robots informáticos) o zombies. Estos equipos son controlados de forma remota por el atacante (denominado bot herder) pudiendo ser utilizados de forma conjunta para realizar actividades maliciosas.

Bug: defecto que presenta un programa creado inconscientemente por una mala programación, que provoca un comportamiento incorrecto e indeseado del software.

Carding: tipo de fraude que consiste obtener de forma ilegítima los datos de tarjetas de crédito, para posteriormente realizar compras no autorizadas.

Cifrado: técnica utilizada para convertir un mensaje, conocido como texto en claro, en uno ininteligible, denominado criptograma, para todo aquel que desconozca el procedimiento seguido para realizar dicha conversión. También se conoce a esta técnica como encriptación.

Cookie: pequeños archivos de texto almacenados en los dispositivos de los usuarios, cuya finalidad es guardar información enviada por los sitios web visitados a través de estos equipos, de manera que dicho sitio puede consultar la actividad previa del usuario.

Criptografía: es el arte o la ciencia que utiliza el cifrado para proteger información de accesos no autorizados.

Dorks: operadores que especifican una condición. Estos símbolos son utilizados para filtrar la información obtenida tras realizar una búsqueda avanzada de Google, permitiendo localizar información concreta de toda la disponible en Internet. Esta técnica es conocida como Google Dorks, Dorking o Google Hacking.

Exploit: secuencia de comandos que se ejecutan en el sistema de la víctima para explotar una vulnerabilidad.

Firewall o cortafuegos: son sistemas de seguridad de una red, cuya función es permitir solo el tráfico autorizado, asegurando que todas las comunicaciones entre la red e internet, cumplan las políticas de seguridad establecidas por los usuarios. Los podemos clasificar en

dos grupos, los formados por software o por hardware, siendo su función la misma en ambos casos.

Footprinting: fase de reconocimiento previo a la realización de un ataque o pentesting, en el que se recopila toda la información posible de la víctima y sus equipos. También se denomina information gathering.

Framework: en el contexto que nos interesa, es un entorno de trabajo que permite la ejecución de diferentes herramientas en una sola aplicación, facilitando el trabajo a los desarrolladores.

Gusano o worm: tipo de malware cuya principal característica es alta tasa de autopropagación, lo que significa que se propaga muy rápidamente y sin necesidad de intervención por parte del usuario.

Hardening: es como se conoce al proceso de securización de los sistemas informáticos al reducir sus vulnerabilidades.

Hoax o bulo: información o noticia falsa creada con la intención de confundir o engañar a la gente, que se difunde mediante las redes sociales, sistemas de mensajería o correo electrónico

HoneyPot: herramienta de seguridad preparada para ser el objetivo de un posible ataque, compuesta por un sistema informático que se configura para que resulte atractivo a los ciberdelincuentes, dicho equipo se utiliza como trampa o señuelo, con el objetivo de recopilar información de los atacantes y de su forma de actuar, en cada una de las intrusiones que sufra.

Hijacking o secuestro: en el contexto informático significa secuestro de cualquier tipo de información que contenga el equipo.

Malware: palabra formada de unión de los vocablos ingleses malicious software (software malintencionado). Es un software diseñado para acceder de forma no autorizada a los sistemas o dañarlos, por lo tanto, engloba gran cantidad de elementos como virus, troyanos, gusanos y un largo etcétera.

Metadatos: datos de control, administración, gestión y configuración de un documento que almacenan información descriptiva de éste, enriqueciendo el documento que los contiene. En el caso de las imágenes se denominan "exif".

Proxy: es un servidor, y su software, que hace de intermediario entre los dispositivos de una red LAN e internet, evitando que los equipos se conecten directamente a los sitios web o servicios, por lo añade una capa de seguridad a la red privada. Además, suelen contener otros elementos de seguridad como son los cortafuegos.

Script: también denominados guiones, son archivos que contienen un conjunto de instrucciones o comandos de ejecución por lotes, cuyo objetivo principal es automatizar tareas

repetitivas

Spyware: software que se instala en el sistema sin consentimiento del propietario, que tiene por objetivo robar información de los equipos infectados, reenviándola a terceros.

Trashing o Dumpster Diving: a diferencia de la mayoría de los conceptos que hemos visto, este término no hace referencia a una actividad digital, si no física e implica la búsqueda de información en la basura real de la víctima.

Troyano: malware que se presenta como programa legítimo para conseguir acceso no autorizado a un sistema. Sus características principales son que no tiene capacidad de autorreplicación, por lo que se suelen utilizar técnicas de ingeniería social para engañar a los usuarios e infectar sus equipos, y que, mientras se ejecutan, el equipo no suele presentar signos aparentes de mal funcionamiento. Su función principal es la creación de backdoors.

4 TIPOS DE USUARIOS

En el mundo de la ciberseguridad podemos encontrarnos con diferentes perfiles de usuarios, los más comunes son:

Black Hat (sombrero negro): persona con conocimientos informáticos avanzados que utilizan explotar las vulnerabilidades de los sistemas con fines ilícitos. También se los conoce como cibercriminales, “cracker” o piratas informáticos.

White Hat (sombrero blanco): usuarios que también disponen de grandes conocimientos informáticos, pero en esta ocasión los utilizan para proteger los equipos o mejorar la seguridad de los sistemas de información realizando pruebas de penetración para detectar brechas de seguridad, siempre con permiso de los propietarios de los sistemas y cumpliendo con la normativa legal. También conocidos como expertos de seguridad informática o “hacker”.

Grey Hat (sombrero gris): sujetos que mezclan o se encuentran entre los dos tipos anteriores, suelen buscar, sin ánimo de lucro, vulnerabilidades en los sistemas, pero lo hacen sin autorización de su propietario, por lo tanto de forma ilegal.

Blue Hat: trabajador que forma parte del equipo encargado de la defensa de los equipos de una organización ante posibles ataques, encargándose también de la respuesta ante incidentes de dicha entidad (blue team).

Red Hat: trabajador que forma parte del equipo encargado de evaluar las medidas de seguridad de una empresa (red team), simulando ciberataques del mismo modo que los llevaría a cabo un cracker.

Phreaker: vocablo formado por la contracción de los términos phone y freak. Son los craker especializados en la exploración y explotación de los sistemas de telecomunicaciones, especialmente de las redes de telefonía, actividad que se conoce phreaking.

Lammer: término que hace referencia a toda persona que presume de ser un hacker o un craker, pero que en realidad no posee conocimientos informáticos profundos, lo único que hace es utilizar scrpits y programas, denominados de botón gordo (automáticas y fáciles de usar), creados por otros usuarios más experimentados, desconociendo como actúan dichas herramientas a bajo nivel. También se les conoce como "Script Kiddie".

Carder: especialista en fraudes con tarjetas de crédito o débito, cuyos datos obtienen y utilizan ilícitamente. Tienen conocimientos que les permiten generar números falsos o robar y clonar las tarjetas, actividad que se conoce como carding.

War drivers: cibercriminales dedicados a la búsqueda de redes wifi en movimiento, o sea, se desplazan en algún tipo de vehículo buscando dichas conexiones, son conscientes que la mayoría de los usuarios no se preocupan en proteger adecuadamente estas redes presentando en gran cantidad de casos configuraciones débiles de seguridad, explotando esta vulnerabilidad.

Pharmer: este tipo de craker se dedica a ejecutar ataques de phishing, basándose en la ingeniería social para engañar a las víctimas y conseguir que se conecten a sitios web fraudulentos muy similares a los legítimos. Esta actividad es conocida como pharming, palabra formada por la combinación de los términos ingleses farming y phishing.

Spammer: se denomina spam a las comunicaciones no solicitadas enviadas masivamente, principalmente a través del correo electrónico. Por tanto, el spammer es el sujeto que se dedica a crear campañas de spam.

Wizard: usuario con conocimientos muy avanzados que conocen a fondo cómo funcionan las redes o los sistemas, por muy complejos que sean, y so capaces de ejecutar las técnicas más avanzadas de hacking. También se les conoce como "élite".

Newbie: término que hace referencia a las personas novatas que se están iniciando en el entorno de la ciberseguridad, consumiendo tutoriales, información de webs o formación reglada. También se los podría catalogar como Green Hat

5 BIBLIOGRAFÍA Y FUENTES UTILIZADAS

<https://www.incibe.es/>

<https://www.ra-ma.es/>

<https://www.uoc.edu/es>

<https://www.foc.es/>

<https://andaluciavuela.es/>

<https://www.comunixgroup.com/>

<https://www.coursera.org/>

<https://www.fundae.es/>



SPPME-A

Revista EMERGENCIAS 092 del Sindicato Profesional de
Policías Municipales de España-Andalucía (SPPME-A) ®
Fundada en 2025
Primera época. Año I. Nº 001. 2026
ISSN 3101-2701 Título clave: Emergencias 092

Edición, dirección y administración
Sindicato Profesional de Policías Municipales de
España-Andalucía (SPPME-A)
Avda. Málaga nº 12, bajo izquierda
41004 Sevilla. Tel: 646 136 645
sppme-a@sppme-a.es
www.sppme-a.es

Maquetación:
ANURA DIGITAL, S.C.