

# EDITORIAL MR

JULIO  
AGOSTO

AÑO  
2025

ISSN 3045-7629



Edición propiedad de @MetroRisk, asociación

## Especial Verano

Fran Medina Cruz  
Gregorio Duro  
Emilio Piñeiro  
Abraham Santana  
Simona Nedkova Veskova

Francisco Javier Gonzales Fuentes  
Mercedes Escudero Carmona  
Adolfo M. Gelder  
Alina Rubio

José Ignacio Olmos  
Antonio Cozano Fernández  
Rosa Fernández  
Elena de la Parte  
Carlos Serrano  
Carlos Miguel Ortiz

@Metrorisk.es

# ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

Presidente:

D. Francisco Medina cruz

Vicepresidente Económico:

D. Abraham Santana Herrera

Vicepresidente Relaciones Institucionales:

D. Juan Carlos Galindo

Secretario General:

D. Emilio Piñero

Vocal Comunicación:

Dña. Elena González de la Parte

Vocal Temas Legales:

Dña. Rosa Fernández Fernández



**MeTroRisk**  
Seguridad Patrimonial y CPTED

Editado por:

Fran Medina Cruz y Elena González de la Parte,  
en Málaga, España

ISSN 3045-7629



## COLABORADORES



## PATROCINADO POR LAS FIRMAS



Los artículos aquí expuestos son respetados en su naturaleza lingüística de país o región.

# VACACIONES, SÍ... PERO CON SEGURIDAD PROFESIONAL

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Fran Medina Cruz**  
Director de MetroRisk

El verano es la época del año donde más se valora el descanso, la desconexión y la libertad. Pero también es, paradójicamente, uno de los periodos con mayor índice de intrusiones en viviendas, sabotajes en comunidades cerradas, y vulnerabilidad operativa en muchos inmuebles vacíos o poco vigilados. ¿La solución? Entender la seguridad no como una reacción, sino como una estrategia previa, técnica y planificada.

## Seguridad no es solo instalar alarmas

A menudo se piensa en seguridad como sinónimo de alarmas, sensores o cámaras. Si bien estos elementos pueden ser necesarios, no son ni mucho menos suficientes. La verdadera seguridad se implementa desde el análisis. Y es aquí donde entra en juego la elaboración de informes de seguridad personalizados, realizados por expertos cualificados, como los consultores de MRConsulting.

Estos informes CPTED y BREEAM SyB11 analizan de forma integral todos los factores que afectan al entorno:

- Iluminación exterior y zonas de sombra
- Accesos y puntos vulnerables
- Diseño arquitectónico (balcones, muros, patios, envoltente)
- Áreas comunes y patios traseros
- Paisajismo y visibilidad natural
- Protocolos de uso durante estancias vacías

## Operativas según el riesgo

No es lo mismo una villa de lujo en una urbanización exclusiva que un edificio patrimonial en rehabilitación o una comunidad costera con múltiples entradas. Por eso, los planes operativos deben ser adaptados a cada entorno y sus vulnerabilidades específicas.

Entre las acciones recomendadas por MRConsulting se encuentran:

- Protocolos de cierre vacacional: verificación física, checklist de ventanas, persianas, accesos secundarios.
- Supervisión programada: visitas periódicas a cargo de personal formado o vigilancia inteligente.
- Uso estratégico de tecnología: cámaras térmicas, luces con sensor crepuscular, domótica.
- Simulación de presencia: automatismos que eviten delatar la ausencia.
- Entrenamiento al usuario: cómo activar el sistema correctamente, y cómo no delatar rutinas.

## Seguridad integrada desde el diseño



## Seguridad integrada desde el diseño

Lo ideal es que esta cultura de prevención se integre desde la concepción del espacio, no cuando el problema ya ha ocurrido. Por eso cada vez más arquitectos, promotores y comunidades de propietarios recurren a la figura del consultor de seguridad como parte de su equipo técnico.

**La seguridad, como el confort o la sostenibilidad, no es un lujo: es una necesidad técnica y emocional. Especialmente en vacaciones, cuando nuestra atención está puesta lejos del hogar. No se trata de vivir con miedo, sino de hacerlo con inteligencia.**

Fran Medina  
CPTED  
Análisis de Sistemas de Implementación





**ÁREA DE CONSULTORÍA**



**ÁREA LEGAL**



**ÁREA FORMACIÓN**



**ÁREA DE URBANISMO**

# ADR Y MEDIACIÓN EN SEGURIDAD PRIVADA: UNA VÍA EFICAZ PARA RESOLVER CONFLICTOS COMERCIALES

## Francisco Javier Gonzales Fuentes Presidente de ADISPO y FIBSEM

En un entorno empresarial cada vez más dinámico y competitivo, las relaciones entre empresas de seguridad privada y sus clientes están sujetas a tensiones naturales: interpretación de cláusulas contractuales, calidad del servicio, cumplimiento de niveles de seguridad, duración de contratos o incluso el cese anticipado de los mismos. Frente a estos escenarios, la Resolución Alternativa de Conflictos (ADR, por sus siglas en inglés) se presenta como una herramienta eficaz, ágil y menos costosa que el litigio tradicional.



### Un marco propicio para la mediación

La mediación mercantil es un mecanismo que encaja especialmente bien en el sector de la Seguridad Privada. A través de un proceso voluntario, confidencial y asistido por un tercero imparcial, las partes pueden alcanzar acuerdos que preserven la relación comercial y eviten la judicialización de los conflictos. Empresas proveedoras de servicios de vigilancia, consultoría o instalación de sistemas de seguridad, así como sus clientes corporativos o institucionales, encuentran en la mediación una vía para resolver desacuerdos sin afectar la continuidad del servicio o la reputación de las partes implicadas.

### Ventajas del ADR en Seguridad Privada

- 1. Rapidez: Los procesos de mediación suelen resolverse en semanas, frente a los meses o años que puede durar un proceso judicial.
- 2. Confidencialidad: Clave en un sector donde la imagen y la seguridad de la información son sensibles.
- 3. Ahorro de costes: Menor inversión económica frente a los gastos judiciales y honorarios prolongados.
- 4. Soluciones creativas: Las partes, no un juez, controlan el resultado y pueden diseñar acuerdos adaptados a sus intereses.
- 5. Preservación de relaciones: Ideal para contratos en vigor donde es preferible reconducir el conflicto antes que romper la relación.

### Casos típicos de mediación en el sector

- Reclamaciones por incumplimiento de niveles de servicio (SLA).
- Disputas sobre la duración o prórroga de contratos de vigilancia.
- Diferencias sobre facturación, penalizaciones o cláusulas de exclusividad.
- Desacuerdos en proyectos de seguridad tecnológica (CCTV, control de accesos, etc.).
- Problemas derivados de la subrogación de personal o condiciones laborales pactadas.

### Un nuevo rol para los directores de seguridad y responsables jurídicos

Los Directores de Seguridad, como responsables del enlace entre el cliente y el proveedor, tienen un papel crucial en la prevención y gestión temprana de conflictos. Formarse en técnicas de mediación o disponer de acceso a profesionales acreditados puede marcar la diferencia en la gestión integral de la seguridad corporativa.

Asimismo, incorporar cláusulas de mediación en los contratos mercantiles de seguridad puede anticipar soluciones sin necesidad de llegar al juzgado. En este caso ADISPO es la primera Asociación profesional de Directores de Seguridad que está inscrita en el Ministerio de Justicia como Institución de Mediación. Web oficial; <https://peritajes.adispo.es/> Registro oficial Ministerio de Justicia;

<https://remediabusador.mjusticia.gob.es/remediabusador/DetalleInstitucion.action?id=3991>

La incorporación del ADR, y particularmente de la mediación mercantil, al ecosistema de la Seguridad Privada no solo responde a una tendencia jurídica moderna, sino que constituye una necesidad práctica. A través de soluciones flexibles, rápidas y eficaces, se fortalece la confianza entre proveedores y clientes, se reducen los tiempos de respuesta y se protege la reputación de las partes. En un sector donde la fiabilidad lo es todo, prevenir y resolver bien los conflictos es también una forma de hacer seguridad



**José Ignacio Olmos Casado**  
Presidente AEAS

En los últimos meses la Asociación Española de Auditores de Seguridad (AEAS) ha retomado su actividad con nuevas incorporaciones dentro de la Junta Directiva. Se pretende aumentar el número de actividades y seguir reforzando el papel del auditor de seguridad en todos los proyectos de consultoría y en sus múltiples campos de actividad.



**CARTA**

En las próximas semanas los socios recibirán información actualizada con las próximas actividades a desarrollar, detalle de las novedades de funcionamiento y estructura de trabajo de la Asociación. Además, firmaremos una serie de convenios con distintos colectivos y asociaciones al objeto de beneficiar a nuestros socios.

Como hemos comentado en ocasiones precedentes AEAS pretende ser un foro donde profesionales de prestigio tengan un lugar de encuentro, tanto para la defensa de sus intereses como para su formación continua. He de resaltar que nuestra Asociación nace claramente con esta vocación, y no con el ánimo de ser mayoritaria; así, el ingreso debe ser aprobado por la Junta Directiva tras examinar la competencia y trayectoria profesional del candidato, no siendo esta una asociación al uso, y en la que la T.I.P. de director de seguridad no es más que el punto de partida, pero absolutamente insuficiente si no va acompañada de experiencia en proyectos de consultoría acreditables para el ingreso dentro de nuestro colectivo profesional.

Nuestro objetivo seguirá siendo contribuir a la mejora de la seguridad integral, prestigiar la figura del auditor y defender los intereses de nuestros asociados



# AEAS

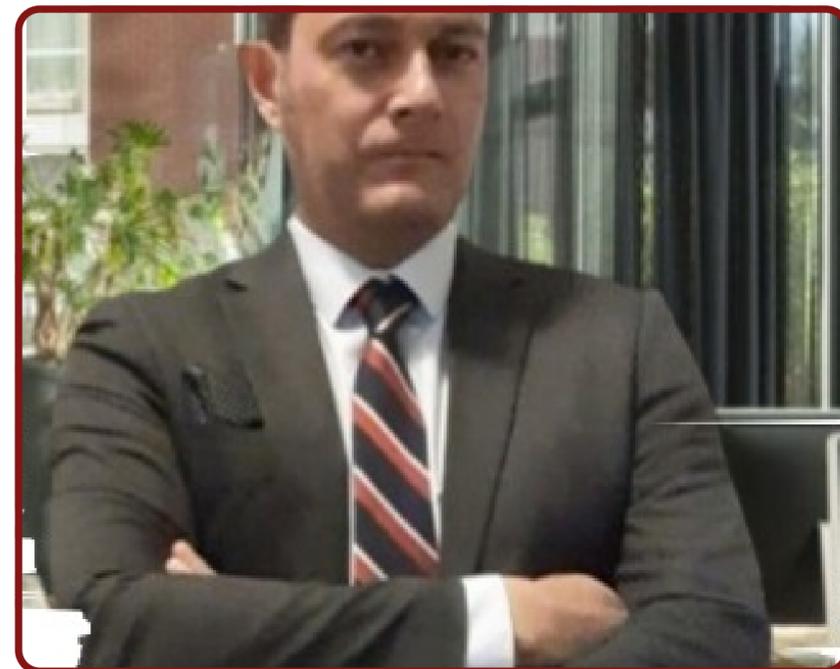
Asociación Española de  
Auditores de Seguridad

**Gregorio Duro**  
Técnico en licitaciones y Proyectos

### MÉTODO DE EULER APLICADO AL PROCESO DE ANÁLISIS DE RIESGOS

En primer término, desde el espacio que me brinda Metrorisk para la difusión y conocimiento de la cultura en nuestro sector quisiera desear a todos nuestros amigos, colaboradores y lectores, un feliz verano y unas merecidas vacaciones. Se trata, bajo mi punto de vista, de una época para dedicar al descanso y a la reflexión sobre futuros proyectos a llevar a cabo. Por eso, os animo a todos a intentar retomar nuevos proyectos con ilusión y alegría a la vuelta de las merecidas vacaciones estivales.

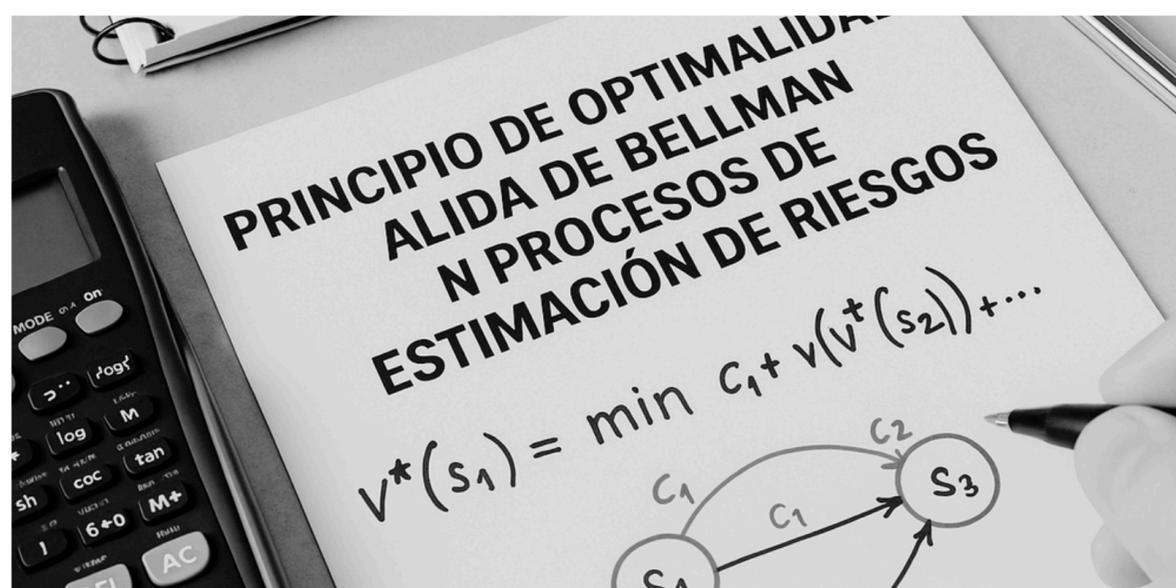
En el presente artículo voy a realizar una introducción sobre la aplicación del método de Euler en un proceso de análisis de riesgos. El cálculo de la probabilidad de un riesgo mediante el método de Euler es un sistema de cálculo que permite estimar cómo evoluciona un riesgo a lo largo del tiempo cuando este no se mantiene constante, sino que cambia de forma progresiva en función de distintos factores, como el entorno, las condiciones de los sistemas de seguridad o la acumulación de vulnerabilidades. Este método, utilizado tradicionalmente en el campo del análisis matemático para resolver problemas dinámicos, resulta especialmente útil en contextos donde se busca comprender cómo un riesgo puede ir incrementándose o modificándose a medida que transcurre el tiempo, permitiendo así una mejor toma de decisiones preventivas. A diferencia de los enfoques estáticos que calculan la probabilidad en un momento puntual y bajo condiciones fijas, el método de Euler permite simular el comportamiento del riesgo paso a paso, partiendo de una condición inicial y avanzando en pequeños intervalos de tiempo, evaluando en cada uno cómo se espera que varíe el riesgo en función de la información disponible en ese instante. Este enfoque resulta especialmente valioso en escenarios donde los factores que influyen en el riesgo son múltiples y cambiantes, como puede ser el caso de una empresa que se enfrenta a amenazas cibernéticas crecientes, donde la probabilidad de sufrir un ataque no es constante, sino que aumenta con el tiempo si no se refuerzan los mecanismos de protección, si se acumulan intentos de acceso no autorizado o si aparecen nuevas vulnerabilidades. Al aplicar el método de Euler, es posible simular cómo esa probabilidad va evolucionando de manera acumulativa, permitiendo anticiparse a momentos críticos en los que el riesgo podría alcanzar niveles inaceptables. Esta aproximación gradual ofrece una visión más realista y ajustada al comportamiento dinámico de los sistemas modernos, facilitando el diseño de estrategias de mitigación activas y basadas en evidencia, ya que permite observar no solo el estado actual del riesgo, sino también su proyección futura en diferentes escenarios. Por tanto, el método de Euler no solo constituye una herramienta matemática eficaz, sino que se convierte en una poderosa aliada para la gestión del riesgo en contextos complejos y en constante cambio.



Por ello, el método de Euler, aunque tradicionalmente utilizado en el ámbito del análisis numérico para aproximar soluciones de ecuaciones diferenciales, ofrece también un enfoque útil y versátil en el contexto del análisis de riesgos, especialmente cuando se requiere modelar la evolución dinámica de un riesgo a lo largo del tiempo. Al permitir estimaciones paso a paso de cómo puede incrementarse o modificarse la probabilidad de un evento no deseado, este método resulta especialmente pertinente en escenarios donde las condiciones cambian constantemente y el riesgo no puede asumirse como un valor fijo. Su aplicación en entornos como la ciberseguridad, la gestión operativa o la evaluación de amenazas emergentes permite anticipar comportamientos críticos y tomar decisiones informadas basadas en proyecciones más realistas. El método de Euler, en este contexto, se convierte en una herramienta complementaria que refuerza la capacidad de análisis predictivo y adaptativo. Su integración en procesos de gestión de riesgos será desarrollada en mayor profundidad en próximos artículos, donde se abordará casos prácticos y metodologías aplicadas.

Agradecer como de costumbre a Metrorisk la difusión mensual de artículos de carácter técnico que aportan un mayor conocimiento de nuestro sector.

**Gregorio Duro Navarro**  
Técnico de Licitaciones y Proyecto



**Dra. Mercedes Escudero Carmona**  
**Presidenta del Capítulo 311 de ASIS International**  
**Directora Electa de la International CPTED**  
**Presidente de CPTED México ICA Chapter.**

## CPTED Y SUS NORMAS ISO ACTUALIZADAS: GUÍA PARA ENTENDER SUS MODIFICACIONES Y APLICACIONES.

En el mes de junio se publicó la versión final de la Norma ISO CPTED 22344 y se le denominó: **ISO 22341-2:2025 Seguridad y Resiliencia — Seguridad Protectora — Parte 2: Directrices CPTED para instalaciones residenciales.**

La transición de la versión borrador ISO/DIS 22344:2024 a la norma final ISO 22341-2:2025 implica varios cambios y consolidaciones clave que reflejan la evolución de esta norma complementaria a la ISO 22341:2021, enfocada en la Metodología de Prevención del Delito mediante el Diseño Ambiental (CPTED) específicamente para instalaciones residenciales.

La emisión de la ISO 22341-2:2025 como un estándar complementario y especializado para el diseño de seguridad en entornos residenciales demuestra la evolución y profundización del campo de la Metodología del CPTED. Esta norma complementa la visión general de la ISO 22341:2021, ofreciendo herramientas más específicas para abordar las vulnerabilidades y necesidades de seguridad en el lugar donde las personas viven, todo bajo el paraguas de un proceso de consenso global validado.

Este documento explica el concepto de delincuencia y riesgo para la seguridad en instalaciones residenciales, así como los factores de riesgo relacionados. También describe las estrategias CPTED, incluyendo estrategias de seguridad específicas para diferentes tipos de espacios, de acuerdo con la jerarquía espacial de los entornos residenciales, para prevenir la delincuencia y los riesgos de seguridad.

### Correcciones y ajustes técnicos:

- Se ajustaron definiciones, términos y referencias para garantizar coherencia terminológica y técnica con la ISO 22341:2021 y otras normas relacionadas.
- Se mejoró la estructura y redacción para facilitar la comprensión y aplicación práctica por parte de profesionales de arquitectura, urbanismo, seguridad y gestión de riesgos.

Aspecto	ISO/DIS 22344:2024	ISO 22341-2:2025
Nombre y estatus	Borrador internacional (DIS)	Norma internacional publicada
Ámbito	Guía CPTED para instalaciones residenciales	Guía CPTED para instalaciones residenciales con énfasis en riesgos específicos y entorno inmediato
Enfoque en percepción	Mención general al miedo al delito	Énfasis explícito en mitigar miedo y mejorar



		percepción de seguridad
Ejemplos y aplicación	Ejemplos generales, menos flexibilidad explícita	Ejemplos generales con flexibilidad y no exhaustividad
Integración normativa	Referencias preliminares a ISO 22341 y otras	Alineación y complementación formal con ISO 22341, ISO 23234 y gestión de riesgos ISO 31000
Ciclo de vida y aplicación	Menos detallado	Aplicación desde planificación hasta operación y mejora continua
Terminología y estructura	En desarrollo, ajustes terminológicos	Terminología y estructura coherentes y consolidadas

La Norma **ISO 22341-2:2025** se enfoca en establecer contramedidas y acciones para tratar riesgos de seguridad contra personas y bienes en viviendas y su entorno inmediato, aplicando estrategias CPTED de forma efectiva y eficiente. Aunque ofrece ejemplos generales de implementación y mejores prácticas, no pretende ser exhaustiva ni limitar las aplicaciones a los ejemplos dados, y utiliza el término "seguridad" en un sentido amplio que abarca todas las aplicaciones específicas de crimen, seguridad y protección.

En resumen, las diferencias y complementos principales entre las normas CPTED son:

ASPECTO	ISO 22341:2021	22341-2:2025
Ámbito de aplicación	Entornos urbanos construidos (nuevos o existentes), diseño urbano y gestión del sitio	Instalaciones residenciales (nuevas o existentes), unidades individuales o múltiples
Enfoque	Estrategia integral de seguridad socio-urbana, prevención del delito desde el diseño urbano y construcción	Estrategias específicas para prevenir y reducir el delito y el miedo al delito en viviendas y su entorno inmediato
Contenido	Principios, elementos, estrategias y procesos generales de CPTED	Directrices para establecer estrategias y contramedidas específicas en entornos residenciales
Aplicación práctica	Incluye capacitación, administración, vigilancia natural y formal,	Recomendaciones para implementación efectiva y eficiente, con



# CPTED

	participación comunitaria	ejemplos de mejores prácticas, sin ser exhaustiva
Uso del término "seguridad"	Seguridad protectora en sentido amplio	Seguridad en sentido amplio, incluyendo crimen, seguridad y protección

Por tanto, la ISO 22341-2:2025 complementa a la ISO 22341:2021 al focalizarse en el ámbito residencial, proporcionando directrices más específicas para este tipo de instalaciones, mientras que la ISO 22341:2021 cubre un espectro más amplio en el diseño ambiental para la prevención del delito en contextos urbanos y de infraestructura física general.

Los principales cambios en la ISO 22341-2:2025 respecto a la versión 2021 (ISO 22341:2021) son:

- Cambio de denominación y consolidación normativa: la norma pasó de denominarse ISO/DIS 22344:2024 (Draft International Standard) a ISO 22341 2:2025, integrándose formalmente como parte de la familia ISO 22341.
- Se refuerza la conexión con principios de gestión de riesgos basados en la ISO 31000:2018 para un análisis estructurado y adaptado al contexto residencial.
- Integración con otras normas y marcos internacionales: la norma se alinea con la ISO 22341:2021 como documento base y complementa otras normas ISO relevantes para la seguridad y resiliencia en el entorno construido, como la ISO 23234:2021 Edificios y obras de ingeniería civil Seguridad - Planificación de medidas de seguridad en el entorno construido.
- Enfoque específico en instalaciones residenciales: mientras que la ISO 22341:2021 aborda la prevención del delito mediante el diseño ambiental (CPTED) en entornos urbanos construidos en general, la ISO 22341-2:2025 se centra en la prevención y reducción del delito y el miedo al delito en instalaciones residenciales nuevas o existentes, incluyendo unidades individuales o múltiples.
- Naturaleza y tipo de delitos tratados: la versión 2025 reconoce que los delitos y riesgos de seguridad en instalaciones residenciales tienen características específicas, como el robo (intrusión), el acceso de visitantes no deseados, la apropiación ilegal de espacios y la degradación ambiental, ampliando el alcance respecto a la versión 2021.
- Directrices para contramedidas específicas: la ISO 22341-2:2025 recomienda establecer contramedidas y acciones concretas para tratar riesgos contra personas y bienes en viviendas y su entorno inmediato mediante estrategias CPTED de manera efectiva y eficiente, mientras que la ISO 22341:2021 ofrece un marco más general para el diseño urbano y la gestión del sitio con un enfoque integral socio-urbano.

La ISO 22341-2:2025 mejora la integración de las estrategias CPTED existentes al especializar y adaptar los principios generales de la ISO 22341:2021 al contexto residencial, aportando un enfoque más detallado, práctico y efectivo para la prevención del delito en viviendas y su entorno inmediato. Entre los aspectos clave destacan:

- Jerarquización clara de espacios: establece una jerarquía de los espacios (público, semipúblico, semiprivado y privado) para diseñar estrategias adecuadas en cada anillo, lo que mejora la coherencia y efectividad de las medidas CPTED al asegurar que la seguridad se gestione desde el espacio público hasta el privado, aumentando la percepción de seguridad y la vulnerabilidad del posible infractor.
- Mejora continua y capacitación: propone la capacitación enfocada y el seguimiento constante para optimizar la administración y operación de las estrategias CPTED, asegurando que las contramedidas se adapten a la evolución de riesgos y necesidades del entorno residencial.
- Complemento tecnológico y social: la norma integra el diseño ambiental con aspectos sociales y tecnológicos, promoviendo un enfoque holístico que incluye vigilancia natural, control de accesos, mantenimiento del espacio y cohesión comunitaria, fortaleciendo así la eficacia de las estrategias CPTED existentes donde el proceso de comunicación es fundamental.
- Prevención integral más allá del robo: no solo se busca proteger contra robos, sino también evitar el acceso de visitantes no deseados, la apropiación ilegal de espacios, la degradación ambiental y mitigar el miedo al delito, aspectos que se incorporan explícitamente en el diseño del entorno residencial.
- Incorporación de la percepción de seguridad: la norma reconoce que la percepción del miedo al delito puede superar el riesgo real, por lo que el diseño debe influir positivamente en la sensación de seguridad de los residentes, integrando estrategias que mejoren la confianza y el bienestar social.
- Proceso estructurado de análisis y evaluación de riesgos: se enfatiza un proceso para analizar y evaluar riesgos de delincuencia y seguridad que orienta el desarrollo, diseño urbano, gestión del sitio y uso del medio ambiente construido o por construir, con una visión preventiva desde las etapas iniciales del proyecto.
- Optimización de recursos y reducción de costos: al prevenir el delito desde el diseño, se busca lograr proyectos sostenibles con menores costos y menor dependencia de tecnologías invasivas, favoreciendo soluciones basadas en el entorno y el comportamiento social.

# CPTED

La ISO 22341:2021 es el manual conceptual y estratégico del CPTED para cualquier tipo de espacio, mientras que la ISO 22341-2:2025 es la guía práctica y detallada para implementar esos mismos principios de CPTED específicamente en comunidades residenciales. Ambas son vitales y trabajan en conjunto para la seguridad a través del diseño.



International  
Standard

**ISO 22341-2**

**Security and resilience — Protective  
security —**

Part 2:  
**Guidelines for crime prevention  
through environmental design for  
residential facilities**

*Sécurité et résilience — Sécurité préventive —*

*Partie 2: Lignes directrices pour la prévention de la criminalité  
par la conception environnementale dans les structures  
d'hébergement*

First edition  
2025-06

Reference number  
ISO 22341-2:2025(en)

© ISO 2025

# VERANO SEGURO EN COMUNIDAD: LA IMPORTANCIA DE CONTAR CON UNA EMPRESA DE SEGURIDAD PROFESIONAL

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Antonio Cozano Fernández**  
CEO Cofer Seguridad.

El verano trae consigo un cambio de hábitos que afecta directamente a la seguridad de nuestras comunidades. Las vacaciones, las viviendas vacías, el aumento del turismo y el tránsito de desconocidos en urbanizaciones residenciales suponen un riesgo real. Sin embargo, muchos de estos riesgos pueden prevenirse si se cuenta con una empresa de seguridad privada profesional, adaptada a las particularidades de cada comunidad.



**COFER**  
SEGURIDAD

TEL: 952 409 846

¿Y SI LO ÚNICO QUE QUIERES ES DORMIR TRANQUILO?

COFER, NO VENDE ALARMAS, GARANTIZA TRANQUILIDAD.

Active su sistema de seguridad en un clic

29,95 € mes+ IVA\*

**Información general**  
info@coferseguridad.com  
952 409 846

Los meses estivales suponen una oportunidad para los delincuentes. Portales abiertos, garajes sin supervisión, viviendas deshabitadas o accesos mal controlados se convierten en puntos críticos. Las comunidades de propietarios no solo albergan múltiples viviendas, sino que también disponen de zonas comunes vulnerables: garajes, trasteros, piscinas, jardines o accesos secundarios.

## ¿Por qué contratar una empresa de seguridad?

Una empresa de seguridad no es un simple "portero con uniforme". Es un proveedor de protección integral que trabaja con medios humanos y tecnológicos para:

- Disuadir intrusiones y actos vandálicos
- Controlar el acceso de personas ajenas a la comunidad
- Detectar actividades sospechosas de forma preventiva
- Responder de manera inmediata ante incidentes
- Coordinarse con fuerzas y cuerpos de seguridad si es necesario
- Aplicar operativas y rutinas adaptadas al tipo de comunidad y sus horarios estivales



El coste de contratar seguridad en verano es insignificante frente al coste económico y emocional de sufrir un robo, un sabotaje o una intrusión. Apostar por una empresa profesional es apostar por la convivencia tranquila, la protección del patrimonio y la confianza de todos los vecinos.

Si algo he aprendido es que es un trabajo duro, poco reconocido y lleno de grandes profesionales que cada día dan lo mejor de sí para que el resto pueda vivir más tranquilo, estos grandes profesionales llamados vigilantes de seguridad, escoltas y resto de especialidades complementan día a día a nuestras fuerzas y cuerpos de seguridad sin dar ruido sin ser protagonistas sin reconocimiento y entregados día a día a una sociedad que aún no reconoce su gran labor al ciudadano, cada día en esta profesión me da nuevas experiencias y a veces grandes satisfacciones, de vez en cuando alguien te da las gracias cuando tú equipo, tus trabajadores le han ayudado en situaciones a veces muy complicadas y con casi cero medios y son estos momentos los que te hacen sentir que estás haciendo algo bueno por los demás..... vigilantes de seguridad los grandes desconocidos de una sociedad que cada vez es menos generosa y ofrece menos reconocimiento a los que velan con todo su afán por el bienestar y descanso del resto de ciudadanos

D. Antonio Cozano Fernández



# ¿Cámaras en la vía pública? SÍ, PERO NO SIEMPRE.

Y DESDE LUEGO, NO CUALQUIERA. ¡NO todo vale!

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Emilio Piñero**  
Especialista en Compliance y Proyectos  
Consultoría | Formador y Conferenciante

## ..te invito a reflexionar:

En **Compliance**, sabemos que no  
"todo lo legal es automático"  
ni todo lo urgente es válido.

La instalación de sistemas de videovigilancia  
en lugares públicos exige algo más  
que tecnología: requiere criterios,  
marco normativo claro y  
proporcionalidad.

He leído con mucho interés el análisis compartido  
por mi estimado **MANUEL CASTILLEJA**,  
una referencia en privacidad,  
(al menos para mí)...

En esta ocasión, sobre el "entramado normativo"  
que regula estos sistemas, desde  
la LO 4/1997 hasta la  
LO 7/2021, pasando  
por RGPD y claro,  
por LOPDGDD.

Como recordatorio clave:

La captación de imágenes en la vía pública está reservada,  
como regla general, a las Fuerzas y Cuerpos de Seguridad.

Los ayuntamientos y empresas privadas deben cumplir  
con exigencias específicas, autorizaciones previas  
y límites definidos en cuanto a necesidad,  
finalidad y minimización.

La proporcionalidad no es un detalle: es un pilar.



**Dónde crees que está el mayor  
riesgo actualmente en materia de  
videovigilancia pública?**

**¿El exceso de confianza  
tecnológica?**

**¿La falta de controles?**

**Seguimos construyendo una  
cultura basada en legalidad, ética  
y responsabilidad.**

**EMILIO  
PIÑERO**



# C2C Consultoría&Compliance



Nos dirigimos al mercado empresas, ayudamos a los departamentos de rrhh, financiero, legal y dirección a consolidar los planes de cumplimiento, a generar itinerarios formativos que apoyen la toma de decisiones y el cambio necesario para generar un proyecto de cumplimiento 360°. Todo ello con el apoyo de la plataforma #EmPrendizaje de formación e-learning, la formación presencial y el aula virtual, poniendo a en su mano la tecnología, la experiencia y el apoyo de la bonificación de Fundae para que cuenten desde la empresa con todos los recursos posibles.



**Apasionados por impulsar la transformación de las organizaciones y potenciar el talento humano”.**

**Contacto:** Emilio Piñeiro  
CEO, Compliance officer, emprendedor  
consultor, docente y divulgador

[info@formacioncorporate.com](mailto:info@formacioncorporate.com)  
[e.pineiro@consultoriacompliance.es](mailto:e.pineiro@consultoriacompliance.es)  
Teléfono: 621 04 79 49

**Delegaciones:** Madrid / Barcelona / Valencia / León /  
Ciudad Real / Zamora / Málaga / San Sebastian / Badajoz

# LA AMENAZA INVISIBLE DEL SOFTWARE SUPPLY CHAIN ATTACKS

## Adolfo M. Gelder S&S Consultores Corporativos C.A.

Vivimos en un mundo hiperconectado, donde el software que usamos a diario rara vez es "hecho en casa". Dependemos de bibliotecas, plataformas de terceros, herramientas de desarrollo... Y aunque eso acelera la innovación, también ha abierto la puerta a una de las amenazas más sigilosas en ciberseguridad: los ataques a la cadena de suministro de software.

Antes, bastaba con proteger nuestros sistemas y redes. Hoy, incluso el software más confiable puede traer sorpresas desagradables si alguien comprometió el proceso en alguna parte del camino. Y lo más preocupante es que muchos de estos ataques se cuelan justo por donde menos lo esperamos: por la confianza (¿qué irónico, ¿no?)

**¿Qué es un ataque a la cadena de suministro?** Imagina que compras una medicina con sello oficial, pero el laboratorio que la fabricó fue hackeado y alguien adulteró la fórmula. Lo mismo pasa cuando se cuelan malware en bibliotecas de código, herramientas de desarrollo o actualizaciones de software. Los atacantes no apuntan directamente a la víctima final: infectan una etapa anterior del proceso, como el entorno de compilación, una dependencia externa o incluso la firma digital que valida el software. Así, el malware llega disfrazado de "producto legítimo" y pasa desapercibido

**¿Cómo lo hacen?** Aquí algunos métodos que usan los atacantes:

- - Código alterado en repositorios: entran al código fuente usando credenciales robadas o suplantando a un desarrollador, y agregan instrucciones maliciosas sin levantar sospechas.
- - Herramientas de desarrollo comprometidas: manipulan software de construcción o de entrega continua, inyectando malware durante el proceso.
- - Librerías externas contaminadas: muchos sistemas usan código abierto. Si una biblioteca popular se ve comprometida, miles de proyectos pueden heredar el problema sin saberlo.
- - Firmas digitales robadas: logran firmar software malicioso con claves legítimas, dándole un sello de "confiable".
- - Actualizaciones trampa: comprometen el canal de distribución para enviar "nuevas versiones" que, en realidad, son puertas traseras.

**Todo esto funciona porque las organizaciones confían en sus proveedores, en los repositorios y en los procesos de automatización. Y esa confianza, irónicamente, es el punto débil.**

*Con todo esto, lo que quiero decir es que los ataques a la cadena de suministro representan una de las mayores amenazas a la ciberseguridad actual. No se trata de si van a ocurrir, sino de cuándo... y cuán preparados estamos para resistirlos y recuperarnos. Adoptar una visión integral —que combine evaluación de proveedores, desarrollo seguro, monitoreo constante y respuesta efectiva— ya no es opcional. Es la única manera de proteger la infraestructura digital que sostiene nuestras vidas, nuestras organizaciones y hasta nuestras sociedades. Más vale prevenir que lamentar*



**¿Qué tan grave puede ser esto?** Muchísimo. Un solo proveedor comprometido puede afectar a decenas, cientos o miles de organizaciones. El caso de SolarWinds en 2020 fue un ejemplo claro: un simple parche oficial llevó un troyano a gobiernos, multinacionales y empresas críticas. Los daños pueden ser masivos:

- - Acceso a redes sensibles sin atacar directamente a la víctima.
- - Presencia silenciosa durante meses, sin que nadie se dé cuenta.
- - Pérdida de confianza y reputación, incluso juicios y multas.
- - Riesgos de seguridad nacional, si se involucran infraestructuras críticas.

**¿Cómo defendernos?** Más allá de antivirus y firewalls. Protegerse requiere algo más que herramientas tradicionales. Aquí algunas medidas clave:

- - Visibilidad total sobre lo que se usa: exigir listas de componentes y entender de dónde viene cada parte del software.
- - Evaluar bien a los proveedores: no solo al principio, sino de forma continua.
- - Seguridad desde el desarrollo: con análisis de código, escaneo de dependencias vulnerables y control estricto de las firmas digitales.- Principio de Confianza Cero: asumir que nada es seguro por defecto, ni siquiera lo interno.
- - Segmentar entornos: separar desarrollo, pruebas y producción para evitar movimientos laterales.
- - Autenticación fuerte y monitoreo constante: con análisis de comportamiento y detección de anomalías apoyadas por IA
- - Preparación para incidentes: planes claros de respuesta, simulacros y colaboración con otras organizaciones para compartir inteligencia.

# DEL DATO AL DELITO: LO QUE TODO PROFESIONAL DE LA SEGURIDAD DEBE SABER

**Rosa Fernández**

## ASUNTO: VIGILANCIA Y PROTECCIÓN DE DATOS CÓMO LIDERAR OPERACIONES DE VIDEOVIGILANCIA Y CONTROL CON GARANTÍAS LEGALES EN LA ERA DEL RGPD

La seguridad privada ya no se limita a custodiar edificios o controlar accesos. Cada imagen captada, cada dato registrado y cada sistema activado puede cruzar la frontera entre la protección legal y la infracción grave. En un entorno hiperregulado por el Reglamento General de Protección de Datos (RGPD) y la LOPDGDD, el reto es claro: garantizar la seguridad sin vulnerar derechos. Si eres un Director de Seguridad, un supervisor de videovigilancia, piloto de drones, encargados de protección de personas, gestores de bienes sensibles y responsables de control operativo que trabajan en sectores como retail, health tech, infraestructuras críticas o vigilancia patrimonial, sigue leyendo porque este artículo te ayudará a trabajar con más tranquilidad y seguridad.

**El dato como vector de riesgo, no solo imágenes.** Tanto si diriges un equipo de vigilancia en un centro comercial como si gestionas un sistema de escolta para personas de alto perfil, estás tratando datos personales. Incluso más: a menudo tratas datos sensibles, como: Conductas, rutinas y hábitos de personas. Localización geográfica (trackers, GPS, CCTV). Incidencias o riesgos asociados a bienes de alto valor. Casuística clave:

📍 Un jefe de seguridad patrimonial activa un protocolo de protección con seguimiento por GPS de un vehículo de obras de arte: trata datos geolocalizados vinculados a una persona concreta.

🔒 Una empresa de vigilancia VIP gestiona informes de amenazas o agresiones anteriores contra la persona protegida: se trata de datos sensibles (seguridad e integridad física).

Recuerda: cualquier dato que identifique directa o indirectamente a una persona está protegido por el RGPD. No se trata solo de nombres e imágenes.

**Vigilancia proporcional y documentada: el equilibrio que evita sanciones.** Toda acción de vigilancia debe justificarse, tanto desde el punto de vista operativo como legal. La proporcionalidad no es negociable. Debes poder demostrar: Que la vigilancia responde a una finalidad legítima. Que no hay una alternativa menos intrusiva. Que el tratamiento está limitado a lo estrictamente necesario. Casuística clave:

🏥 Un responsable de seguridad en un hospital decide instalar cámaras en la zona de urgencias tras varios incidentes de agresión: requiere Evaluación de Impacto y consulta al DPD, dado que se capta información médica y flujos de pacientes.

🏛️ Una galería de arte decide implantar vigilancia 24/7 con IA analítica sobre movimientos sospechosos: debe analizarse si el sistema genera perfiles automatizados, lo cual implica obligaciones adicionales. Si no puedes justificar la instalación de una cámara en términos legales, probablemente esa cámara no debería estar ahí



**Transparencia activa, el cartel no basta.** Muchos operadores creen que colocar un cartel con la cámara es cumplir. Error. Todo sistema de vigilancia debe garantizar: Información clara y accesible sobre el tratamiento de datos. Canales para ejercer derechos ARSOPL. Registro interno del tratamiento. Casuística clave:

📺 Una empresa de seguridad en un centro comercial graba con cámaras ocultas por motivos operativos. Si no hay justificación legal y no se ha informado al público, es sancionable por opacidad.

🏢 Un equipo de control en una sede corporativa utiliza grabaciones para fines disciplinarios sin informar previamente en la política interna: se vulnera el derecho a la información y puede generar nulidad de pruebas

**El personal, tu primera vulnerabilidad (o tu mejor blindaje)** Sin formación, no hay protección. Los operadores de cámara, vigilantes, técnicos o supervisores deben conocer: Qué pueden grabar y qué no. Cuándo deben conservar o eliminar imágenes. Cómo actuar ante una solicitud de acceso a datos. Casuística clave:

📱 Un operador de seguridad reenvía por WhatsApp un vídeo de un intento de hurto a su grupo de trabajo: eso ya es una cesión ilícita de datos.

🔑 Un vigilante usa un acceso genérico a los grabadores y no hay trazabilidad de acceso: riesgo de fuga o alteración sin control. Establece protocolos escritos, accesos restringidos y formación continua para tu equipo. Exige lo mismo de tus colaboradores.

**Consultora jurídica. ©2025**

**Miembro del Comité Técnico de MetroRisk, área de seguridad jurídica y derecho tecnológico**

**Tecnología sin ética es solo exposición** La innovación (IA, biometría, análisis de comportamiento) puede ayudarte a proteger, pero también puede hundirte legalmente si no la gestionas con responsabilidad. Si trabajas con soluciones con IA no sólo tendrás que tener en cuenta el RGPD sino también el RIA (Reglamento Europeo de Inteligencia Artificial). Checklist para no cruzar la línea:

- ✓ ¿Has hecho una EIPD?
- ✓ ¿Está documentado el interés legítimo?
- ✓ ¿Tu proveedor cumple con RGPD?
- ✓ ¿Se ha implicado al DPD desde el inicio?
- ✓ ¿Has contemplado derechos como oposición o supresión?

Recuerda: el RGPD exige responsabilidad proactiva. El "no lo sabía" ya no vale. La ignorancia de la ley no excusa de su cumplimiento.

Desde el control de accesos en un estadio hasta la vigilancia discreta de una persona VIP o la custodia de un cuadro de Goya, la seguridad hoy es también jurídica. Tienes que tener en cuenta todas las medidas de seguridad para cada caso. Cada decisión, cada sistema y cada grabación puede marcar la diferencia entre actuar con diligencia... o cometer un delito. Porque, en seguridad, ya no basta con vigilar. También hay que proteger el dato y los derechos que conlleva

¿Te gustaría conocer tu nivel de cumplimiento, o necesitas más información para evitar este tipo de riesgos?

TU ELIGES EL NIVEL DE SEGURIDAD Y DE PROFESIONALIDAD. ✓ ¿Quieres saber si cumples la ley al 100%? ¿Trabajas con IA en tu empresa?

CONECTA CON NORMA :  
 TU ASESORA VIRTUAL EN RGPD. 📧✍️  
 Visita ZonaVigilada.net 📧👉 Conecta  
 conmigo en  
 ✉️ rosaf@zonavigilada.net  
 Te damos respuestas y te ayudamos a  
 mejorar tu seguridad jurídica



**ZONAVIGILADA.NET**

TU ELIGES EL NIVEL DE SEGURIDAD

**Consultoría Jurídica**  
**Implantación RGPD RIA**  
**Formación con IA**  
**Mantenimiento RGPD**  
**Guías especializadas**

**Rosa 6.0**  
 Código Experiencia

Diplomada en Derecho, Tecnología e Innovación  
 Compliance (RGPD, RIA, LOPDgdd, LSICE)  
 Consultora Sr Calidad (ISO, EFQM, 5S)  
 Consultora Jurídica  
 Técnica en Ciberseguridad  
 Formadora veterana\*  
 Diseñadora de material didáctico

Miembro Comité Técnico Asesor en MetroRisk  
 Socia de ENATIC, asociación de Abogacía Digital

**Competencias técnicas:**  
 WORDPRESS, PRESTASHOP, POWTOON, DOODLY,  
 ADOBE AUDITION, MOODLE, OBS, VIMEO, IA.

\*+ de 25 años formando a profesionales




# POR QUÉ EL CICLO FORMATIVO DE GRADO MEDIO EN SEGURIDAD NO REEMPLAZARÁ AL CERTIFICADO PROFESIONAL EN SEGURIDAD PRIVADA

## Carlos Serrano Director de Contenidos de Seguridad y Empleo

En el sector de la seguridad privada, la constante evolución de la formación es esencial para cubrir la demanda de profesionales competentes y actualizados. Recientemente, la creación del ciclo formativo de grado medio en seguridad ha generado algunas dudas en cuanto a su impacto en el futuro de los certificados profesionales en seguridad privada. Sin embargo, es fundamental entender que ambos tipos de formación no solo son complementarios, sino que el certificado profesional sigue teniendo un papel esencial en el desarrollo de competencias específicas. A continuación, exploraremos las razones clave por las que el ciclo formativo de grado medio no reemplazará al certificado profesional y cómo ambos forman una sinergia fundamental en la capacitación de estos profesionales.

**1. Complementariedad en lugar de reemplazo** El ciclo formativo de grado medio en seguridad y el certificado profesional en seguridad privada no se diseñaron para competir entre sí, sino para ofrecer una ruta de formación coherente y progresiva. Mientras el ciclo formativo de grado medio cubre una formación más amplia y estructurada en el ámbito de la seguridad, el certificado profesional responde a necesidades específicas del sector, ofreciendo un aprendizaje especializado en competencias concretas, como la vigilancia, la protección de bienes y personas, y la aplicación de protocolos de emergencia.

De hecho, la mayoría de las organizaciones de formación, junto con el Instituto Nacional de las Cualificaciones (INCUAL), respaldan la idea de que estos dos niveles de formación van de la mano. Un profesional con el certificado puede, de manera más ágil, continuar su desarrollo en el ciclo formativo de grado medio gracias a la convalidación de módulos formativos específicos.

Esto no solo optimiza el tiempo y recursos de los estudiantes, sino que fomenta una ruta clara de progreso profesional



[www.seguridadyempleo.com](http://www.seguridadyempleo.com)



## 2. El valor del certificado profesional en el sector

En seguridad privada, el certificado profesional es un requisito esencial para acceder a ciertas acreditaciones y puestos de trabajo. Este certificado avala que el profesional posee las competencias técnicas y prácticas necesarias para cumplir con los estándares de seguridad requeridos por la legislación y por las empresas. Así, el certificado profesional continúa siendo el documento que muchas empresas reconocen y valoran, especialmente para puestos de nivel operativo, como vigilantes de seguridad.

Además, el certificado profesional permite a los trabajadores acceder a una formación específica y actualizada en un período relativamente breve, lo cual facilita su incorporación rápida al mercado laboral. Esto es una ventaja importante en un sector que exige actualización constante y personal cualificado en todo momento. Por lo tanto, aunque el ciclo formativo de grado medio puede ampliar conocimientos y ofrecer más oportunidades, el certificado profesional sigue siendo indispensable para quienes desean ingresar rápidamente en el ámbito laboral de la seguridad privada.

## 3. Facilidades para continuar la formación

Uno de los beneficios de contar con un certificado profesional en seguridad privada es la posibilidad de acceder al ciclo formativo de grado medio de forma más rápida y efectiva. Gracias a la convalidación de algunos módulos formativos, los profesionales certificados pueden reducir la carga académica al cursar el ciclo medio, lo cual representa una ventaja para aquellos que desean ampliar sus competencias y cualificaciones sin repetir formación que ya han acreditado.

**Carlos Serrano**  
Director de la Web, Seguridad y Empleo

La INCUAL respalda estas convalidaciones y reconoce el esfuerzo y los conocimientos adquiridos previamente a través del certificado profesional, por lo que los estudiantes pueden enfocarse en aprender nuevas habilidades y especializarse más en su carrera sin tener que empezar desde cero. Esta flexibilidad fomenta el crecimiento profesional y permite a los trabajadores adaptar sus conocimientos a las demandas actuales del sector.

#### **4. La visión de una carrera progresiva y especializada**

La coexistencia del ciclo formativo de grado medio y del certificado profesional ofrece una ventaja en cuanto a la posibilidad de construir una carrera sólida y progresiva en seguridad privada. En lugar de optar por una única vía formativa, los profesionales pueden decidir el nivel de especialización que desean adquirir en función de sus aspiraciones y del tipo de funciones que buscan desempeñar.

El ciclo de grado medio aporta una perspectiva más global de la seguridad, ideal para aquellos que desean eventualmente desempeñarse en puestos de mayor responsabilidad o gestión en el sector. Sin embargo, el certificado profesional sigue siendo una opción esencial para quienes desean especializarse en tareas específicas y obtener una rápida inserción laboral, sin dejar de tener la puerta abierta para continuar sus estudios en el ciclo formativo de grado medio si así lo desean.

**Conclusión:** La Nueva Ley de FP y su impacto en la formación en seguridad privada.

Con la entrada en vigor de la nueva Ley Orgánica de Ordenación e Integración de la Formación Profesional, se han introducido importantes cambios en el sistema educativo, incluyendo la creación de nuevos grados y titulaciones que refuerzan las oportunidades de desarrollo profesional en seguridad privada. Esta ley introduce un modelo más flexible y escalonado que facilita la adquisición de competencias progresivas y el reconocimiento de la experiencia profesional

La coexistencia del ciclo formativo de grado medio en seguridad, del certificado profesional y de los nuevos grados de especialización garantiza que el sector de la seguridad privada cuente con profesionales altamente cualificados y que cada persona pueda elegir el camino de formación más adecuado para sus objetivos. Lejos de ser una competencia, estas formaciones se complementan y fortalecen entre sí, brindando una estructura que se adapta a las necesidades reales del mercado y de los trabajadores en este ámbito.

# SEGURIDAD AEROPORTUARIA: DEL CONTROL DE ACCESO AL CIELO

**Abraham Santana Herrera**  
Director de seguridad. Perito

En la actualidad, los aeropuertos son uno de los entornos con mayor exigencia en materia de seguridad. La protección de infraestructuras críticas, el control masivo de pasajeros y equipajes, y la prevención de amenazas en vuelo, convierten a cada aeropuerto en un ecosistema de seguridad altamente especializado.

## Antes del vuelo: seguridad terrestre y acceso controlado

Desde que un pasajero entra en el recinto aeroportuario, la seguridad empieza a actuar. No se trata solo de detectar amenazas, sino de gestionar flujos, minimizar riesgos y mantener la operativa sin colapsos. Estas son las capas fundamentales:

- Control perimetral y acceso a zonas restringidas: vallas, lectores biométricos, videovigilancia perimetral, sensores de movimiento y patrullaje constante.
- Inspección de equipajes: mediante escáneres de rayos X, análisis de trazas explosivas y perfiles de comportamiento.
- Control de pasajeros (PIF): escáneres corporales, arcos de detección de metales, validación documental y entrevistas breves si se detectan anomalías.
- Seguridad operacional: vehículos de apoyo en pista, personal acreditado, zonas de servicio, acceso a combustible y catering están monitorizados y sujetos a inspecciones continuas.

Todo esto es supervisado por empresas de seguridad privada en colaboración directa con fuerzas policiales y cuerpos específicos como la Guardia Civil o la Policía Nacional en España.



## Durante el vuelo: seguridad aérea y comportamientos de riesgo

Una vez en vuelo, la seguridad cambia de forma pero no de propósito. Se centra en la prevención de actos hostiles, la contención de incidentes a bordo y la coordinación con el centro de control en tierra.

- Tripulación formada en seguridad: los auxiliares de vuelo no solo sirven bebidas. Están entrenados en autoprotección, control de pasajeros agresivos y primeros auxilios.
- Cabina blindada y sellada: tras los atentados del 11S, todas las aeronaves comerciales deben contar con una cabina de pilotos inaccesible desde el pasillo sin autorización expresa.
- Tecnología a bordo: los vuelos están protegidos por sistemas de comunicación encriptada, geoposicionamiento constante, y protocolos ante intentos de secuestro o sabotaje.
- Pasajeros como eslabón activo: hoy más que nunca, se pide la colaboración ciudadana. Desde la observación de conductas extrañas hasta seguir las instrucciones sin generar conflicto.

## Seguridad invisible pero constante

Muchos de los sistemas de seguridad operan sin que el pasajero lo perciba: cámaras con IA que analizan el comportamiento, algoritmos que cruzan datos de documentos, y perfiles de riesgo que se actualizan en tiempo real.

Cada vez más aeropuertos están adoptando inteligencia artificial, análisis predictivo y vigilancia por capas, lo que permite un equilibrio entre fluidez y control exhaustivo.

**La seguridad aeroportuaria no es un conjunto de barreras, sino una red de protección pensada para garantizar que cada vuelo sea una experiencia segura y eficiente. Desde el acceso al recinto hasta el aterrizaje final, hay decenas de capas invisibles diseñadas para un solo objetivo: proteger la vida de las personas y la continuidad del transporte aéreo global.**



# SEGUROS Y SEGURIDAD PRIVADA EN EVENTOS: DOS PILARES DE UNA GESTIÓN RESPONSABLE

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

## Alina Rubio de las Casas Experta en Seguros Generales

En el mundo de la seguridad privada, la protección no termina en la verja del recinto ni con el cambio de turno. Cada profesional de este sector —ya sea vigilante, escolta, técnico, director de seguridad o consultor operativo— vive expuesto, a diario, a situaciones de tensión, vigilancia prolongada, enfrentamiento con la incertidumbre, e incluso, en algunos casos, a la violencia física.

*Agente exclusivo, Generali Seguros  
Planes diseñados a medida de tus necesidades,  
con atención directa y profesional  
alinarubiodecasas@gmail.com*

Sin embargo, una paradoja persiste: quienes trabajan para proteger a los demás, a menudo descuidan su propia protección personal y patrimonial.

### Una realidad ignorada: el vacío asegurador

Los profesionales de la seguridad operan en un entorno laboral cargado de riesgos:

- Jornadas nocturnas y rotativas
- Entornos conflictivos o vulnerables (eventos, aeropuertos, instalaciones críticas)
- Posibles agresiones o represalias
- Accidentes en desplazamientos o durante intervenciones
- Estrés crónico, desgaste físico y mental

A pesar de ello, muchos carecen de un seguro de vida o de accidentes personales adecuado, confiando únicamente en las coberturas básicas de sus empleadores o en el sistema público. Pero eso no es suficiente.

### ¿Por qué un seguro específico?

Un seguro de vida o accidentes para una profesión de riesgo no es solo una póliza: es una herramienta de continuidad. Proporciona respaldo económico ante:

- Incapacidad permanente o parcial
- Fallecimiento por causas laborales o extralaborales
- Indemnización para la familia en caso de accidente mortal
- Coberturas complementarias: hospitalización, asistencia psicológica, cirugía, etc.
- Protección del nivel de vida y del futuro familiar

Y, especialmente en el caso de autónomos, freelance o profesionales externos, representa una garantía de ingresos y tranquilidad ante lo inesperado.



### Una decisión personal con impacto profesional

El profesional que se protege a sí mismo transmite una cultura de prevención, coherencia y responsabilidad. Es, además, un acto de dignidad hacia su trabajo y su familia. Porque nadie está exento de un imprevisto, y menos quien trabaja en un sector donde lo imprevisto es la norma.

Ser profesional de la seguridad implica asumir riesgos, pero no ser víctima de ellos. La contratación de un seguro de vida y accidentes adaptado a nuestra actividad no es una opción; es una necesidad ética, financiera y humana.

Recomiendo y acompaño a los profesionales en la elección de coberturas adecuadas, entendiendo las particularidades del sector y asesorando en la integración de protección personal dentro del desarrollo profesional.

**Protege lo que haces.  
Protege lo que eres.**



# GALINDO BENLLOCH

Somos expertos en compliance penal, prevención del blanqueo de capitales y seguridad de la información. Prestamos servicios de Cumplimiento normativo ofreciéndote la solución más eficaz, rentable y confidencial, a través de un equipo de profesionales que te acompañarán en todo momento.

Nuestra especialidad es la elaboración de informes periciales enfocados a la recuperación de activos sustraídos mediante técnicas de ingeniería social (estafas informáticas), tanto en dinero tradicional, como en Criptomonedas. Nuestros casos de éxito ante los tribunales de justicia nos avalan.

La orientación al cliente no es solo una palabra para nosotros, por eso siempre nos ajustaremos al presupuesto y tamaño de tu empresa.

## Unidad de acción

CIERRA EL CÍRCULO CON GALINDO BENLLOCH



### FORMACIÓN

Es el nexo de todos nuestros principios. Obtenemos información de la empresa y la analizamos, así como aportamos el conocimiento necesario. Con el resultado de ambas lo convertimos en formación continua totalmente personalizada. Mediante la cual, generamos conocimiento y valor a toda la plantilla, partes y contra partes

### PREVENCIÓN

Te ayudamos a anticiparte a incumplimientos regulatorios y riesgos empresariales. Cumpliendo con la ley de prevención del blanqueo de capitales, seguridad de la información, responsabilidad penal de persona jurídica, fraude interno y externo, cibercrimes y delitos económicos.

### DETECCIÓN

Implementamos procesos y alertas tempranas para situarnos con ventaja en la toma de decisiones. Ya que esta información será vital, para nuestras acciones posteriores. Bien comunicando a los organismos reguladores o judiciales pertinentes, o bien cumpliendo con las obligaciones internas de conservación.

### INVESTIGACIÓN

Investigamos todos las sospechas o indicios de incumplimiento regulatorio o de la presunta comisión de un delito, para salvaguardar la responsabilidad empresarial de los mismos. Los resultados se vuelcan en un informe técnico pericial con valor probatorio en las jurisdicciones pertinentes. Haciendo hincapié en las investigaciones internas derivadas de las denuncias interpuestas en los sistemas internos de información. Donde un tercero independiente garantiza la solidez de la investigación interna.

### SEGURIDAD INTEGRAL

Realizamos consultoría de seguridad física, lógica y cibernética. Para nosotros la unidad de acción es un principio fundamental como prestadores de servicios. Uniendo en un solo proveedor los servicios de Ciberseguridad, seguridad física y lógica.

## Elena de la Parte

**Aferrémonos fuerte con la más rigurosa seguridad, desde la velocidad vertiginosa de los monoplazas hasta la presencia de aficionados. Ya no se trata solo de la adrenalina en el circuito: Palpas como esta adrenalina Se difunde y se vive. Las personas VIP y famosas se enfrentan a numerosos desafíos en cuanto a su seguridad personal. Con el aumento de la fama y el acceso a la información de estas personas, es cada vez más importante contar con medidas de seguridad adecuadas para proteger su integridad física y su privacidad.**

**La Ley 5/2014, de Seguridad Privada: Define el papel de las empresas de seguridad privada en eventos masivos, garantizando su colaboración con organismos públicos.**

Además de la Ley de Seguridad Privada, existen otras normativas específicas que se aplican a la protección de personas VIP y famosas. Por ejemplo, la Ley de Protección de Datos de Carácter Personal establece las medidas de seguridad que deben adoptarse para garantizar la confidencialidad y privacidad de la información personal de estas personas. Otra normativa relevante en este ámbito es la Ley de Prevención de Riesgos Laborales, que establece las medidas de seguridad y salud en el trabajo que deben cumplirse para proteger a los trabajadores, incluyendo a los profesionales de la seguridad privada encargados de la protección de personas VIP y famosas. Como escritora apasionada del deporte y la seguridad, he observado con fascinación cómo el periodismo deportivo ha mutado en una era donde lo tradicional y lo digital convergen para crear una narrativa más rica, accesible y dinámica.

Este artículo nos sumerge en el Renacimiento de la narrativa deportiva, donde la velocidad de los monoplazas se encuentra con la velocidad de la información.

La Fórmula 1 ha sido transformada por la convergencia de medios tradicionales con plataformas digitales. Esta revolución ha democratizado la información, pero también ha generado retos en seguridad y veracidad. La interacción constante con los aficionados y el uso de datos en tiempo real ha impulsado un nuevo periodismo deportivo, en que la precisión y transparencia son esenciales para su evolución. Se ha convertido en una tarea titánica para los medios y los propios redefiniendo el periodismo deportivo.

La seguridad privada en eventos masivos implica en la planificación de seguridad mucho antes de que un evento se lleve a cabo. La Seguridad en eventos deportivos requiere un enfoque holístico que integre prevención, tecnología y coordinación. Las normativas existentes, complementadas con buenas prácticas y recursos adecuados, permiten garantizar entornos seguros y satisfactorios para todos los participantes.



La Ley 5/2014, de Seguridad Privada: Define el rol de las empresas de seguridad privada en eventos masivos, garantizando su colaboración con organismos públicos. La principal misión de las Fuerzas y Cuerpos de Seguridad es garantizar un nivel óptimo de seguridad ciudadana y orden público durante la celebración de los eventos de formula 1.

El Campeonato Mundial de Pilotos y Constructores de Fórmula 1, es la competición de automovilismo internacional más popular y prestigiosa. La Federación Internacional del Automóvil (FIA), se encarga de la dirección y su máxima representación. El plan de seguridad de un evento deportivo es fundamental para garantizar la seguridad de los participantes, los voluntarios, "los comisarios", el público y todo el personal involucrado y para ello debe incluir todos los elementos necesarios. Este plan debe contar con medidas preventivas y medidas reactivas (para actuar de manera efectiva si ocurren emergencias) y cumplir con los requisitos de un Plan de Autoprotección y un-Plan MOT (Mantenimiento del Orden y la Tranquilidad), que son esencia para la gestión del evento. La aplicación inquebrantable de los protocolos de seguridad coordinados es lo que realmente garantiza el éxito y la integridad en cada evento.

Durante la celebración de este, las empresas del sector suelen prestar los siguientes servicios:

- Control de acceso: Este servicio es de vital importancia para evitar que personas no autorizadas accedan al recinto. Protegiendo, asegurando la custodia de los objetos que esté prohibido portar.
- Monitoreo del recinto: Mediante el sistema de videovigilancia (CCTV) Detección de explosivos: Algunas empresas de seguridad privada poseen unidades caninas especializadas en la detección de explosivos.
- Rondas de vigilancia. Asimismo, los elementos de seguridad privada pueden vigilar zonas estratégicas de un recinto para prevenir situaciones de riesgo
- Protección de invitados y personalidades: Del mismo modo, las empresas de seguridad privada ofrecen servicios de escolta para proteger a invitados VIP y personalidades durante la celebración de un evento.



**La Fórmula 1 es la categoría máxima del automovilismo deportivo a nivel mundial, considerada la cúspide del deporte del motor. Se caracteriza por ser una competición de velocidad y destreza técnica en la que pilotos y equipos compiten en una serie de carreras a lo largo de una temporada, utilizando monoplazas especialmente diseñados y contruidos para alcanzar velocidades extremadamente altas en circuitos de carreras de todo el mundo.**

La Federación Internacional del Automóvil (FIA). Uno de los objetivos principales de la FIA a la hora de establecer las normas de seguridad es garantizar la seguridad de todos los competidores, espectadores, y trabajadores relacionados con la Fórmula 1. La FIA realiza campañas de seguridad en las carreteras por todo el mundo, y no hay mayor forma de dar ejemplo que garantizando la máxima seguridad en las categorías que gobierna: Fórmula 3, Fórmula 4, Fórmula E, mundial de Rallies entre muchas otras, sin dejarnos las competiciones de Karting de las que salen los futuros pilotos. Todos los elementos de seguridad y vehículos, así como las pistas y protecciones en ellas deben cumplir con la normativa de la FIA.

Existe una normativa de seguridad común para todas las competiciones, como la homologación de los cascos. Pero la mayoría de las normas de seguridad son específicas para cada categoría, y no os podéis ni imaginar la cantidad de normas de seguridad que tienen que cumplir en Fórmula 1. Empezando por la homologación del chasis de cada equipo, lo cual conlleva superar las famosas pruebas de impacto o «crash test», y continuando por los elementos de seguridad que llevan los monoplazas en Fórmula 1

**El cumplimiento de normas estrictas establecidas por la FIA. Estos reglamentos aseguran tanto la seguridad de los pilotos como la igualdad de oportunidades entre los equipos en términos de tecnología y capacidades del coche. Los reglamentos técnicos y deportivos se actualizan frecuentemente para asegurar que el deporte se mantenga competitivo y seguro, lo que obliga a los equipos a innovar constantemente dentro de los límites establecidos**

- Coche de seguridad: Un coche de seguridad está en pista, y todos los pilotos deben reducir la velocidad y alinearse detrás del coche. Está prohibido adelantar.
- Coche de seguridad virtual (VSC) desplegado: Todos los pilotos deben reducir la velocidad a un delta de tiempo específico para mantener una velocidad segura, sin adelantamientos.
- Fin del coche de seguridad virtual (VSC): Esta condición indica el momento en el que el coche de seguridad virtual se retira y se reanuda la carrera con normalidad

La principal misión de las Fuerzas y Cuerpos de Seguridad es garantizar un nivel óptimo de seguridad ciudadana y orden público durante la celebración. También cubrir las exigencias de protección de las personas y bienes, garantizando los derechos fundamentales, que radican en diferentes textos legislativos de ámbito nacional e internacional, y que se citan algunos a continuación:

La de Declaración Universal de los Derechos Humanos de 1948:

- Artículo 3. Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona.
  - Artículo 104.1. Las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.
  - Artículo 149.1. 29.ª El Estado tiene competencia exclusiva sobre las siguientes materias: Seguridad pública, sin perjuicio de la posibilidad de creación de policías por las Comunidades Autónomas en la forma que se establezca en los respectivos Estatutos en el marco de lo que disponga una ley orgánica.
  - Artículo 1.4. El mantenimiento de la seguridad pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad.
  - Artículo 11.1. Las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: a) Auxiliar y proteger a las personas y asegurar la conservación y custodia de los bienes que se encuentren en situación de peligro por cualquier causa. b) Velar por la protección y seguridad de altas personalidades.
1. Establecimiento de un dispositivo operativo en el que se incluyan otros servicios de emergencia.
  2. Garantizar la información, coordinación y dirección de todos los servicios de emergencia involucrados.
  3. Garantizar la protección exterior de las instalaciones sensibles y lugares de aglomeración ciudadana, que puedan ser objetivo de atentado terrorista.
  4. Mantenimiento y si fuera necesario restablecimiento de la seguridad ciudadana y del orden público tanto en el circuito y como en la localidad.
  5. Prevención y represión de la comisión de posibles hechos delictivos en la demarcación territorial y en el circuito.
  6. Realización de controles en las principales vías circulación y lugares públicos estratégicos.



***Algunos ciudadanos consideran que este evento no compensa los problemas derivados del ruido y del tráfico ni se muestra favorable ante el hecho de que este acontecimiento esté pensado para el disfrute de la población. Tampoco muestra una tendencia positiva ante aspectos como la creación de empleo, la mejora de la seguridad o el incremento del orgullo de vivir en la ciudad como consecuencia de la celebración de este acontecimiento deportivo***

Efectos nocivos; Físicos/medioambiental:

- Daño ecológico.
- Cambios en los procesos naturales.
- Contaminación arquitectónica.
- Destrucción del patrimonio.
- Superpoblación.
- Inutilización de las instalaciones.

El Consejo Superior de Deportes y todas las entidades deportivas tienen la responsabilidad de velar por la sostenibilidad y la eficiencia energética de todas las instalaciones e infraestructuras deportivas del país, atendiendo aspectos relacionados con:

- El cumplimiento de los requisitos y normativas medioambientales vigentes.
- La promoción del ahorro energético y del agua durante los eventos deportivos.
- Intentar mitigar la huella de carbono personal, en la medida de lo posible.

En cambio, otros aficionados, sí que muestran una tendencia favorable en aspectos como los beneficios económicos, la mejora de la imagen y de las infraestructuras de la zona, el incremento del prestigio deportivo y la apertura al mundo de la ciudad como consecuencia de su celebración.

“Como todo en esta vida, existe el ying y el yang” ¿Quién no ha vibrado desde su “Fan zone”o zona de confort de su deporte favorito? Personalmente recuerdo con gran satisfacción a el piloto, Fernando Alonso. El primer año de Alonso como piloto titular llegaría en 2003, temporada en la que consiguió su primera victoria. El piloto asturiano ha dejado instantáneas que también se han quedado marcadas en las retinas de los aficionados del mundo de la Fórmula 1

“Para robustecer la seguridad en nuestras operaciones; fomentemos una cultura de prevención, donde la anticipación de riesgos y la comunicación proactiva sean la norma ineludible”

**Elena Parte 2025**



# PILOTOS DE UAS EN SEGURIDAD PRIVADA: OPORTUNIDAD TECNOLÓGICA Y RIESGOS CONTRACTUALES

## Introducción: Seguridad privada en la era de los drones

La seguridad privada vive una profunda transformación impulsada por la incorporación de nuevas tecnologías. Entre ellas, los Sistemas de Aeronaves no Tripuladas (UAS), más conocidos como drones, se han consolidado como herramientas versátiles, eficaces y de alta demanda, tanto para vigilancia perimetral como para operaciones en entornos críticos o de difícil acceso.

Esta evolución, sin embargo, no ha venido exenta de desajustes normativos, incertidumbres laborales y, en algunos casos, prácticas abusivas que afectan de lleno a los vigilantes de seguridad y a los responsables de los servicios.

La formación específica como piloto UAS se ha convertido en un terreno fértil para la desinformación y los desequilibrios contractuales. Este artículo tiene como objetivo arrojar luz sobre el marco legal, los derechos de los profesionales, los deberes de las empresas y las alternativas de formación transparente, profesional y ética, como la que ofrece RITRAC International, referente en el sector.

### 1. UAS y Seguridad Privada: dos marcos normativos complementarios

1.1. Legislación aeronáutica: competencias y certificación  
Desde el 1 de enero de 2021, el uso de drones en la Unión Europea está regulado por el Reglamento de Ejecución (UE) 2019/947, aplicable en todos los Estados miembros. En España, su aplicación y supervisión corresponde a la Agencia Estatal de Seguridad Aérea (AESA)

Las operaciones con UAS se clasifican en tres categorías principales:

- Categoría abierta (riesgo bajo): Subcategorías A1, A2 y A3.
- Categoría específica (riesgo medio): Operaciones más complejas que requieren autorización previa.
- Categoría certificada (riesgo alto): Por ejemplo, vuelos sobre multitudes o transporte de mercancías peligrosas.

El operador (empresa o profesional autónomo) debe estar registrado en AESA, y el piloto debe poseer una certificación teórica y práctica, expedida por una entidad reconocida. Esta formación puede obtenerse en centros privados acreditados o a través de plataformas autorizadas

#### 1.2. Legislación de seguridad privada: requisitos sectoriales

La Ley 5/2014 de Seguridad Privada y sus desarrollos posteriores (especialmente la Orden INT/318/2011) establecen que los vigilantes que empleen medios tecnológicos especiales —como los UAS— deben recibir formación específica, homologada por el Ministerio del Interior, a través de centros autorizados. Por tanto, no basta con disponer del certificado de piloto UAS: para operar drones en el marco de un servicio de vigilancia privada, es obligatorio:

- Estar habilitado como vigilante de seguridad.
- Contar con formación específica homologada en UAS para seguridad privada.
- Operar bajo la cobertura legal adecuada (registro de operador, seguro, autorización si aplica, etc.).



### 2. Problemas detectados: precios inflados y cláusulas contractuales abusivas

2.1. Formación interna con costes desproporcionados  
Numerosos profesionales del sector denuncian que sus empresas les ofrecen —o directamente les imponen— cursos de formación UAS a precios muy superiores a los del mercado. Mientras que la certificación A1/A3 o A2 puede obtenerse por menos de 250 € en entidades acreditadas como RITRAC International, algunas empresas facturan internamente más de 1.200 € por trabajador, sin detallar qué incluye el curso ni si cuenta con reconocimiento oficial. Esta falta de transparencia es especialmente grave cuando:

- No se identifica qué entidad imparte la formación.
- No se informa de si el curso está homologado por AESA o por el Ministerio del Interior.
- Se oculta al trabajador la posibilidad de formarse externamente en condiciones más ventajosas

2.2. Cláusulas de permanencia laboral  
A estos sobrecostes se suman las denominadas cláusulas de permanencia: compromisos contractuales que obligan al vigilante a mantenerse en la empresa durante un periodo de hasta tres años si acepta la formación interna, bajo la amenaza de tener que abonar el curso si causa baja.

Estas cláusulas, cuando no están debidamente justificadas ni firmadas voluntariamente, pueden considerarse nulas o abusivas, generando situaciones de inseguridad jurídica y desprotección profesional.



### 3. Marco jurídico: ¿Qué dice realmente la ley?

#### 3.1. Estatuto de los Trabajadores

El artículo 21.4 del Estatuto de los Trabajadores permite la existencia de acuerdos de permanencia solo si concurren tres requisitos simultáneos:

- 1. Que la empresa haya sufragado una formación especializada.
- 2. Que exista una mejora profesional y laboral real derivada de esa formación.
- 3. Que se haya firmado un acuerdo individualizado entre empresa y trabajador.

Si alguno de estos requisitos no se cumple —por ejemplo, si el trabajador paga el curso o si no existe un acuerdo voluntario firmado— la permanencia no es válida legalmente

3.2. Formación externa: totalmente legítima Todo profesional habilitado como vigilante tiene derecho a formarse por su cuenta en entidades externas. Centros como RITRAC International, acreditado por AESA y con experiencia específica en el sector de la seguridad privada, permiten a cualquier profesional obtener:

- Certificaciones oficiales en categoría abierta o específica.
- Formación práctica adaptada a escenarios reales de vigilancia.
- Programas homologados por el Ministerio del Interior para habilitación como operador UAS en seguridad.

**4. RITRAC International:** Formación con garantías para la seguridad privada. En este contexto de opacidad y abusos, es imprescindible destacar a RITRAC International como un modelo de formación profesional, ética y transparente. Su propuesta para vigilantes y responsables de seguridad incluye:

- Cursos adaptados al marco legal vigente, tanto aeronáutico como de seguridad privada.
- Formación teórica y práctica en UAS, impartida por instructores certificados.
- Integración con la formación específica exigida por el Ministerio del Interior para operar drones en servicios de seguridad
- Precios ajustados al mercado y sin cláusulas contractuales abusivas.
- Asesoramiento a empresas para la correcta implementación de UAS en sus servicios

**Conclusión:** Tecnología, sí. Abusos, no El uso de UAS representa un paso adelante en la profesionalización de la seguridad privada. Sin embargo, no puede ir acompañado de una precarización formativa ni de tácticas de retención laboral ilegítimas. La innovación debe ir de la mano de la ética y el cumplimiento normativo. Entidades como RITRAC International demuestran que es posible avanzar hacia un modelo donde tecnología y derechos laborales convivan, ofreciendo a los vigilantes y a los responsables de seguridad las herramientas necesarias para operar con seguridad jurídica, técnica y profesional. La formación no debe ser una trampa, sino una puerta de entrada a un futuro más digno, eficaz y seguro

### Carlos Miguel Ortiz

Delegado Regional

Comunidad Autónoma de Madrid

Piloto remoto UAS certificado EASA

Instructor-examinador UAS certificado RITRAC

Ritrac International UAS professional services worldwide RUPSW



Correo electrónico: [cmiguel@ritrac.eu](mailto:cmiguel@ritrac.eu)

Móvil/Whatsapp: +34 685040875

Sitio web: <https://ritrac.eu>

Plataforma formación: <https://remotepilot.online>

Reuniones telemáticas: <http://webex.ritrac.eu>

Gracias a su enfoque integral, RITRAC International se ha consolidado como un aliado estratégico del sector, facilitando la profesionalización sin sacrificar los derechos laborales

### 5. Recomendaciones y hoja de ruta Para profesionales:

- Consulta directamente con AESA qué centros están autorizados.
- Si vas a firmar una cláusula de permanencia, exige una copia por escrito y consulta con asesoría jurídica.
- Evita formaciones internas si no se te facilita toda la información por adelantado.
- Explora opciones externas como RITRAC International, donde puedes certificarte de forma independiente y profesional.

#### Para empresas:

- Selecciona centros formativos homologados y transparentes.
- No impongas condiciones de permanencia abusivas: Genera compromiso a través de la confianza y el desarrollo profesional.
- Apuesta por formaciones que incluyan no solo conocimientos técnicos, sino también el enfoque operativo y legal específico de la seguridad privada.
- Considera a RITRAC International como proveedor formativo de confianza, tanto por su solvencia como por su adecuación normativa.

# LA PROTECCIÓN DE DATOS EN LA INVESTIGACIÓN DEL DETECTIVE PRIVADO

**SIMONA NEDKOVA VESKOVA**

Artículo sobre la importancia de proteger los datos que se manejan en el ejercicio de la profesión no solo de detectives privados, sino todo aquel que trate con información sensible en seguridad privada

**DETECTIVE PRIVADO,  
DOCENTE PARA LAS HABILITACIONES DE SEGURIDAD PRIVADA,  
CONCEJALÍA DE SEGURIDAD CIUDADANA:  
UNIDAD DE GESTIÓN DE LA POLICÍA LOCAL DE FUENGIROL**

Las investigaciones de los detectives privados pueden realizarse en diversos ámbitos: laboral (competencias desleales, absentismos injustificados), personal (procedimientos judiciales en separaciones, custodias), empresarial (fraudes, robos, actividades sospechosas), localización de personas desaparecidas, colaboración con abogados y Fuerzas y Cuerpos de Seguridad del Estado, etcétera. Dichas labores se regulan en España por la Ley de Seguridad Privada (Ley 5/2014) y el Real Decreto 2364/1994. Es una profesión altamente regulada, y así se consigue contribuir a la resolución de conflictos en armonía con la seguridad pública.

Además de las pruebas recopiladas, el trabajo del detective es plasmado en un informe que puede ser ratificado en juicios. Las investigaciones que realizan los detectives privados incluyen todo tipo de metodologías que han evolucionado con el tiempo, al igual que las pruebas que se recopilan. Es por ello que radica de gran importancia la protección de datos, la ciberseguridad y la seguridad de los dispositivos físicos que la almacenan (cosa que muchas veces se pasa por alto en los planes de seguridad de muchas empresas).

Los detectives incluyen en los contratos con los clientes la política de protección de datos, entre otras cuestiones, sin embargo, no están establecidas pautas comunes de actuación para proteger los diferentes tipos de información, y eso es lo que falta por hacer en muchas profesiones. Por ello, reside en manos de cada profesional el cuidado minucioso de la seguridad de la información con la que trabaja. El entendimiento de los peligros que acarrearán las nuevas tecnologías, junto a las ventajas que nos ofrecen, y que tan abiertamente hemos aceptado, es una parte más para garantizar su disfrute, y garantizar un servicio adecuado como investigadores privados



En las investigaciones se utilizan tecnologías con sistemas de vigilancia avanzados y grabaciones en alta definición, almacenamiento de los mismos, análisis de datos recopilados y OSINT, entre otros. La información obtenida es, por supuesto, confidencial. Es por esas razones que la concienciación es tan importante, no solo a nivel individual sino a nivel profesional, y conocer hasta qué punto la prevención es la mejor precursora de la seguridad en nuestra sociedad.



**ANOMIS**  
Detective Privado



**Servicios de Peritaje y Consultoría en Andalucía y Ceuta,  
España.**

**Due Diligence - Debida Diligencia, a Nivel Nacional como  
Internacional.**

**✓ Nuestro Compromiso, es Proporcionar Asesoramiento  
Experto en Peritajes, Consultoría y Due Diligence (Debida  
Diligencia),  
para Apoyar a nuestros Clientes en el Ambito Legal y Técnico.**

**✓ Para ofrecer el Máximo Servicio a Nuestro Clientes, y por el  
Valor que Ofrece el Servicio Consultora de Formación e  
Implementación de Arquitecturas y Proyectos de Seguridad.**

**Colaboramos con MR-CONSULTING.**



**Asesoramiento Técnico  
Especializado, para Situaciones  
legales y Técnicas:  
En el Ámbito de la:**  
Seguridad Privada, Balística Forense.  
Ciberseguridad, Inteligencia y  
Geopolítica.  
Seguros de Embarcaciones Recreo.  
Grafología, Documentoscopia,  
Grafopsicopatología Criminal y  
Forense.  
Due Diligence (Debida Diligencia).

**[https://www.oterotrillogabinetepericial-  
andaluciaceuta.es/](https://www.oterotrillogabinetepericial-andaluciaceuta.es/)**

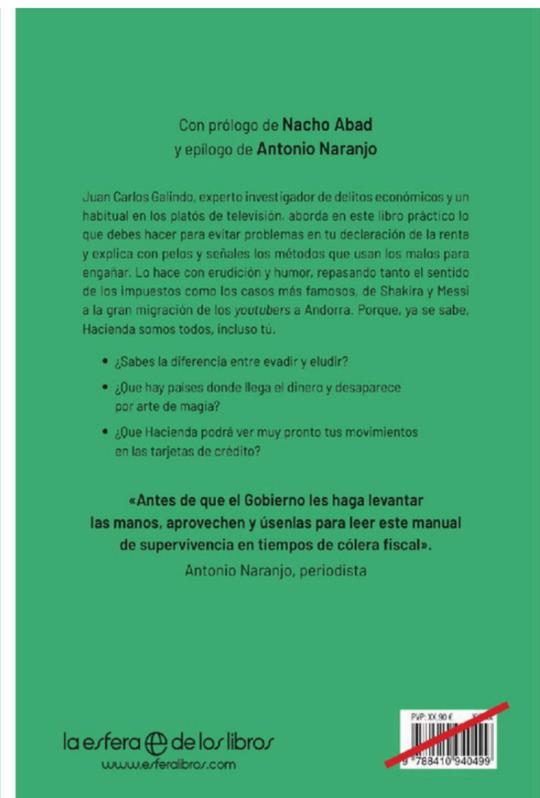
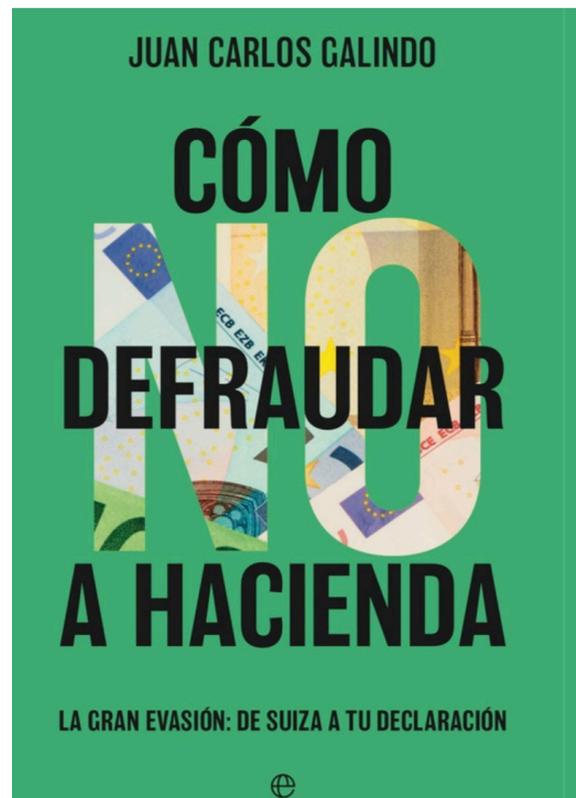
# AGENDA

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

## RADIO

**TODOS LOS LUNES! ES NOCHE DE INFORME GALINDO, DESDE LAS 22.00 Y HASTA LAS 23.00H, DA COMIENZO UNA NUEVA EDICIÓN DE INFORME GALINDO EN RADIO INTERECONOMIA DESDE EL ESTUDIO 1 DE RADIO INTERECONOMÍA VALENCIA PARA TODA ESPAÑA.**



**EL CANAL DEL CORONEL**



**LOS CONSEJOS DE CIBERSEGURIDAD DE ADOLFO GELDER.**

en: [www.linkedin.com/in/adolfo-gelder-b2327bb4/](https://www.linkedin.com/in/adolfo-gelder-b2327bb4/)

**WWW.ALBERTORAY.COM**

El blog de Alberto Ray, donde encontrarás todo lo relacionado con: #amenazas, #gerencia, #seguridad y #complejidad





# Metrorisk

# Proyecto Asociativo

[www.metrorisk.es](http://www.metrorisk.es)