

# EDITORIAL MR

OCTUBRE

AÑO  
2025



ISSN 3045-7629

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz  
Francisco Javier Gonzales Fuentes  
José Ignacio Olmos  
Gregorio Duro  
Mercedes Escudero Carmona  
Antonio Cozano Fernández  
Emilio Piñeiro  
Rosa Fernández  
Carlos Serrano  
Abraham Santana  
Alina Rubio  
Elena de la Parte  
Carlos Miguel Ortiz  
Jonatthan Hermida Sosa  
Carlos E Pérez Barrios

@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 Piñeiro

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.

# LA SEGURIDAD COMO LENGUAJE COMÚN: UNA NECESIDAD DE COMUNICACIÓN SOCIAL

**Fran Medina Cruz**  
Director de MetroRisk

La seguridad, esa profesión que muchos ejercemos con entrega y de la que constantemente aprendemos, no puede permanecer en la sombra. Es una disciplina que se nutre de la experiencia, de la técnica y del compromiso con las personas, y que sin embargo aún carece de la presencia mediática y social que merece. En un mundo donde la comunicación atraviesa todos los ámbitos, televisión, prensa escrita e internet, resulta imprescindible que la seguridad encuentre su espacio.

No se trata únicamente de transmitir incidentes o hechos aislados, sino de generar cultura de seguridad. La ciudadanía necesita comprender que vivir seguros no es un privilegio, sino un derecho, y que para alcanzarlo es necesario contar con profesionales que trabajen con rigor y responsabilidad. La seguridad debe calar en todos los niveles de la sociedad, desde el hogar hasta los espacios públicos, desde la empresa privada hasta las instituciones gubernamentales.

Por ello, la exigencia de un ejercicio profesional y cualificado no puede ser negociable. La seguridad improvisada o superficial no aporta valor; por el contrario, puede agravar los riesgos. Es fundamental que el sector proyecte hacia la sociedad una imagen sólida, transparente y accesible, que permita a todos entender su papel como instrumento básico para la convivencia y el desarrollo.

La seguridad privada, en particular, debe dar un paso al frente y abrirse a la ciudadanía, a los poderes públicos y al tejido empresarial. No como un actor secundario, sino como un aliado estratégico en la prevención, la resiliencia y la protección integral. Comunicar con claridad lo que hacemos, explicar cómo la seguridad se integra en la vida cotidiana y demostrar con hechos su valor añadido son los pilares de este reto.

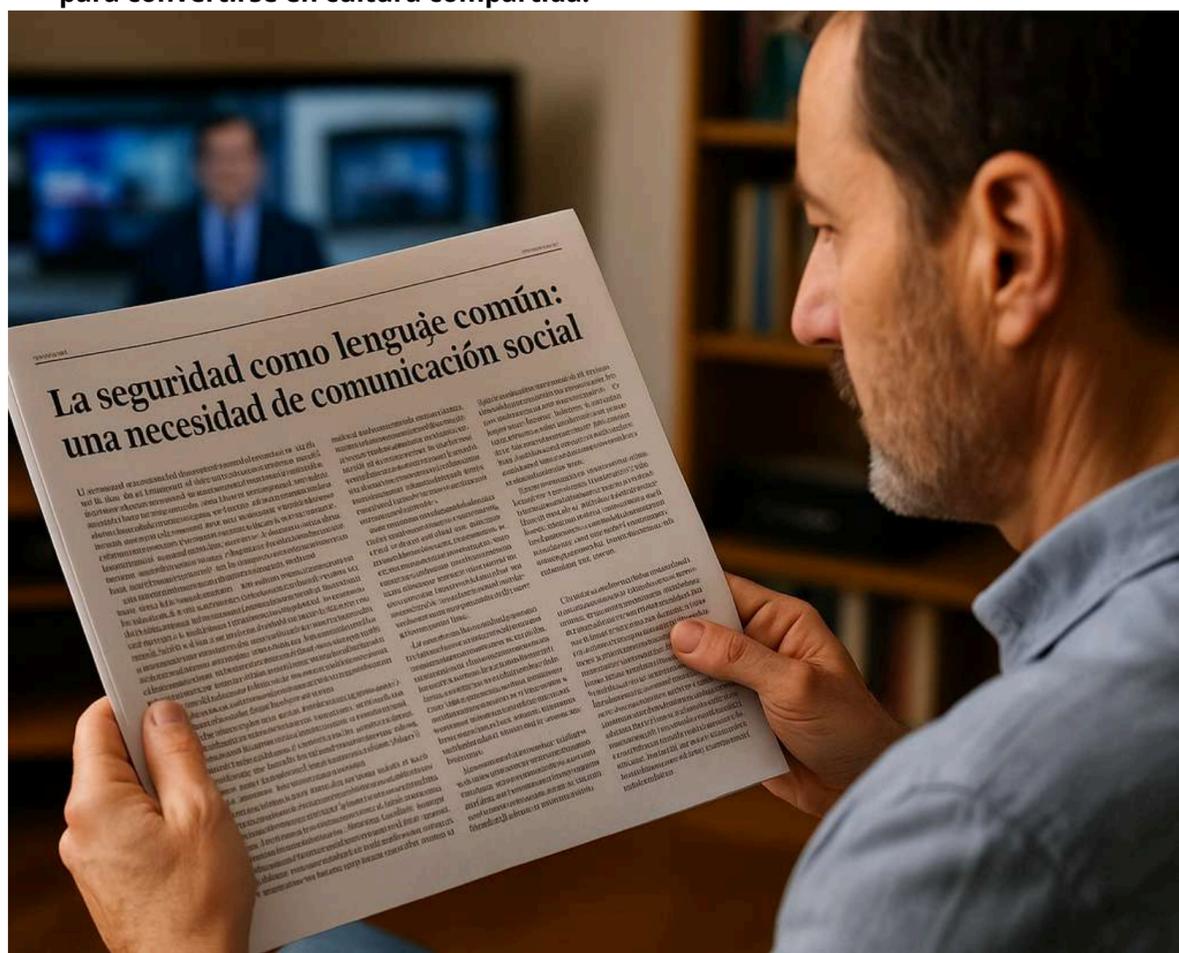
En definitiva, la seguridad debe revelarse como lo que verdaderamente es: un servicio esencial, una profesión noble y un motor de confianza social. Solo cuando logremos situarla en el centro del discurso público, la seguridad dejará de ser percibida como un "recurso reactivo" y pasará a ser reconocida como el elemento preventivo y estructural que sostiene la calidad de vida en nuestra sociedad.



La seguridad es una profesión de enorme valor social, pero aún insuficientemente reconocida en el espacio público. No basta con que sea ejercida de forma técnica y rigurosa: es necesario que su importancia se comunique con claridad a todos los niveles de la sociedad.

Televisión, prensa e internet deben convertirse en altavoces de una realidad esencial: vivir seguros es un derecho colectivo. Para ello, la seguridad debe abrirse, mostrarse y proyectarse como lo que es: un servicio básico, un instrumento que sostiene la convivencia y la confianza ciudadana.

**La profesionalización es aquí una exigencia, no una opción. Solo con especialistas cualificados se pueden prevenir riesgos y dar respuestas eficaces. La seguridad privada, en particular, está llamada a ser un aliado estratégico de las instituciones públicas y privadas. Hacer visible su valor es el reto, porque solo así la seguridad dejará de ser invisible para convertirse en cultura compartida.**



# FRAN MEDINA CRUZ

CONSULTOR Y ASESOR EN SEGURIDAD POR  
DISEÑO - ESPECIALISTA CPTED Y BREEAM

La diferencia entre instalar  
seguridad y diseñarla para vivir *seguro*



Un informe de seguridad MRConsulting no se limita a recomendar cámaras o alarmas; es un análisis técnico y personalizado que vlia la arquitectura, el entorno y el uso de la vivienda para prevenir el delito antes de que ocurra; incluye soluciones integradas en el diseño, siguiendo los mas altos estandares internacionales, como CPTED y BREEAM, para garantizar entornos seguros, funcionales y sostenibles.

## MRCONSULTING

SEGURIDAD INTELIGENTE PARA VIVIENDAS DE ALTO STANDING

# EL DIRECTOR DE SEGURIDAD: REALIDAD ACTUAL, NUEVOS HORIZONTES Y RETOS

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Francisco Javier Gonzales Fuentes**  
Presidente de ADISPO y FIBSEM

La figura del Director de Seguridad se encuentra en plena transformación. Tradicionalmente asociado a la gestión de medios humanos y tecnológicos orientados a la protección de instalaciones, hoy su papel va mucho más allá: integra la estrategia corporativa, aporta valor a la continuidad de negocio y se convierte en un puente imprescindible entre el ámbito público y privado.



## INTELFORENSIC G&F SOLUCIONES

LA EVIDENCIA, HABLA  
Y MUESTRA EL CAMINO...



### SERVICIOS PERICIALES ESPECIALIZADOS

- Informática Forense y Análisis Digital
- Periciales en Seguridad y PRL
- Investigación de Incendios
- Asesoría Criminalista y Criminal Profiling
- Análisis de Falsedad Documental
- Servicios de Mediación Técnica y Legal
- Periciales Judiciales y Extrajudiciales Personalizadas

CONSULTORÍA FORENSE INTEGRAL PARA EMPRESAS,  
ABOGADOS Y PARTICULARES.

CONTÁCTANOS Y PERMITE QUE LA EVIDENCIA HALE!

Tifo. de contacto:  
+(34) 911765 366

info@forensicgf.com  
L - V: 8.00am - 18.00 mm

FIBSEM presente en la I Convención Hemisférica Interamericana de Seguridad y Defensa 🌍👏

👏 Con orgullo destacamos la participación de nuestra Junta Directiva:

👤 [Francisco Javier González Fuentes](#), Presidente de FIBSEM y Asociación de directores de seguridad ADISPO

👤 [Fernando Montoya Cerio](#), Presidente de AIMCSE Asociación Seguridad y Emerg. y Vicepresidente de FIBSEM

👤 [Luis Miguel Hurtado Zabaleta](#), Secretario General de ADISPO y responsable del Órgano de Dirección de Aimcse

📌 La Convención fue un verdadero éxito, resaltando la importancia de los grupos de trabajo y las valiosas conclusiones presentadas.

🏆 FIBSEM fue reconocida con un diploma en la clausura, presidida por el Director del CESEDEN

🙏 Agradecimiento especial a ADESyD, ASOCID Ecuador y el Colegio Interamericano de Defensa por su impecable organización.

🌟 ¡Enhorabuena por el gran trabajo en esta primera edición que marca un hito para la seguridad y defensa hemisférica!





# Seguridad y Prevención de Riesgos Laborales: una relación inseparable en el marco del cumplimiento normativo y la responsabilidad penal

**La seguridad y la prevención de riesgos laborales (PRL) constituyen dos pilares fundamentales en la protección de personas, bienes y organizaciones. En el ámbito empresarial, ambos conceptos han dejado de ser elementos opcionales o meramente formales, para convertirse en exigencias legales y éticas que impactan directamente en la continuidad del negocio, la reputación corporativa y, cada vez más, en la responsabilidad penal de las personas jurídicas en España.**

## **Seguridad y Prevención: un binomio necesario**

Aunque tradicionalmente la seguridad corporativa y la prevención de riesgos laborales se han concebido como disciplinas distintas, la realidad práctica y normativa demuestra que están condenadas a entenderse: La seguridad corporativa protege frente a amenazas externas e internas: intrusiones, sabotajes, fraudes, terrorismo, violencia laboral, entre otras. La prevención de riesgos laborales busca eliminar o reducir los riesgos derivados de la actividad productiva: accidentes, enfermedades profesionales y daños a la salud de los trabajadores. Ambas comparten un objetivo común: preservar la integridad de las personas y el normal desarrollo de la organización. Cuando trabajan de forma coordinada, no solo se reducen incidentes, sino que se optimizan recursos y se fortalece la cultura de cumplimiento.

## **Cumplimiento normativo y exigencias legales**

En España, la Ley de Prevención de Riesgos Laborales (Ley 31/1995) establece la obligación de las empresas de garantizar la seguridad y salud de los trabajadores. A su vez, otras normativas sectoriales (seguridad privada, infraestructuras críticas, seguridad industrial, etc.) imponen obligaciones complementarias. En el marco del compliance, las organizaciones deben integrar sistemas de gestión que aseguren el cumplimiento de todas estas normas. La ISO 45001 (seguridad y salud en el trabajo) y la ISO 37301 (compliance) constituyen herramientas internacionales que facilitan esta integración. No se trata solo de cumplir por obligación, sino de entender que la prevención y la seguridad son parte del valor corporativo y de la sostenibilidad empresarial.

**Francisco Javier Gonzales Fuentes**  
**Presidente de ADISPO y FIBSEM**

## **La responsabilidad penal de las personas jurídicas**

Desde la reforma del Código Penal (LO 5/2010 y LO 1/2015), las personas jurídicas en España pueden ser penalmente responsables por delitos cometidos en el seno de la organización. Entre ellos destacan: Delitos contra la seguridad de los trabajadores (art. 316 CP), cuando se infringen las normas de prevención y se pone en peligro grave la vida o salud de los empleados. Delitos de omisión de medidas de seguridad, que pueden acarrear sanciones económicas, inhabilitación para contratar con la administración o incluso la disolución de la empresa. La jurisprudencia ha dejado claro que no basta con delegar responsabilidades en un servicio de prevención ajeno o en un departamento de seguridad. Es la alta dirección la que debe garantizar una cultura de cumplimiento, implementar protocolos efectivos y supervisar su aplicación.

## **Convergencia estratégica**

En este escenario, la seguridad y la prevención de riesgos laborales no pueden caminar por senderos separados. La integración de ambas disciplinas permite: Anticiparse a riesgos emergentes (ciberseguridad laboral, violencia de terceros, emergencias complejas). Dar coherencia a los planes de autoprotección, continuidad de negocio y planes de prevención. Responder de manera coordinada ante incidentes con impacto legal, laboral y reputacional. El director de seguridad y el responsable de prevención deben colaborar estrechamente, alineando protocolos, intercambiando información y participando juntos en los comités de cumplimiento.

## **Conclusión**

La seguridad y la prevención de riesgos laborales son dos caras de la misma moneda. Su correcta integración garantiza el cumplimiento normativo, protege a los trabajadores, refuerza la resiliencia organizacional y, lo más importante, evita responsabilidades penales que pueden comprometer la viabilidad de la empresa. En un contexto donde la responsabilidad penal de las personas jurídicas es una realidad tangible, no se trata solo de cumplir la ley, sino de demostrar con hechos que la empresa apuesta por una cultura preventiva y de seguridad integral.

# LA ASOCIACIÓN ESPAÑOLA DE AUDITORES DE SEGURIDAD COGE IMPULSO

**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.**



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



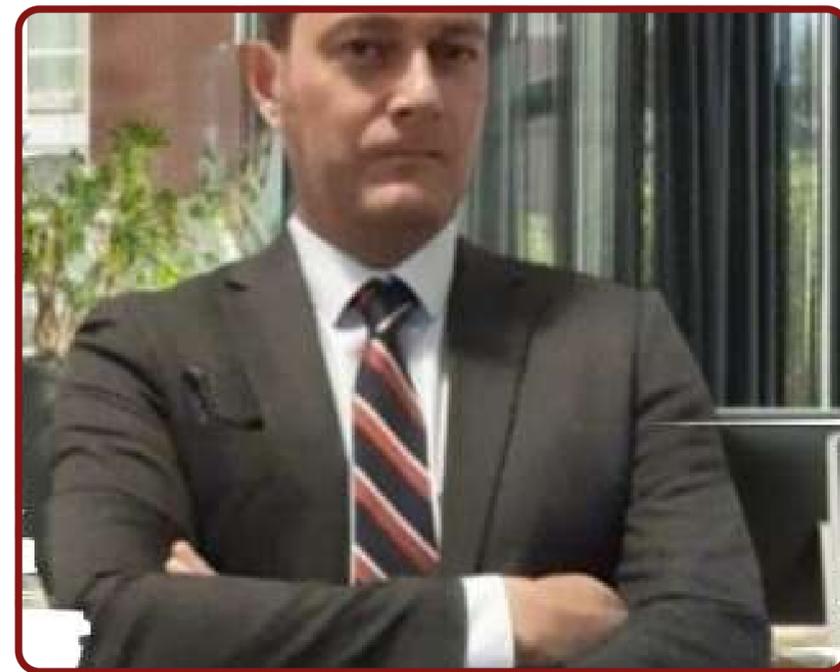
**Gregorio Duro**  
Técnico en licitaciones y Proyectos

### INTRODUCCIÓN AL ANÁLISIS DE RIESGO OPERACIONAL

En el artículo de este mes, me gustaría abordar una introducción teórica en el entorno del denominado riesgo operacional el cual se ha convertido en un componente clave dentro de la gestión integral de riesgos de las organizaciones actuales. Este tipo de riesgo se refiere a la posibilidad de pérdidas derivadas de procesos internos ineficientes, fallos tecnológicos, errores humanos o eventos externos que otros afecten el normal funcionamiento de la empresa. A diferencia de riesgos más fácilmente cuantificables, como los financieros o de mercado, el riesgo operacional requiere una aproximación integral que combine análisis, prevención y mitigación. **Comprender su naturaleza, identificar sus fuentes y establecer mecanismos de control efectivos no solo protege los recursos de la organización, sino que también fortalece su resiliencia y sostenibilidad en un entorno cada vez más dinámico y competitivo.**

El riesgo operacional cobra especial relevancia cuando se analiza en el entorno de los riesgos físicos, ya que estos representan amenazas tangibles capaces de interrumpir la continuidad de las operaciones y comprometer tanto la seguridad de los activos como la integridad de las personas; en este contexto, incidentes como incendios, inundaciones, explosiones, fallas en la infraestructura o accidentes industriales no solo generan impactos directos en los recursos materiales, sino que también afectan la capacidad de la organización para mantener su funcionamiento normal, incrementando costos, retrasando proyectos y debilitando su reputación, por lo que resulta fundamental incorporar el análisis de riesgos físicos dentro del marco del riesgo operacional, utilizando metodologías que permitan identificar vulnerabilidades, evaluar probabilidades de ocurrencia y cuantificar consecuencias, de modo que se logren diseñar estrategias preventivas y planes de respuesta que fortalezcan la resiliencia organizacional y aseguren la continuidad del negocio frente a eventos de naturaleza física que, aunque a menudo inevitables, pueden ser gestionados y mitigados eficazmente.

En una primera fase, el análisis del riesgo operacional asociado a riesgos físicos debe centrarse en la identificación sistemática y la evaluación cuantitativa y cualitativa de los eventos potenciales, considerando tanto la exposición de los activos como la vulnerabilidad de los procesos críticos lo cual implica recopilar información histórica de incidentes, analizar condiciones ambientales y técnicas, y modelar escenarios de probabilidad e impacto que permitan priorizar amenazas según su severidad. A través de herramientas como matrices de riesgos, modelos de regresión, análisis de escenarios o simulaciones específicas, se busca no solo estimar la ocurrencia de eventos como incendios, inundaciones o fallas estructurales, sino también comprender cómo dichos eventos afectan directamente la continuidad operativa y la estabilidad financiera de la organización.



Esta fase no se limita a la detección de amenazas evidentes, sino que también incorpora factores internos como la preparación del personal, la calidad de los planes de contingencia o la frecuencia de mantenimiento de los sistemas críticos que pueden agravar o mitigar el efecto de un riesgo físico, lo que permite a la organización establecer un diagnóstico integral y fundamentado que servirá como base para la posterior fase de definición de estrategias de mitigación y respuesta.

En una segunda fase, el análisis de riesgos físicos dentro del marco del riesgo operacional se orienta a la gestión activa y a la implementación de medidas de mitigación, donde el objetivo principal es transformar la información obtenida en acciones concretas que reduzcan tanto la probabilidad de ocurrencia como la magnitud de las consecuencias; en esta etapa se diseñan e implementan controles técnicos, como sistemas avanzados de detección y supresión de incendios, planes de mantenimiento preventivo de infraestructuras críticas o mejoras en la resistencia de las edificaciones, al mismo tiempo que se fortalecen medidas organizacionales, tales como la capacitación continua del personal en protocolos de emergencia, la elaboración de simulacros periódicos, la definición de roles y responsabilidades y el establecimiento de canales de comunicación eficientes para la gestión de crisis incluyendo además estrategias financieras como la contratación de seguros o la creación de reservas económicas, que actúan como respaldo en caso de materialización del riesgo, garantizando la continuidad operativa; en síntesis, esta fase convierte el análisis en decisiones estratégicas y acciones preventivas, cerrando el ciclo de gestión de riesgos al transformar la vulnerabilidad en resiliencia y asegurando que la organización no solo pueda enfrentar eventos físicos adversos, sino también recuperarse de manera eficiente y sostenible.





Finalmente, en una tercera fase, el análisis del riesgo operacional frente a riesgos físicos debe consolidarse a través de un proceso de supervisión y mejora continua, reconociendo que las amenazas, los entornos y las propias organizaciones se encuentran en constante transformación; en esta etapa se establecen indicadores clave de desempeño (KPIs) que permiten medir la eficacia de las medidas implementadas, se diseñan sistemas de alerta temprana que garanticen la detección oportuna de anomalías, y se aplican auditorías internas y externas que verifiquen el cumplimiento de protocolos de seguridad, todo ello con el fin de garantizar que los planes de mitigación y respuesta se mantengan actualizados y eficaces. Asimismo, el seguimiento permite incorporar los resultados obtenidos tras la materialización de incidentes o la realización de simulacros, retroalimentando el modelo de análisis para adaptarlo a nuevas condiciones regulatorias, tecnológicas o ambientales. Este enfoque cíclico asegura que la organización no solo reaccione a los riesgos físicos, sino que evolucione constantemente en su capacidad de anticipación, prevención y resiliencia, integrando el riesgo operacional en una cultura organizacional de gestión proactiva y sostenida en el tiempo.

Quiero expresar mi gratitud a Metrorisk por la difusión mensual de artículos técnicos que enriquecen nuestro conocimiento, fomentan el análisis crítico de nuevas metodologías y fortalecen la cultura de gestión de riesgos mediante ideas innovadoras que apoyan la toma de decisiones en entornos complejos.

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



**MRConsulting**  
 Seguridad desde el diseño

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

## OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS) & CPTED

La relación entre CPTED, la ISO 18091:2019 (Sistemas de Gestión de la Calidad - Directrices para la aplicación de la ISO 9001:2015 en los gobiernos locales) y los Objetivos de Desarrollo Sostenible (ODS) de la ONU es un ejemplo claro de cómo la seguridad urbana se entrelaza con el desarrollo integral.

La ISO 18091 es una herramienta que ayuda a los gobiernos locales a mejorar la calidad de sus servicios y a gestionar de manera más eficaz sus procesos. Al aplicar esta norma, las administraciones locales pueden integrar CPTED de forma sistemática y transparente en su planificación urbana y políticas públicas.

La norma ISO 18091:2019 es una guía para que los gobiernos locales implementen un sistema de gestión de la calidad que cumpla con los requisitos de la norma ISO 9001:2015. Su propósito es ayudar a estas entidades a mejorar la calidad de sus productos y servicios, así como a aumentar la satisfacción de sus ciudadanos y otras partes interesadas. A través de un enfoque basado en procesos y en la gestión de riesgos, la norma busca que los gobiernos locales sean más transparentes, responsables y eficaces, lo que a su vez fomenta la confianza pública y el desarrollo sostenible de la comunidad local.

La guía se estructura para ser aplicable a todos los procesos y niveles de un gobierno local, desde el estratégico hasta el operativo, asegurando una gestión integral. Para ello, proporciona directrices para traducir temas como los Objetivos de Desarrollo Sostenible (ODS) de la ONU a indicadores de políticas públicas locales.

Por lo anterior, hablamos de un Sistema de Gestión de Riesgos Socio Urbanos CPTED®, ya que para realizar las acciones que nos lleven a cumplir con la Agenda de Desarrollo Sostenible de la ONU y sus ODS, cualquier intervención socio-urbana la realizaremos siguiendo los lineamientos de la Norma ISO 22341 y gestionada a través de la ISO 18091, contribuye directamente a varios ODS:

- ODS 11: Ciudades y Comunidades Sostenibles: este es el vínculo más directo. Una intervención CPTED bien planificada, que utiliza la ISO 22341, crea ciudades más seguras e inclusivas. Se enfoca en la seguridad y la resiliencia, promoviendo espacios públicos seguros y accesibles para todos, lo que es un pilar fundamental del ODS 11.



- ODS 16: Paz, Justicia e Instituciones Sólidas: CPTED es una estrategia de prevención que fortalece las instituciones a nivel local al fomentar la colaboración entre la policía, urbanistas y la comunidad. Al reducir el delito, promueve sociedades pacíficas e inclusivas. La ISO 18091 ayuda a los gobiernos a ser más efectivos y transparentes en la gestión de la seguridad, lo que se alinea con la meta de instituciones responsables.
- ODS 3: Salud y Bienestar: un entorno seguro reduce el estrés y el miedo, mejorando la salud mental y física de los residentes. La confianza en la seguridad del entorno invita a la gente a usar más los espacios públicos, fomentando la actividad física y la interacción social.
- ODS 10: Reducción de las Desigualdades: las intervenciones de CPTED bien diseñadas deben ser equitativas. La aplicación de la ISO 22341 y la ISO 18091 garantiza que las mejoras en seguridad no se limiten a ciertas áreas, sino que se distribuyan de forma justa en toda la ciudad, beneficiando a las comunidades más vulnerables.





# CPTED

La intervención socio-urbana CPTED es más que una estrategia de seguridad; es una herramienta de desarrollo sostenible. Al apoyarse en las normas ISO 22341 (para las directrices de CPTED) y la ISO 18091 (para la gestión local), se convierte en un enfoque sistemático, medible y eficaz para construir ciudades más seguras, justas y resilientes, cumpliendo así con la visión de los ODS de la ONU. El Sistema de Gestión de Calidad de la ISO 18091 realiza su evaluación mediante un diagnóstico integral que clasifica en cuatro dimensiones las acciones de un gobierno local, las cuales a su vez se desglosan en 39 indicadores clave. Este sistema, diseñado para medir la gestión de las políticas públicas, permite a los gobiernos locales evaluar su desempeño de manera responsable y transparente, con el objetivo de ser considerados "confiables".

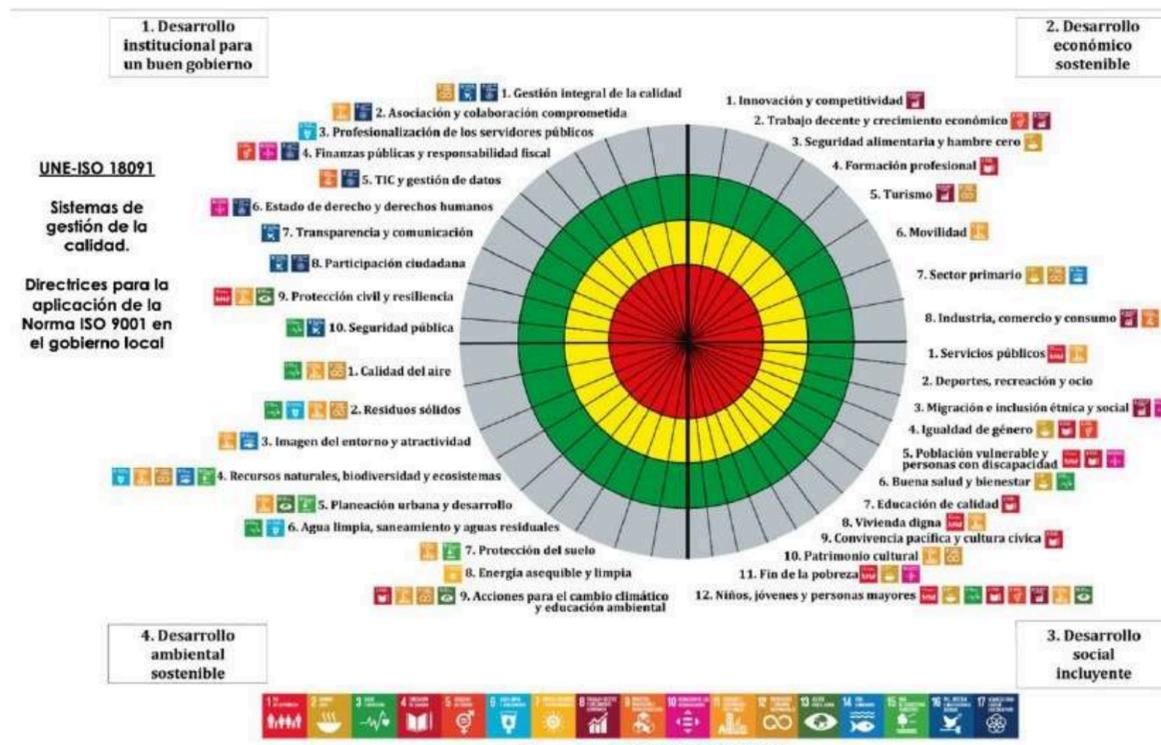
Las cuatro dimensiones son:

**1. Desarrollo Institucional para un Buen Gobierno:** esta dimensión, que incluye 10 indicadores, se centra en la capacidad de un gobierno para ser confiable y transparente. Evalúa si la gestión es integral y si existen mecanismos de asociación y colaboración con otros niveles de gobierno y partes interesadas. También analiza la profesionalización de los servidores públicos, el uso de las TIC para la gestión de datos, la responsabilidad fiscal y la promoción del estado de derecho y los derechos humanos. Además, valora la transparencia, la rendición de cuentas y la participación ciudadana, así como la resiliencia y la seguridad pública para enfrentar emergencias y la delincuencia.

**2. Desarrollo Económico Sostenible:** con 8 indicadores, esta dimensión se enfoca en la capacidad del gobierno para fomentar un crecimiento económico equitativo y a largo plazo. Examina la promoción de la innovación y la competitividad, la creación de trabajo decente y el crecimiento económico, y la garantía de la seguridad alimentaria. También evalúa la formación profesional, el desarrollo de industrias, el comercio y el turismo, y la mejora de la movilidad, tanto de personas como de mercancías. Finalmente, considera el apoyo al sector primario, como la agricultura y la ganadería.

**3. Desarrollo Social Incluyente:** esta dimensión se compone de 12 indicadores y mide el compromiso de un gobierno para mejorar la calidad de vida de todos sus ciudadanos, especialmente los más vulnerables. Aborda la calidad de los servicios públicos, las oportunidades para el deporte y el ocio, y la inclusión social y étnica. También evalúa la igualdad de género, el apoyo a la población vulnerable y personas con discapacidad, la promoción de la salud y la educación de calidad, y el acceso a la vivienda digna. Además, considera la convivencia pacífica, la protección del patrimonio cultural y la erradicación de la pobreza, prestando especial atención a niños, jóvenes y adultos mayores.

**4. Desarrollo Ambiental Sostenible:** esta dimensión, con 9 indicadores, se centra en la gestión del gobierno para proteger el medio ambiente y promover la resiliencia. Evalúa las acciones para cuidar la calidad del aire y la gestión de residuos sólidos. Considera la mejora de la imagen del entorno, la conservación de los recursos naturales y la biodiversidad, y la planificación urbana. También examina la disponibilidad de agua limpia y saneamiento, la protección del suelo, el acceso a energías asequibles y limpias, y las acciones para combatir el cambio climático y la educación ambiental.



## DESARROLLO INSTITUCIONAL PARA UN BUEN GOBIERNO

La Prevención del Delito a Través del Diseño Ambiental (CPTED), guiada por la norma ISO 22341, es una estrategia fundamental para la seguridad y la resiliencia urbana. Sin embargo, su verdadero potencial se libera cuando se integra en un sistema de gestión que incluye la calidad gubernamental, como el establecido por la ISO 18091. Esta integración no solo fortalece la seguridad pública, sino que también fomenta una gobernanza confiable y transparente, un pilar esencial para el desarrollo institucional, empresarial y social. La ISO 18091 define diez indicadores clave. La aplicación de la CPTED, particularmente en su enfoque de tercera generación, contribuye directamente a estos indicadores, creando un ciclo de mejora continua en la gestión pública.



# CPTED

- **Gestión integral de la calidad:** evalúa la existencia de un sistema de gestión de la calidad que asegure la mejora continua de los servicios y procesos gubernamentales, buscando la satisfacción ciudadana. La ISO 22341 proporciona un marco estandarizado para la implementación de CPTED, convirtiendo la prevención del delito en un proceso estructurado y medible. Al integrar los principios CPTED en la planificación urbana y la gestión de proyectos, se asegura que la seguridad sea un atributo de calidad en el diseño de todos los espacios públicos y servicios, lo cual se gestiona y mejora continuamente bajo un sistema de calidad ISO 18091.
- **Asociación y colaboración comprometida:** evalúa la capacidad del gobierno para establecer alianzas estratégicas y colaborar efectivamente con diversas partes interesadas. CPTED, especialmente en su segunda y tercera generación, depende inherentemente de la colaboración interinstitucional (policía, urbanistas, servicios sociales) y la participación ciudadana. La ISO 22341 enfatiza la necesidad de consultar a las partes interesadas y formar equipos multidisciplinarios. Al hacerlo, se fortalecen las alianzas entre gobierno, comunidad y sector privado en pro de la seguridad, un indicador clave de la ISO 18091.
- **Profesionalización de los servidores públicos:** evalúa la capacitación y desarrollo continuo de los empleados públicos para asegurar sus competencias y ética. La implementación efectiva de CPTED requiere la formación de profesionales en diversas áreas (urbanistas, arquitectos, planificadores, fuerzas de seguridad) sobre los principios del diseño para la prevención del delito. La ISO 22341 fomenta esta capacitación especializada, lo que eleva el nivel de profesionalismo en la administración pública, haciendo a los servidores más competentes en la creación de entornos seguros.
- **Finanzas públicas y responsabilidad fiscal:** evalúa la eficiencia, transparencia y sostenibilidad en la gestión de los recursos financieros públicos. Las intervenciones CPTED bien planificadas, según la ISO 22341, se consideran inversiones preventivas que pueden reducir significativamente los costos a largo plazo asociados al crimen (daños, reparaciones, mayores servicios policiales). Una inversión inicial en diseño seguro puede generar ahorros fiscales, lo que demuestra una gestión financiera responsable y eficiente.
- **TIC y gestión de datos:** evalúa: el uso estratégico de las Tecnologías de la Información y las Comunicaciones (TIC) para mejorar la gestión pública, la transparencia y la participación, así como la adecuada gestión de los datos. La ISO 22341, al abordar la evaluación de riesgos, se beneficia del uso de sistemas de información geográfica (SIG), análisis predictivo y plataformas de reporte ciudadano para identificar patrones delictivos, monitorear la efectividad de las intervenciones de diseño y gestionar la información de seguridad de forma proactiva.
- **Estado de derecho y derechos humanos:** evalúa el compromiso del gobierno local con el respeto y la promoción del estado de derecho y los derechos humanos. La ISO 22341 establece que CPTED debe aplicarse de manera equitativa y universal, sin crear estigmas ni violar derechos. Un diseño urbano que promueve la seguridad sin recurrir a medidas excesivamente punitivas o discriminatorias, y que garantiza el acceso igualitario a espacios seguros, refuerza el estado de derecho y protege los derechos humanos, contribuyendo a una sociedad más justa.
- **Transparencia y participación ciudadana:** evalúa la existencia de mecanismos efectivos que garanticen el acceso a la información pública, la rendición de cuentas y la participación activa de los ciudadanos. La ISO 22341 enfatiza la importancia de involucrar a la comunidad en el proceso de diseño y planificación de la seguridad. Al consultar a los ciudadanos sobre sus percepciones de seguridad y al mostrarles cómo el diseño CPTED abordará sus preocupaciones, el gobierno actúa de manera transparente y fomenta la participación, elementos clave para la confianza y la rendición de cuentas.
- **Protección civil y resiliencia:** evalúa la capacidad del gobierno local para prevenir, prepararse, responder y recuperarse eficazmente de desastres y para construir comunidades resilientes. Un entorno diseñado con principios CPTED (claridad en los caminos, vigilancia natural, control de acceso) facilita no solo la prevención del delito, sino también la respuesta ante emergencias, la evacuación y la asistencia en caso de desastre. La ISO 22341 contribuye a la creación de espacios urbanos que son intrínsecamente más ordenados y fáciles de gestionar en situaciones críticas, mejorando la resiliencia general de la comunidad.



# CPTED

- Seguridad pública: evalúa la implementación de políticas y programas efectivos para la prevención del delito, la reducción de la violencia y el fomento de la paz social. Este es el núcleo de CPTED. La ISO 22341 proporciona las directrices para aplicar los principios de seguridad por diseño que reducen las oportunidades para el crimen y el miedo al crimen impactando directamente en la mejora de la seguridad pública y la promoción de la paz social.
- Calidad del aire: evalúa la existencia de programas para monitorear y mejorar la calidad del aire, reduciendo la contaminación. Aunque indirectamente, CPTED promueve el diseño de espacios públicos seguros y esto anima a la gente a caminar o usar bicicletas, reduciendo el tráfico vehicular. Un diseño que incorpora zonas verdes y áreas de esparcimiento seguras (facilitado por la ISO 22341) puede mejorar la calidad del aire al aumentar la vegetación y disminuir la dependencia del automóvil en zonas urbanas.

Al alinear estos avances con los principios de transparencia y rendición de cuentas de la ISO 18091, se construye un modelo de gobernanza abierta y eficaz, donde la seguridad no es solo un objetivo, sino un resultado de una gestión pública confiable y orientada a los resultados. La implementación estratégica de CPTED con los lineamientos de la ISO 22341 y la ISO 18091, es una herramienta poderosa para el desarrollo económico sostenible. Al priorizar la seguridad, la innovación y la gestión de la calidad, un gobierno local puede crear un círculo virtuoso de prosperidad, donde un entorno más seguro es sinónimo de una economía más fuerte y resiliente.

## CPTED Y EL DESARROLLO ECONÓMICO SOSTENIBLE

La ISO 18091 evalúa la gestión de los gobiernos locales a través de varios indicadores, ocho de los cuales se agrupan en la categoría de Desarrollo Económico Sostenible. CPTED, en su enfoque se alinea con estos indicadores de manera proactiva e innovadora.

- Crecimiento Económico Sostenible: CPTED crea entornos seguros que reducen el riesgo y el costo de la delincuencia para las empresas. Un gobierno local que promueve la seguridad pública a través de la CPTED mejora la confianza de los inversionistas y empresarios, fomentando el crecimiento económico.
- Generación de Empleo y Salarios Justos: seguridad urbana es un factor clave para la creación de empleos dignos. Un entorno seguro anima a las empresas a expandirse y contratar, y permite a los trabajadores realizar sus labores sin miedo. CPTED contribuye a un mercado laboral más estable y justo.
- Movilidad Urbana, Segura y Sostenible: CPTED, al mejorar la seguridad de las calles y el transporte público, promueve la movilidad sostenible, lo que beneficia directamente a la economía local. Los ciudadanos pueden moverse con más libertad y seguridad. Las empresas de transporte y servicios de movilidad pueden operar de manera más eficiente.
- Innovación e Infraestructura Sostenible: CPTED de tercera generación, utiliza la tecnología para la prevención del delito, lo que se alinea con la innovación y la infraestructura sostenible que evalúa la ISO 18091. La inversión en sistemas de vigilancia inteligentes, alumbrado eficiente y redes de sensores no solo aumenta la seguridad, sino que también promueve el uso de tecnologías limpias y avanzadas.
- Tecnología de la Información y la Comunicación (TIC) y Gestión de Datos: un gobierno local confiable tiene programas para la promoción de las TIC y su uso sistemático para la gestión pública. CPTED utiliza datos georreferenciados para analizar los puntos de riesgo y optimizar la respuesta de la policía y otros servicios, lo que se traduce en una gestión más eficiente y transparente de la seguridad pública.
- Desarrollo del Turismo Local y Sostenible: los turistas buscan entornos seguros y atractivos. CPTED, al mejorar la seguridad de los espacios públicos, monumentos y zonas turísticas, hace que un destino sea más atractivo y competitivo. Un gobierno local que aplica CPTED de manera estratégica aumenta los ingresos del sector turístico y promueve un turismo más responsable.
- Industria, Negocios y Pequeñas y Medianas Empresas (PYMES): la delincuencia afecta directamente a las PYMES, causando pérdidas económicas y desalentando la inversión. Un gobierno local confiable tiene programas que apoyan el desarrollo de la industria local. CPTED contribuye a este objetivo al reducir la inseguridad y crear un ambiente favorable para los negocios.
- Resiliencia Urbana y Gobernanza Confiable: un entorno seguro es un factor de resiliencia urbana que ayuda a las comunidades a recuperarse de crisis económicas y sociales. La ISO 18091 y la ISO 22341 relacionan la resiliencia con la gobernanza confiable y el apoyo a las comunidades para que se conviertan en agentes de cambio. CPTED promueve la colaboración entre la policía, urbanistas, empresarios y la comunidad, fortaleciendo la gobernanza y la capacidad de las comunidades para enfrentar desafíos.



La CPTED de tercera generación representa una evolución que integra el diseño físico, la cohesión social y la tecnología para impulsar el desarrollo económico. Se basa en la idea de que la seguridad no es un costo, sino una inversión. Al usar datos y análisis predictivos, un gobierno puede destinar recursos de manera más eficiente, enfocándose en la prevención de delitos en lugar de la reacción. Esto reduce los costos de la seguridad pública y libera fondos para invertir en infraestructura y servicios que promuevan el crecimiento económico sostenible

- **Innovación en Seguridad Pública:** CPTED no solo utiliza la tecnología para vigilar, sino también para crear soluciones innovadoras. Por ejemplo, los sensores de ruido pueden detectar actos de vandalismo en tiempo real, permitiendo una respuesta inmediata y reduciendo el costo de las reparaciones. Las aplicaciones móviles pueden permitir a los ciudadanos reportar problemas en el entorno, lo que ayuda a las autoridades a identificar y mitigar riesgos focalizados.
- **Eficiencia Económica:** al mejorar la seguridad y la percepción de seguridad, la CPTED aumenta la vitalidad de los barrios, lo que a su vez eleva el valor de las propiedades y el atractivo de las zonas comerciales. Un entorno seguro fomenta el consumo local y reduce las pérdidas por robo o vandalismo, lo que beneficia directamente a los negocios locales.

Al ser una intervención socio urbana siguiendo los lineamientos de la Norma ISO 22341 CPTED, es mucho más que una simple estrategia de seguridad; es un catalizador para el desarrollo económico sostenible. Al ser implementada por un gobierno local que se rige por los principios de la ISO 18091, CPTED contribuye a la creación de entornos urbanos que no solo son más seguros, sino también más atractivos para la inversión, el comercio y el turismo. Esta sinergia demuestra que la seguridad es un motor económico fundamental

#### **CPTED Y EL DESARROLLO SOCIAL INCLUYENTE**

La ISO 18091, en su anexo A, establece un sistema de diagnóstico con 39 indicadores para evaluar la gestión de gobiernos locales, de los cuales 12 se centran en el Desarrollo Social Inuyente. La aplicación de CPTED, en línea con la ISO 22341, contribuye directamente a estos indicadores, promoviendo entornos más seguros y equitativos.

***“Al entrelazar la visión de la ISO 18091 para una gobernanza de calidad y confiable con las directrices proactivas de la seguridad por diseño de la ISO 22341 (CPTED), no solo diseñamos ciudades más seguras, sino que construimos el cimiento para un futuro urbano verdaderamente sostenible, equitativo y próspero para todos.”***

- **Servicios Públicos de Calidad:** un gobierno local confiable asegura la cobertura de servicios básicos en todas las comunidades y viviendas, de manera responsable y asequible. CPTED mejora la seguridad de la infraestructura y los espacios donde se proporcionan estos servicios, fomentando la confianza de los ciudadanos en su uso y acceso.
- **Deportes, Recreación y Ocio:** CPTED promueve la creación y el mantenimiento de infraestructura deportiva y recreativa para el uso seguro de las personas. Un entorno bien cuidado y con buena vigilancia natural anima la participación de las personas de todas las edades en actividades de esparcimiento, mejorando la salud y el bienestar.
- **Migración e Inclusión Étnica y Social:** el gobierno local debe tener programas para proteger a los migrantes, combatir la discriminación y promover la igualdad de derechos. CPTED social de segunda generación, enfocado en la cohesión y conectividad comunitaria, crea espacios donde los ciudadanos de todos los grupos étnicos y sociales pueden reunirse y discutir asuntos locales, fomentando la integración y el respeto mutuo.
- **Igualdad de Género:** CPTED debe aplicarse de manera universal e igualitaria, sin prejuicios. Un gobierno confiable cuenta con un departamento responsable de implementar políticas y actividades para promover la igualdad de género y empoderar a todas las niñas y mujeres. El diseño de espacios seguros y libres de miedo es un paso fundamental para lograr este objetivo.
- **Población Vulnerable y Personas con Discapacidad:** la ISO 18091 destaca que un gobierno local confiable tiene un diagnóstico de las personas con discapacidad, de su población en riesgo y vulnerable. CPTED asegura que la infraestructura sea segura y accesible para todos, eliminando barreras físicas y mejorando la seguridad en general, permitiendo la plena participación de personas con discapacidad en la vida comunitaria.
- **Buena Salud y Bienestar:** la promoción de entornos seguros tiene un impacto positivo en la salud mental y física de la comunidad. Un gobierno local confiable promueve el derecho a la salud a través de programas de prevención y atención. CPTED contribuye indirectamente al reducir los factores de estrés asociados a la inseguridad y se enfoca en la salud mental.
- **Educación de Calidad:** un gobierno local confiable promueve la educación básica inclusiva y de calidad, asegurando la inversión en infraestructura básica y mejoras en la calidad de la educación. CPTED garantiza que los entornos escolares sean seguros y propicios para el aprendizaje, tanto dentro como fuera de las instalaciones.
- **Vivienda Digna:** CPTED puede ayudar a asegurar la seguridad física de la tenencia y a regularizar asentamientos ilegales, lo que está en línea con los programas de vivienda digna que promueve la ISO 18091. Un entorno seguro y bien planificado es un componente esencial de la calidad de vida en una vivienda.



- **Convivencia Pacífica y Cultura Cívica:** un gobierno confiable tiene un programa para promover los derechos políticos y sociales, la educación cívica y la convivencia pacífica. CPTED, al crear espacios que fomentan la interacción y la vigilancia natural, fortalece el tejido social y la cultura cívica.
- **Patrimonio Cultural:** CPTED ayuda a proteger y preservar el patrimonio local. Un entorno seguro es un requisito para que los ciudadanos se apropien de su patrimonio, lo valoren y participen en su conservación.
- **Fin de la Pobreza:** el gobierno local debe tener programas para proveer atención y servicios especiales a la población en situación de pobreza. CPTED contribuye a garantizar que las intervenciones en estas áreas sean seguras y dignas, sin generar estigmas o barreras adicionales y, con ello, se reduzcan las brechas sociales.
- **Niños, Jóvenes y Personas Mayores:** un gobierno local confiable tiene programas para la protección, inclusión y desarrollo de estos segmentos de la población. CPTED proporciona un marco para diseñar espacios que satisfagan las necesidades de cada grupo social, promoviendo su seguridad y participación activa.

Al adoptar CPTED y alinearla con los principios de la ISO 18091 y la ISO 22341, los gobiernos locales no solo previenen el delito, sino que también construyen un futuro más seguro, inclusivo, eficiente y sostenible para todos sus ciudadanos.

#### **CPTED Y EL DESARROLLO AMBIENTAL SOSTENIBLE**

La Norma ISO 18091 promueve un sistema de gestión de la calidad integral en los gobiernos locales. Un componente crucial de este sistema es la categoría de Desarrollo Ambiental Sostenible, que incluye nueve indicadores clave que evalúan la eficacia de la gestión ambiental de una ciudad. CPTED, enmarcada en la ISO 22341, se alinea con estos nueve indicadores de la siguiente manera:

- **Calidad del Aire:** un enfoque CPTED que promueve la movilidad sostenible (bicicletas, transporte público) y la creación de espacios verdes para la recreación puede contribuir a una menor emisión de contaminantes y a una mejor calidad del aire. Al hacer los espacios públicos más seguros, se incentiva a los ciudadanos a optar por medios de transporte menos contaminantes, lo que se refleja en los programas de inspección de emisiones y los planes de contingencia para la contaminación del aire.
- **Residuos Sólidos:** el diseño ambiental puede influir en la gestión de residuos. CPTED verde recomienda el uso de materiales robustos y a prueba de vandalismo para el mobiliario urbano y los contenedores de basura, facilitando su mantenimiento y evitando la proliferación de desechos. Un sistema de recolección de residuos que cubra la mayor parte del territorio y un programa de separación y reciclaje son indicadores de un gobierno confiable.

- **Imagen del Entorno y Atractividad:** el diseño de espacios atractivos y bien cuidados, libres de vandalismo y deterioro, es un principio fundamental de CPTED, basado en la teoría de las "ventanas rotas". La ISO 18091 relaciona la mejora de la imagen del entorno con la promoción del sentido de identidad y pertenencia de los ciudadanos.
- **Recursos Naturales, Biodiversidad y Ecosistemas:** CPTED verde se enfoca en la planificación de espacios que no solo sean seguros, sino que también contribuyan a la conservación de la flora, fauna y recursos naturales. La ISO 18091 establece que un gobierno local confiable cuenta con un diagnóstico, programas y un departamento responsable de la conservación de estos recursos.
- **Planificación Urbana y Desarrollo:** CPTED es una herramienta clave en la planificación urbana. La ISO 18091 indica que un gobierno local debe tener un sistema de planificación y regulación del crecimiento de los centros de población, que se actualice continuamente e involucre la participación de los interesados. El diseño CPTED ayuda a dar forma a este crecimiento de manera segura, desde la concepción del plan hasta su implementación.
- **Agua Limpia, Saneamiento y Aguas Residuales:** la seguridad de los sistemas de agua y saneamiento es crítica. CPTED puede aplicarse para proteger la infraestructura hídrica y garantizar su correcto funcionamiento, mientras que la ISO 18091 evalúa los programas para la calidad, conservación y mantenimiento de las fuentes de suministro de agua.
- **Protección del Suelo:** CPTED verde se extiende a la protección del suelo a través del control de la erosión, la reforestación y la conservación. Estas estrategias contribuyen a la resiliencia de los ecosistemas y están alineadas con los programas de protección del suelo evaluados por la ISO 18091.
- **Energía Asequible y Limpia:** la iluminación adecuada es un pilar de CPTED para la vigilancia natural. La ISO 18091 promueve el uso de energía asequible y limpia. Ambas normas se complementan al abogar por sistemas de alumbrado público que no solo aumenten la seguridad, sino que también sean energéticamente eficientes y sostenibles.
- **Acciones para el Cambio Climático y Educación Ambiental:** la ISO 18091 evalúa los programas locales para combatir el cambio climático y promover la educación ambiental. CPTED, al crear espacios públicos seguros y atractivos, puede ser el vehículo para implementar programas de educación y concientización. Estos lugares se convierten en laboratorios al aire libre donde los ciudadanos pueden participar en la mejora continua de su entorno, aprendiendo sobre la biodiversidad, la gestión de residuos y la protección del medio ambiente en un espacio que se siente seguro.

# EL DESAFÍO DE LAS EMPRESAS DE SEGURIDAD ANTE LOS NUEVOS PARADIGMAS

**Antonio Cozano Fernández**  
CEO Cofer Seguridad.

El sector de la seguridad atraviesa una etapa de transformación profunda. Las empresas se ven obligadas a adaptarse a un entorno en el que los paradigmas tradicionales ya no bastan para responder a las exigencias de la sociedad y de los mercados. Tres factores están marcando especialmente esta transición: la fiscalidad, la falta de profesionales y el aumento del índice de bajas laborales.



**Información general**  
[info@coferseguridad.com](mailto:info@coferseguridad.com)  
952 409 846

An advertisement for COFER SEGURIDAD. It features a woman sitting in bed, looking at her smartphone. The text on the ad includes: "¿Y SI LO ÚNICO QUE QUIERES ES DORMIR TRANQUILO? COFER, NO VENDE ALARMAS, GARANTIZA TRANQUILIDAD." and "Active su sistema de seguridad en un clic". At the bottom, it says "29,95 € mes+ IVA\*" and shows the COFER SEGURIDAD logo.

**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\*

En primer lugar, la fiscalidad se ha convertido en un elemento que desequilibra la balanza competencial. Los elevados costes impositivos y las cargas sociales limitan la capacidad de las empresas de seguridad para competir en igualdad de condiciones. Esta situación genera distorsiones en la contratación, fomentando prácticas de bajo coste que, a medio plazo, erosionan la calidad del servicio y la confianza del cliente.

A ello se suma la carencia de nuevos profesionales. La seguridad, pese a ser un sector estratégico, no atrae a suficientes jóvenes preparados para asumir el relevo generacional. La falta de programas formativos adaptados a la realidad tecnológica y social, junto con la percepción de condiciones laborales poco atractivas, están dificultando la creación de un talento sólido y especializado.

Finalmente, el crecimiento del índice de bajas laborales es una señal de alerta. La presión del servicio, la exposición constante al riesgo y, en muchos casos, la precariedad de recursos, repercuten directamente en la salud física y mental de los trabajadores. Este fenómeno incrementa los costes internos y merma la capacidad operativa de las empresas, reduciendo su competitividad.

El futuro del sector dependerá de la capacidad de las empresas y de las instituciones de redefinir el marco fiscal, profesional y laboral. La seguridad no puede seguir tratándose como un servicio secundario, sino como una actividad esencial que requiere inversión, reconocimiento y proyección social. Afrontar estos retos con visión estratégica será la única vía para que el sector se fortalezca y pueda responder a los nuevos paradigmas con eficacia y profesionalidad.

Redacción de Metrorisk.



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

## Las profecías del Compliance

La profecía de la puerta abierta (y por qué la ciberseguridad es también Compliance)

Quizá leer sobre **Compliance** no esté en tus planes... Sin embargo, en los míos sí lo está escribir.

Y aquí continúa...

**"Las Profecías del Compliance"**.

Los antiguos temían a las profecías de Nostradamus, como advertencias de catástrofes inevitables.

Hoy, muchas organizaciones conviven con su propia catástrofe anunciada: la **ciberseguridad** ignorada.

**Aquí va la cuarta profecía:**

*"Donde la ciberseguridad se descuide, el fraude hallará puerta abierta."*

- No hacen falta visiones místicas para saberlo.
- Un solo clic, una contraseña débil, un software sin parchear...

Y de pronto, el negocio se paraliza, los datos se filtran, la confianza se rompe.

- Ciberseguridad no es solo TI.



Es cultura.  
Es estrategia.  
Es Compliance.

Hoy regulaciones como **NIS2** y **DORA** no son opcionales, son exigencias que marcan cómo proteger lo más valioso: los datos, la continuidad de negocio y la reputación.

**ISO27001** y **ENS**, no pueden ser el último escalón estratégico

Un descuido digital es como dejar la puerta abierta en plena noche.  
El fraude y riesgo, no entra por magia, entra porque le dejamos paso.

▪ **Pregunta dominical:**

¿Tu organización protege su presente con una ciberseguridad real, o mantiene una puerta abierta esperando a que ocurra la profecía?



# 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

# CONFIAR SOLO EN EL RGPD: EL PUNTO DÉBIL DE TU EMPRESA

**Rosa Fernández**

## ASUNTO: CUMPLIMIENTO 360º

*En seguridad privada, la videovigilancia, drones y biometría exigen un blindaje jurídico que va mucho más allá del RGPD. Tu empresa necesita tener un Cumplimiento 360º.*

*En seguridad privada, la videovigilancia, drones y biometría exigen un blindaje jurídico que va mucho más allá del RGPD. Tu empresa necesita tener un Cumplimiento 360º. En un mercado donde la confianza es el activo más valioso, muchas empresas de seguridad privada creen que tener el "sello RGPD" es suficiente. La realidad es muy distinta: el Reglamento General de Protección de Datos es solo la base, pero hoy los riesgos tecnológicos, regulatorios y legales exigen un cumplimiento 360º.*

¿Por qué con el RGPD ya no basta?

☛ Porque la seguridad privada ya no solo gestiona cámaras o alarmas. Ahora se usan para trabajar mejor y dar servicios de valor añadido, ampliando el perímetro de seguridad de tu cliente:

- Sistemas de videovigilancia inteligente con reconocimiento facial.
- Mirillas digitales y dispositivos conectados en hogares y oficinas.
- Drones para control perimetral.
- Controles termográficos y sistemas de detección biométrica.
- Tecnología anti-robo conectada a la nube. Cada uno de estos equipos genera datos sensibles, biométricos y conductuales que no solo están regulados por el RGPD, sino también por un ecosistema normativo que no se puede, ni se debe ignorar.

Como sabes, el espacio europeo es el más garante de derechos del planeta Tierra. ¿Cómo lo hacen? Con normas que obligan a quienes tratamos datos, que no son nuestros, a tener medidas de seguridad IMPLANTADAS, no adaptadas, en la empresa, en los proyectos, en la actividad operativa y en los procesos. En España, nuestro ordenamiento jurídico integra diferentes normas (y con ello diferentes obligaciones) para ello. No sólo el RGPD. Las normas que impactan directamente al sector:

LOPDGDD → Ajusta el RGPD a la realidad española, con sanciones específicas y obligaciones reforzadas para seguridad privada. OBLIGATORIA. SI o SI.

LSSI-CE → Regula servicios electrónicos, comunicaciones y sistemas en red, clave cuando los dispositivos transmiten datos a centros de control.

OBLIGATORIA. SI o SI. Si tienes web o vendes servicios en espacios digitales. Directiva ePrivacy → Impacta en el uso de cookies, geolocalización y metadatos de comunicación de dispositivos conectados. OBLIGATORIA. SI o SI.

REIA (Reglamento Europeo de Inteligencia Artificial) → Fundamental si se usan algoritmos de reconocimiento facial, análisis conductual o predicción de riesgos. OBLIGATORIA. SI o SI Norma ISO 27001 (seguridad de la información) y ISO 10002 (gestión de reclamaciones) → Necesarias para demostrar control, trazabilidad y capacidad de respuesta. OPCIONALES. Las implantas porque quieres, debes o te conviene.



DATA ACT (Digital Services & AI Act) Normativas europeas emergentes que impondrán nuevas obligaciones en materia de ciberseguridad y responsabilidad en el uso de tecnologías avanzadas. Protege datos no personales. OBLIGATORIA. SI o SI.

¿Qué debe hacer una empresa de seguridad privada como la tuya?

- ✓ Mapa de riesgos normativos: identificar qué normas aplican según cada dispositivo y servicio.
- ✓ Evaluaciones de impacto (EIPD / REIA): obligatorias para videovigilancia, biometría y drones.
- Políticas de Bring Your Own Device (BYOD): protocolos claros cuando se usan dispositivos propios o de clientes.
- ✓ Auditorías de ciberseguridad y privacidad: no solo en servidores, también en los equipos de campo. Por ejemplo: en una empresa de seguridad privada que usa drones con cámaras para vigilancia perimetral. El servidor central almacena las grabaciones → necesita cifrado, control de accesos, registro de logs. Pero los drones de campo también procesan datos en tiempo real (imágenes de personas, matrículas). Si un dron se pierde, hackean su firmware o alguien accede a la tarjeta SD, se produce una brecha de seguridad.
- ✓ Formación El Artículo 4 del Reglamento Europeo de Inteligencia Artificial obliga a proveedores y responsables del despliegue de sistemas de IA a garantizar que su personal y las personas que utilicen esos sistemas en su nombre tengan un nivel adecuado de formación/alfabetización en IA, teniendo en cuenta los conocimientos, experiencia y el contexto, para entender sus riesgos, limitaciones y responsabilidades, incluyendo cuando se manejan datos sensibles. OBLIGATORIA para las empresas que usan soluciones con IA.
- ✓ Integración ISO-RGPD: crear un sistema de cumplimiento 360º que unifique datos, calidad, quejas y seguridad

Consultora jurídica. ©2025

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

¿Qué pasa si tu empresa no cumple?

- Multas millonarias: hasta el 4% de la facturación global.
  - Pérdida de contratos: cada vez más clientes exigen auditorías de cumplimiento completas.
  - Daño reputacional: un fallo en videovigilancia o en drones afecta directamente la confianza, y sin confianza no hay negocio. La seguridad privada ya no solo protege espacios físicos, protege datos, derechos y confianza.
- El cliente no compra ni elige a quien tenga más cámaras, sino a quien demuestre que cumple con todo el marco normativo europeo, que usa dispositivos y tecnología con responsabilidad y que garantiza un blindaje jurídico y tecnológico total. Tu cliente quiere un Cumplimiento 360°.

¿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](mailto:rosaf@zonavigilada.net)  
Te damos respuestas y te ayudamos a  
mejorar tu seguridad jurídica

👉 No te preguntes si tu empresa cumple el RGPD...  
Pregúntate si estás preparado para cumplir con todo  
lo que viene.



**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

 [rosaf@zonavigilada.net](mailto:rosaf@zonavigilada.net)

 **ESTRATEGIA LEGAL**  
[WWW.ZONAVIGILADA.NET](http://WWW.ZONAVIGILADA.NET)

# LA SEGURIDAD PRIVADA EN LA PROTECCIÓN DE INFRAESTRUCTURAS DURANTE RIESGOS METEOROLÓGICOS

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Carlos Serrano**  
Director de Contenidos de Seguridad y Empleo

En un contexto marcado por el cambio climático y el incremento de fenómenos meteorológicos adversos, la seguridad privada se ha consolidado como un actor clave en la protección de infraestructuras críticas y estratégicas. Tormentas, inundaciones, olas de calor, temporales de nieve o fuertes rachas de viento no solo ponen en riesgo la continuidad de los servicios esenciales, sino también la seguridad de los trabajadores y de la ciudadanía.

## El papel de la seguridad privada en situaciones de riesgo

Los profesionales de la seguridad privada cumplen funciones que van más allá de la vigilancia convencional. En escenarios de riesgo meteorológico, su misión se centra en:

- Prevención y anticipación: verificar planes de emergencia, comprobar el estado de accesos, sistemas eléctricos y de comunicaciones, así como anticipar posibles incidentes derivados de las condiciones climáticas.
- Apoyo a la protección civil: colaborar con las autoridades locales y equipos de emergencia, aportando información en tiempo real sobre incidencias en infraestructuras.
- Control de accesos y evacuaciones: garantizar que el tránsito de personas y vehículos se realice de forma segura en aeropuertos, estaciones ferroviarias, hospitales o centros de operaciones críticas.
- Protección de bienes e instalaciones: evitar actos de vandalismo, robos o sabotajes en momentos de vulnerabilidad, cuando la atención se centra en la emergencia.

## Ámbitos de actuación prioritarios

Entre las infraestructuras más sensibles a los efectos de fenómenos meteorológicos extremos destacan:

- Redes de transporte y movilidad (aeropuertos, estaciones de tren y metro, carreteras y puertos).
- Suministros básicos (eléctricos, hídricos y de telecomunicaciones).
- Centros sanitarios y asistenciales, cuyo funcionamiento es crítico en emergencias.
- Espacios industriales y logísticos, que pueden sufrir graves pérdidas materiales por inundaciones o incendios derivados de tormentas eléctricas.

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



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



## Importancia de la evaluación de riesgos

La planificación de la seguridad frente a fenómenos meteorológicos debe partir de una evaluación de riesgos sistemática, que permita identificar vulnerabilidades y establecer prioridades de actuación. No todas las infraestructuras se ven afectadas del mismo modo: una estación ferroviaria expuesta a lluvias torrenciales requiere protocolos diferentes a una subestación eléctrica expuesta a vientos huracanados. En este sentido, la seguridad privada contribuye activamente a la detección de amenazas y a la actualización de planes de autoprotección, asegurando que los recursos humanos y materiales se ajusten a los escenarios más probables.

## Aplicación del método Mosler

Uno de los enfoques más útiles en la gestión de riesgos es el método Mosler, que permite evaluar las amenazas a partir de la combinación de tres factores:

1. Peligrosidad: la probabilidad de que se produzca un fenómeno meteorológico adverso.
2. Vulnerabilidad: el grado de exposición de la infraestructura frente al fenómeno.
3. Daño esperado: las consecuencias económicas, sociales y operativas derivadas de dicho fenómeno.



# LA SEGURIDAD PRIVADA Y SU IMPLICACIÓN EN LAS FFCCSE

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

**Desde el primer momento debemos entender que, en esencia, la seguridad privada y las Fuerzas y Cuerpos de Seguridad del Estado se dedican a lo mismo: la defensa de la Constitución española como base del ordenamiento jurídico nacional, así como velar por la prevención y la seguridad de todos los españoles y su patrimonio. Debemos recordar que el Estado tiene el monopolio de la seguridad y que cualquier acto que se requiera de esta es operativo de las FFCCSE.**

Es aquí donde entra el perfil de la seguridad privada. Y esto es debido a que en la Ley 5/2014, de 4 de abril se reconoce que el Estado español no puede estar presente en todo lugar y momento, y por ello, le da a la seguridad privada la condición de cuerpo auxiliar a las FCSSE. En dicho preámbulo de la ley que regula este sector dice que la función de seguridad privada es la prevención de cualquier tipo de riesgo, con obligada participación y colaboración con las Fuerzas y Cuerpos de seguridad.

En la referida ley la seguridad privada, como un cuerpo auxiliar a los Cuerpos de seguridad del Estado, está subordinada, inspeccionada, sancionada y mencionada por el Cuerpo Superior de la Policía Nacional, en su sección de Seguridad Privada, sin dejar de estar subordinada a las directrices de cualquier otro Cuerpo de Seguridad del Estado. Esta condición atañe tanto a personal operativo como a las empresas de seguridad privada, empresas instaladoras de sistemas y a los usuarios de seguridad privada. Ya han pasado muchos años desde que los antiguos Guardias Jurados contaban con el carácter de agente de la autoridad, condición que perdieron en la publicación de la Ley 23/92 (del 30 de julio), pérdida que ha sido mantenida, en la ley 5/2014, por lo que pasan a denominarse Vigilantes de Seguridad. Pero debemos tener en cuenta que un vigilante de seguridad adquiere el carácter de agente de la autoridad una vez que es requerido por un miembro de las FFCCSE, como así indica la ley actual, obteniendo protección jurídica, como recogen los artículos 550 y 551 del Código Penal

Pero este artículo no va de la seguridad privada en sí misma, sino de cómo, desde su humilde labor, influye, aporta y suma a la seguridad ciudadana desde su perfil auxiliar a las FFCCSE. Sin entrar en muchos tecnicismos, pero hablando desde mi propia experiencia como vigilante de seguridad y tras haber participado en algunos operativos policiales, de diferente índole, puedo exponer la fluida colaboración entre la seguridad privada y los Cuerpos policiales.

Habitualmente, esta colaboración entre vigilantes de seguridad y policías o Guardias se da en diferentes operativos, que van desde los eventos deportivos y socioculturales a infraestructuras críticas y otros tipos de supuestos.



Podemos citar como ejemplo el control de personas y objetos a los complejos deportivos, por parte de los vigilantes bajo la supervisión de la Policía Nacional, o la vigilancia en las fiestas locales, donde los vigilantes no solo hacen el control de accesos a los eventos municipales, sino que a su vez velan por el buen desarrollo de las actividades y de los equipos técnicos instalados para dichos eventos.

También podemos ver el control de personas y equipajes que realiza la seguridad privada en los aeropuertos bajo la supervisión de la Guardia Civil. En las grandes ciudades, la seguridad privada protege las paradas de metro y, más allá de comprobar que los viajeros entren con el ticket pagado, colaboran activamente en la detección de carteristas y en su detención y puesta en custodia ante la Policía Nacional. Pero también existe otro tipo de colaboración entre la seguridad privada y las FFCCSE. Existen casos donde los vigilantes han formado parte de seguimientos de sospechosos, bajo indicaciones de la Policía Nacional o la Guardia Civil, como en operativos antidrogas en las urbanizaciones de Marbella o Estepona, por ejemplo.

Debemos recordar que la seguridad privada no puede legalmente actuar por iniciativa propia ni establecer un ámbito de investigación en asuntos de seguridad ciudadana. Pero cierto es que en el 90 por ciento de los casos la seguridad privada ya está ahí cuando se produce el delito, siendo la primera en actuar en situaciones de peligro de seguridad ciudadana. En la mayoría de los casos esta labor pasa inadvertida, tanto para la ciudadanía como para los medios de comunicación, ya que en la mayoría de los casos la seguridad privada trabaja desde la humildad con actitud de servicio hacia la ciudadanía. En cualquier caso, es evidente que las administraciones tienen un profundo desconocimiento de la seguridad privada y de su aporte a la seguridad ciudadana

# La particular coordinación entre seguridad privada y Cuerpos de Policía Local, José Antonio Vergara

Como ya hemos dicho, la seguridad privada es un cuerpo auxiliar a las Fuerzas y cuerpos de seguridad, y no será difícil ver en diferentes municipios, tanto grandes como los más pequeños, utilizar a Protección Civil como auxiliar de seguridad. Esto supone un profundo error. Ya desde la ley Ley 2/1985, de 21 de enero sobre Protección Civil, hoy por hoy derogada, se establece que las agrupaciones de Protección Civil son un cuerpo de voluntarios que tan solo pueden adquirir la condición de agentes de seguridad en situaciones de catástrofe o calamidad pública, siempre y cuando estén bajo mando de un agente de la autoridad. Esta directriz sigue vigente en la ley actual Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.

De hecho, ha habido municipios sancionados por utilizar a los operativos de Protección Civil para funciones de seguridad, fuera de su ámbito. ¿Esto es un ataque a la Protección Civil? En absoluto, sino que se trata de dos conceptos diferentes de seguridad las asumidas por la Protección Civil y la seguridad privada. Sin más, creo que queda más que demostrado que la seguridad privada, desde su humilde perfil, contribuye diariamente a la seguridad ciudadana de forma positiva, apoyando sin duda alguna a las Fuerzas y Cuerpos de Seguridad del Estado, como las auténticas herramientas del Estado español, en la defensa de la Constitución Española y del bienestar de todos sus ciudadanos

## José Antonio Vergara, Policía Local

En este punto de la cuestión debemos concretar uno de los niveles más operativos y prácticos de la relación entre la seguridad privada y las Fuerzas y Cuerpos de Seguridad, es decir, la coordinación con los ayuntamientos y, por consiguiente, con sus cuerpos de Policía Local.

Una vez llevado a cabo todo el minucioso proceso de autorización para el efectivo desarrollo de servicios por parte de las empresas de seguridad privada contratadas por las administraciones locales, queda analizar la coordinación que se da entre ambos entes en el nivel operativo, práctico, generalmente en la celebración de eventos públicos como pueden ser ferias locales, espectáculos públicos, etc. Y es que, en el día a día se dan situaciones en las que dicha coordinación brilla por su ausencia, donde los dispositivos de seguridad privada se despliegan conforme a la autorización otorgada (la determinación del espacio físico donde deben llevar a cabo su labor) y conforme a las funciones legalmente conferidas, pero en ningún momento se produce una coordinación efectiva con los responsables policiales locales que cubren dicho evento. Ocurre que, en numerosas ocasiones, la contratación de los servicios de seguridad privada por parte de un ayuntamiento no está centralizada en un área determinada, es decir, que cualquier concejalía puede llevar a cabo una contratación acorde a su presupuesto y para cubrir el evento que particularmente organice (con las debidas autorizaciones y procedimientos administrativos), y ello conlleva a que se produzcan situaciones de falta de comunicación y coordinación con la principal concejalía encargada de la seguridad pública, en la que se incardina el Cuerpo de la Policía Local. Es más, la Policía Local en la mayoría de los municipios es la que cubre los eventos, por lo que la coordinación de la seguridad privada con los Cuerpos de Seguridad del Estado de dichos municipios (póngase como ejemplo al caso la Guardia Civil) es mucho menor. Por tanto, la coordinación con los servicios de seguridad privada durante el desarrollo de los eventos a menudo queda en manos de la iniciativa de los responsables policiales de servicio o de los responsables del dispositivo de seguridad privada. Todo ello sin ánimo de generalizar, pero es la realidad de muchos municipios españoles y, por supuesto, no hablamos de las funciones que deben desarrollar los efectivos de seguridad privada, que están bastante bien delimitadas en la ley, sino del asunto de la coordinación con las Fuerzas y Cuerpos de Seguridad locales.



# José Antonio Vergara

Pues bien, si analizamos la normativa vigente en materia de seguridad privada, la más que conocida Ley 5/2014, de 4 de abril, de Seguridad Privada y la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, podemos desgranar los mecanismos de coordinación establecidos, para acabar en el nivel que nos interesa, el nivel de la administración local. Primero y, aunque pudiera parecer evidente, conviene recordar que el término Fuerzas y Cuerpos de Seguridad incluye a todos los cuerpos policiales con despliegue actual en España, es decir, Policía Nacional (con sus respectivas adscripciones a las Comunidades Autónomas), Guardia Civil, Policías Autonómicas y Policías Locales (artículo segundo de la LO 2/1986).

Por contra, el término Fuerzas y Cuerpos de Seguridad del Estado incluye en exclusiva a la Policía Nacional y a la Guardia Civil (artículo noveno de la meritada Ley Orgánica), ostentando la Policía Nacional la competencia de control de las entidades y servicios privados de seguridad, vigilancia e investigación, de su personal, medios y actuaciones (artículo doceavo). Resulta interesante ver cómo se refiere a la competencia de "control de sus actuaciones" cuando en la inmensa mayoría de los municipios no se encuentra desplegado dicho cuerpo policial y, aunque pudiera encargarse la Guardia Civil de forma subsidiaria, no es el caso como hemos indicado más arriba. Por tanto, sigamos analizando la normativa, donde encontramos como origen de la coordinación el artículo cuarto, punto segundo de la LO 2/1986:

**2. Las personas y entidades que ejerzan funciones de vigilancia, seguridad o custodia referidas a personal y bienes o servicios de titularidad pública o privada tienen especial obligación de auxiliar o colaborar en todo momento con las Fuerzas y Cuerpos de Seguridad.**

Por otra parte, en el preámbulo de la Ley 5/2014 se establece que "para que la actuación de las distintas administraciones públicas sea coherente con el mantenimiento de la armonía del sistema, es fundamental incidir en los principios de coordinación y cooperación interadministrativa. Al objeto de evitar interferencias y duplicidades, se prevén mecanismos de coordinación institucional, se clarifica el reparto de competencias estatales y autonómicas, se afianza la competencia exclusiva del Estado en materia normativa y se sitúan en la órbita ejecutiva las competencias de las comunidades autónomas". Una clara apuesta por la coordinación, pero como se puede observar, se deja fuera a la administración local y, además, parece que solo aluda a las Comunidades Autónomas con competencias adquiridas en materia de protección de personas y bienes y el mantenimiento del orden público, por lo que el resto de Comunidades (la mayoría) no entrarían, en principio, en esa declaración de intenciones, aunque cierto es que alguna de ellas presentan competencias

ejecutivas en esta materia, tal y como es el caso de la Comunidad Autónoma de Andalucía que establece en el artículo 67 de su Estatuto que "corresponden a la Comunidad Autónoma competencias ejecutivas en materia de seguridad privada cuando así lo establezca la legislación del Estado". A continuación, en el preámbulo de la ley se establece un objetivo fundamental en relación al tema que nos ocupa, concretamente que el Título I destaca la importancia de la coordinación entre seguridad privada y Fuerzas de Seguridad, para mejorar la seguridad pública mediante el intercambio legal de información y órganos de encuentro más proactivos.

Dicho principio se origina en el artículo 1 de la propia ley, aunque no es hasta los artículos doce y trece donde volvemos a encontrar el término coordinación, en las competencias de la Administración General del Estado y de las comunidades autónomas respectivamente. En el primero vemos la competencia para la coordinación de los servicios de seguridad e investigación privadas con los de las Fuerzas y Cuerpos de Seguridad del Estado, y en el segundo la competencia para la coordinación de los servicios de seguridad e investigación privadas prestados en la comunidad autónoma con los de la policía autonómica y las policías locales. Destacamos aquí la incorporación a los términos de coordinación a los Cuerpos de Policía Local, aunque no podemos dejar de reseñar que el artículo trece se refiere solo a las comunidades autónomas con competencias para la protección de personas y bienes y para el mantenimiento del orden público.

El artículo dieciséis vuelve a incidir en la creación de órganos de coordinación, pero en la misma línea de Estado - comunidades autónomas con competencias asumidas. Por último, la ley al fin establece una obligación en el ámbito de la coordinación general con las Fuerzas y Cuerpos de Seguridad, donde por supuesto se incluyen las Policías Locales, concretamente en el artículo 41.2:

**"2. Requerirán autorización previa por parte del órgano competente los siguientes servicios de vigilancia y protección, que se prestarán en coordinación, cuando proceda, con las Fuerzas y Cuerpos de Seguridad, y de acuerdo con sus instrucciones: c) La vigilancia en acontecimientos culturales, deportivos o cualquier otro evento de relevancia social que se desarrolle en vías o espacios públicos o de uso común, en coordinación, en todo caso, con las Fuerzas y Cuerpos de Seguridad".**



# SEGUROS DE VIDA: UNA PROTECCIÓN IMPRESCINDIBLE PARA LOS PROFESIONALES DE LA SEGURIDAD

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

## Alina Rubio de las Casas Experta en Seguros Generales

La profesión de la seguridad privada se caracteriza por una realidad innegable: el riesgo es parte de la jornada laboral. Desde vigilantes en espacios conflictivos hasta escoltas en misiones de alta responsabilidad, todos los profesionales del sector conviven con situaciones que pueden poner en compromiso no solo su integridad física, sino también la estabilidad de sus familias.

**Agente exclusivo, Generali Seguros**  
**Planes diseñados a medida de tus necesidades,**  
**con atención directa y profesional**  
**[alinarubiodecasas@gmail.com](mailto:alinarubiodecasas@gmail.com)**



En este contexto, el seguro de vida no debe ser entendido como un gasto, sino como una inversión estratégica. Proporciona una cobertura esencial que garantiza que, en caso de accidente o fallecimiento, los familiares directos cuenten con un respaldo económico que les permita mantener su calidad de vida. Para quienes trabajan en seguridad, donde la exposición al peligro es mayor que en otras profesiones, esta previsión adquiere un valor aún más evidente.

Además, los seguros de vida ofrecen una doble función:

- Tranquilidad personal, al saber que cualquier eventualidad no dejará a la familia desprotegida.
- Seguridad colectiva, al reforzar la imagen del sector como una profesión responsable, donde se piensa no solo en el servicio que se presta, sino también en el bienestar integral de quienes lo ejercen.

La importancia de contar con esta cobertura debería formar parte de la cultura corporativa de las empresas de seguridad, integrándola como un beneficio laboral y como un mensaje de cuidado hacia sus empleados. Y, al mismo tiempo, debería ser una decisión individual de cada profesional, consciente de que su labor exige contemplar escenarios de riesgo que no siempre se pueden evitar.

En definitiva, en una profesión que protege a los demás, el seguro de vida se convierte en el mecanismo más honesto y coherente para proteger a quienes más importan: nuestras familias.

Un seguro de vida adaptado al sector de la seguridad no es un gasto, es una inversión. Aporta tranquilidad al trabajador, refuerza la confianza de su familia y proyecta una imagen responsable de la empresa que lo ofrece como beneficio.

En un sector donde la exposición al peligro es constante, garantizar una cobertura sólida no solo es un acto de justicia, es también una ventaja competitiva: atrae talento, fideliza a los equipos y muestra compromiso real con quienes sostienen la seguridad de todos.

**Invertir en seguros de vida para profesionales de la seguridad es, en definitiva, proteger a quienes protegen.**



*Alina Rubio*

Protejo lo que más importa: tu patrimonio,  
tu familia y tu tranquilidad.

 GRUPO BORRERO

# 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 todas 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.

# CIBERSEGURIDAD: NAVEGANDO POR EL GLOBO DIGITAL.

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

## Elena de la Parte

**En nuestra editorial prevalece la: ética, seguridad, protección de datos y la ciberseguridad. En este artículo, abordó un tema crucial: el Reglamento de la IA de la Unión Europea. Reglamento (UE) 2024/1689. La ISO/IEC 42001 es una norma técnica internacional para los sistemas de gestión de la IA.**

Imaginemos nuestro mundo digital como un inmenso globo terrestre interactivo de LEGO. Cada país, empresa, institución, individuo, es una compleja construcción de piezas interconectadas. Este globo digital no está quieto: gira constantemente con un flujo ininterrumpido de información tecnológica (TIC). Los ciberataques son como fuerzas invisibles que intentan desestabilizar estas construcciones de LEGO. “Un terremoto digital puede derrumbar los servidores de una empresa”, mientras que un “maremoto de datos” puede robar información crucial. Aquí es donde entra en juego el rol crucial de la ciberseguridad. Visualicemos un UAS, dron de última generación sobrevolando nuestro mapa del mundo. Este dron es el sistema de ciberseguridad que, con una visión panorámica, puede identificar patrones de ataque, detectar piezas debilitadas (vulnerabilidades) y enviar equipos de “reparación”, (parches de seguridad), antes de que el daño sea irreversible. Este dron es nuestro escudo de defensa del mundo digital.

El rol clave de la Regulación y la Geopolítica. El ciberespionaje y los ataques cibernéticos han trascendido su condición de incidentes aislados para erigirse como un pilar fundamental en la agenda de la política exterior. Si nos estuviéramos refiriendo a el ciclismo, el cabeza del pelotón o el maillot amarillo es para China. Posicionándose este país como un actor clave en este ámbito. Actualmente, hay normativas que obligan a las empresas a adherirse y cumplir con toda la protección de datos, incluyendo la RGPD y las regulaciones del mercado financiero. La Ley de ciberseguridad y Resiliencia (DORA) o la Ley NIS2 son ejemplos de esto.

El Reglamento de Inteligencia Artificial (IA Act), de la Unión Europea, no es un capricho Legislativo. Sino una respuesta a la creciente adopción de la IA. Su objetivo es garantizar que los sistemas de IA sean; seguros, confiables, éticos, nítidos y cristalinos, basándose en un enfoque de riesgos:

- Riesgo inaceptable: sistemas que manipulan el comportamiento humano están prohibidos.
- Riesgo limitado: Sistemas que interactúan con nosotros, las personas, como los chatbots. Los desarrolladores y programadores, deben informar a los usuarios que están interactuando con la IA y no con una persona.
- Riesgo alto: Sistemas que tienen un impacto significativo en la vida de las personas, como por ejemplo los utilizados en el departamento de (RRHH), para servir de ayuda en la selección de personal.
- Riesgo mínimo o nulo: La mayoría de las aplicaciones de IA, como los filtros de spam. Están exentas de regulaciones estrictas



**El Reglamento Interno de la IA, se enfoca en garantizar que las herramientas sean seguras y cristalinas.**

La Ley exige que los chatbots, informen claramente a los usuarios que son IA y no una persona u administrador. Además, es de obligado cumplimiento que el uso de los datos personales cumpla con la legislación de RGPD y a que los algoritmos eviten cualquier tipo de sesgo. Para estar preparado y entrenado, debes preguntarte. ¿Qué datos usa la IA? Qué nivel de riesgo posee tu sistema y si este es lo suficientemente transparente. El primer pionero en defender el globo digital, en esta metáfora que hoy podéis leer tras estas líneas fue: EE. UU. En la historia de la ciberseguridad, un actor clave en levantar “este tipo de dron” es Estados Unidos. A finales de los años 80, tras la aparición de virus, gusanos (worm) Malware, Troyano, (Trojan horse), spyware y los demás que se han agregado en el tiempo hasta ahora, .etc .....El gobierno estadounidense fue pionero en la creación del (CERT), Computer Emergency Response Team. Este hito marcó el inicio de la formalización de la ciberseguridad como una disciplina crítica para la seguridad nacional, estableciendo las bases que otros países también lanzarán sus propios “drones de defensa”.

Desde esta Editorial os dejo unos consejos esenciales de ciberseguridad e IA. Con el objetivo de protegerlos en este entorno digital, es crucial seguir una serie de prácticas tanto a nivel personal como empresarial. **Ciberseguridad:**

- Autenticación de Dos factores: (2FA): utiliza siempre 2FA, en tus cuentas para añadir una capa de seguridad extra.
- Contraseñas fuertes y únicas: Usa gestores de contraseñas para crear y recordar contraseñas fuertes y complejas.
- Actualizaciones constantes: mantén tu software, sistemas operativos y aplicaciones al día para protegerte de vulnerabilidades.

“Si consideramos que cada pieza del engranaje digital, desde el individuo hasta la gran corporación empresarial, está unida por un hilo invisible. El cumplimiento normativo, la formación continua actualizada, son las manos expertas, que evitan que una sola pieza de LEGO caiga. Provocando un devastador efecto dominó que tumbaría toda la continuidad empresarial

# EL PAPEL DE LOS DRONES EN LA SEGURIDAD PRIVADA: DE LA VIGILANCIA AÉREA A LA DETECCIÓN DE AMENAZAS

*En la última década, los sistemas de aeronaves no tripuladas (UAS), comúnmente conocidos como drones, han pasado de ser una curiosidad tecnológica a consolidarse como herramientas de alto valor en la vigilancia, la protección de infraestructuras y la gestión de riesgos. El sector de la seguridad privada ya integra drones en servicios avanzados, aprovechando su capacidad para cubrir grandes áreas, reducir tiempos de respuesta y recopilar información en tiempo real. Con la entrada en vigor del Real Decreto 517/2024, que adapta la normativa española a los Reglamentos europeos (UE 2019/947 y 2019/945), el uso de drones se sitúa en un punto de inflexión: es necesario combinar innovación tecnológica, cumplimiento normativo, formación especializada y nuevas estrategias operativas.*

## Drones como complemento estratégico

Los drones no sustituyen a los vigilantes, sino que multiplican sus capacidades.

- En polígonos industriales o parques logísticos, una ronda aérea cubre en minutos lo que un vigilante tardaría decenas de minutos en recorrer.
- En protocolos de verificación de alarmas, el dron se despliega primero para evaluar riesgos sin exponer al personal.
- En seguridad perimetral, la combinación de vigilancia terrestre y aérea reduce vulnerabilidades y aumenta la capacidad disuasoria.

El dron debe entenderse como un recurso táctico integrado, no como un elemento aislado.

## Aplicaciones en infraestructuras críticas

La protección de infraestructuras críticas (centrales eléctricas, plantas industriales, depósitos de agua, puertos o aeropuertos) se beneficia especialmente de las capacidades UAS:

- Cámaras térmicas y multispectrales para detección nocturna.
- Vigilancia de zonas inaccesibles o de riesgo (cubiertas, torres, tuberías elevadas).
- Detección temprana de intrusos antes de que alcancen el vallado perimetral.

Además, el dron aporta un doble valor: seguridad + mantenimiento preventivo, generando mayor retorno de inversión para el cliente final.

## Seguridad en eventos masivos

Conciertos, ferias y romerías representan un reto para la seguridad privada. Los drones permiten:

- Monitorizar flujos de personas y detectar aglomeraciones.
- Vigilar accesos y zonas de riesgo.
- Transmitir imágenes en tiempo real a Centros de Control (CRA) para coordinar la respuesta.

No obstante, operar en espacios urbanos requiere permisos específicos y coordinación con las FCSE, debido a la restricción del espacio aéreo. La formación certificada de los pilotos es decisiva en este contexto.



## La amenaza de los drones hostiles

El auge de drones hostiles o no autorizados plantea un desafío adicional:

- Espionaje industrial.
- Introducción de contrabando en prisiones.
- Interferencia en aeropuertos o instalaciones sensibles.

Aunque la neutralización activa (inhibidores, sistemas antidron) está restringida a las FCSE, la seguridad privada puede ser la primera línea de detección mediante sistemas de monitorización RF, sensores acústicos y protocolos de alerta inmediata.

## Formación y cumplimiento normativo

El RD 517/2024 introduce cambios clave:

- Formación de pilotos UAS en niveles A1/A3 y A2, además de escenarios estándar (STS).
- Nuevos requisitos de seguro adaptados al riesgo operacional.
- U-Space y zonificación del espacio aéreo, que obligan a las empresas a actualizar constantemente sus mapas y software.

La formación continua y el cumplimiento riguroso del marco legal se convierten en factores competitivos en el sector.

## Ciberseguridad y protección de datos

Los drones son también sistemas conectados, vulnerables a ataques:

- GPS spoofing: manipulación de coordenadas.
- Jamming: bloqueo de señales de control.
- Hackeo de vídeo y telemetría.
- Filtración de datos sensibles recogidos en operaciones.

Las empresas deben implementar protocolos de ciberseguridad específicos, desde el cifrado de comunicaciones hasta auditorías regulares de firmware, garantizando la confidencialidad y la integridad de la información.

## Inteligencia Artificial aplicada a drones en seguridad privada

La incorporación de IA marca un salto cualitativo en el uso de drones. Dejan de ser un mero "ojo aéreo" para convertirse en sistemas inteligentes capaces de:

- Analizar vídeo en tiempo real para detectar personas, vehículos u objetos sospechosos.
- Identificar patrones de intrusión perimetral o movimientos anómalos.
- Gestionar multitudes, contabilizando personas o detectando aglomeraciones peligrosas.
- Diferenciar mediante visión térmica animales vs. personas en vigilancia nocturna.
- Ejecutar respuestas autónomas: modificar su ruta de vuelo, coordinarse con otros drones o seguir a un intruso de forma automática.

Existen dos modelos de integración de IA:

- IA embarcada: el dron procesa datos localmente, útil en zonas sin cobertura.
- IA centralizada: las imágenes se envían a servidores o plataformas en la nube, donde algoritmos más potentes procesan la información.

La IA reduce la carga de los operadores humanos, pasando de vigilancia pasiva a detección proactiva. No obstante, plantea retos legales y éticos:

- El reconocimiento facial y biométrico está fuertemente regulado en la UE.
- Los algoritmos deben ser transparentes y auditables para evitar sesgos.
- La ciberseguridad debe incluir medidas contra ataques a modelos de IA (data poisoning).

En conclusión, la IA convierte al dron en un actor activo en la seguridad privada, avanzando hacia un modelo de seguridad predictiva.

## Retorno de inversión (ROI)

La inversión en drones y formación se justifica en:

- Reducción de costes en rondas físicas.
- Disminución de riesgos laborales para vigilantes.
- Mayor valor añadido para clientes al ofrecer tecnología avanzada.
- Optimización de recursos humanos mediante asignación a tareas críticas.

## Perspectivas de futuro

Las tendencias más inmediatas en la seguridad privada con drones incluyen:

- Operaciones BVLOS para ampliar autonomía y alcance.
- Enjambres coordinados, capaces de cubrir grandes superficies de manera simultánea.
- IA embarcada cada vez más potente, con algoritmos de autoaprendizaje.
- Integración con smart cities y con plataformas de gestión de emergencias.

## Conclusión

**Los drones ya son una pieza clave en el presente de la seguridad privada. Su verdadero valor está en la integración con vigilantes, centros de control, inteligencia artificial y sistemas de gestión de incidentes. El futuro inmediato apunta a una seguridad preventiva, eficiente y predictiva, en la que los drones, potenciados con IA y respaldados por formación y cumplimiento normativo, se consolidan como un pilar esencial de la vigilancia en el siglo XXI.**

### 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>

# LA CORPORACIÓN BAJO ASEDIO, ESTRATEGIAS DE RESILIENCIA EN UN ENTORNO DE CRISIS SISTÉMICA – SINALOA 2024-2025

**Jonatthan Hermida Sosa SAPPC,  
SAFPC, ISOC, DAS, CPO, GER.**

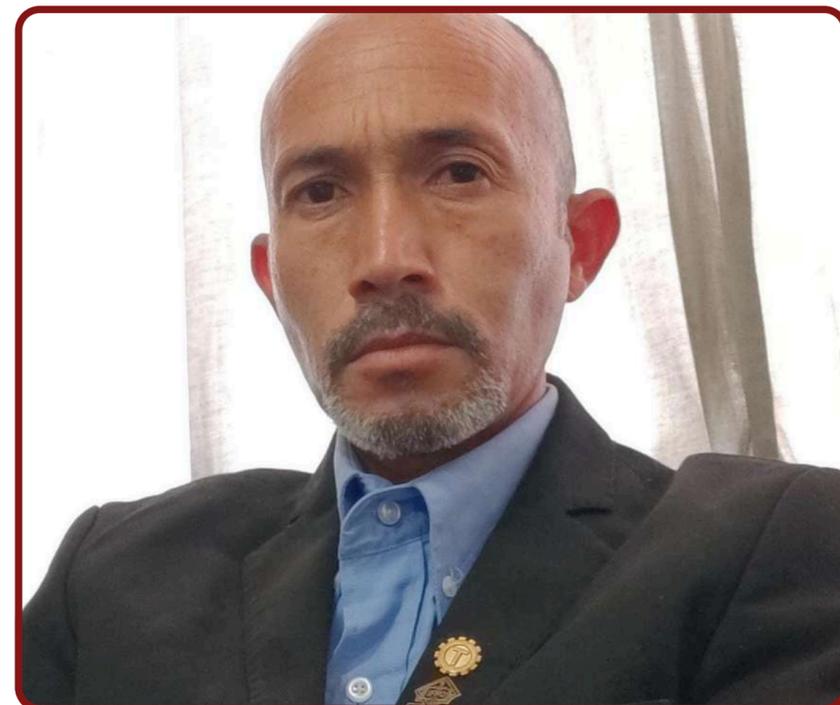
Desde septiembre de 2024 hasta septiembre de 2025, el estado de Sinaloa, México, se ha erigido como un caso de estudio paradigmático y profundamente alarmante sobre los límites de la seguridad pública y los desafíos extremos que enfrenta la seguridad corporativa en el siglo XXI. Este periodo, marcado por una escalada de violencia multifacética, no solo ha desgarrado el tejido social sino que ha forzado una reingeniería total de los paradigmas de protección empresarial, situando a los directores de seguridad en una encrucijada donde deben actuar como diplomáticos, analistas de riesgo geopolítico y estrategias militares, todo al mismo tiempo.

El contexto es la guerra abierta entre el Cártel de Sinaloa—fracturado tras eventos carcelarios y disputas de liderazgo ampliamente reportados—y el Cártel Jalisco Nueva Generación (CJNG), por el control de plazas, corredores logísticos y mercados locales de extorsión. Este conflicto, lejos de ser una mera disputa delictiva, se ha convertido en una fuerza desestabilizadora de primer orden, cuyas repercusiones económicas reverberan desde las pequeñas comercios de Culiacán hasta las cadenas de suministro globales que dependen de los puertos y corredores agrícolas del estado. La economía local ha enfrentado una contracción severa; según estimaciones de cámaras empresariales, la inversión privada se contrajo un 22% interanual, mientras que sectores clave como el agroindustrial y el turístico reportan pérdidas billonarias por vandalismo, bloqueos carreteros, una táctica de presión constante, y el “impuesto de guerra” que grupos delictivos imponen a transportistas y empresarios, paralizando la libre circulación de mercancías.

Dos eventos durante este periodo funcionaron como puntos de inflexión que encapsularon la gravedad de la crisis para la comunidad empresarial internacional. Primero, la suspensión sin precedentes de las festividades del Grito de Independencia en septiembre de 2024 y septiembre 2025 (dos años consecutivos) en múltiples municipios, incluida la capital, Culiacán, por “motivos de seguridad”. Esta decisión gubernamental, un acto de realpolitik sombría, envió una señal inequívoca al mundo: la autoridad estatal había sido temporalmente suplantada, y el simbolismo de la soberanía nacional cedía ante la pragmática de la supervivencia. Para un director de seguridad corporativa, este evento no fue una anécdota cultural, sino el indicador último del nivel de amenaza, obligando a reevaluar la continuidad operativa de instalaciones y la seguridad del personal expatriado en fechas críticas. Segundo, la ola de marchas y protestas, muchas de ellas cooptadas o instigadas por actores criminales, que bloquearon infraestructura vital, como la carretera federal 15D, y los homicidios selectivos de empresarios y funcionarios, que alcanzaron cifras récord, crearon un ambiente de terror psicológico que es tan dañino para los negocios como la violencia física. Medios como The Financial Times y The Wall Street Journal han documentado en sus reportes desde “México’s Heartland” cómo estas tácticas han llevado a una fuga de capitales y a un colapso en la confianza del consumidor, comparando el clima de inversión con el de regiones en conflicto activo de baja intensidad.

**Autor: Licenciado en Seguridad Pública y Criminología.**

**Jonatthan Hermida Sosa**  
[www.hermidaseguridad.org](http://www.hermidaseguridad.org)



Ante este panorama, los responsables de seguridad corporativa han tenido que evolucionar de gestores de riesgos tradicionales a arquitectos de resiliencia integral. Los retos son monumentales: la hibridación de las amenazas, donde un bloqueo carretero (una protesta aparentemente social) es en realidad una operación del crimen organizado, requiere capacidades analíticas de inteligencia para discernir el origen real de la disrupción. Las estrategias ahora son holísticas: la segmentación y redundancia de las cadenas de suministro, utilizando tecnología satelital y GPS para redirigir convoyes en tiempo real; la ciber-seguridad reforzada para proteger datos sensibles de extorsión digital; la formación avanzada del personal en protocolos de secuestro y confinamiento; y, crucialmente, la diplomacia corporativa con actores locales y nacionales para navegar el complejo panorama. La militarización del estado, con la Guardia Nacional y el ejército desplegados en tareas de seguridad ciudadana, reemplazando de facto a corporaciones policiales locales consideradas corruptas o infiltradas, crea un escenario paradójico. Por un lado, ofrece una fuerza de disuasión de mayor capacidad y, se presume, menor corrupción, lo que puede garantizar corredores seguros para operaciones críticas. Por otro, como señalan analistas de International Crisis Group en contextos similares, la militarización prolongada erosiona las libertades civiles, puede generar fricciones con las comunidades y no aborda las causas raíz de la criminalidad, manteniendo el riesgo latente. La seguridad corporativa debe, por tanto, operar en esta dualidad: coordinar logística con mandos castrenses mientras mantiene su independencia operativa y compromiso ético

*Finalmente, la comparación con países bélicos o en estado de conflicto permanente no es hiperbólica sino analítica. Sinaloa, en este periodo, presentó indicadores de violencia, homicidios por cada 100,000 habitantes, desplazamiento forzado, control territorial por facciones no estatales, que rivalizan con los de regiones en conflicto en otras latitudes. La lección para la seguridad corporativa global es clara: el mapa de riesgos geopolíticos ya no solo incluye estados fallidos en continentes lejanos; incluye enclaves dentro de naciones con economías emergentes G20 donde el monopolio estatal de la fuerza está en entredicho. La resiliencia ya no es opcional; es la nueva currency de la supervivencia empresarial.*

# INSEGURIDAD EN VENEZUELA: DONDE EL CRIMEN Y LA POLÍTICA VIVEN EN CONCUBINATO

**Carlos Enrique Perez Barrios**  
Director General de GLOBAL  
SECURITY ACADEMY USA

## En clave política

De "Tierra de Gracia" a tierra de miedo.

Es muy importante poner sobre la mesa un tema tan terrible como temible: la relación entre la política y el crimen, que ha convertido el diario vivir en Venezuela en sencillamente, un asunto de supervivencia. La otra Venezuela, Tierra de Gracia, país en franco desarrollo donde se recibía al extranjero con aprecio y los brazos abiertos, quedó atrás. La seguridad de los años previos a la tiranía comunista y criminal del socialismo del siglo XXI se fue esfumando, transformando el pujante y alegre ambiente social, en un entorno peligroso para todos sus habitantes.

### El concubinato político-criminal

¿Qué pasó? ¿Cómo se generó esta triste y peligrosa realidad?

En mi opinión, la política y el crimen se conocieron y se enamoraron, convirtiéndose en enfermizos concubinos que transformaron negativamente la vida de los venezolanos. Desde el inicio, el régimen chavista buscó generar, mantener y profundizar la relación entre criminales, civiles y militares, y lo hizo de múltiples formas.

### Los colectivos: brazo armado de la revolución

Hugo Chávez y su corte se encargaron de crear un ambiente oscuro, donde las bandas delincuenciales pasaron a ser consideradas como el brazo armado de la revolución. Esto convirtió a organismos de seguridad, cuerpos de investigación, jueces, fiscales y el sistema penitenciario en concubinos de hecho y derecho del mundo criminal. Poco a poco, paso a paso las instituciones del Estado ya no responden a códigos morales, solo estaban al servicio de los intereses del régimen que, en todos sus actos, y por acción u omisión dejaron de servir al pueblo para convertirse en miembros activos de una banda criminal con objetivos e intereses inconfesables.

Los llamados colectivos chavistas fueron dotados de armamento por parte de miembros de las Fuerzas Armadas, recibieron importantes financiamientos, y fueron y siguen siendo protegidos por el gobierno, mientras la oposición, observaba un silencio cómplice y complaciente, abandonando a su suerte a la gente que decían representar.

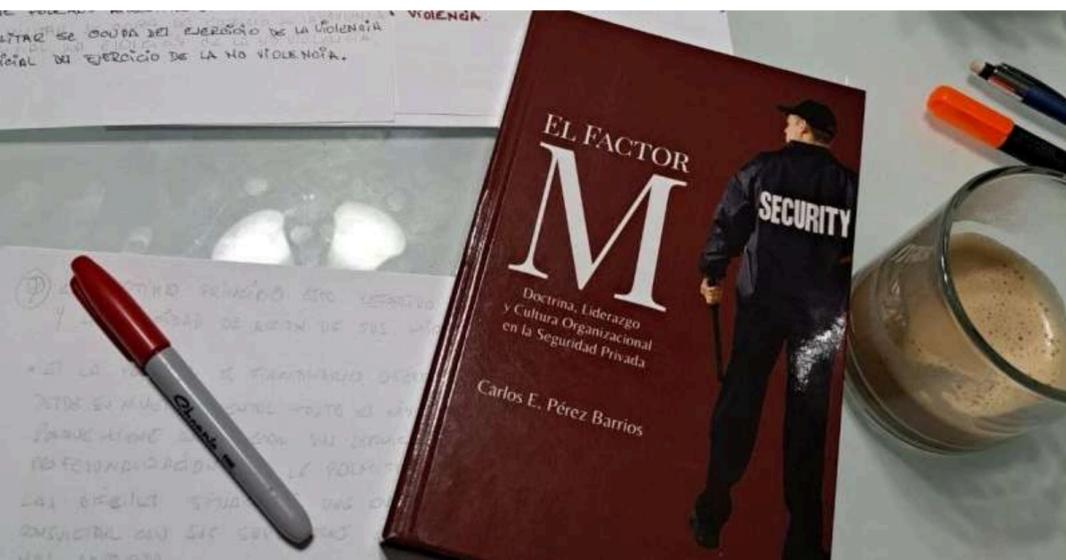


### La corrupción de las Fuerzas Armadas

Otro elemento clave fue la destrucción moral de las Fuerzas Armadas. El régimen propició que el germen de la corrupción hiciera metástasis en sus miembros, inyectando a través de programas sociales disfrazados cantidades millonarias de dinero sin control alguno. La primera medida que tomó Hugo Chavez, ya como Presidente y Comandante en Jefe de las Fuerzas Armadas fue el Plan Bolívar 2000. Era supuestamente un programa de acción social, pero su objetivo estratégico no era otro que corromper a los militares, de todos los niveles de la organización. Eso pudrió las bases morales del sector castrense y fortaleció la pandilla criminal chavista.

### Zonas de paz y entrega del territorio

No solo se quebró la institución militar con dinero mal habido. También se instalaron las llamadas zonas de paz en centros urbanos y estados fronterizos, donde se ordenó a las unidades militares no actuar contra grupos guerrilleros colombianos como la FARC y el M19. Estas fuerzas guerrilleras colombianas, dedicadas al crimen y el narcotráfico, encontraron en los Estados fronterizos, en territorio Venezolano, una zona de alivio, de descanso con facilidades sanitarias y bajo la protección del régimen chavista, su paraguas ideológico y su socio en el negocio internacional de las drogas. Con el tiempo, estas fuerzas extranjeras criminales y narcotraficantes pasaron a controlar pueblos, rutas y economías locales, consolidando un corredor de narcotráfico y violencia en territorio venezolano pisoteando la soberanía venezolana.





# Carlos E Pérez Barrios

## “En clave política”

### Cárceles bajo el poder de los pranés

El sistema penitenciario no escapó a esta lógica de entrega del poder al crimen. Al igual que en las “zonas de paz”, las cárceles fueron abandonadas por el Estado y entregadas al dominio de los pranés, líderes criminales que convirtieron los recintos penitenciarios en verdaderos territorios autónomos. Desde esas cárceles, los pranés organizaban bandas dedicadas a la extorsión, secuestros, tráfico de drogas y armas, proyectando su poder fuera de los espacios penitenciarios, y convirtiendo las prisiones, de manera increíble, en espacios con todo tipo de comodidades, discotecas, bares, bancos, centros de comunicaciones y otras facilidades que le permitían dirigir sus operaciones con la mayor facilidad, seguridad e impunidad. Con el tiempo, estas estructuras se convirtieron en artículos de exportación, irradiando el crimen hacia países vecinos e incluso hacia los Estados Unidos, transformándose en herramientas de destrucción y violencia en toda América, con organizaciones internacionales de todo tipo de delitos, narcotráfico, extorsión, prostitución y sicariato, teniendo como ejemplo bandera, la organización llamada el Tren de Aragua.

### Evidencias internacionales

Diversas fuentes de reconocida solvencia avalan este diagnóstico:

- Observatorio Venezolano de la Violencia
- Human Rights Watch / Amnistía Internacional
- Departamento de Estado de EE. UU.
- OEA y organizaciones nacionales

Todos coinciden en señalar ejecuciones extrajudiciales, tortura, falta de independencia judicial, impunidad y el franco deterioro del Estado de Derecho.

### El reto de la reconstrucción

Todo este ambiente criminal y de quiebre institucional sólo podrá superarse con el desplazamiento de la mafia en el poder y una ruptura total con el sistema imperante actual. La refundación del país requiere:

- Un gobierno fuerte, exigente en protocolos morales y de justicia.
- Depuración de todos los cuerpos policiales y militares.
- Recuperación de territorios bajo control criminal.
- Reconstrucción del sistema judicial y penitenciario bajo la autoridad real del Estado.
- Construcción de instituciones sólidas, democráticas y éticas.

### Hacia un nuevo pacto moral

Venezuela necesita un nuevo sistema político y un gobierno con total autoridad capaz de sostener esta transición, por los años que sean necesarios, para darle al país la oportunidad de recuperar un sistema democrático, justo y moralmente sólido.

Solo así podremos aspirar a una sociedad más segura, libre y feliz para todos los venezolanos.

*Artículo preparado por Carlos E Pérez Barrios, MSc en Seguridad y Defensa Nacional, experto en Seguridad, Analista Político Militar, Director General de Global Security Academy, Profesor Internacional de Seguridad, Gerencia estratégica de Organizaciones de Seguridad Pública y Privada, conferencista internacional y articulista.*

*Es autor de los libros Control de Riesgos y El Factor M Pompano Beach, Florida, USA, Septiembre 29 del 2025*



**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.**

LOS LUNES A LAS 22H

**INFORME GALINDO**

**JUAN CARLOS GALINDO**

**EL CANAL DEL CORONEL**

**PEDRO BAÑOS**

JUAN CARLOS GALINDO

**CÓMO NO DEFRAUDAR A HACIENDA**

LA GRAN EVASIÓN: DE SUIZA A TU DECLARACIÓN

Con prólogo de Nacho Abad y epílogo de Antonio Naranjo

Juan Carlos Galindo, experto investigador de delitos económicos y un habitual en los platos de televisión, aborda en este libro práctico lo que debes hacer para evitar problemas en tu declaración de la renta y explica con pelos y señales los métodos que usan los malos para engañar. Lo hace con erudición y humor, repasando tanto el sentido de los impuestos como los casos más famosos, de Shakira y Messi a la gran migración de los youtubers a Andorra. Porque, ya se sabe, Hacienda somos todos, incluso tú.

- ¿Sabes la diferencia entre evadir y eludir?
- ¿Que hay países donde llega el dinero y desaparece por arte de magia?
- ¿Que Hacienda podrá ver muy pronto tus movimientos en las tarjetas de crédito?

«Antes de que el Gobierno les haga levantar las manos, aprovechen y úsenlas para leer este manual de supervivencia en tiempos de cólera fiscal».

Antonio Naranjo, periodista

la esfera de los libros  
www.esferalibros.com

**1er. Encuentro AIMCE CAP. ECUADOR/25**

**“Sociedad Conectada: Innovación Digital y Resiliencia en la Gestión de Emergencias”**

**Fecha:** sábado 4 octubre 2025  
**Hora:** 09:00 Hs. GMT-5 Quito  
**Modalidad:** Virtual (Gratuito)

- La tecnología al servicio de la seguridad.
- Inclusión digital accesible a la sociedad.
- Creación de redes ciudadanas colaborativas.

CFDSS EN LA MIRA COP INTERFIRENSIS seIN NATIONAL AIMCE

**PERCEBE87®**

**DIVULGADOR**

DEBATES - NOTICIAS - ACTUALIDAD



# Metrorisk

# Proyecto Asociativo

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