

# EDITORIAL MR



ISSN 3045-7629

ESPECIAL  
NAVIDAD

AÑO  
2025/26

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz  
Francisco Javier Gonzales Fuentes  
Carlos G. Barrett  
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.



# CERRAMOS UN AÑO Y ABRIMOS OTRO CON UNA MISIÓN COMÚN: UN 2026 MÁS SEGURO

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Fran Medina Cruz**  
Director de MetroRisk

Terminamos un año intenso para quienes trabajamos en el ámbito de la seguridad. Un año que vuelve a recordarnos que nuestra profesión no es un mero engranaje en el sistema social: es un pilar silencioso, imprescindible, que sostiene el día a día de miles de personas, infraestructuras y organizaciones.

En estas fechas en las que el calendario se detiene y nos invita a mirar hacia atrás, quiero felicitar las fiestas a todos nuestros lectores, colaboradores y compañeros de sector. A quienes impulsan cada día un enfoque más profesional, más innovador y más consciente del papel que la seguridad tiene en la sociedad actual.

Pero esta felicitación tiene también un nombre propio: los verdaderos héroes cotidianos.

A los vigilantes de seguridad que comienzan su turno cuando la ciudad duerme, que permanecen en condiciones difíciles, a menudo invisibles para la mayoría, pero presentes y alerta para todos. Ellos representan la esencia de nuestra actividad: vocación, responsabilidad y riesgo. Un trabajo exigente y, muchas veces, incomprendido, pero absolutamente esencial.

A los directores y consultores de seguridad que actúan como arquitectos del riesgo, diseñando estrategias, protocolos y soluciones que mantienen operativas empresas, instituciones y entornos urbanos. Son los que se anticipan al problema, analizan cada amenaza y convierten la incertidumbre en planificación. Representan la inteligencia del sector.

Y a todos los profesionales que han impulsado este año la mejora continua, la certificación, la innovación tecnológica y la cultura preventiva. Cada paso que avanza nuestro sector, cada nuevo marco regulatorio, cada proyecto de seguridad, cada aplicación o cada mejora en la cadena de seguridad tiene detrás el trabajo de muchos que aún creen que un mundo más seguro no es una ilusión, sino una responsabilidad compartida.

Este año hemos demostrado una vez más que la seguridad evoluciona con la sociedad, que el futuro ya no es solo la prevención del riesgo, sino la construcción de entornos sostenibles, resilientes y humanos.



Por eso, desde esta revista queremos transmitir un mensaje claro: que el año que viene sea todavía más seguro, más consciente y más innovador.



Que sigamos creando valor desde nuestra profesión, defendiendo la importancia del análisis, del diagnóstico, de la planificación estratégica y de la seguridad como motor de progreso y bienestar.

Que afrontemos el 2026 con el compromiso que nos define y con el orgullo de saber que nuestra labor importa. Que somos parte de la solución, parte de la protección y parte del avance social.

Felices fiestas a todos los que formáis este gran sector.

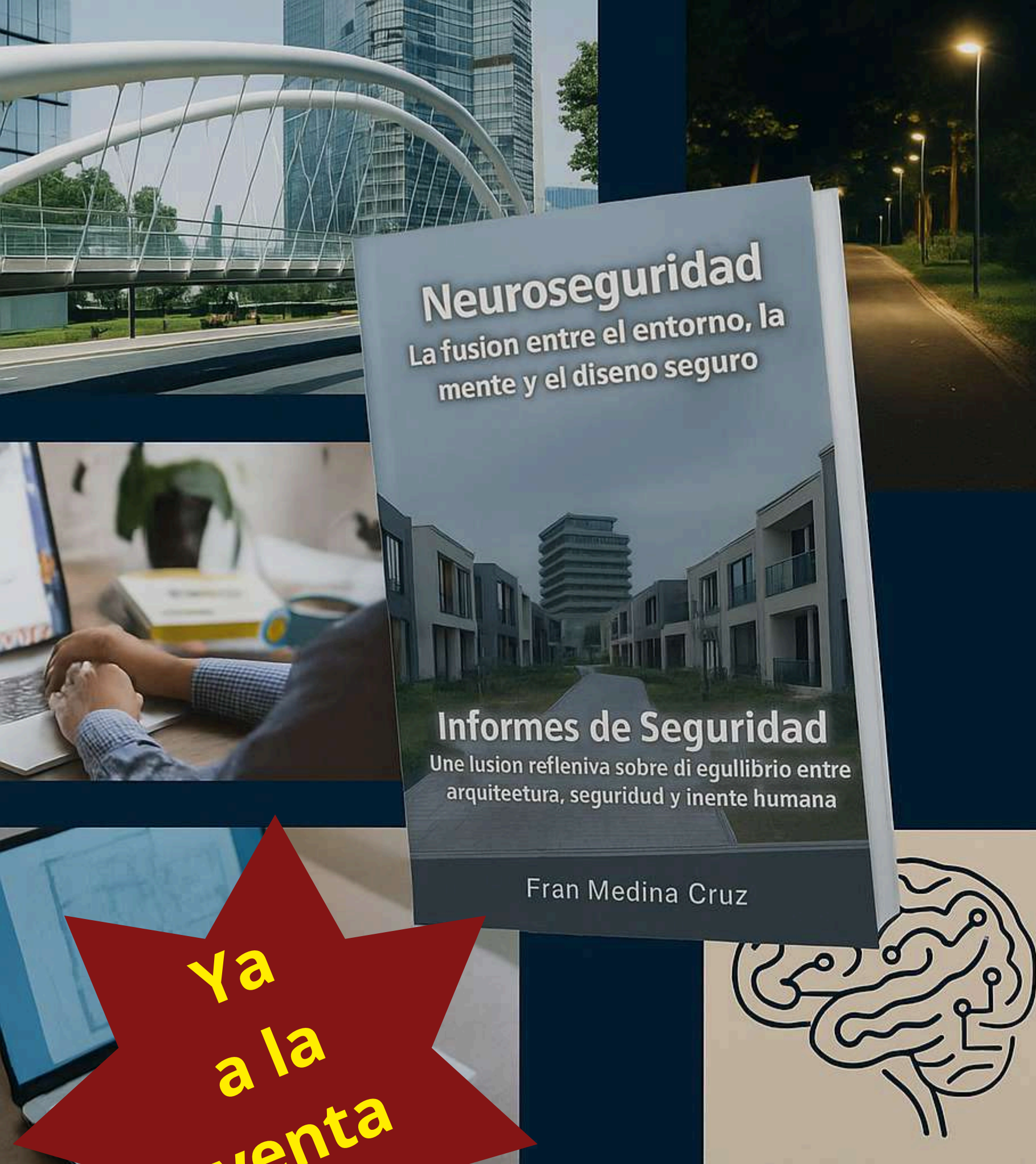
Que el nuevo año llegue con salud, éxito, sostenibilidad y seguridad.

Porque nuestro trabajo no solo protege edificios o activos: protege vidas, proyectos y futuro.

**Feliz y seguro 2026.**







Una nueva visión  
sobre la seguridad:  
el equilibrio entre  
mente, entorno y  
diseño urbano

Disponible ahora

Fran Medina Cruz  
MRConsulting

# NEUROSEGURIDAD

El equilibrio entre la mente,  
el entorno y la seguridad

*La seguridad no solo se construye,  
también se siente.*

Fran Medina Cruz · MRConsulting

MRconsulting

Felices  
Fiestas



*Felices Fiestas*

y un 2026 lleno de  
buenos proyectos



*Fran Medina*



# IBEROSEC: CERTIFICACIÓN PROFESIONAL DE REFERENCIA PARA LA SEGURIDAD Y EMERGENCIAS EN IBEROAMÉRICA

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

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

En un contexto global cada vez más complejo, con desafíos crecientes en seguridad corporativa, emergencias, ciberseguridad e inteligencia corporativa... la profesionalización del sector se convierte en una necesidad ineludible. Con ese objetivo nació la certificación IBEROSEC - FIBSEM & Bureau Veritas, una iniciativa conjunta que aspira a elevar los estándares de formación y competencia de los profesionales de seguridad y emergencias en Iberoamérica.



La certificación cuenta con el respaldo de las asociaciones que integran el foro, entre ellas la ADISPO (Asociación de Directores de Seguridad) y la AIMCSE (Asociación Internacional de Miembros de Cuerpos de Seguridad y Emergencias), lo que le dota de una amplia base de profesionales, más de 5.000 socios en la comunidad FIBSEM, y una presencia significativa en el ámbito iberoamericano.

**¿Qué ofrece IBEROSEC?** La certificación IBEROSEC propone un sistema de acreditación profesional que combina formación, evaluación de competencias y reconocimiento formal, con alcance internacional.

Áreas de especialización disponibles actualmente:

- Seguridad Corporativa
- Prevención de Riesgos
- Emergencias
- Protección Contra Incendios
- Inteligencia Corporativa
- Seguridad Integral y Ciberseguridad

**Destinatarios: quiénes pueden optar a la certificación**

Podrán postularse como candidatos todos aquellos profesionales vinculados al ámbito de la seguridad y emergencias que sean socios de FIBSEM a través de ADISPO o AIMCSE. Esta condición garantiza que la certificación esté destinada a profesionales comprometidos con la seguridad pública, privada, emergencias, protección civil, prevención de riesgos, inteligencia, entre otros campos afines —tal como tu perfil lo evidencia.

Itinerarios formativos: formación a través de la Universidad Corporativa FIBSEM + EducaPro Para preparar a los candidatos, la Universidad Corporativa FIBSEM, en colaboración con EducaPro, ofrece una plataforma de formación especializada, adaptada a los requerimientos de la certificación IBEROSEC.



## Características de la formación

- Acceso a un catálogo amplio de cursos: desde especialidades técnicas hasta formación transversal.
- Programas adaptados a cada área de certificación: Seguridad Corporativa, Emergencias, Inteligencia, Ciberseguridad, etc.
- Flexibilidad: formación online, autogestionable —ideal para profesionales con cargas laborales intensas—.
- Valor añadido: para socios de ADISPO/AIMCSE la cuota anual es reducida — permitiendo acceso ilimitado a los programas formativos.

De esta manera, la formación prepara al candidato no solo desde un punto de vista teórico, sino también práctico y actualizado, alineada con las exigencias reales del sector.

## Proceso de acreditación: de la candidatura al certificado

1. Candidatura: El profesional interesado, siendo socio de FIBSEM por ADISPO o AIMCSE, descarga y rellena el formulario de candidatura, y lo envía a la dirección indicada por FIBSEM.
2. Formación: Accede al itinerario formativo correspondiente mediante la Universidad Corporativa FIBSEM / EducaPro, completando los módulos necesarios según la especialidad elegida.
3. Evaluación: Una vez completada la formación, el candidato debe superar los exámenes oficiales convocados por Bureau Veritas.
4. Certificación: Tras superar la evaluación, el aspirante obtiene la certificación IBEROSEC —aval de competencia profesional reconocida internacionalmente.
5. Seguimiento / mantenimiento (según lo que defina Bureau Veritas en su esquema de certificación de personas). En general, las certificaciones gestionadas por Bureau Veritas incluyen auditorías de seguimiento y recertificación en plazos definidos.



**IntelForensic**  
**G&F Soluciones**





**Este proceso combina formación, acreditación formal y control de calidad, garantizando que la certificación mantenga su prestigio y validez**

#### **Ventajas de IBEROSEC para profesionales de seguridad en Iberoamérica**

- Reconocimiento internacional: Al estar certificada por Bureau Veritas, la credencial tiene un respaldo reconocido globalmente, lo que potencia la movilidad profesional y la confianza del mercado.
- Profesionalización del sector: Con estándares unificados, la certificación promueve la elevación del perfil profesional y profesionalización real, algo clave en entornos de seguridad y emergencias.
- Acceso a formación especializada y actualizada: A través de la Universidad Corporativa, los profesionales pueden actualizar competencias técnicas, tácticas y estratégicas, adaptadas a las realidades iberoamericanas.
- Red de profesionales: Formar parte de una comunidad amplia (FIBSEM + ADISPO + AIMCSE), lo que facilita intercambio de experiencias, colaboración transnacional y sinergias profesionales.
- Valor añadido en empleabilidad y prestigio: Para quien ya trabaja —o aspira a trabajar— en seguridad privada, emergencias, consultoría, peritaje, inteligencia corporativa, etc., la certificación aporta un distintivo de calidad diferencial.
- Flexibilidad y accesibilidad: A través de formación online, cuotas asequibles para socios, y posibilidad de seguir trabajando mientras se certifica.

#### **Importancia estratégica de IBEROSEC en el contexto iberoamericano.**

La realidad latinoamericana y española en materia de seguridad y emergencias demanda cada vez más profesionales cualificados, versátiles y con formación homologada. Con IBEROSEC se da un paso decisivo hacia la consolidación de un estándar iberoamericano que:

- Homogeneiza criterios de competencia entre distintos países y jurisdicciones.
- Facilita la colaboración internacional en operaciones de seguridad, emergencias, inteligencia y protección.
- Eleva los niveles de exigencia profesional, lo que redundará en un mejor servicio a la sociedad en materia de seguridad, prevención de riesgos, emergencias y protección.

Además, para asociaciones como ADISPO y AIMCSE, IBEROSEC supone un instrumento potente de valor añadido para sus socios: un reconocimiento formal que refuerza la profesionalidad del colectivo y su compromiso con la excelencia.

#### **Conclusión**

La certificación IBEROSEC – promovida por FIBSEM en alianza con Bureau Veritas — representa una oportunidad histórica para los profesionales de la seguridad y emergencias en Iberoamérica. Una formación de calidad, acreditación internacional y pertenencia a una red amplia de profesionales. Para quienes —como tú— ya cuentan con una dilatada experiencia en seguridad, policía, protección, consultoría o inteligencia, IBEROSEC ofrece no solo un sello de reconocimiento. También un camino para consolidar su perfil, abrir nuevas oportunidades laborales y reforzar su compromiso profesional con los estándares más exigentes.





# ESTIMADO LECTOR: FELICES FIESTAS Y PROSPERO 2026 INVESTIGACIÓN PRIVADA.

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Carlos G. Barrett**  
Gerente general en Spy Investigación & Barrett

En estas fechas en las que el tiempo parece detenerse un instante para permitirnos mirar hacia atrás y reconocer lo aprendido, deseo compartir una reflexión profunda sobre el valor real que la investigación privada aporta a nuestra sociedad. Resulta especialmente significativo hacerlo ahora, cuando la Navidad nos invita a la serenidad, a la claridad y a volver a confiar en aquello que sostiene la convivencia y la justicia cotidiana. Dentro de ese entramado silencioso pero imprescindible se encuentra la labor del investigador privado, un profesional que opera allí donde los hechos deben ser esclarecidos, donde la verdad necesita ser reconstruida y donde la seguridad requiere información precisa, verificada y útil.

La investigación privada se ha convertido en una herramienta esencial para ciudadanos, empresas y administraciones que necesitan respuestas fiables en un contexto cada vez más complejo. Su importancia radica en que permite abordar conflictos, dudas o situaciones que no pueden esperar a procesos lentos ni pueden resolverse desde la intuición, sino mediante la obtención técnica y metódica de datos sustentados en la ética, la legalidad y la profesionalidad. Este trabajo discreto ofrece garantías, aporta transparencia donde antes había incertidumbre y permite tomar decisiones fundamentadas que protegen derechos, intereses legítimos y la integridad de las personas y de las organizaciones.

Cuando un investigador privado interviene, lo hace desde la responsabilidad de preservar la verdad objetiva, entendiendo que su misión no es solo descifrar hechos, sino sostener el equilibrio que permite que la sociedad funcione sin caer en la desconfianza permanente. Su labor se apoya en la observación rigurosa, en la recopilación sistemática de indicios, en la verificación de versiones contrapuestas y en la construcción de un relato comprobado que ayuda a resolver disputas laborales, familiares, empresariales o patrimoniales. En ese sentido, su papel es una pieza clave del ecosistema de seguridad, porque allí donde existe información precisa y bien documentada, existe también justicia posible, decisiones acertadas y prevención de riesgos.

La investigación privada es, además, un ejercicio de responsabilidad social. Al intervenir en situaciones sensibles, evita que los conflictos escalen, permite detectar vulnerabilidades ocultas y contribuye a que las organizaciones adopten mejores prácticas de gestión y control. Es una profesión que actúa en silencio, sin protagonismos, pero cuyo impacto se refleja en la mejora de la convivencia, en la protección de activos y en el fortalecimiento de la confianza ciudadana. En un mundo donde la desinformación y la apariencias pueden confundir, el trabajo del investigador privado representa una brújula que devuelve orientación y claridad.

**Nuestros Servicios**

- Empresas**  
El encargo de investigaciones empresariales se ha convertido en un hábito común y usual en el mundo empresarial. Las empresas de investigación que quieren mantener y aumentar su posición en ...
- Aseguradoras y Mutuas**  
El sector de las compañías aseguradoras viene soportando año tras año unos altos costes derivados de la existencia de procesos fraudulentos por parte de algunos de sus asegurados. El pago ...
- Abogados**  
Proporcionamos soporte directo a despachos de abogados, ofreciendo minuciosos informes y constante asesoramiento. Aportamos pruebas testificales válidas ante cualquier proceso judicial, ya sean es ...
- Particulares**  
Las relaciones familiares son la parte más importante en la vida de cualquier persona, tratamos de aportar los medios y mecanismos necesarios para la resolución de posibles problemas en el ...



Por todo ello, este es un buen momento del año para reconocer la dedicación y el compromiso de quienes ejercen esta disciplina, así como de quienes confían en ella como una vía legítima y profesional para resolver incertidumbres. La Navidad nos recuerda la importancia de la paz interior y del orden en nuestras vidas, y pocas actividades contribuyen tan directamente a restablecer la armonía como aquella que busca la verdad con método, discreción y rigor.

Que estas semanas festivas nos inviten a valorar la relevancia social de la investigación privada y nos impulsen a entrar en el nuevo año con una visión renovada sobre la importancia de proteger lo que nos importa a través de la información verificada y la certeza.

Reciba mis mejores deseos para una Feliz Navidad y que el próximo Año Nuevo llegue colmado de salud, serenidad y prosperidad. Que el 2026 nos encuentre más conscientes del valor de la verdad, más comprometidos con la seguridad y más unidos en la convicción de que la investigación privada seguirá siendo un pilar fundamental para una sociedad más justa y confiable.

Con mis más sinceras felicitaciones,

**CARLOS G. BARRETT**

**Investigador Privado  
Experto en Criminalística**



**Gregorio Duro**  
**Técnico en licitaciones y Proyectos**

## RIESGOS SIMÉTRICOS Y ASIMÉTRICOS

Al acercarse el final del año, es natural detenerse un momento para reflexionar sobre los últimos meses y cómo hemos aprendido a comprender mejor los riesgos que nos rodean. Estas fechas nos invitan también a mirar hacia el nuevo año, lleno de proyectos, ideas e ilusiones por descubrir. Con ese ánimo, comparto en Metrorisk este artículo sobre los riesgos simétricos y asimétricos, esperando ofrecer una mirada cercana y útil sobre un tema relevante.

### Comprensión general de los riesgos simétricos

En el ámbito del análisis de riesgos aplicado a la seguridad, los riesgos simétricos constituyen la base tradicional sobre la que históricamente se ha construido la mayor parte de los modelos de evaluación. Se caracterizan por presentar una relación proporcional, estable y comprensible entre la probabilidad de materialización y el impacto previsto, lo que permite estructurar su estudio mediante herramientas clásicas de análisis cuantitativo y cualitativo. Este tipo de riesgo suele derivarse de factores operativos, técnicos o ambientales que generan situaciones repetitivas y, por tanto, susceptibles de ser medidas, comparadas y gestionadas con precisión. Su presencia se vincula habitualmente a incidentes de naturaleza previsible, tales como averías de sistemas eléctricos, fallos mecánicos, desgaste físico de infraestructuras, errores humanos derivados de la actividad rutinaria o actos vandálicos de baja intensidad que se producen dentro de patrones conocidos. La ventaja principal de los riesgos simétricos es que permiten incorporar datos históricos, estadísticas internas, registros de incidencias y modelos de recurrencia, ofreciendo una base sólida para la toma de decisiones y el diseño de medidas preventivas. Gracias a este carácter predecible, es posible aplicar políticas de mantenimiento planificado, mejorar la capacitación operativa del personal, diseñar protocolos estándares y ajustar sus recursos en función de la experiencia acumulada. En definitiva, los riesgos simétricos son aquellos que pueden anticiparse mediante un enfoque estructurado, lo que favorece una gestión eficiente y una mitigación proporcional a su naturaleza.

### Naturaleza y complejidad de los riesgos asimétricos.

Frente a la estabilidad relativa de los riesgos simétricos, los riesgos asimétricos representan el ámbito más complejo del análisis de seguridad ya que se caracterizan por la ausencia de proporcionalidad entre probabilidad e impacto, así como por una alta incertidumbre en su comportamiento. En este tipo de riesgo, incluso una probabilidad baja puede desembocar en consecuencias de impacto extraordinario, afectando gravemente a la continuidad de un proceso, la imagen externa, la estabilidad social, la integridad física de las personas o la operatividad de infraestructuras críticas



Lo que hace particularmente complejos estos riesgos es que suelen estar asociados a actores deliberados, inteligentes y en constante evolución, capaces de explotar vulnerabilidades no evidentes para generar un impacto desproporcionado. Entre los ejemplos más representativos se encuentran el terrorismo, la delincuencia organizada, las ciberamenazas avanzadas (APT), el sabotaje interno, la manipulación de sistemas, la ingeniería social dirigida, las acciones hostiles encubiertas o las disrupciones motivadas por conflictos geopolíticos. La dificultad principal radica en que estos riesgos no se comportan de forma lineal, pueden mutar rápidamente y requieren una interpretación estratégica del entorno, ya que la ausencia de patrones históricos fiables obliga a recurrir a la inteligencia operativa, la monitorización de señales iniciales, el análisis sociotécnico y las acciones prospectivas. Además, los riesgos asimétricos suelen manifestarse en escenarios complejos donde múltiples factores interactúan: tecnología en rápida evolución, motivación del adversario, cambios regulatorios, entornos híbridos y tendencias globales. Por ello, su gestión demanda un enfoque altamente adaptativo, flexible y anticipativo, donde la capacidad de identificar tendencias emergentes es tan importante como la preparación para escenarios de alto impacto

### Integración metodológica de riesgos simétricos y asimétricos

La combinación de riesgos simétricos y asimétricos en un único marco de análisis exige adoptar modelos metodológicos mixtos, capaces de abordar tanto lo previsible como lo incierto. En la práctica, esto implica desarrollar un sistema de gestión del riesgo que no dependa exclusivamente de matrices clásicas de probabilidad-impacto, sino que incorpore perspectivas dinámicas basadas en inteligencia, monitorización continua y escenarios prospectivos. Para los riesgos simétricos, se mantiene la utilidad de las herramientas tradicionales, como auditorías, análisis estadísticos, indicadores de tendencia, ratios de siniestralidad o comparaciones históricas que permiten predecir la frecuencia y la magnitud de eventos repetitivos. Sin embargo, para los riesgos asimétricos es necesario emplear enfoques cualitativos avanzados, tales como análisis de amenazas dirigidas, modelado de adversarios, identificación de vulnerabilidades críticas, simulación de crisis, análisis DELPHI, mapas de calor estratégicos y metodologías centradas en resiliencia. Todo ello se complementa con sistemas de alerta temprana, vigilancia tecnológica y estructuras de toma de decisiones basadas en inteligencia.



# Merry Christmas

La integración metodológica también obliga a redefinir los criterios de priorización, ya que los riesgos asimétricos no pueden valorarse únicamente por su probabilidad, sino por su capacidad disruptiva y su repercusión transversal. Este enfoque mixto crea un análisis más completo, permitiendo a la organización comprender no solo los riesgos ordinarios que forman parte del día a día, sino también aquellos escenarios excepcionales que, aunque poco frecuentes, pueden comprometer gravemente la seguridad y continuidad operativa.

## **Hacia un sistema de seguridad integral frente a riesgos previsibles y disruptivos**

La integración efectiva de riesgos simétricos y asimétricos en un único modelo de análisis permite construir un sistema de seguridad más sólido, mejor preparado y con capacidad de adaptación ante la complejidad del entorno. La gestión integral resultante combina, por un lado, la eficiencia operativa necesaria para controlar los riesgos previsibles —mantener instalaciones, reforzar procedimientos, mejorar la formación, implantar controles preventivos, asegurar la supervisión continua— y, por otro, la flexibilidad estratégica indispensable para hacer frente a amenazas disruptivas capaces de superar las barreras tradicionales. Un sistema de seguridad moderno debe ser resiliente, anticipativo y capaz de reconfigurar sus respuestas en función de señales emergentes, lo que implica no solo disponer de medios técnicos avanzados, sino también fomentar una cultura organizativa orientada a la prevención, la vigilancia activa y la toma de decisiones informada. Esta visión dual permite una preparación previa para gestionar desde incidentes rutinarios hasta eventos críticos de alto impacto, garantizando así protección integral, continuidad operativa y capacidad de respuesta incluso en los escenarios más complejos. En última instancia, un enfoque que comprenda y articule correctamente tanto riesgos simétricos como asimétricos no solo fortalece la seguridad física y tecnológica, sino que mejora la resiliencia global, incrementa la madurez del sistema y fomenta una capacidad real para afrontar un mundo en constante cambio, donde lo improbable también debe ser previsto.

**Agradecer, como de costumbre, a Metrorisk la difusión mensual de artículos de carácter técnico, cuyo compromiso constante contribuye a enriquecer el conocimiento de nuestro sector y a mantener un espacio de reflexión y actualización que resulta imprescindible para todos los profesionales de la seguridad.**

**Gregorio Duro Navarro**  
**Licitaciones y Proyecto**





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

### CPTED, ISO Y ONU: LA TRIADA PARA EL DISEÑO DE CIUDADES SEGURAS Y SOSTENIBLES

La seguridad en el entorno construido ha evolucionado de un enfoque reactivo (centrado en la respuesta policial) a una estrategia proactiva e integral basada en el diseño y la planificación. Esta transformación se articula a través de una poderosa triada conceptual.



El primer pilar es la Prevención del Delito Mediante el Diseño Ambiental (CPTED), una filosofía que utiliza la configuración física del espacio para reducir la oportunidad delictiva y el miedo a la delincuencia, enfocándose en principios como la vigilancia natural y el refuerzo territorial.

El segundo pilar es la Organización Internacional de Normalización (ISO), que, a través de normas como la ISO 22341:2021 y 22341-2:2025, estandariza y proporciona un marco de gestión de riesgos auditable para aplicar el CPTED. Estas normas aseguran que las soluciones de seguridad sean sistemáticas, sostenibles y se integren desde las fases tempranas del diseño urbano, trascendiendo las soluciones puntuales y garantizando la resiliencia a largo plazo.

El tercer pilar es la Organización de las Naciones Unidas (ONU), que proporciona el marco de acción global y la dimensión social y de sostenibilidad a esta metodología. La ONU, principalmente a través de la Nueva Agenda Urbana y el Objetivo de Desarrollo Sostenible (ODS) 11 ("Ciudades y Comunidades Sostenibles"), exige que el diseño urbano sea inclusivo, seguro y resiliente. Herramientas de la ONU-Hábitat, como la Metodología de Implementación Urbana (OUI), sirven como el motor operativo, asegurando que la aplicación técnica del CPTED (estandarizada por la ISO) se realice con la participación de la comunidad y la perspectiva de género, transformando así los estándares de seguridad en proyectos de desarrollo urbano que cumplen con los más altos ideales de sostenibilidad social y ambiental.

La ambición global de crear ciudades que sean seguras, inclusivas y resilientes (Objetivo de Desarrollo Sostenible ODS 11 de las Naciones Unidas) requiere la integración de metodologías de diseño y planificación robustas. Esta integración se materializa a través de la sinergia entre la metodología de Prevención del Delito Mediante el Diseño Ambiental (CPTED), los lineamientos de la Organización Internacional de Normalización (ISO 22341:2021 y la ISO 22341-2:2025), y el marco de acción de la Metodología de Implementación Urbana (OUI) de ONU-Hábitat.

CPTED e ISO: el Estándar de Seguridad por Diseño: CPTED es el fundamento teórico que postula que la modificación planificada del entorno construido puede reducir la oportunidad y la percepción del delito. La ISO proporciona el marco de gestión y estandarización de este enfoque

**1. ISO 22341:2021 – Directrices Generales (el "Qué"):** La ISO 22341 estandariza el proceso de aplicación de CPTED en la gestión del riesgo urbano. No solo describe los cinco principios del CPTED (Vigilancia Natural, Control de Acceso Natural, Refuerzo Territorial, Mantenimiento y Apoyo a la Actividad), sino que exige que su implementación sea:

- Basada en el análisis y gestión del riesgo: integrada con la ISO 31000 (Gestión del Riesgo), asegurando que el diseño de seguridad se base en un análisis exhaustivo de amenazas y vulnerabilidades.
- Sostenible y Resiliente: Los diseños deben ser costo-efectivos, adaptativos y duraderos, lo cual es un pilar de la planificación sostenible de la ONU.

**2. ISO 22341-2:2025 – Enfoque Residencial (la especificidad):** La ISO 22341-2:2025 es crucial porque se enfoca específicamente en la aplicación del CPTED en instalaciones residenciales. Al detallar cómo aplicar los principios en la escala del hogar y la comunidad inmediata, esta norma asegura que la seguridad y la inclusión se extiendan hasta el nivel de barrio, clave para el ODS 11.

**3. La Metodología OUI de ONU-Hábitat: el "Cómo" y el "Para Quién":** La Metodología de Implementación Urbana (OUI) de ONU-Hábitat es el vehículo que permite a los planificadores urbanos traducir los estándares de seguridad (ISO/CPTED) en proyectos reales y sostenibles. La OUI no es una norma de diseño, sino un marco operativo y participativo para la implementación de la Nueva Agenda Urbana y los Objetivos de Desarrollo Sostenible (ODS)





# CPTED, ISO Y ONU: LA TRIADA PARA EL DISEÑO DE CIUDADES

La OUI consta de un ciclo de tres pasos principales que aseguran la acción local y la inclusión:

Paso 1: Diagnóstico (la conexión de datos): El OUI comienza con una evaluación profunda de las condiciones urbanas. En esta etapa, el CPTED es vital:

- Se realizan auditorías de seguridad (CPTED Assessments), mapeando puntos críticos, flujos peatonales y percepción de inseguridad (ej. a través de caminatas de seguridad con perspectiva de género).
- Se recaban datos georreferenciados sobre incidentes delictivos.
- Sinergia: los datos de seguridad CPTED informan al diagnóstico OUI, asegurando que las futuras intervenciones estén basadas en la evidencia de inseguridad real y percibida.

Paso 2: Intervención Estratégica (la Solución Integrada): Con base en el diagnóstico, el OUI guía la selección e implementación de proyectos. Aquí es donde los principios de la ISO/CPTED se convierten en diseños físicos:

- Diseño CPTED: los proyectos se diseñan en el ecosistema ISO aplicando directamente los principios de la ISO 22341 y las 29 normas ISO más que hacen transversalidad para la óptima implementación y ejecución de proyectos CPTED con la ISO 22341 y la ISO 22341-2.
- Sostenibilidad y Género: la OUI asegura que las intervenciones CPTED no sean solo de seguridad, sino que también promuevan la equidad de género y la sostenibilidad ambiental.
- Sinergia: la OUI asegura que el diseño CPTED no opere de forma aislada, sino que se integre con planes de movilidad, vivienda y uso de suelo, garantizando una solución urbana holística que cumplirá con lo establecido en el ODS 11.

Paso 3: Monitoreo y Evaluación (El Impacto): El OUI exige un seguimiento constante y una evaluación del impacto de las intervenciones:

- Se mide la reducción real del delito y la mejora en la percepción de seguridad post-implementación CPTED.
- Se evalúa la sostenibilidad y la resiliencia del proyecto.
- Sinergia: este ciclo de retroalimentación es clave para el principio de Mejora Continua (Plan Deming) que exige la ISO 22341, permitiendo que la ciudad se adapte a nuevas dinámicas delictivas y sociales, construyendo verdadera resiliencia urbana.

## Conclusión:

La planificación de ciudades sostenibles y seguras es un proceso riguroso que requiere un marco metodológico triple:

- 1. CPTED proporciona la filosofía de diseño para la prevención del delito.
- 2. Las ISO 22341:2021 y la ISO 22341-2:2025 proporciona el estándar global y el sistema de gestión de riesgos para aplicar CPTED de manera auditable y sostenible.
- 3. La Metodología OUI de ONU-Hábitat proporciona el marco operativo participativo para llevar estos estándares al campo, asegurando la inclusión, la adaptación local y la coherencia con los objetivos globales de desarrollo.

Al operar en conjunto, estas herramientas permiten a los gobiernos y planificadores diseñar no solo espacios seguros, sino comunidades socialmente cohesionadas, económicamente viables y ambientalmente responsables.



Diseño con IA: Triada de la Planificación Urbana: Sostenible y Segura



# CARTA DE FELICITACIÓN DE NAVIDAD

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Antonio Cozano Fernández**  
CEO Cofer Seguridad.

Estimados clientes, colaboradores y amigos:

Se acerca el final de un nuevo año y, como siempre, es momento de hacer balance. En nuestro sector, cada día y cada servicio cuentan. Desde el primer turno de la mañana hasta la última ronda nocturna, miles de profesionales velan por la seguridad de empresas, personas, espacios públicos y privados. Y nada de lo que hacemos tendría sentido sin la confianza que depositan en nosotros.



**COFER**  
SEGURIDAD

TEL: 952 409 846

¿Y SI LO ÚNICO QUE QUIERES  
ES DORMIR TRANQUILO?

**COFER, NO VENDE  
ALARMAS, GARANTIZA  
TRANQUILIDAD.**

Active su sistema  
de seguridad en  
un clic

**29,95 € mes+ IVA\***

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



Por eso queremos dirigirles unas palabras especialmente cercanas: gracias por permitirnos proteger lo que es importante para ustedes.

Este 2025 ha sido un año de retos, cambios y nuevas exigencias de seguridad. Hemos seguido creciendo como profesionales y reforzando nuestra misión: estar presentes donde somos necesarios, anticiparnos al riesgo y aportar tranquilidad allí donde otros solo ven infraestructura.

Desde nuestra compañía queremos felicitar estas fiestas recordando algo que pocas veces se dice en voz alta: detrás de cada sistema de seguridad, detrás de cada plan operativo o de cada protocolo de prevención, siempre hay personas. Vigilantes de seguridad que trabajan en primera línea, supervisores que coordinan medios, jefes de equipo que responden ante emergencias y clientes que confían en nuestro criterio profesional.

Este es nuestro mayor orgullo: los hombres y mujeres que forman esta gran familia profesional, que salen cada día a cumplir una labor esencial con dedicación, responsabilidad y una vocación que se mantiene intacta.

Con ese espíritu, les deseamos una Navidad llena de calma, prosperidad y buenos momentos en compañía de sus seres queridos. Y que el año nuevo llegue cargado de proyectos, protección, salud y seguridad.

Seguiremos haciendo lo que mejor sabemos hacer: proteger, acompañar y garantizar un entorno seguro para todos.

Gracias por caminar a nuestro lado.  
Felices Fiestas y un próspero y seguro 2026.





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

## El 99% de los fallos en notificación vienen por lo mismo: falta de preparación proactiva

**AI Act (Art. 73):**  
el mayor riesgo no es el incidente... es no reportarlo bien.

🔑 El 99% de los fallos en notificación vienen por lo mismo: falta de preparación.

Si trabajas con IA de alto riesgo, esto te interesa (mucho).

**Qué cambia** (en serio)

- Quién reporta:  
el proveedor del sistema (y el desplegador, si el proveedor no responde).

- Qué se reporta:

incidentes graves → vida/salud, infracción crítica, derechos fundamentales, daños severos a propiedad/medioambiente.

**Plazos que te pueden dejar K.O.:**

- 🕒 15 días (regla general)
- 🕒 10 días (si hay fallecimiento)
- 🕒 2 días (infracción generalizada o infra crítica).

Permite reporte inicial incompleto:  
mejor avisar a tiempo que tarde y "perfecto".

✅ El check de realidad (te aplica si...)

- Desarrollas, integras o despliegas IA de alto riesgo (Annex III).
- Operas en sectores con aplicación de NIS2, DORA, sanitario, financiero...
- Tu sistema puede causar daño directo o indirecto en su uso previsto o razonablemente previsible.

❌ Los 5 errores que hunden a las empresas

- Confundir un incidente de TI con un incidente grave del AI Act.
- Esperar a "tener toda la info" → y llegar fuera de plazo.
- Alterar el sistema antes de reportar (pierdes evidencias y credibilidad).
- No coordinar con GDPR/NIS2/DORA → duplicidades y sanciones.
- No tener un RACI claro (quién detecta, evalúa, firma y reporta).



🔧 **Mini playbook 24-48-72 h (ONK)**

- 24 h → Detectar y escalar. Canal único + guardia.
- 48 h → Preservar evidencias (logs, datasets, modelo). Custodia WORM.
- 72 h → Enviar reporte inicial (aunque incompleto). Alinear ventanas con GDPR/NIS2/DORA.

¿Cómo te puedo ayudar?

- SOP de notificación Art. 73 (paso a paso, roles, checklists).
- Plantilla editable del reporte (v1.0.0) y árbol de decisión "incidente grave".
- Orquestación regulatoria: AI Act × GDPR × NIS2 × DORA.
- Simulacros (table-top) con casos de daño indirecto y en infra crítica.





# 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



# LAS 12 CAMPANADAS DE LA SEGURIDAD Y LA PRIVACIDAD

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Rosa Fernández**

## ASUNTO: SEGURA NAVIDAD Y PROTEGIDO AÑO NUEVO

En el sector de la seguridad, cada campanada de fin de año marca algo más que un cambio de fecha: es un recordatorio de que la confianza se gana con prevención y con protección. En el último artículo del año quiero compartir contigo las 12 claves que nos preparan para un 2026 más seguro y competitivo. Las 12 campanadas que nos llevan a un 2026 más protegido:

- 1) Alfabetización obligatoria en IA. Formar a equipos en un uso ético, responsable y seguro de la IA ya no es opcional. La ventaja real está en certificar competencias.
- 2) El dato como activo crítico (y riesgo). El RGPD y la LOPDGDD exigen consentimiento, finalidad, minimización y trazabilidad. Si sigues sin cumplir, expones tu reputación y pones en riesgo a tu cliente.
- 3) CiberVigilante. Competencias híbridas que favorecen la Vigilancia física + ciberseguridad operativa: personas entrenadas para detectar phishing, USB maliciosos y anomalías de sistemas en tiempo real.
- 4) IA con ética y privacidad desde el diseño. Analítica de vídeo, biometría y scoring conductual requieren una EIPD, pruebas de sesgo y controles anti-discriminación, así como una gestión documental trazable.
- 5) Las personas, primero. La formación continua y la preparación de tu equipo, reduce incidentes más que cualquier operativo. Las personas seguimos siendo el eslabón más débil en la cadena de la seguridad.
- 6) Seguridad integrada (CPTED/ISO). Como dice nuestro Director Fran Medina “no hay lujo sin seguridad”, y nadie quiere vivir en zonas o barrios inseguros, así que con una buena y competente consultoría se diseña la seguridad desde el plano.
- 7) Responsabilidad proactiva. Si no puedes demostrar cómo cumples, es como si no cumplieras. Política, procedimiento, auditoría y evidencia. Recuerda que tienes que demostrar que cumples la ley.
- 8) Datos sensibles en movimiento GPS, drones, bodycams, gafas inteligentes: cada flujo exige una base jurídica adecuada, una EIPD y un buen soporte documental.
- 9) Cliente informado, cliente fiel. Cartelería e información ampliada superan el “cartel de cámara”. Transparencia = confianza = retención y fidelización.
- 10) Ecosistema colaborativo. Proveedor, Director de Seguridad, Delegado de Protección de datos en el mismo proceso. La seguridad la hacemos entre todos.
- 11) Innovación con control IA, IoT y biometría, sí; pero con solidas políticas, usuarios autorizados, evaluaciones de impacto, análisis de riesgos y auditorías periódicas.
- 12) Un objetivo con Propósito. Cada procedimiento que aplicamos no solo protege infraestructuras: protege vidas, derechos y la confianza que sostiene a nuestra sociedad.

**Consultora jurídica. ©2025**  
**Miembro del Comité Técnico de MetroRisk,**  
**área de seguridad jurídica y derecho**  
**tecnológico**



**Y Después de las campanadas ¿qué?** pues que comienza el minuto uno del cumplimiento. Cuando el reloj marque el inicio de 2026, las empresas del sector estarán trabajando por la seguridad y la buena marcha de la fiesta. Es el momento de poner en marcha lo aprendido: revisar protocolos, reforzar la formación, evaluar riesgos y documentar la trazabilidad de cada decisión. La seguridad no es estática: evoluciona cada día con las personas, la tecnología y las amenazas. Por eso, la ventaja competitiva real en este nuevo año no estará en tener más cámaras, más sistemas o más contraseñas, sino en tener más criterio, más formación, más competencias y más coherencia operativa. Las compañías que logren integrar sus sistemas de vigilancia con los marcos de cumplimiento normativo y con una cultura corporativa basada en la responsabilidad y el conocimiento de las nuevas competencias, serán las que lideren el mercado y ganen confianza social, y por supuesto, los contratos con sus clientes.

**La nueva brújula del 2026: datos, talento y reputación.** Este año nos obliga a mirar más allá del control técnico. El talento humano será el nuevo perímetro de seguridad, el dato será el activo que más debemos proteger, y la reputación será el indicador más valioso de nuestra madurez como sector. Cada decisión, cada proveedor y cada solución tecnológica, deberá responder a tres preguntas esenciales: 1. ¿Es seguro? 2. ¿Es ético? 3. ¿Es proporcional? Solo así conseguiremos pasar del cumplimiento formal al cumplimiento con propósito, que no solo evita sanciones, sino que construye confianza.

Desde MetroRisk y ZonaVigilada, seguiremos impulsando la profesionalización de la seguridad, ayudando a directores de seguridad, consultores y responsables de cumplimiento a integrar normas ISO, RGPD y REIA en sus estrategias diarias. Y como cada año, aquí estaremos para acompañarte en cada paso, ayudándote a transformar el cumplimiento en estrategia, para que vendas más con seguridad. 2026 será el año de la seguridad con inteligencia y competencia.

**¿Estás preparado? ¡FELIZ Y SEGURO AÑO NUEVO!**




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

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

CONECTA CON NORMA :  
TU ASESORA VIRTUAL EN RGPD. ✎  
Visita ZonaVigilada.net ✎ Conecta  
conmigo en

✉ rosaf@zonavigilada.net  
Te damos respuestas y te ayudamos a  
mejorar tu seguridad jurídica

✎ 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



# LA CAMPAÑA NAVIDEÑA

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

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

La campaña navideña convierte a los grandes almacenes en uno de los entornos comerciales más sensibles desde el punto de vista de la seguridad. El incremento masivo de afluencia, la presión operativa y las extensas jornadas de actividad generan un escenario donde cualquier mínimo fallo puede multiplicarse rápidamente. En esta época, la seguridad privada adquiere un papel estratégico que va mucho más allá de “vigilar”: se convierte en un elemento esencial para la prevención, la disuasión y la continuidad del negocio.

## La importancia de revisar los elementos de detección

Antes del inicio de la campaña, resulta imprescindible una revisión exhaustiva de todos los sistemas de detección: CCTV, arcos antihurto, alarmas técnicas, pulsadores, iluminación, señalización, megafonía y software de control. En Navidad, la saturación de pasillos, cajas y accesos puede neutralizar parte de la eficacia de estos sistemas sino están correctamente mantenidos o configurados. Un sistema que falla en estas fechas no solo provoca pérdidas económicas: genera incertidumbre, ralentiza la evacuación ante una emergencia y resta capacidad operativa a todo el equipo de seguridad.

## Vigilancia del fraude y del robo interno

El hurto externo suele aumentar significativamente en diciembre, pero no es el único problema. Cada año, los grandes almacenes asumen importantes pérdidas económicas derivadas del robo interno, especialmente en campañas de alta intensidad laboral y contratación temporal. Aquí el vigilante de seguridad cumple una función clave:

- Control de accesos del personal.
- Supervisión discreta en zonas sensibles.
- Análisis del comportamiento no verbal.
- Apoyo al departamento de seguridad del centro.

La combinación de tecnología + presencia humana es, en estas fechas, la única fórmula realmente eficaz para minimizar el fraude.

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



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

## Sistemas de evacuación: nada puede fallar

En grandes superficies con miles de personas dentro al mismo tiempo, una evacuación eficaz es sinónimo de vida. En plena campaña navideña, con familias, carritos de compra y zonas sobreesaturadas, la revisión de:

- Rutas de evacuación
- Salidas de emergencia
- Señalización
- Iluminación de emergencia
- Comunicación interna debe ser una prioridad absoluta.

Los simulacros previos, incluso los realizados de forma parcial o por turnos, permiten:

## Prevención y disuasión: el verdadero valor de la seguridad privada

Aunque muchas veces pase desapercibida, la presencia del vigilante es uno de los elementos más eficaces para evitar situaciones de riesgo. Su sola presencia disuade hurtos, evita conflictos, frena conductas agresivas y aporta una sensación de control que reduce la percepción de inseguridad. Además, en estas fechas, los vigilantes suelen asumir funciones adicionales:

- Gestión de grandes colas
- Atención y orientación a clientes
- Control de aforos
- Intervención ante incidentes relacionados con estrés, aglomeraciones y conflictos leves

La seguridad privada se convierte en un pilar de estabilidad para el comercio y para la ciudadanía.





# TECNOLOGÍA, PREVENCIÓN Y ESPÍRITU NAVIDEÑO: ASÍ SE GESTIONA LA SEGURIDAD EN UNA EMPRESA MODERNA

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

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



En estas fechas en las que las luces iluminan calles y ciudades, también se iluminan los centros comerciales, polígonos, estaciones, aeropuertos y espacios que no pueden detener su actividad. Mientras muchos celebran, nuestro sector entra en una de sus etapas más exigentes: **vigilancia reforzada, control de accesos, eventos multitudinarios, transporte de mercancías y aumento del riesgo. La Navidad no detiene la seguridad; la exige aún más.**

Y detrás de cada operación eficiente hay algo fundamental que define el presente y el futuro de nuestro sector: la correcta gestión de los recursos tecnológicos.

La seguridad ya no es solo presencia: es inteligencia operativa. Hace apenas una década, la tecnología era un apoyo. Hoy es un pilar estratégico. Una empresa de seguridad moderna no solo despliega vigilantes; despliega:

- sistemas de videovigilancia inteligente,
- control de accesos biométrico,
- análisis de comportamiento,
- centros de control operativos,
- comunicaciones cifradas,
- sensores IoT,
- sistemas automáticos de alarma y respuesta.

Y todo esto no sustituye a la seguridad humana. La potencia.

Porque un vigilante que cuenta con la información adecuada, apoyo remoto y medios tecnológicos, se convierte en un profesional más eficiente, más protegido y más resolutivo.

**Planificación en clave de Navidad:** cuando el riesgo cambia. Las fiestas alteran patrones y eso exige capacidad de adaptación:

- horarios extendidos,
- más afluencia de público,
- logística masiva,
- eventos especiales,
- vigilancia adicional en exteriores.

Planificar correctamente significa algo más que reforzar turnos. Significa integrar tecnología y personal en una estrategia común. Desde un centro de control se puede:

- optimizar rondas,
- reducir tiempos de reacción,
- evitar falsas alarmas,
- coordinar equipos,
- anticipar incidentes,
- evaluar situaciones en tiempo real.

Es aquí donde la gestión técnica marca la diferencia entre reaccionar y prevenir.

## La tecnología como espíritu protector

La Navidad también nos recuerda que la seguridad tiene un componente humano. Que la tecnología no existe para sustituir personas, sino para protegerlas. Y que la innovación debe estar alineada con un propósito:

garantizar que empresas, familias y espacios sigan funcionando con normalidad, incluso cuando nadie ve el trabajo que hay detrás.

La responsabilidad de nuestra industria es asegurar esa protección invisible: la que permite que los demás disfruten, viajen, trabajen o celebren sin preocuparse por lo que no ven.

Navidad es también reconocer a quienes sostienen la seguridad.

A los vigilantes que patrullan centros comerciales cuando todos compran regalos.

A los operadores que coordinan emergencias en noches frías.

A los técnicos que mantienen sistemas funcionando a pleno rendimiento.

A los supervisores que garantizan que nada quede sin control.

La seguridad es un conjunto, y la tecnología es parte del equipo.

## Mirando al próximo año

Si algo nos enseña cada cierre de ejercicio es que el futuro del sector dependerá de tres pilares:

1. Integración de soluciones técnicas.
2. Formación continua.
3. Coordinación operativa humano-tecnológica.

Porque no se trata solo de comprar sistemas; se trata de gestionarlos con criterio, estrategia y profesionalidad.



# CARTA DE NAVIDAD DESDE EL MUNDO DE LOS SEGUROS Y LA SEGURIDAD

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Alina Rubio de las Casas**  
**Experta en Seguros Generales**

Estimados clientes, colaboradores y compañeros del sector:

Con la llegada de estas fechas, el cierre de un nuevo ejercicio nos invita a detenernos y mirar con perspectiva. Desde la especialización en seguros generales, conocemos bien una verdad que compartimos con la seguridad privada: nuestra misión es proteger aquello que para otros es irremplazable.

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



Cada póliza, cada cobertura, cada análisis de riesgos y cada auditoría preventiva representa el mismo propósito que mueve a un vigilante en su puesto, a un jefe de seguridad diseñando un plan operativo o a un consultor estableciendo medidas de protección: evitar el daño antes de que ocurra.

Por eso, esta felicitación navideña no es simplemente un mensaje de cortesía: es un reconocimiento mutuo.

Los seguros y la seguridad privada no son sectores aislados; son aliados naturales.

- Ambos anticipamos amenazas.
- Ambos analizamos el riesgo.
- Ambos trabajamos con previsión y responsabilidad.

Ambos sabemos que cuando algo sucede, cada minuto cuenta. Y en este año que termina hemos vuelto a ver cómo la protección no es solo un servicio o un trámite. Es un compromiso profesional y humano.

Quiero felicitar especialmente a todos los que desde la primera línea de la seguridad privada han cumplido su labor con vocación y sacrificio: desde los vigilantes que patrullan cuando la ciudad duerme, hasta los equipos de supervisión, control y dirección que diseñan estrategias para que empresas, personas y bienes continúen su actividad sin interrupciones.

Del mismo modo que en los seguros estudiamos escenarios, coberturas y contingencias, ellos trabajan en la prevención activa y en la respuesta inmediata. Somos ramas diferentes del mismo árbol: la gestión del riesgo, la continuidad y la tranquilidad.

**Que estas fiestas nos recuerden el valor de lo invisible:** los incidentes que no ocurrieron, las pérdidas que se evitaron, los bienes que permanecen protegidos gracias a la profesionalidad de dos mundos que trabajan codo con codo.

Desde nuestra actividad aseguradora, seguiremos promoviendo la prevención, la protección y la colaboración con la seguridad privada, porque juntos construimos el mismo propósito: proteger el presente y asegurar el futuro.

Les deseamos una Navidad llena de serenidad y un nuevo año próspero, sostenible y seguro. Que el 2026 llegue cargado de salud, estabilidad y confianza en todos los proyectos que están por venir.

Felices fiestas y gracias por acompañarnos en este camino compartido.

*Alina Rubio*

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

 GRUPO BORRERO







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.



# DOCTRINA: EL MANIFIESTO DEL LIDERAZGO INTEGRAL 2026

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

## Elena de la Parte

El reloj de arena de 2025 ha llegado a su fin, y con él una certeza ineludible: la ciberseguridad y la seguridad han trascendido la etiqueta de “merma” para consolidarse como el habilitador estratégico. Diciembre es un umbral nos invita a cerrar el capítulo de un intenso 2025 y a mirar el 2026 con la pasión visionaria que define. La integración de la seguridad moderna se sostiene sobre pilares que deben interactuar con la precisión de un reloj suizo. El liderazgo de hoy no es jerárquico es orquestal.

La inteligencia artificial ( IA) se ha afianzado con el paradigma tecnológico de la década, pero su impacto en la ciberseguridad es un arma de doble filo. Si bien la IA es crucial para automatizar la detección y respuesta a incidentes, ( reduciendo el tiempo de respuesta con un indicador crítico), también está en manos de los atacantes para refinar el phishing y generar código malicioso incluso automatizar los ataques. A esto se suma la creciente injerencia de la geopolítica. Los ataques ya no son puramente económicos; un número significativo está impulsado por intereses estatales o conflictos. Esta “ciber fragmentación” aumenta la complejidad, obligando a gestionar riesgos que antes solo incumben a los gobiernos.

Esta función sólo es legítima si está blindada por un compliance transparente, garantizando que el uso de la tecnología respete los derechos y la dignidad de cada ciudadano. Frente a este panorama, el compliance se erige como el Código de ética indispensable, garantizando que el uso de la IA se embarque en la legalidad y la responsabilidad, blindando la estrategia de negocio. Nuestra industria ha evolucionado de manera vertiginosa, y el liderazgo hoy reside en la capacidad de tejer todos los hilos:

- Protección del entorno: Seguridad privada y CPTED: los profesionales de la seguridad privada son los custodios del día a día y su labor debe ser amplificada por él CPTED (Crime Prevention Through Environmental Design). Diseñar entornos que disuaden el riesgo de reconocer que la prevención empieza en el plano. Es la seguridad física la que abraza la inteligencia ambiental.
- El Campo de juego, las Smart Cities: La ciudad es nuestro estadio. Las Smart Cities son el ecosistema donde estos pilares se encuentran. Si la ciberseguridad protege la infraestructura de datos y el CPTED, diseña espacios seguros, la fusión de ambos crea un entorno inteligente y verdaderamente resiliente.

El hilo conductor de esta integración es el liderazgo. Adoptando la visión audaz que caracteriza a los evangelistas de la seguridad.

**Liderazgo: de la jerarquía a la capitania.** El líder en seguridad hoy debe ser:

- Tecnológico: debe entenderla IA y la ciberseguridad, no para programar sino para garantizar una cultura de seguridad, mejora continua y optimización empresarial.
- Humano: debe potenciar a los profesionales de la seguridad privada, dotándolos de las herramientas y la formación dual. “La fortaleza no es un blindaje, es la disciplina continua de la adaptación”
- Inspirador: debe comunicar la importancia del compliance como un valor ético. “La protección de datos no es una copia de respaldo, es la inversión fundamental del progreso”.



El desafío del 2026 es lograr que los datos de la ciberseguridad se traduzcan en acciones preventivas físicas, (CPTED), implementadas y validadas por la seguridad, todo bajo la guía ética del compliance y el liderazgo que fomenta esta visión total. La epopeya requiere coherencia y propósito. La seguridad no puede contarse en capítulos separados. Desde Metrorisk, el propósito de nuestro liderazgo debe ser audaz para dismantelar las barreras entre lo físico y lo digital, promoviendo una cultura donde la inversión en prevención sea la narrativa central. Los invito a abrazar este manifiesto; el futuro súbito, se diseña y blindo con una visión integral. Cerramos el 2025 con una verdad ineludible; la seguridad ya no es una función es una doctrina.

- “La ciberseguridad no es un perímetro cerrado ,es la identidad verificada de cada nodo IoT”
- “La seguridad digital no es un código cerrado, es el talento humano en constante defensa” “La seguridad no se negocia se integra. “ La seguridad es vital; lo trivial es la excusa para ignorarla”.

Los invito a cerrar 2025 con la convicción de que solo una estrategia cohesionada, consciente y resiliente nos permitirá liderar el 2026. ¡Que tengan unas fiestas inspiradoras y un 2026 de integración total!

# DOCTRINA EL MANIFIESTO DEL LIDERAZGO INTEGRAL 2026





# MÁS ALLÁ DE LAS CÁMARAS: LA NUEVA SEGURIDAD INTEGRAL EN LOS CENTROS COMERCIALES

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

**Carlos Miguel Ortiz**

*Los centros comerciales son espacios donde la seguridad debe respirarse, no solo vigilarse. Este artículo explora cómo la integración entre profesionales cualificados, tecnología inteligente y drones redefine el concepto de seguridad integral*

**Centros comerciales: microciudades en movimiento:** Los centros comerciales modernos han dejado de ser simples espacios de compra: se han transformado en microciudades donde confluyen ocio, trabajo y tránsito constante de miles de personas cada día. Esta alta concentración de actividad y diversidad de situaciones convierte a estos entornos en escenarios complejos de gestión de seguridad, donde cada detalle puede marcar la diferencia entre la prevención efectiva y un incidente crítico. Si bien la videovigilancia y los sistemas tecnológicos han evolucionado de manera notable, no pueden sostener por sí mismos la protección integral de un centro comercial. La verdadera seguridad surge de un equilibrio entre el factor humano, la tecnología y la prevención proactiva, creando un ecosistema en el que cada componente refuerza al otro.

**El técnico de seguridad: el eje humano de la protección:** El técnico de seguridad privada es la piedra angular de cualquier estrategia integral de seguridad. Su papel no se limita a observar: interpreta el contexto, anticipa riesgos y coordina respuestas inmediatas. Entre sus funciones clave se encuentran:

- Vigilancia presencial y preventiva: patrullar zonas críticas, identificar patrones inusuales y mantener la calma en áreas de alto tránsito.
- Atención al cliente y gestión de conflictos: actuar con criterio y empatía frente a situaciones que podrían escalar.
- Coordinación con centros de control y emergencias: ser el primer punto de enlace en cualquier incidente, desde emergencias médicas hasta conatos de incendio.
- Supervisión técnica de los sistemas de seguridad: verificar que cámaras, sensores y alarmas funcionen correctamente, detectando fallos antes de que afecten la protección.

Su conocimiento del entorno y la rutina del centro le permite detectar señales que la tecnología no percibe: gestos, actitudes o comportamientos sospechosos, así como situaciones de riesgo potencial que podrían pasar desapercibidas para un sistema automatizado. Ejemplo práctico: un técnico nota que un paquete ha sido dejado en un pasillo poco transitado. Mientras la cámara registra el objeto, es el juicio del profesional el que decide activar protocolos de revisión y vigilancia, evitando un posible incidente antes de que ocurra.

**Tecnología al servicio de la inteligencia humana:** Los sistemas tecnológicos en los centros comerciales —cámaras de alta resolución, sensores de movimiento, control de accesos, analítica de vídeo e inteligencia artificial— proporcionan información valiosa, pero su eficacia depende del criterio humano que la interpreta.



El técnico de seguridad actúa como un “traductor” de la tecnología: convierte datos en decisiones. Mientras una cámara puede generar una alerta por un movimiento inusual, solo un profesional puede evaluar el contexto, distinguir entre un falso positivo y un riesgo real, y actuar de manera proporcional. En este sentido, la videovigilancia se entiende como un complemento indispensable, pero no como el núcleo de la seguridad. La prevención real sigue siendo el resultado de la observación activa, la experiencia y la capacidad de anticipación del personal de seguridad.

**Drones: vigilancia aérea y apoyo operativo:** La incorporación de drones en la seguridad privada de centros comerciales ha revolucionado el concepto de supervisión y respuesta rápida. Estas aeronaves no tripuladas permiten:

- Vigilancia aérea de zonas exteriores y aparcamientos donde la presencia física es limitada.
- Supervisión en emergencias como incendios o evacuaciones, proporcionando información en tiempo real a los equipos de control.
- Inspección de techos y cubiertas sin riesgos para el personal.
- Seguimiento de situaciones de riesgo en coordinación con el centro de control y el personal de seguridad.

El uso eficiente de drones depende de operadores altamente capacitados, capaces de integrar la información aérea con la observación directa y los sistemas de videovigilancia. Aquí es donde RITRAC International destaca como entidad formadora, preparando a profesionales en operaciones UAS dentro de entornos comerciales, garantizando seguridad, cumplimiento normativo y eficacia en la respuesta ante incidentes



**HEKA3: innovación que potencia la labor humana** La tecnología aplicada a la seguridad no se limita a dispositivos y drones: requiere soluciones inteligentes que faciliten la toma de decisiones. HEKA3 se posiciona como referente en este campo, ofreciendo herramientas que combinan análisis de datos, inteligencia situacional y apoyo operativo.

Gracias a sus soluciones, el técnico de seguridad puede anticiparse a incidentes, gestionar alarmas con mayor precisión y coordinar la respuesta ante emergencias de manera más eficiente.

El enfoque de HEKA3 es claro: la tecnología amplifica, pero no sustituye, la capacidad de los profesionales, reforzando la prevención y la protección en todo el centro comercial.

#### **Prevención y coordinación: la base de la seguridad integral**

Un sistema de seguridad eficaz se fundamenta en tres pilares:

- 1. Prevención: anticipar riesgos mediante patrullas activas, control de accesos y observación constante.
- 2. Coordinación: integrar la labor del personal, la videovigilancia, los drones y los protocolos de emergencia para asegurar una respuesta rápida y ordenada.
- 3. Formación continua: mantener a los profesionales actualizados en normativas, gestión de emergencias, primeros auxilios, comunicación efectiva y uso de nuevas tecnologías

Por ejemplo, ante un conato de altercado en una zona concurrida, un técnico puede alertar al centro de control, mientras un dron supervisa la zona desde el aire y las cámaras capturan la incidencia para documentación y análisis posterior. Esta acción coordinada reduce riesgos, protege al público y permite decisiones más rápidas y seguras.

**Cultura de seguridad y experiencia del cliente** La seguridad en un centro comercial no solo protege bienes materiales; protege personas y confianza.

La presencia visible de profesionales capacitados, apoyados por tecnología inteligente, genera un entorno de tranquilidad que influye directamente en la percepción del cliente y la reputación del centro. El cliente percibe seguridad no por las cámaras ni por los drones en sí, sino por la capacidad del personal para anticipar riesgos, gestionar situaciones críticas y mantener el control del entorno.

Esta percepción de seguridad es un activo estratégico que impacta en la experiencia de compra y en la fidelización del público.

**Seguridad viva y humana** La seguridad integral en los centros comerciales va más allá de la tecnología. Es un ecosistema donde convergen:

- El juicio y la experiencia del técnico de seguridad.
- El soporte de sistemas de videovigilancia y otras tecnologías de monitoreo.
- La flexibilidad y cobertura de los drones, capaces de extender la observación más allá del alcance humano.
- La innovación de empresas como HEKA3 y la formación especializada de RITRAC International, que garantizan competencia y actualización constante del personal.

**La verdadera protección surge cuando persona y tecnología trabajan en armonía, creando un entorno seguro y confiable para todos los visitantes. En este sentido, la seguridad ya no es solo un servicio: se convierte en un elemento integral de la experiencia comercial, donde cada acción, cada decisión y cada herramienta contribuye a proteger lo más valioso: la vida y la confianza de las personas.**

### **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>





# EL FACTOR HUMANO EN 2025: MÁS ALLÁ DEL TRAINING, HACIA UNA CULTURA DE SEGURIDAD INNATA

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

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

## La Evolución de la Concienciación: De la Formación Obligatoria a la Experiencia Integrada y el Poder de la Influencia Interna.

Al cerrar el año 2025, la ciberseguridad enfrenta una paradoja ineludible: pese a inversiones récord en herramientas de defensa perimetral, IA y sistemas de detección, el eslabón humano sigue siendo tanto la principal vulnerabilidad como la última línea de defensa. Sin embargo, hemos presenciado un cambio de paradigma fundamental. Ya no basta con el "training" anual obligatorio, ese checkmark en la lista de cumplimiento. La vanguardia en 2025 se ha movido decididamente hacia la construcción de una cultura de seguridad innata, donde las conductas seguras no se imponen, sino que se cultivan, se experimentan y se socializan de forma orgánica. Revisemos las estrategias que han definido este año.

### 1. Simulacros Inmersivos con Realidad Virtual (VR): De la Teoría al Instinto

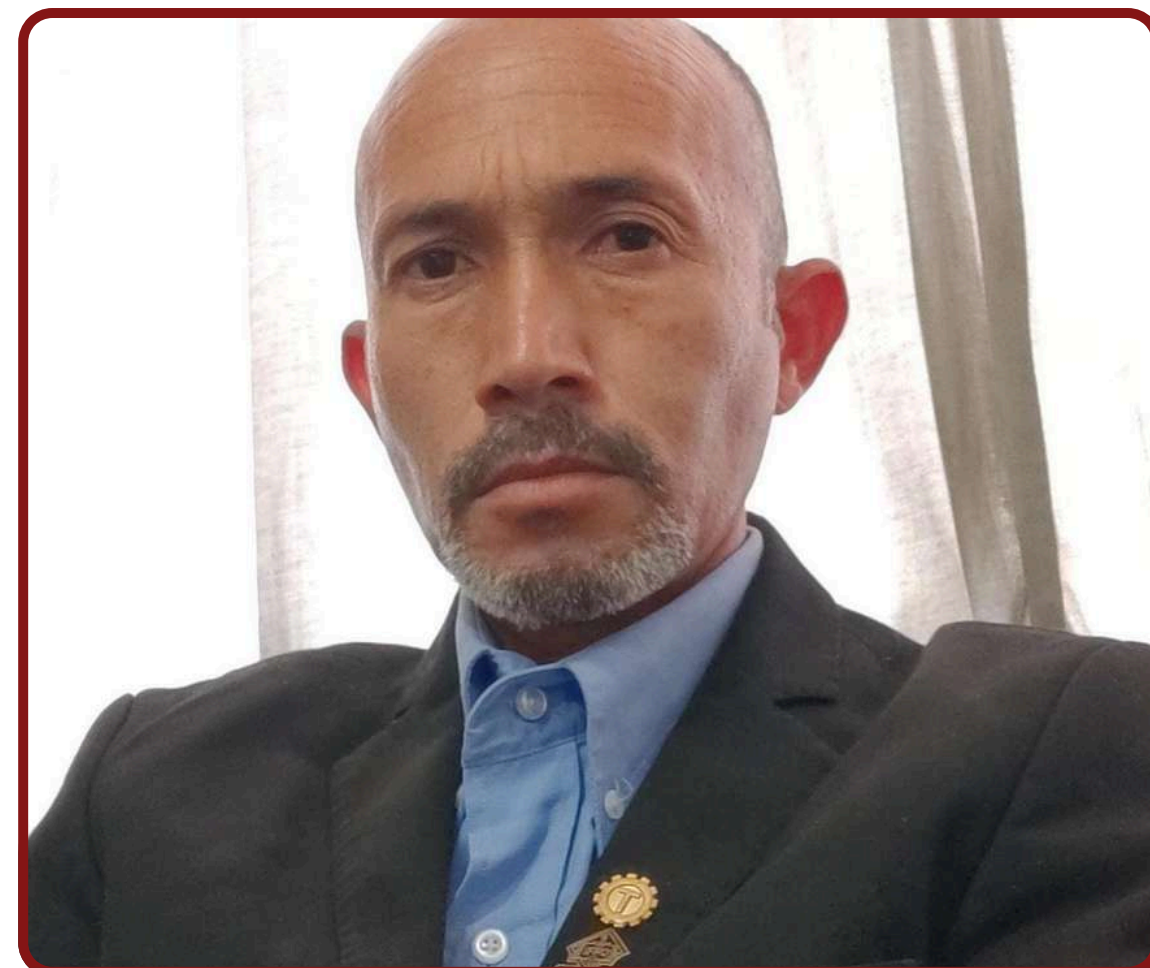
El "clic" en un enlace malicioso ya no es un ejercicio de imaginación. En 2025, los simulacros con VR han llevado la capacitación a un nivel visceral. Los empleados, con sus visores, viven las consecuencias de sus acciones en un entorno digital simulado pero profundamente realista. ¿Qué se siente al ver cómo se cifran los archivos de tu departamento tras descargar un adjunto? ¿O al presenciar la filtración de datos confidenciales por un error en una videollamada suplantada? Esta experiencia emocional, libre de riesgos reales, genera una memoria muscular cognitiva. La seguridad deja de ser un abstracto para convertirse en un instinto, forjado en la adrenalina y el impacto controlado de la simulación.

### 2. Micro-Learnings Gamificados: La Concienciación en el Flujo de Trabajo

El concepto del "curso anual" ha quedado obsoleto. En su lugar, 2025 ha consolidado el uso de píldoras de conocimiento gamificadas, integradas directamente en las herramientas cotidianas (Slack, Teams, el propio correo). Breves cuestionarios interactivos, mini-juegos de identificar la amenaza en un correo falso, o challenges semanales de equipos por puntos, han hecho que el aprendizaje sea continuo, accesible y divertido. Este enfoque respeta el tiempo del empleado, combate la fatiga formativa y mantiene la seguridad en un constante "goteo" de recordatorios prácticos, reforzando los comportamientos correctos en el momento justo.

### 3. Los "Influencers Internos" de Seguridad: La Humanización del Mensaje

Quizás la estrategia más transformadora del año ha sido el reconocimiento del capital social interno. Los departamentos de Seguridad y RR.HH. han identificado y empoderado a "influencers internos" de seguridad: colegas respetados, de diversos departamentos (no solo IT), que actúan como embajadores y multiplicadores del mensaje.



Su poder reside en la credibilidad y la confianza que ya tienen dentro de sus redes informales. Un post de uno de ellos en el intranet sobre un "casi incidente", un consejo práctico en un tono cercano, o un testimonio en un webinar interno, tiene un impacto multiplicador muy superior al email corporativo genérico. Humanizan la ciberseguridad, la despojan de su aura técnico-amenazante y la convierten en una conversación entre pares.

### Tejiendo el Tejido Cultural

El 2025 ha demostrado que la batalla por el factor humano no se gana con más horas de formación obligatoria, sino integrando la seguridad en el ADN organizacional. La combinación de la experiencia inmersiva (VR), el refuerzo continuo y lúdico (micro-learning) y el poder del ejemplo y la influencia social (influencers internos) está creando un ecosistema donde la conducta segura es la norma natural, no la excepción forzada.

Ya no se trata solo de "saber" qué es un phishing, sino de sentir el riesgo, practicar la defensa a diario y escuchar a quienes admiras dentro de la empresa hablando de ello. Estamos, más que nunca, transitando del training a la cultura de seguridad innata. Un cambio profundo que, a fin de cuentas, transforma a cada empleado de eslabón débil a guardián activo. Este es el legado más prometedor del 2025 en la eterna ecuación de la ciberseguridad.

**Autor: Licenciado en Seguridad Pública y Criminología.  
Jonatthan Hermida Sosa  
[www.hermidaseguridad.org](http://www.hermidaseguridad.org)**





# SIN SEGURIDAD DEL ESTADO NO HAY REPÚBLICA POSIBLE

Metro  
Risk

Edición propiedad de @MetroRisk, asociación

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

## En clave política

**Cuando un país colapsa —cuando sus instituciones dejan de funcionar, cuando el crimen se mezcla con el poder político, cuando la justicia es sustituida por lealtades partidistas y cuando el ciudadano queda abandonado frente a mafias, milicias o grupos armados— la sociedad enfrenta una verdad incómoda: ya no vive en un Estado, sino bajo un régimen que ocupa un territorio. Y un territorio dominado por un régimen criminal no se reconstruye con buenas intenciones ni con llamados abstractos a la democracia.**



La historia es clara, implacable y reiterada: antes de que una democracia pueda renacer, la República debe ser reconstruida, y esa reconstrucción solo tiene un punto de partida posible: la Seguridad del Estado.

La discusión sobre la seguridad del Estado venezolano no puede seguir reduciéndose a diagnósticos superficiales ni a percepciones aisladas. Para comprender la verdadera magnitud del colapso institucional, es necesario analizar cómo, en las últimas décadas, la estructura fundamental del Estado fue deliberadamente desmantelada, distorsionada y sometida a intereses ajenos a la República. La seguridad del Estado, concebida en cualquier nación moderna como una arquitectura estratégica que garantiza la continuidad institucional, el orden constitucional, la integridad territorial y la protección de los ciudadanos, fue sustituida progresivamente por un sistema híbrido que combina rasgos autoritarios, lógicas criminales y la intervención de actores externos.

**VENEZUELA: UN SISTEMA POLÍTICO COLAPSADO.** A lo largo de este proceso, las instituciones constitucionales encargadas de resguardar la soberanía y el Estado de Derecho fueron vaciadas de contenido. El poder político creó estructuras paralelas que sustituyeron al sistema de inteligencia, alteraron la cadena de mando formal, politizaron la Fuerza Armada y convirtieron los organismos de seguridad en instrumentos de control interno en lugar de defensores de la nación.

La seguridad del Estado dejó de funcionar como un espacio técnico y profesional para transformarse en un mecanismo represivo y partidista, sin proyecto nacional y sin arraigo institucional. De esta forma, la seguridad del Estado quedó subordinada a intereses particulares, lo que no sólo debilitó la capacidad del país para protegerse, sino que abrió las puertas para que organizaciones criminales y grupos irregulares encontraran espacios para operar.

La ausencia de un sistema auténtico de seguridad del Estado generó un vacío estratégico que ha comprometido la existencia misma de la República. Cuando el aparato estatal pierde capacidad de anticipación, control y respuesta; cuando los cuerpos de seguridad actúan bajo criterios ideológicos o económicos en lugar de hacerlo bajo criterios técnicos; cuando la inteligencia del Estado deja de proteger la Constitución para proteger a un grupo político, el resultado inevitable es la vulnerabilidad permanente del país frente a actores internos y externos, legales e ilegales. Un Estado sin seguridad deja de ser un Estado funcional.

Este deterioro estructural ha tenido consecuencias directas sobre la vida nacional. La infiltración de grupos irregulares, el fortalecimiento de economías ilícitas, la fragmentación del monopolio de la fuerza, la expansión del narcotráfico y la pérdida de control territorial son elementos que se desarrollaron precisamente porque no existía una política de seguridad del Estado capaz de impedirlo. La República quedó expuesta a una dinámica donde actores armados obtuvieron poder fáctico, creando zonas de influencia propias y afectando la gobernabilidad. Esta degradación derivó en un escenario donde la seguridad ciudadana también colapsó, pues un Estado que no puede garantizar su propia existencia es incapaz de garantizar la vida, los bienes o los derechos de sus ciudadanos.

Por ello, cuando se plantea la reconstrucción de Venezuela, el punto de partida no puede ser únicamente la recuperación económica, la reforma institucional o la lucha contra la corrupción. Debe comenzarse por definir con precisión un nuevo sistema de seguridad del Estado, moderno, profesional y democráticamente alineado, capaz de evitar la repetición del ciclo destructivo que nos trajo hasta aquí. Ningún proyecto republicano es sostenible si el Estado carece de herramientas para defenderse. Ningún proceso político puede florecer en un entorno donde la inteligencia institucional no sirve al país, sino a un grupo. Ninguna democracia puede estabilizarse si los órganos de seguridad están cooptados por intereses ilegales o subordinados a actores extranjeros.





**LA SEGURIDAD DEL ESTADO COMO POLÍTICA DE ESTADO** La seguridad del Estado debe ser una política de Estado, no de gobierno. Su orientación debe estar sustentada en la doctrina constitucional, en la defensa de los valores republicanos, en la protección del territorio y en el resguardo de los ciudadanos.

La reconstrucción debe incluir la profesionalización de los cuerpos de seguridad, la restitución de la inteligencia estratégica, la despolitización total de la Fuerza Armada, la neutralización de los actores irregulares y la recuperación de la soberanía física y funcional del territorio. Sin seguridad del Estado no hay República, porque la República es, ante todo, un pacto institucional que exige estabilidad, continuidad y resguardo.

Un país puede sobrevivir a crisis económicas severas, a conflictos políticos prolongados y a cambios bruscos de liderazgo, pero no puede sobrevivir a la pérdida de su seguridad estructural. Cuando el Estado deja de protegerse, deja de existir. Y cuando el Estado deja de existir, la República se convierte en un concepto vacío, sin capacidad de sostener derechos, libertad ni proyecto nacional.

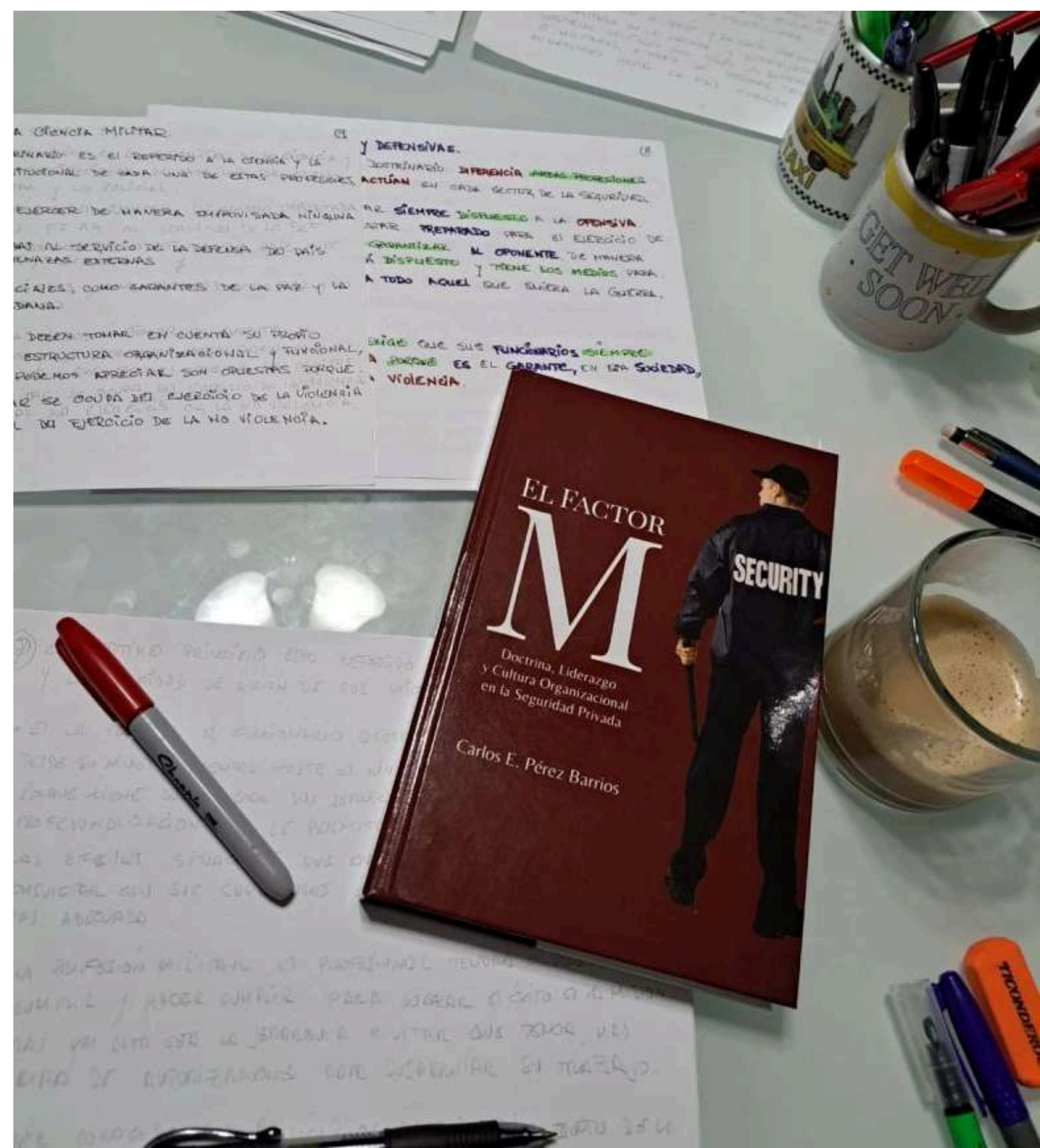
Reconstruir la seguridad del Estado venezolano es, por tanto, la prioridad absoluta para garantizar la supervivencia de la República y permitir el restablecimiento de un orden democrático. Es la condición de posibilidad para todo lo demás. Solo a partir de un Estado seguro será viable reconstruir instituciones, reimpulsar la economía, restablecer la justicia y garantizar la libertad de los ciudadanos. La historia muestra que los países que no protegen su Estado terminan perdiéndolo. Por eso, hoy más que nunca, Venezuela necesita recuperar la noción estratégica de su seguridad como fundamento esencial de su futuro republicano.



**LA CONCLUSIÓN QUE NADIE DEBERÍA ESQUIVAR** Un país puede renacer. Una República puede reconstruirse. Una democracia puede volver a florecer. Pero solo si se coloca la Seguridad del Estado como columna vertebral del proceso, se recupera el monopolio de la fuerza, se depura el sistema militar y policial, se restablece una justicia real, y para lograrlo se requiere un gobierno transitorio fuerte, limitado y supervisado que reconstruya las bases del Estado. Todo lo demás es ilusión. Todo lo demás es repetir el ciclo. Todo lo demás es caer nuevamente en el abismo. La República renace desde la fuerza legítima, desde la estrategia, desde la seguridad. Nunca desde la improvisación, la ingenuidad ni la debilidad política. No se puede edulcorar: todo país devastado necesita una fase de autoridad fuerte, disciplinada, temporal y supervisada internacionalmente.

No para instaurar una dictadura: para impedir que las mafias y grupos criminales impongan la suya. Europa lo hizo después de 1945. Japón lo hizo. Alemania Federal lo hizo. Corea del Sur lo hizo. Varios países latinoamericanos lo hicieron. Solo después de estabilizar el Estado, reconstruir instituciones, recuperar el territorio y neutralizar amenazas, fue posible reinstalar la democracia. Sin una etapa de autoridad legítima y eficaz, el ciclo es siempre el mismo:

**caos → ingobernabilidad → regreso del régimen criminal.**





**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/)**



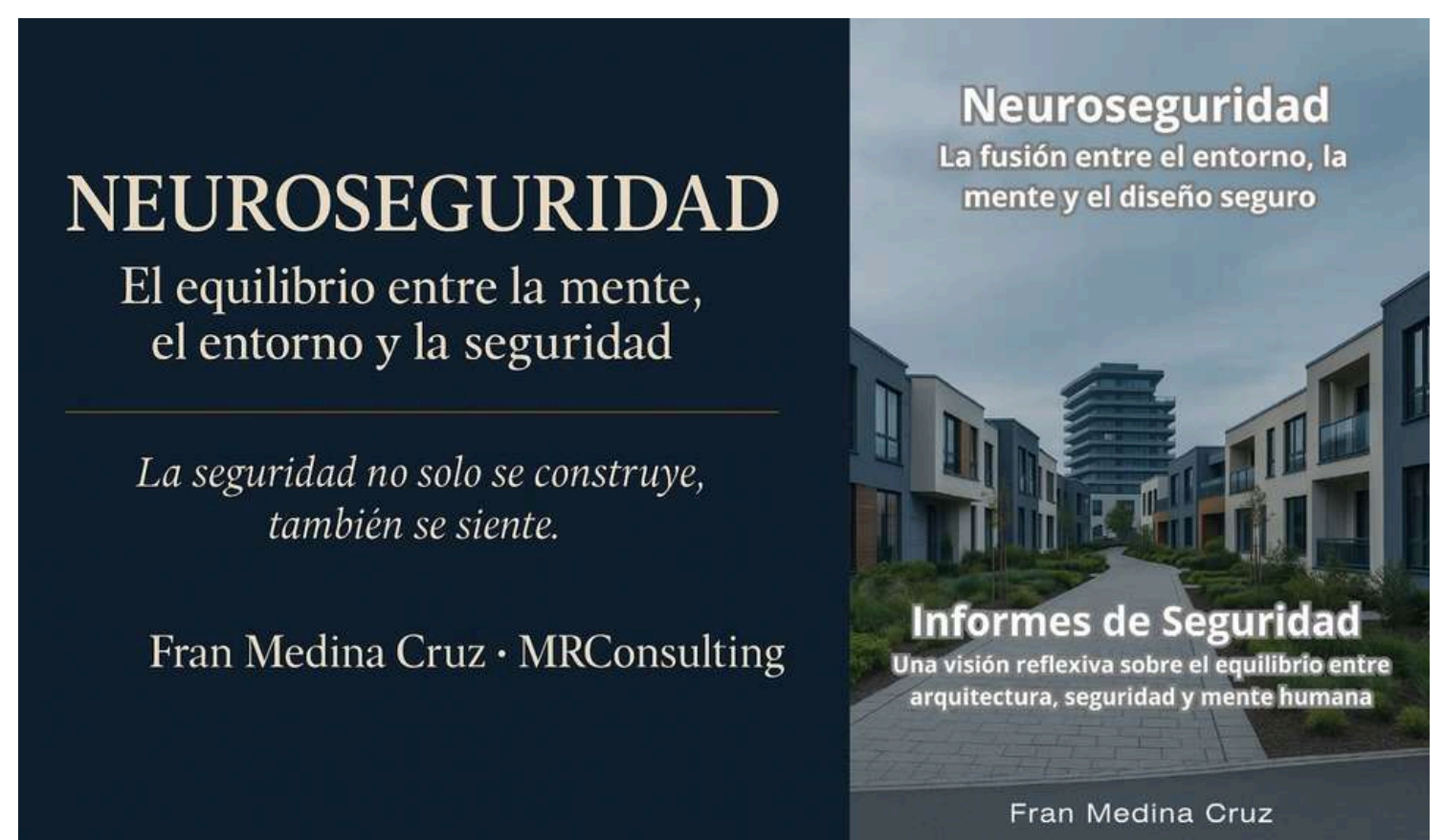
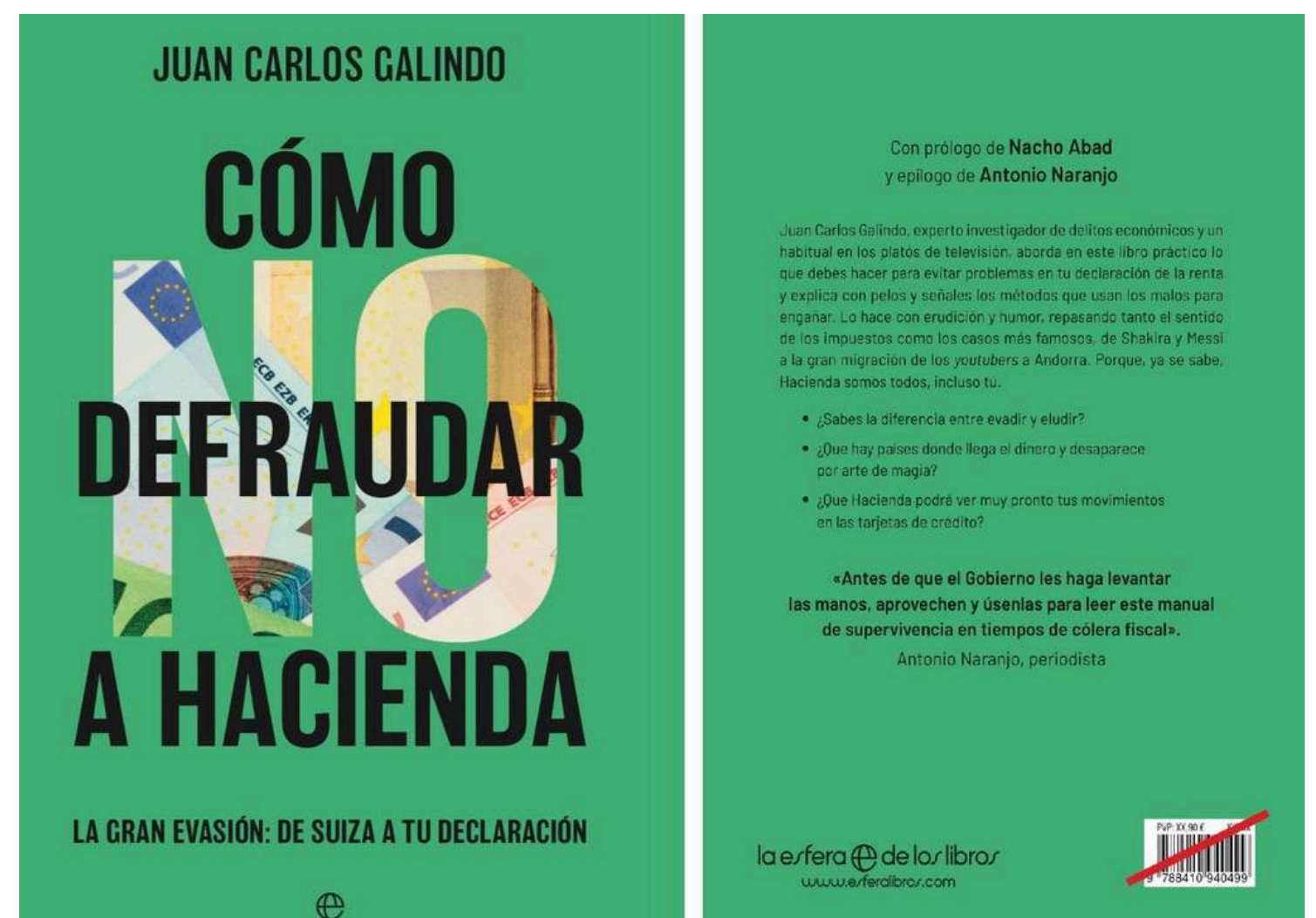
# AGENDA

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.







# Metrorisk Proyecto Asociativo

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