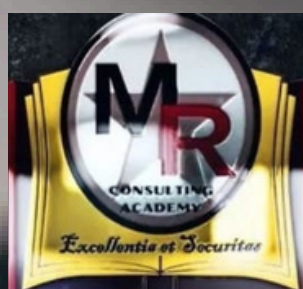


EDITORIAL MR



ISSN 3045-7629

MARZO
ABRIL

AÑO
2026

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz
Francisco Javier Gonzales Fuentes
Carlos G. Barrett
Gregorio Duro
Mercedes Escudero Carmona
Iván Cantalapiedra
Emilio Piñeiro
Joaquín Sampedro
Rosa Fernández
Carlos Serrano
Abraham Santana
Alina Rubio
Elena de la Parte
Carlos Ortiz
Rafael Ortega Quintana
Jonatthan Hermida Sosa
Carlos E Pérez Barrios
Salvador Romani.
Rafael Soler Penadés
Edison Cadena Ayala

@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 IMPORTANCIA DE LAS CERTIFICACIONES EN LOS SERVICIOS DE SEGURIDAD

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz
Director de MetroRisk

Garantía técnica, confianza y eficacia real de los sistemas implementados

En el ámbito de la seguridad, especialmente en entornos residenciales, corporativos, hoteleros o de alto valor, no basta con instalar cámaras, alarmas o puertas blindadas. La eficacia real de un sistema de seguridad depende de que los materiales, equipos y soluciones implementadas estén certificados conforme a normas técnicas reconocidas.

Las certificaciones constituyen el mecanismo mediante el cual organismos independientes verifican que un producto o sistema cumple con criterios objetivos de resistencia, fiabilidad, durabilidad y eficacia frente a amenazas reales.

Sin estas certificaciones, la seguridad se convierte en una cuestión meramente comercial o estética, pero no necesariamente técnica ni efectiva.

En el ámbito de la seguridad existe una idea ampliamente extendida que, sin embargo, resulta engañosa: pensar que la seguridad se logra simplemente instalando dispositivos visibles. Cámaras, alarmas, puertas blindadas o controles de acceso suelen asociarse de manera automática con protección. No obstante, la verdadera eficacia de un sistema de seguridad no reside únicamente en su presencia, sino en la calidad técnica de los elementos que lo componen y, sobre todo, en la verificación objetiva de que esos elementos funcionan realmente como deben hacerlo. En este punto es donde las certificaciones adquieren un valor fundamental.

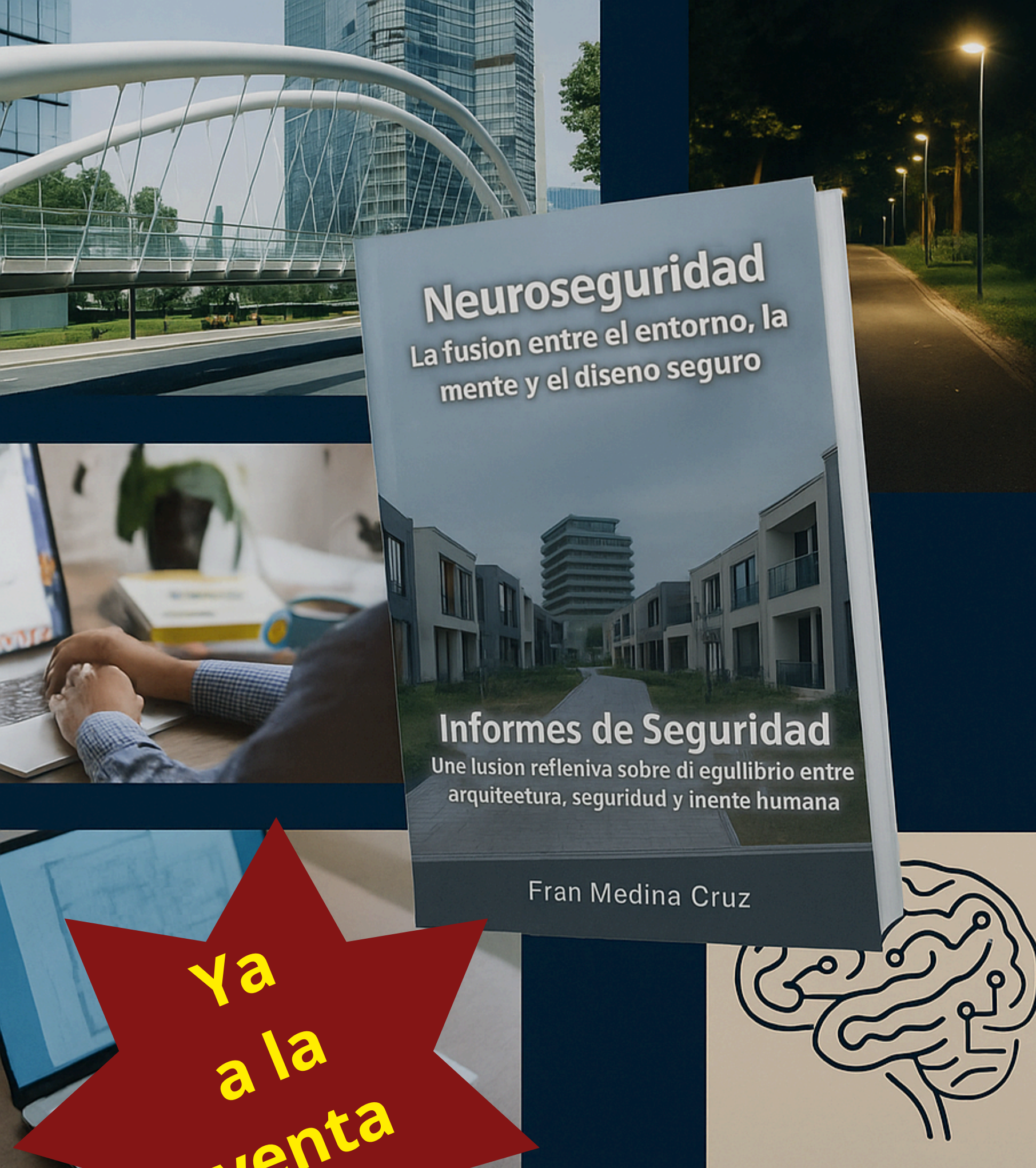
Las certificaciones constituyen el mecanismo mediante el cual un organismo técnico independiente evalúa un producto o sistema de seguridad y confirma que cumple determinados estándares de resistencia, fiabilidad y eficacia frente a amenazas reales. No se trata de una simple etiqueta comercial ni de una declaración del fabricante. Una certificación implica que el producto ha sido sometido a ensayos técnicos, pruebas de laboratorio y procedimientos de verificación que permiten medir su comportamiento frente a intentos de intrusión, manipulación o deterioro. De este modo, la seguridad deja de basarse en promesas o percepciones y pasa a sustentarse en criterios verificables.



Cuando un elemento de seguridad está certificado, existe una referencia técnica clara que permite conocer sus capacidades reales. Una puerta de seguridad, por ejemplo, puede ser visualmente robusta y transmitir una sensación de protección considerable, pero esa percepción no garantiza necesariamente que resista un ataque. Solo mediante una certificación basada en normas técnicas específicas se puede determinar el nivel de resistencia frente a herramientas, impactos o intentos de forzamiento. Lo mismo ocurre con los vidrios de seguridad, las cerraduras, los sistemas de alarma o los dispositivos de videovigilancia. La certificación establece un lenguaje común que permite comparar productos y comprender cuál es su verdadero nivel de protección.

La ausencia de certificaciones en los materiales o sistemas de seguridad es, en muchos casos, uno de los factores que explica por qué determinados entornos aparentemente protegidos presentan vulnerabilidades importantes. En el mercado existen numerosos productos que se presentan como soluciones de seguridad pero que no han sido sometidos a procesos rigurosos de ensayo. En estas circunstancias, la seguridad puede terminar convirtiéndose en un elemento meramente estético o comercial, donde la apariencia de robustez sustituye al rendimiento real frente a un ataque. El resultado es una falsa sensación de seguridad que puede resultar especialmente peligrosa en entornos donde la protección debería ser un elemento prioritario.

Las certificaciones aportan también un elemento esencial para el diseño técnico de los sistemas de seguridad: la estandarización. Gracias a las normas técnicas, arquitectos, ingenieros, consultores de seguridad, instaladores y propietarios pueden trabajar sobre criterios objetivos. En lugar de recurrir a descripciones ambiguas como "puerta segura" o "sistema de alarma eficaz", es posible especificar niveles de resistencia, grados de seguridad o estándares de calidad que han sido previamente definidos por organismos técnicos internacionales. Este marco común permite diseñar proyectos con mayor precisión y garantiza que todos los actores implicados comprendan exactamente qué nivel de seguridad se está implementando.



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



LA CONSULTORÍA EN COMPLIANCE Y EL DIRECTOR DE SEGURIDAD COMO OFICIAL DE CUMPLIMIENTO NORMATIVO

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

En los últimos años, el Compliance o cumplimiento normativo ha dejado de ser un elemento accesorio en las organizaciones para convertirse en un pilar estratégico de gobernanza corporativa. La evolución legislativa, la responsabilidad penal de las personas jurídicas, la presión reputacional y la creciente complejidad regulatoria han situado el cumplimiento en el centro de la gestión empresarial.



En este contexto, la consultoría en Compliance y el papel del Director de Seguridad como Oficial de Cumplimiento Normativo adquieren una relevancia cada vez mayor.

1. La consultoría en Compliance: más que una obligación, una ventaja competitiva

El Compliance no debe entenderse únicamente como un mecanismo de defensa frente a sanciones administrativas o penales. Bien implementado, es un sistema de gestión que:

- Reduce riesgos legales y reputacionales.
- Refuerza la cultura ética corporativa.
- Mejora la confianza de inversores, clientes y socios.
- Facilita la internacionalización y la contratación pública.

La consultoría especializada en cumplimiento normativo aporta metodología, independencia y visión estratégica. No se trata solo de elaborar un “manual de prevención”, sino de diseñar un modelo integral de gestión de riesgos, que incluya:

- Identificación y evaluación de riesgos (mapa de riesgos).
- Protocolos y procedimientos internos.
- Canales de denuncia y protección del informante.
- Formación y sensibilización.
- Supervisión, auditoría y mejora continua.

El Compliance moderno es dinámico, transversal y alineado con estándares internacionales (ISO 37301, UNE 19601, entre otros).

2. El Director de Seguridad: un perfil natural para el Compliance

El Director de Seguridad, tradicionalmente vinculado a la protección de personas, activos e información, posee competencias que encajan de forma natural con la función de Oficial de Cumplimiento:

- Cultura de prevención y análisis de riesgos.
- Experiencia en investigación interna.
- Conocimiento normativo sectorial.
- Gestión de crisis y protección reputacional.
- Coordinación con autoridades y organismos públicos.

El cumplimiento normativo no es ajeno a la seguridad corporativa; al contrario, forma parte de una visión integral del riesgo. El Director de Seguridad ya trabaja con matrices de riesgo, protocolos operativos, auditorías internas y controles de cumplimiento. La transición hacia funciones de Compliance es, en muchos casos, una evolución lógica.



3. Oficial de Cumplimiento: independencia y responsabilidad

Para que el Director de Seguridad asuma la función de Oficial de Cumplimiento Normativo, deben cumplirse ciertos principios:

- Autonomía funcional.
- Acceso directo al órgano de administración.
- Recursos adecuados.
- Capacidad de supervisión real y no meramente formal.

El Compliance no puede convertirse en una función simbólica. La jurisprudencia exige modelos eficaces y supervisión efectiva para que tengan valor eximente o atenuante en materia penal. En organizaciones medianas y grandes, puede optarse por estructuras diferenciadas (Seguridad y Compliance separados). Sin embargo, en muchas empresas, especialmente en sectores regulados, el Director de Seguridad puede asumir esta responsabilidad con formación específica y marco de independencia adecuado.

4. Compliance como cultura corporativa

El verdadero cumplimiento no se limita a documentos, sino que implica cultura. Y aquí el Director de Seguridad tiene un papel estratégico:

- Promover una ética organizacional clara.
- Impulsar formación continua.
- Detectar riesgos emergentes (ciberseguridad, corrupción, fraude interno, protección de datos).
- Integrar seguridad física, lógica y jurídica en una misma estrategia de protección.

5. Una oportunidad profesional para el sector de la Seguridad

La evolución normativa y las exigencias regulatorias están abriendo una nueva línea de especialización profesional. El Director de Seguridad, con formación complementaria en Compliance y gestión normativa, puede posicionarse como:

- Oficial de Cumplimiento.
- Consultor externo en sistemas de prevención.
- Auditor interno de modelos de cumplimiento.

Experto judicial en materia de responsabilidad corporativa. No es una sustitución de funciones, sino una ampliación del campo de actuación.

ASPECTOS ÉTICOS Y LEGALES EN LA INVESTIGACIÓN PRIVADA EN ESPAÑA

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Carlos G. Barrett
Gerente general en Spy Investigación & Barrett

La investigación privada constituye una actividad profesional reconocida y regulada en España, cuyo objetivo principal es la obtención de información y pruebas sobre hechos o conductas privadas que puedan tener relevancia jurídica o contractual. Sin embargo, el ejercicio de esta actividad se encuentra sometido a un marco normativo estricto y a principios éticos que delimitan claramente su actuación. La combinación de legalidad, proporcionalidad y respeto a los derechos fundamentales es lo que diferencia la investigación profesional de cualquier forma de espionaje ilícito o intromisión ilegítima en la vida privada.



La investigación privada en España se mueve en un territorio delicado, donde la búsqueda de la verdad debe convivir necesariamente con el respeto absoluto a la legalidad y a los derechos fundamentales. Quien se dedica profesionalmente a esta actividad sabe que no se trata simplemente de observar, seguir o descubrir información, sino de hacerlo dentro de un marco jurídico muy claro que define qué puede hacerse y qué nunca debe hacerse.

En España, la investigación privada está regulada por la Ley 5/2014 de Seguridad Privada, que reconoce la figura del detective privado como un profesional habilitado por el Ministerio del Interior. Su función consiste en realizar averiguaciones sobre hechos o conductas privadas cuando exista un interés legítimo por parte de quien encarga la investigación. Este detalle es esencial: nadie puede ser investigado por simple curiosidad o por un deseo personal de vigilancia. Debe existir una relación directa entre el cliente y el hecho investigado.

La actividad del investigador privado se desarrolla principalmente en ámbitos laborales, familiares, mercantiles o patrimoniales. Sin embargo, el margen de actuación tiene límites muy claros. Un detective no puede investigar delitos públicos ni realizar funciones propias de las fuerzas de seguridad. Si durante una investigación aparecieran indicios de delito, la obligación profesional es ponerlo en conocimiento de las autoridades.



Más allá de la ley, existe una dimensión ética que define el verdadero carácter de la profesión. El investigador privado trabaja con información sensible sobre la vida de las personas, por lo que la confidencialidad, la objetividad y la proporcionalidad deben guiar cada actuación. La observación solo puede realizarse en espacios públicos o lugares accesibles, evitando cualquier intromisión en la intimidad personal, como domicilios, comunicaciones privadas o datos protegidos.

La calidad de una investigación no se mide únicamente por la información obtenida, sino por la forma en que esa información ha sido obtenida. Una prueba obtenida vulnerando derechos fundamentales pierde su valor ante un tribunal y puede convertir al propio investigador en responsable de una infracción o delito.

Por ello, el investigador privado profesional no actúa como un espía ni como un vigilante clandestino. Su trabajo se parece más al de un observador técnico que documenta hechos de manera rigurosa para que puedan ser utilizados en un procedimiento judicial si fuera necesario.

En definitiva, la investigación privada en España se sostiene sobre un equilibrio constante: buscar la verdad sin cruzar la línea que protege la libertad y la intimidad de las personas. Ese equilibrio, más que una limitación, es lo que otorga legitimidad y credibilidad a la profesión.

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...

CONTACTA con nosotros a través de:

-Email : informacion@spyinvestigacion.com

-Tlf / Whatsapp : +34 660 359 806

- www.spyinvestigacion.com

CARLOS G. BARRETT

Investigador Privado
Experto en Criminalística

Gregorio Duro
Técnico en licitaciones y Proyectos

INTRODUCCIÓN A LAS CADENAS DE MARKOV EN EL ENTORNO DEL ANÁLISIS DE RIESGOS

En el artículo de este número exploramos cómo las Cadenas de Markov permiten anticipar la evolución de los riesgos, ofreciendo una herramienta sencilla y práctica para gestionar amenazas y tomar decisiones más informadas en seguridad.

Comprender el riesgo como un proceso en movimiento. En el ámbito de la seguridad, el riesgo no es una fotografía fija, sino una realidad cambiante que evoluciona con el tiempo. Las amenazas aparecen, se transforman o desaparecen; las vulnerabilidades pueden reducirse con inversiones adecuadas o incrementarse por falta de mantenimiento; y el impacto de un incidente depende del contexto operativo del momento. En este escenario dinámico, las Cadenas de Markov, desarrolladas por el matemático ruso Andréi Márkov a comienzos del siglo XX, ofrecen una herramienta especialmente útil para analizar cómo un sistema puede pasar de una situación de riesgo a otra a lo largo del tiempo. Su principal valor radica en que permiten realizar modelos de transiciones entre estados de forma estructurada y cuantificable, facilitando la toma de decisiones basada en probabilidades y no únicamente en intuiciones o escenarios estáticos.

Qué es una Cadena de Markov y por qué resulta útil en seguridad

Una Cadena de Markov es un modelo matemático que describe un sistema compuesto por distintos “estados” y las probabilidades de pasar de uno a otro en intervalos de tiempo sucesivos. La característica fundamental es que la probabilidad del estado futuro depende únicamente del estado actual, no de la trayectoria completa previa. En términos de seguridad, un estado puede representar, por ejemplo, una situación de “normalidad operativa”, “incremento de vulnerabilidad”, “incidente en curso” o “recuperación tras incidente”. La cadena permite estimar con qué probabilidad el sistema pasará de un estado a otro en el siguiente periodo de análisis. Esto resulta especialmente útil cuando se quiere entender la evolución de un riesgo a lo largo del tiempo, valorar la eficacia de medidas correctoras o anticipar la probabilidad acumulada de que ocurra un incidente.



Aplicación práctica en un entorno de seguridad física Imaginemos una instalación crítica con tres posibles estados operativos vinculados al riesgo de intrusión:

- Estado 1: Sistema en condiciones normales.
- Estado 2: Sistema con vulnerabilidades detectadas (por ejemplo, fallo parcial en cámaras o sensores).
- Estado 3: Intrusión materializada.

A partir de datos históricos o estimaciones técnicas, se puede construir una matriz de transición que recoja las probabilidades de pasar de un estado a otro en cada periodo (por ejemplo, mensual). Supongamos que las probabilidades estimadas son las siguientes:

- Desde el estado 1: 90 % de permanecer en estado 1, 8 % de pasar a estado 2 y 2 % de pasar directamente a estado 3.
- Desde el estado 2: 60 % de volver al estado 1 tras corrección, 30 % de permanecer en estado 2 y 10 % de evolucionar a estado 3.
- Desde el estado 3: 70 % de volver al estado 1 tras resolución y 30 % de permanecer en estado 3 durante el siguiente periodo (impacto prolongado).

Estas probabilidades se organizan en una matriz de transición

$P = \begin{bmatrix} 0,90 & 0,08 & 0,02 \\ 0,60 & 0,30 & 0,10 \\ 0,70 & 0,00 & 0,30 \end{bmatrix}$

Si en el momento inicial el sistema se encuentra en estado 1, el vector inicial puede representarse como:

$$V_0 = (1, 0, 0)$$

Para conocer la probabilidad de encontrarse en cada estado en el siguiente periodo, se multiplica el vector inicial por la matriz de transición: $V_1 = V_0 * P$ El resultado será el siguiente:

$$V_1 = (0,90, 0,08, 0,02)$$

Significa que después del periodo analizado:

- 90 % de probabilidad de que siga en estado 1 (normal)
- 8 % de probabilidad de que pase a estado 2 (vulnerable)
- 2 % de probabilidad de que ocurra un incidente crítico (estado 3)

El 2 % corresponde a la probabilidad de que ocurra el fallo crítico después de un periodo, calculada directamente de la multiplicación del vector inicial por la matriz de transición. Es decir, tras un periodo, existe un 2 % de probabilidad de que se haya producido una intrusión.



Interpretación resultados estratégica de los resultados

El verdadero valor del modelo no reside solo en el cálculo matemático, sino en su interpretación. Por ejemplo, si al elevar la matriz a potencias sucesivas se observa que la probabilidad de encontrarse en estado 3 tiende a estabilizarse en un determinado valor, ese valor representa el nivel de riesgo estructural del sistema bajo las condiciones actuales. Si se toma la decisión de reforzar el mantenimiento preventivo o mejorar la redundancia tecnológica, las probabilidades de transición cambiarán. Bastará con ajustar la matriz y recalcular para comprobar el impacto real de la inversión sobre el riesgo a medio y largo plazo. De esta forma, las decisiones estratégicas dejan de apoyarse exclusivamente en escenarios hipotéticos y pasan a basarse en modelos cuantificables.

Ventajas tradicionales frente a enfoques Los métodos clásicos de análisis de riesgos suelen centrarse en estimaciones puntuales de probabilidad e impacto. Las Cadenas de Markov, en cambio, introducen la dimensión temporal de manera explícita. No solo preguntan “¿cuál es la probabilidad de que ocurra un incidente?”, sino también “¿cómo evoluciona esa probabilidad con el tiempo si no se actúa?” o “¿cómo cambia si se modifica la política de mantenimiento?”. Además, permiten integrar información empírica procedente de registros históricos, auditorías técnicas o indicadores operativos

dotando al análisis de una base más sólida y menos subjetiva.

Una herramienta matemática al servicio de la gestión

Aunque el desarrollo matemático pueda parecer complejo, la lógica subyacente es sencilla: definir estados, estimar probabilidades de transición y analizar la evolución temporal del sistema. Hoy en día, herramientas informáticas básicas permiten realizar estos cálculos con facilidad, lo que convierte a las Cadenas de Markov en un recurso accesible para departamentos de seguridad que deseen avanzar hacia modelos más predictivos. Incorporar este enfoque al análisis de riesgos supone dar un paso hacia una gestión más rigurosa, dinámica y orientada a la anticipación. No se trata únicamente de medir el riesgo presente, sino de comprender su trayectoria probable y actuar antes de que el escenario desfavorable se materialice. Quiero manifestar mi profundo agradecimiento a Metrorisk por la publicación mensual de artículos técnicos, cuyo esfuerzo continuo no solo aporta valiosa información, sino que también crea un espacio constante de análisis, reflexión y actualización para los profesionales del sector.

Gregorio Duro Navarro
Licitaciones y Proyecto



SECCIÓN

PREVENCIÓN DEL CRIMEN.

CPTED

Metro
Risk

Edición propiedad de @MetroRisk, asociación

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

HACIA LA CUARTA GENERACIÓN DE CPTED: INTELIGENCIA ARTESANAL HUMANA® COMO BASE DEL DISEÑO SOCIO-DIGITAL DE CIUDADES

Este artículo constituye una propuesta técnica y académica encaminándonos hacia una Cuarta Generación de la Metodología de Prevención del Crimen mediante el Diseño Ambiental (CPTED) como un Diseño de Ciudades y Barrios desde la perspectiva socio digital. Los lineamientos los establece Gregory Saville, uno de los fundadores de la International CPTED Association, en el White Paper: Artificial Intelligence and CPTED: Navigating the Ethical Threshold.

Como establece Gregory Saville en el libro blanco de la ICA, la Inteligencia Artificial (IA) ha dejado de ser una herramienta para convertirse en una "inteligencia aliena" que procesa la realidad urbana de formas no siempre comprensibles para el ser humano. En este contexto, nos perfilamos hacia una Cuarta Generación de CPTED, donde el espacio digital y los flujos de datos son tan influyentes en la oportunidad delictiva como la arquitectura física. Para que esta evolución no derive en una "eficiencia sin alma", la visión que propongo introduce la Inteligencia Artesanal Humana® (IAH) como el pilar fundamental que garantiza que el algoritmo sea el pincel, y no el guía, de la seguridad.

1. El Sistema de Gestión de Riesgos Socio Urbano CPTED®: de lo Estático a lo Adaptativo. La visión del camino hacia una 4ª Generación de CPTED propuesta transforma los principios estáticos de la 1ª Generación (iluminación, barreras) en un ecosistema socio digital adaptativo.

- Gestión Dinámica: utilizando las bases de Saville sobre IA Predictiva, el sistema de Escudero permite que el entorno físico reaccione en tiempo real (ej. ajuste de alumbrado o flujos peatonales) según el análisis de riesgos dinámicos.
- Prevención Proactiva: se desplaza el enfoque de la reacción a la anticipación, identificando combinaciones de variables (clima, eventos masivos, percepción ciudadana) que la IA procesa pero que la IAH® debe validar para evitar falsos positivos o "alucinaciones" algorítmicas

2. La Curaduría de Dominio contra la "Inteligencia que Aliena": Saville advierte en su reporte sobre el riesgo de las "alucinaciones" (datos falsos presentados como ciertos) y los sesgos que criminalizan zonas o grupos.

- La Respuesta de la IAH®: planteo que la verdadera resiliencia no reside en un sensor, sino en la comunidad. La Inteligencia Artesanal Humana® actúa como un filtro crítico de Curaduría de Dominio. Esto significa que los modelos de IA no se dejan al azar del Big Data, sino que son entrenados y supervisados por expertos con pensamiento crítico y ética humanista.
- Puntos de Intervención Centrados en el Humano (HCIP): coincidiendo con la exigencia de Saville, el sistema de gestión que propongo asegura que en cada nodo crítico de decisión exista un experto humano.. Es el "cocinar a fuego lento" de la IAH® contra la automatización indiscriminada. Esto es: introducir una pausa necesaria para que el experto decodifique la experiencia táctica y la traduzca en estructuras con rigor analítico

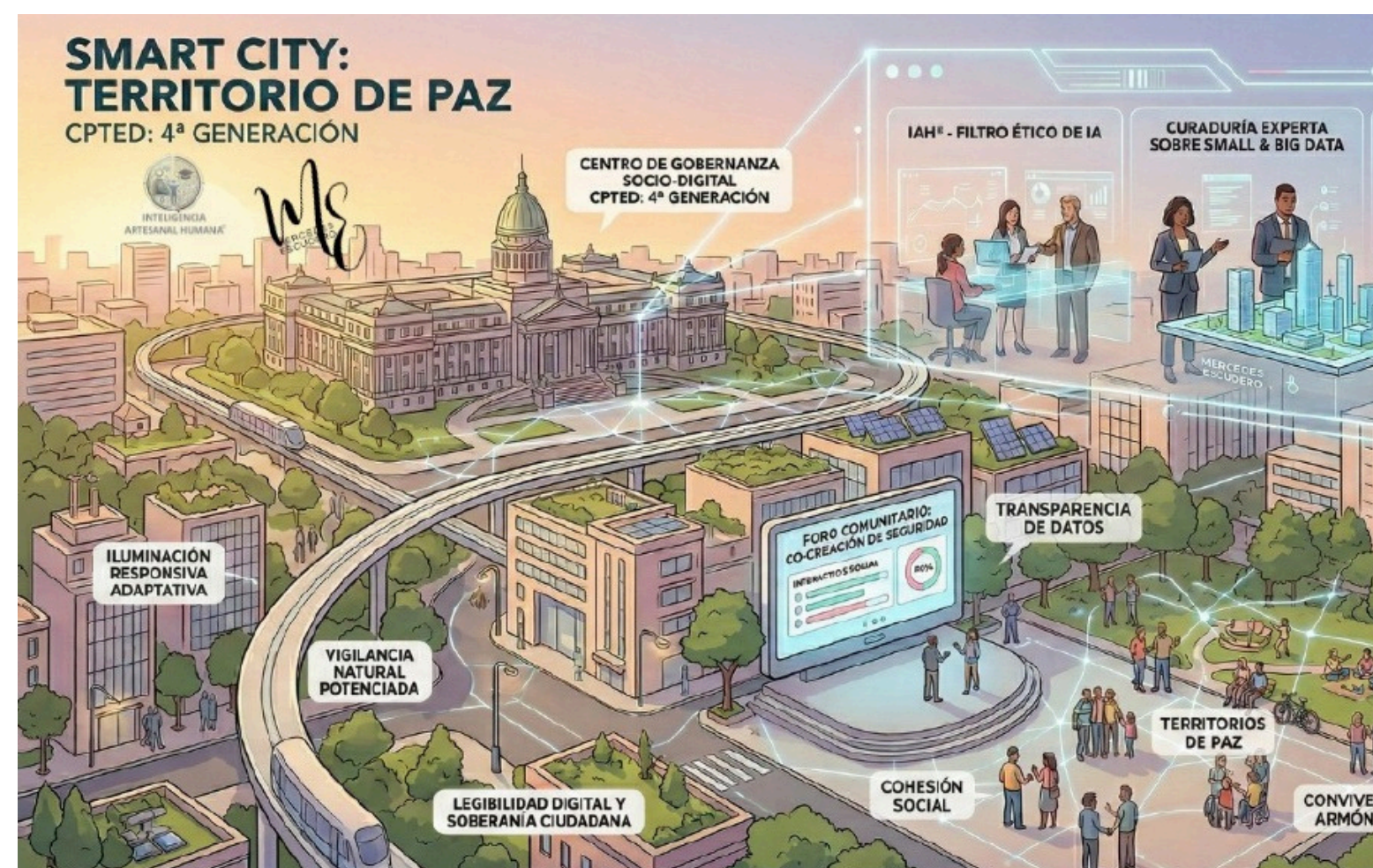


3. El Principio de Legibilidad Digital y Cohesión Social: Uno de los puntos más robustos de esta fusión es la evolución del concepto de "Legibilidad Urbana" de Kevin Lynch hacia la Legibilidad Digital.

- Transparencia y Territorialidad: Saville enfatiza que las comunidades deben saber qué sistemas las vigilan. Escudero integra esto en su sistema mediante la participación ciudadana activa, asegurando que la tecnología no erosione la "Vigilancia Natural" de los vecinos, sino que la potencie.
- Gobernanza Ética: el diseño socio-digital debe ser pedagógico. La IAH® busca que el ciudadano no sea un objeto de datos, sino un actor soberano en un territorio de paz, donde la IA mitiga sesgos bajo la supervisión de una ética artesanal humana.

La Cuarta Generación de CPTED no es una victoria de la máquina sobre el entorno, sino el renacimiento del ser humano como el artesano de su propia seguridad. La fusión de la advertencia ética de Saville y la metodología operativa de la IAH® de Escudero establece que el éxito de un barrio no se mide por el número de cámaras, sino por la capacidad de sus sistemas para respetar la dignidad humana.

En el Diseño Socio-Digital, la Inteligencia Artificial nos da la vista, pero la Inteligencia Artesanal Humana® nos da la visión. Como afirma la Dra. Escudero: "Es momento de que el algoritmo deje de ser el guía para convertirse en el pincel de nuestra propia Inteligencia Artesanal"





Pilares de Aplicación Inmediata:

- 1. Auditoría de IA bajo IAH®: revisión experta de algoritmos de vigilancia para eliminar sesgos.
- 2. Implementación de HCIP: creación de protocolos donde ninguna decisión de seguridad urbana sea 100% autónoma.
- 3. Diseño de Barrios Socio-Digitales: integración de interfaces ciudadanas transparentes en proyectos de recuperación de espacios públicos.

Para trascender las Smart Cities genéricas, debemos migrar hacia un Diseño Socio-Digital que priorice la legibilidad y la soberanía ciudadana. En este nuevo paradigma, la verdadera seguridad no reside en algoritmos que vigilan, sino en comunidades que se reconocen; por ello, el diseño de seguridad futuro se debe construir de la mano del nativo experto, quien aporta su Inteligencia Artesanal Humana®. Solo así podremos diseñar y desarrollar con ética, auténticos Territorios de Paz donde la innovación no oculte el rostro de las personas, sino que potencie una convivencia libre de miedo.



SICUR: EL PUNTO DE ENCUENTRO DEL SECTOR DE LA SEGURIDAD

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Iván Cantalapiedra. Director de Seguridad. CEO IONIQ Seguridad

Recientemente he tenido la oportunidad de visitar una nueva edición de SICUR, la Feria Internacional de la Seguridad que se celebra de forma bianual en Madrid y que se ha consolidado como uno de los principales puntos de encuentro del sector en España. En esta ocasión acudí en representación de IONIQ Seguridad, acompañado por algunos compañeros de nuestro equipo. La visita nos permitió conocer de primera mano las novedades tecnológicas del sector, mantener reuniones con proveedores y, sobre todo, compartir impresiones con otros profesionales de la seguridad tanto pública como privada.

Un punto de encuentro para el sector

SICUR es, sin duda, una feria de referencia dentro del ámbito de la seguridad. En ella se concentran fabricantes, empresas de tecnología, empresas de seguridad, departamentos de seguridad corporativa y organismos públicos. Este tipo de eventos permiten tomar el pulso al sector, conocer hacia dónde evolucionan las soluciones tecnológicas y observar cuáles son las tendencias que marcarán el futuro de la seguridad.

Pero más allá de la exposición de productos y sistemas, SICUR cumple una función muy importante como espacio de encuentro entre profesionales. Durante la feria es habitual coincidir con directores y responsables de Departamentos de seguridad, mandos de las Fuerzas y Cuerpos de Seguridad, así como con compañeros del sector con los que intercambiar experiencias y puntos de vista. En este sentido, la feria se convierte en un lugar donde se generan sinergias, se refuerzan relaciones profesionales y se abren nuevas oportunidades de colaboración.

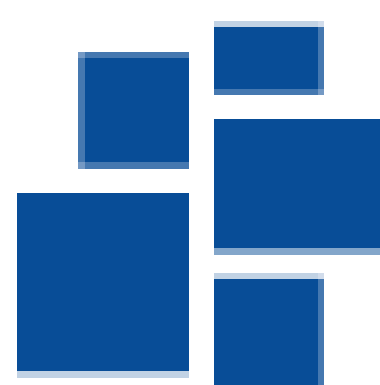
Tecnología e innovación en seguridad Uno de los aspectos más llamativos de la feria es la presencia cada vez mayor de soluciones tecnológicas avanzadas. Sistemas de videovigilancia con inteligencia artificial, analítica de vídeo, control de accesos inteligente, soluciones de ciberseguridad o integración de sistemas son algunas de las áreas que están experimentando una evolución muy significativa. La tecnología continúa ganando peso dentro del sector, permitiendo mejorar la eficiencia de los sistemas de seguridad y optimizar los recursos disponibles. No obstante, conviene recordar que la tecnología debe entenderse siempre como una herramienta al servicio de la estrategia de seguridad, y no como un fin en sí misma. El verdadero valor se encuentra en la correcta integración entre tecnología, procedimientos y factor humano.



Una feria orientada a la dirección y a la empresa Desde mi punto de vista, SICUR no es una feria especialmente orientada al personal operativo de seguridad privada, como pueden ser los Vigilantes de Seguridad que desempeñan su trabajo diariamente en los distintos servicios. Su enfoque está más dirigido hacia empresas de seguridad, fabricantes, departamentos de seguridad corporativa y perfiles de dirección y gestión del sector, así como de Seguridad Pública. Por ello, el perfil predominante de visitante suele ser el de directores de seguridad, responsables de empresas del sector, técnicos especializados, responsables de compras o gestores de seguridad corporativa. En definitiva, se trata de un entorno claramente orientado a la toma de decisiones, la innovación y el desarrollo de negocio dentro del ámbito de la Seguridad y las Emergencias.

La importancia de estar presentes Para empresas como IONIQ Seguridad, asistir a este tipo de encuentros resulta especialmente interesante. Permite mantener contacto directo con proveedores, conocer nuevas soluciones que pueden mejorar nuestros servicios y reforzar nuestra relación con otros profesionales del sector. Además, estas visitas ayudan a mantener una visión actualizada del mercado y a continuar avanzando hacia un modelo de seguridad cada vez más profesional, tecnológico y adaptado a las necesidades reales de los clientes.

SICUR sigue siendo, edición tras edición, uno de los principales escaparates del sector de la seguridad en España. Más allá de la tecnología que se presenta, su verdadero valor reside en reunir a los profesionales que trabajan diariamente para mejorar la seguridad en distintos ámbitos. Porque al final, la seguridad no solo se construye con sistemas o herramientas, sino también a través del conocimiento compartido, la colaboración entre profesionales y el compromiso del sector con su propia evolución.



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

**PROTECCIÓN DEL INFORMANTE
Y REFORMA LABORAL**

La protección del informante se ha consolidado como uno de los pilares estructurales del moderno ecosistema de cumplimiento normativo. Con la transposición de la Directiva (UE) 2019/1937 y la aprobación de la Ley 2/2023 (Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción), España inició un proceso de maduración institucional orientado a reforzar la integridad pública y privada.

El nuevo Anteproyecto de Ley que modifica el Estatuto de los Trabajadores (ET) y la Ley Reguladora de la Jurisdicción Social (LRJS) supone un paso decisivo en este camino, al incorporar de forma expresa —y con rango laboral— garantías esenciales para quienes informan de buena fe sobre irregularidades, delitos o infracciones normativas.

El presente BluePaper Territorio Compliance by Emilio Piñeiro ofrece un análisis jurídico, técnico y de Compliance del Anteproyecto, interpretando su alcance desde una perspectiva transversal que integra la responsabilidad penal de la persona jurídica, los modelos de gestión UNE 19601 (Sistema de Gestión de Compliance Penal) y UNE 19604 (Sistema de Gestión de Compliance Sociolaboral), así como la gobernanza asociada a los Sistemas Internos de Información (SII) y a la Autoridad Independiente de Protección del Informante (AIPI).

La finalidad es proporcionar a las organizaciones, a los profesionales del cumplimiento y a las administraciones públicas una lectura integral que permita comprender no solo qué cambia, sino por qué cambia y cómo debe adaptarse el marco organizativo para cumplir y liderar con integridad.

El texto que sigue aspira a ser una guía clara y rigurosa para navegar una reforma normativa que refuerza la prohibición de represalias, amplía la esfera subjetiva de protección, redefine la relación entre empresa y persona informante y eleva la exigencia de cultura ética dentro de las organizaciones. Este documento se dirige a quienes trabajan cada día por consolidar estructuras robustas de Compliance, prevenir la corrupción, profesionalizar la gestión sociolaboral y construir entornos en los que la transparencia no sea una declaración de intenciones, sino una práctica sostenida.

Territorio Compliance reafirma con esta edición su compromiso con la excelencia técnica, la divulgación práctica y la creación de valor para un ecosistema empresarial que demanda claridad, serenidad normativa y visión estratégica. Este BluePaper pretende ser una herramienta útil, aplicable y alineada con los estándares internacionales, contribuyendo al fortalecimiento de una cultura corporativa basada en la ética, la protección efectiva del informante y el respeto a los derechos fundamentales.



BluePaper · Asociación Territorio Compliance
Edición especial · 01/2026

**PROTECCIÓN DEL INFORMANTE
Y REFORMA LABORAL**

Análisis del Anteproyecto de modificación
del Estatuto de los Trabajadores y la LRJS

Integración de la Ley 2/2023 en el ámbito sociolaboral

Emilio Piñeiro Carrascosa
Autor

Con la colaboración de:
Estela Martín · Iñaki Jauregui

Territorio Compliance
Cumple · Crece · Lidera



Joaquín Sampedro Diseñador de Arquitectura de Seguridad Seguridad por Diseño

¿Cuál es el recuerdo vívido de tu infancia que te ha moldeado como persona? El taller familiar. El olor a metal, el sonido de las herramientas y la responsabilidad de abrir una puerta cuando alguien lo necesitaba. Aprendí que la seguridad no es un producto. Es servicio. Es compromiso. Es estar cuando hace falta. Eso me marcó más que cualquier formación posterior.

¿Tu medio de transporte preferido para viajar? El coche. Porque me da independencia. Me da libertad de movimiento. Y conducir me relaja. Me gusta atravesar territorios, entender cómo se construyen, cómo se habitan. Observar barrios, accesos, iluminación, flujos. La seguridad también empieza mirando. Antes de diseñar, hay que saber leer el entorno.

¿Si cambiaras de país para vivir, a cuál irías? Austria o Alemania. Países donde la ingeniería, la precisión y la planificación son cultura. Me interesa vivir donde el diseño técnico forma parte de la identidad social.

¿Qué modificarías hoy en día en nuestro país si fueras presidente? Impulsaría la integración de la Seguridad por Diseño dentro de la formación en arquitectura y construcción. Hoy hablamos mucho —y con razón— de eficiencia energética, sostenibilidad o certificaciones como BREEAM. Pero la seguridad todavía se incorpora en muchas ocasiones como un añadido técnico, no como una decisión estructural desde el proyecto. No se trata de imponer más normativa. Se trata de formar mejor. Dotar a jóvenes arquitectos y proyectistas de herramientas para:— entender la seguridad como parte de la arquitectura— anticipar riesgos desde fase de diseño— tomar decisiones de prescripción más informadas— integrar capas físicas y digitales con coherencia. Cuando la seguridad se piensa desde plano, el edificio funciona mejor durante décadas. Y eso no es solo protección. Es calidad constructiva.

¿Tu frase preferida? “La seguridad empieza dentro.” Porque todo sistema externo nace primero como decisión interna. Escoge 1 podcast para recomendar a tus seguidores “No es asunto vuestro” de Jordi Wild, por su diversidad de perspectivas. Escuchar puntos de vista distintos te obliga a pensar mejor. Y pensar mejor te hace decidir mejor. En seguridad —y en la vida— el criterio lo es todo.

¿Cuál es la importancia de la ciberseguridad en tu organización? Es estructural. Hoy la seguridad física y la digital son una sola arquitectura. Diseñar accesos inteligentes sin proteger la capa digital es dejar la puerta entreabierta. La seguridad moderna es híbrida o no es seguridad.

¿Un superhéroe en el que te gustaría tener sus superpoderes? ¿y por qué? Batman. No por los poderes, sino por la preparación. Es estrategia, anticipación y análisis. La seguridad real funciona así.



¿Si pudieras volver a vivir un año de tu vida, cuál sería y por qué? 2024. El año en que decidí reinventarme profesionalmente. Fue incómodo. Hubo dudas. Hubo silencio. Venía de años difíciles desde 2020. Caí por circunstancias personales y profesionales, y durante mucho tiempo todo fue incertidumbre. Tuve oportunidades de elegir caminos rápidos y cómodos. No los elegí. Elegí el camino que me obligaba a crecer. 2024 fue el año en que alineé lo que hacía con lo que soy.

¿Si pudieras aprender cualquier habilidad nueva en tu vida cuál sería y por qué? Arquitectura formal. No para cambiar de oficio, sino para integrar aún más profundamente la seguridad desde el plano. Mi vocación no es instalar dispositivos. Es diseñar sistemas que acompañen la vida. Siempre he tenido una virtud clara: la creatividad. Cuando me implico en algo, me aílo. Entro en foco absoluto. Solo pienso en eso hasta que toma forma. Admiro a arquitectos como Oscar Niemeyer y espacios como el Centro Niemeyer en Avilés, porque demuestran que la creatividad no es estética vacía, es visión estructural. Cuando la creatividad fluye, te da energía. Es una vitamina interna. Y no hay sensación mayor que verla materializada. Ejecutada. Convertida en algo que mejora la vida de las personas. Ese es mi objetivo: Que lo que diseño no impresione. Que funcione. Que proteja. Que aporte valor real a la sociedad.

Si pudieras vivir en cualquier época histórica, ¿cuál elegirías y por qué? El momento actual. Estamos viviendo la transformación más profunda de la seguridad: digitalización, datos, automatización, experiencia de usuario. Es el momento de diseñar la nueva arquitectura de confianza. Y en ese contexto, la Inteligencia Artificial no es una amenaza, es una herramienta. Muchos creen que la IA viene a sustituir personas. No lo comparto.

¿Un nuevo EPI para la seguridad de tu organización o empresa y para tu hogar, que no exista actualmente? Un sistema predictivo integral que combine:— comportamiento humano— datos digitales— análisis de entorno físico y que anticipe riesgos antes de que se materialicen. No reaccionar.

Anticipar.
Ese es el futuro

Joaquín Sampedro

Seguridad inteligente para vivir con confianza



SegurIA

SOLUTIONS

Protegiendo el presente.
Anticipando el futuro.

Joaquín Sampedro es consultor especializado en seguridad por diseño para proyectos de Real Estate residencial. Su metodología integra la seguridad desde la fase de diseño arquitectónico, no como un añadido posterior.

Con más de 15 años de experiencia en el sector, ha desarrollado un enfoque único que combina definición funcional, norma aplicable, criterio de ensayo (FAT/SAT) y límites de uso(incluyendo modo offline) para cada proyecto

La Metodología Joaquín Sampedro

"La experiencia sin norma confunde. La norma sin experiencia fracasa."

La metodología se estructura en 6 fases que cubren todo el ciclo de vida del proyecto: desde el análisis inicial de riesgos hasta la operación y mantenimiento, pasando por diseño, especificación, ejecución y puesta en marcha.

Cada entregable incluye siempre cuatro elementos: definición funcional clara, norma técnica aplicable, criterios de ensayo verificables y límites de uso documentados.

Contacto

Pza. Los Luceros 7-9
03003 Alicante, España
hola@seguriasolutions.com
[965 52 87 22](tel:965528722)+34 616 02 06 59



CÁMARAS CORPORALES EN SEGURIDAD PRIVADA: BREVE GUÍA DE CÓMO IMPLANTAR SU USO SIN GENERAR UN PROBLEMA LEGAL EN TU EMPRESA.

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Rosa Fernández

ASUNTO: GOBERNANZA Y CONTROL

Cada vez más empresas de seguridad privada en España están incorporando cámaras corporales a sus servicios. La decisión suele responder a una combinación de factores: mayor conflictividad en determinados entornos, necesidad de proteger al vigilante, exigencias del cliente o búsqueda de pruebas ante reclamaciones. Sin embargo, comprar cámaras y repartirlas entre el personal no equivale a implantar un sistema legalmente válido.

Desde el punto de vista de la protección de datos, hacerlo sin una mínima planificación convierte una medida pensada para proteger en una fuente directa de riesgo jurídico y reputacional. La clave no está en la cámara.

Está en cómo la empresa decide implantarla, gestionarla y controlarla. Primer error habitual: tratar la cámara como un simple “equipamiento”. Desde una lógica operativa, muchas empresas abordan la bodycam como otro medio de trabajo: uniforme, emisora, linterna. Pero desde el punto de vista legal, una cámara corporal no es equipamiento neutro.

Es un sistema que: capta imágenes de personas identificadas o identificables, registra actuaciones en contextos sensibles, y genera ficheros de datos personales. Eso sitúa automáticamente a la empresa en el ámbito del RGPD y la LOPDGDD, con todas sus obligaciones.

MAPA DE RESPONSABILIDADES. Quién decide, quién responde y quién trata los datos. Cuando una empresa de seguridad privada entrega cámaras corporales a su plantilla, debe tener claro el reparto de roles: El cliente suele ser el responsable del tratamiento (decide la finalidad del servicio). La empresa de seguridad actúa como encargada del tratamiento. El vigilante es un usuario autorizado, que trata datos por cuenta de otros. Este Mapa de Responsabilidades determina quién responde si algo se hace mal.

OJO. el vigilante no graba “para sí mismo”, graba para la EMPRESA

¿CÓMO LO HAGO LEGAL? Una implantación correcta empieza antes de que el vigilante se coloque la cámara.

- 1□ Definir la finalidad (y dejarla por escrito) Sin finalidad clara, no hay base legal sólida.
- 2□ Regular el uso mediante un protocolo interno No basta con una instrucción verbal. Debe existir un protocolo de uso, conocido y firmado Este documento protege a la empresa y al vigilante.
- 3□ Limitar el acceso a las grabaciones .
- 4□ Establecer plazos de conservación Las imágenes no pueden guardarse indefinidamente. Guardar “por si hay un problema” no es un criterio válido.
- 5□ Informar adecuadamente La transparencia no es opcional: es un requisito legal



Formación: el eslabón que más se descuida. Una de las mayores debilidades en la práctica es la formación. Entregar una cámara sin formarles en esto, es trasladar el riesgo directamente al vigilante... y devolverlo multiplicado a la empresa. La formación no debe ser genérica. Debe estar adaptada al servicio, al entorno y al tipo de intervención. Su práctica (y riesgos) más habitual de lo que piensas. ·Centro comercial: la cámara se activa durante todas las intervenciones, sin distinguir gravedad ni contexto → quejas reiteradas de ciudadanos. ·Estación de transporte: grabaciones continuas sin criterio → dificultad para justificar la necesidad del tratamiento. ·Urbanización privada: combinación de bodycams y móviles personales → pérdida total de control sobre las imágenes. En todos los casos, el problema no es la cámara, sino la ausencia de un sistema de gestión detrás.

El problema es la falta de gobernanza. Antes de repartir cámaras corporales, conviene analizar y preguntarse: ¿Tenemos claro qué se graba, por qué se graba, quién accede a las imágenes y cuánto tiempo se conservan? Si la respuesta no es clara, la empresa no está implantando una medida de protección, sino un nuevo riesgo.

Las cámaras corporales pueden ser una herramienta útil en seguridad privada. Pero solo lo son cuando forman parte de un sistema bien diseñado, con reglas claras, formación adecuada y control real. Comprar tecnología es fácil.

Implantarla conforme a la ley es lo que marca la diferencia entre proteger un servicio o ponerlo en riesgo

¿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

-Un cambio silencioso en el enfoque de responsabilidad El nuevo contexto regulatorio europeo y la evolución de los criterios de responsabilidad apuntan en una dirección clara: ya no se evaluará únicamente si una empresa cumplía formalmente la norma, sino si administraba correctamente los medios técnicos de los que disponía y si podía haber evitado razonablemente un daño. En este marco, la falta de gestión, de formación o de control sobre el uso de la tecnología deja de ser una carencia técnica para convertirse en una decisión empresarial con consecuencias jurídicas y económicas. La seguridad privada entra así en una etapa en la que el cumplimiento mínimo deja de ser un escudo suficiente. -Administrar la tecnología, no solo utilizarla

La respuesta no pasa por añadir más burocracia ni por exigir al sector una especialización inasumible. Pasa por algo más básico y, al mismo tiempo, más estratégico: administrar correctamente el uso de la tecnología y formar en alfabetización IA a su personal. Definir cómo se utiliza, en qué condiciones, con qué límites y con qué competencias asociadas. Ajustar las herramientas a la realidad operativa del personal. Anticipar escenarios de riesgo antes de que se conviertan en conflictos.

En 2026, prácticamente todas las empresas de seguridad privada utilizarán tecnología avanzada e inteligencia artificial. La diferencia no estará en quién la tiene, sino en quién sabe gestionarla y administrarla con criterio. La diferencia la marcarán las organizaciones que entienden que la tecnología mal administrada genera riesgo, y las que confían en que nada ocurra, poniendo en riesgo jurídico a sus clientes. Y en un sector donde la confianza lo es todo, esa diferencia será determinante.



Rosa 6.0

Código Experiencia

35 años transformando normativa en resultados



Diplomada en Derecho, Tecnología e Innovación

Data Tech Compliance 360° (RGPD, REIA, DATA ACT, LOPDgdd, LSICE)

Consultora Sr Calidad (ISO, EFQM, 5S)

Consultora Jurídica

Formadora Senior*

Diseñadora de material didáctico

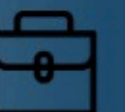
Miembro Comité Técnico Asesor en MetroRisk
Socia de ENATIC, asociación de Abogacía Digital

Competencias técnicas:

IA · MOODLE · WORDPRESS · PRESTASHOP ·
DOODLE/VÍDEO DIDÁCTICO



***+ de 25 años formando a profesionales**



LA IMPORTANCIA DE LA COLABORACIÓN ENTRE LA SEGURIDAD PRIVADA Y LA POLICÍA EN LA PREVENCIÓN DE ROBOS EN CENTROS COMERCIALES

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Carlos Serrano
Coordinador de Servicios Grupo Sureste

Cuando pensamos en la seguridad de un centro comercial, muchas veces lo primero que nos viene a la cabeza es la presencia de un vigilante uniformado recorriendo los pasillos o controlando accesos. Sin embargo, detrás de esa imagen cotidiana existe un trabajo mucho más complejo que combina la labor de la seguridad privada con la de las Fuerzas y Cuerpos de Seguridad del Estado.

Los centros comerciales son espacios donde cada día pasan cientos o incluso miles de personas. Esta gran afluencia de público también atrae a quienes buscan aprovecharse de la situación para cometer hurtos o robos. Desde pequeños robos en tiendas hasta grupos organizados especializados en la sustracción de productos, la realidad es que la prevención del delito requiere una vigilancia constante y bien coordinada.

Aquí es donde entra en juego la figura del vigilante de seguridad. En la práctica, son los profesionales que están más cerca del problema. Son quienes observan el comportamiento de los clientes, detectan movimientos sospechosos y, muchas veces, logran evitar que un hurto llegue a producirse simplemente con su presencia.

El vigilante conoce el centro, conoce las tiendas, conoce los horarios y también reconoce comportamientos que pueden resultar anómalos. Esa experiencia diaria se convierte en una herramienta fundamental para anticiparse a muchos incidentes. Pero la seguridad privada no trabaja sola.

Cuando se produce un delito o una situación que requiere una intervención mayor, la colaboración con la policía es esencial. Los vigilantes pueden retener a una persona sorprendida cometiendo un delito flagrante, recoger información o facilitar grabaciones de videovigilancia, pero la actuación policial es la que permite continuar con el procedimiento legal.

Esta relación de colaboración está contemplada en la Ley de Seguridad Privada, que establece que la seguridad privada actúa como complemento de la seguridad pública. En la práctica, esto significa que ambos ámbitos deben trabajar de forma coordinada.

En muchos centros comerciales esta cooperación funciona de manera muy fluida. Los vigilantes conocen a los agentes de la zona, existen canales de comunicación directos y se comparten avisos cuando se detectan grupos especializados en hurtos que se desplazan de un centro a otro.



www.seguridadyempleo.com



La tecnología también juega un papel importante. Los sistemas de videovigilancia, los controles de accesos o las alarmas permiten detectar incidentes rápidamente y aportar pruebas cuando es necesario. Sin embargo, por muy avanzada que sea la tecnología, sigue siendo imprescindible el factor humano: la observación, la experiencia y la capacidad de actuación de los profesionales.

La realidad demuestra que la seguridad funciona mejor cuando existe una verdadera cooperación entre todos los actores implicados. La seguridad privada aporta presencia constante y capacidad de prevención dentro de los centros comerciales, mientras que las Fuerzas y Cuerpos de Seguridad aportan autoridad policial y capacidad de investigación.

Cuando ambos trabajan en la misma dirección, el resultado es un entorno más seguro para todos: trabajadores, comerciantes y clientes.

Porque al final, la seguridad no es solo reaccionar cuando ocurre un problema. La verdadera seguridad consiste en evitar que el problema llegue a producirse. Y en ese objetivo, la colaboración entre seguridad privada y policía sigue siendo una pieza fundamental.



LAS FERIAS PROFESIONALES

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Abraham Santana Herrera
Director de seguridad. Perito

Las ferias profesionales han sido, desde hace décadas, uno de los principales puntos de encuentro para los sectores tecnológicos e industriales. En el ámbito de la seguridad privada, estos espacios adquieren una relevancia especial porque permiten algo que resulta difícil conseguir en otros entornos: reunir en un mismo lugar a fabricantes, instaladores, consultores, responsables de seguridad, instituciones y empresas usuarias de soluciones de protección. En ese contexto, encuentros como SICUR, la feria internacional de seguridad que se celebra en Madrid, se han convertido en una referencia imprescindible para comprender la evolución del sector y anticipar sus futuras transformaciones.



La seguridad privada es una actividad profundamente influenciada por la innovación tecnológica. Cada año aparecen nuevos sistemas de detección, herramientas de análisis de datos, dispositivos de control de accesos, soluciones de videovigilancia inteligente o materiales de protección física capaces de mejorar significativamente la capacidad de prevención y respuesta frente a amenazas. Sin embargo, la tecnología por sí sola no genera conocimiento aplicado. Es necesario un espacio donde los profesionales puedan observarla, analizarla, discutirla y comprender cómo integrarla correctamente en los sistemas de seguridad. Las ferias especializadas cumplen precisamente esa función: actuar como un laboratorio abierto donde el sector se observa a sí mismo y reflexiona sobre su propia evolución.

En eventos como SICUR no solo se presentan productos; se presentan ideas, enfoques estratégicos y modelos de gestión. Para los profesionales de la seguridad privada, recorrer los pabellones de una feria de este tipo supone tomar contacto directo con el estado real de la industria. Allí se pueden comparar soluciones, entender las tendencias de los fabricantes y comprobar hacia dónde se orienta el desarrollo tecnológico en materias como la inteligencia artificial aplicada a la videovigilancia, la integración de sistemas, la ciberseguridad o la protección de infraestructuras críticas.

Pero el valor de estas ferias no se limita a la tecnología. Su verdadera importancia reside también en el intercambio de conocimiento entre profesionales. Directores de seguridad, responsables de operaciones, consultores especializados y empresas proveedoras comparten experiencias, analizan problemas comunes y debaten sobre los retos que enfrenta el sector. Este diálogo permite que la seguridad privada avance no solo desde el punto de vista técnico, sino también desde la perspectiva estratégica y organizativa.

En un momento en el que la seguridad se ha convertido en un factor esencial para el funcionamiento de ciudades, infraestructuras, empresas y espacios públicos, el papel de los profesionales del sector adquiere una dimensión cada vez más relevante. La seguridad ya no se entiende únicamente como un servicio reactivo, destinado a responder ante incidentes, sino como una disciplina que debe integrarse en el diseño de los entornos, en la gestión de riesgos y en la planificación de actividades económicas. En este sentido, ferias como SICUR contribuyen a reforzar la identidad profesional del sector, ofreciendo un escenario donde se visibiliza su importancia dentro de la sociedad contemporánea.

Otro aspecto fundamental es la capacidad de estos encuentros para generar redes profesionales. Muchos proyectos, colaboraciones e iniciativas nacen precisamente en los pasillos de una feria, en una conversación entre especialistas o en una presentación técnica. La seguridad privada es un campo en el que la cooperación entre diferentes actores resulta imprescindible: fabricantes, instaladores, consultores, empresas de seguridad, administraciones públicas y usuarios finales deben trabajar de forma coordinada para crear entornos realmente seguros. Las ferias facilitan ese contacto directo que, en muchas ocasiones, se convierte en el inicio de futuras alianzas.

Además, estos eventos permiten evaluar el grado de madurez del propio sector. La presencia de determinadas tecnologías, la forma en que se presentan las soluciones o los temas que protagonizan las jornadas técnicas reflejan las preocupaciones y prioridades del momento. En los últimos años, por ejemplo, la integración entre seguridad física y ciberseguridad, el uso de analítica avanzada o la aplicación de inteligencia artificial han pasado a ocupar un lugar central en la conversación profesional. Este tipo de tendencias se perciben con claridad en ferias como SICUR, donde la industria muestra hacia dónde se dirige.

Para muchos profesionales, asistir a estos encuentros supone también una oportunidad de actualización y aprendizaje. Conferencias, demostraciones y presentaciones técnicas permiten conocer nuevas metodologías, normativas y enfoques de gestión del riesgo. En un sector en constante transformación, mantenerse al día es una necesidad, y las ferias ofrecen un entorno privilegiado para adquirir ese conocimiento de manera directa.



NO ASEGURES LO QUE VALE MÁS. ASEGURA LO QUE MÁS TE DOLERÁ PERDER

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Alina Rubio de las Casas Experta en Seguros Generales

En muchas ocasiones, cuando se habla de seguridad o de protección, las personas tienden a pensar en términos materiales. Se protege aquello que tiene un valor económico visible: una vivienda, un vehículo, un negocio o determinados bienes que representan un patrimonio acumulado con el tiempo. Sin embargo, si se observa con detenimiento, la verdadera lógica de la seguridad no reside únicamente en proteger lo que cuesta más dinero, sino en proteger aquello cuya pérdida tendría un impacto más profundo en nuestra vida.

Existe una reflexión que resume bien esta idea: no se trata de asegurar lo que vale más, sino de asegurar lo que más dolería perder. Muchas personas aseguran el coche más caro o la casa más grande, pero olvidan proteger aquello que realmente sostiene su vida cotidiana. Los bienes materiales pueden reemplazarse. Un objeto puede volver a comprarse. Incluso una propiedad puede reconstruirse. Pero hay cosas cuya pérdida genera un vacío mucho más difícil de reparar. Esta reflexión adquiere una dimensión especial cuando se observa desde la perspectiva del sector de la seguridad privada y de quienes trabajan en él. Detrás de cada sistema de seguridad, de cada protocolo y de cada tecnología instalada, existe una idea fundamental: la protección de aquello que realmente importa. La seguridad no se limita a evitar robos o intrusiones; su propósito último es preservar la estabilidad de las personas, de las empresas y de las comunidades.

Los profesionales de la seguridad privada comprenden bien esta realidad. Cuando un director de seguridad diseña un sistema de protección, cuando un consultor analiza vulnerabilidades o cuando un vigilante protege una instalación, en realidad está trabajando para evitar consecuencias que podrían afectar profundamente a la vida de otros. La pérdida de un activo crítico, la interrupción de una actividad empresarial o un incidente que afecte a las personas puede tener efectos que van mucho más allá del valor económico de los bienes protegidos.

En el ámbito empresarial ocurre algo similar a lo que sucede en la vida personal. Muchas organizaciones invierten en proteger sus instalaciones, su tecnología o sus activos físicos, pero a veces olvidan que lo más importante que poseen es su capacidad de seguir funcionando. Un incidente de seguridad no solo implica una pérdida material; puede significar la paralización de la actividad, la pérdida de confianza de los clientes o un daño reputacional difícil de reparar. Por eso, la seguridad moderna ha evolucionado hacia una visión más amplia basada en el análisis de riesgos. Ya no se trata únicamente de proteger lo más caro, sino de identificar aquello cuya pérdida tendría consecuencias más graves para la continuidad de la organización o para la seguridad de las personas. La pregunta clave deja de ser cuánto vale un objeto y pasa a ser qué ocurriría si desaparece o deja de funcionar.

Alina Rubio

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

GRUPO BORRERO



**No asegures lo que vale más.
Asegura lo que más te dolerá perder.**

**La gente se obsesiona con asegurar el coche más caro, la casa más grande.
Pero se olvidan de asegurar lo que realmente importa.**

**Cuando tuve a mi primera hija en 2013, todo cambió.
Ya no era solo yo. Ya no era solo "sobrevivir". Era proteger a alguien
que dependía completamente de mí.**

**Y me di cuenta de algo:
Podía perder el coche y seguir adelante. Podía perder muebles,
ropa, objetos.**

**Pero si perdía mi capacidad de trabajar, si algo me pasaba a mí...
Mi hija lo perdía TODO.**

**Por eso ya no hablo de asegurar coches o casas. Hablo de asegurar
tu capacidad de cuidar a los tuyos.**

Porque puedes reemplazar un móvil. Puedes comprar otro sofá.

Pero no puedes reemplazar a mamá. O a papá.

No puedes reemplazar tu capacidad de generar ingresos.

**Entonces, la pregunta no es: "¿Cuánto vale esto que quiero
asegurar?"**

La pregunta es: "¿Qué pasaría si lo pierdo?"

**Si la respuesta es "nada grave", probablemente no necesitas
asegurarlo.**

Si la respuesta te quita el sueño, entonces sí.

Asegura lo que más te dolerá perder. No lo que más dinero cuesta.

EL EFECTO DOMINÓ

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Elena de la Parte

Imagina un salón majestuoso en lo alto de un castillo gótico, enclavado en el corazón de una metrópolis futurista. Allí, entre brindis de networking de élite, varias empresas, están jugando al dominó. Cada ficha que cae, es una decisión de Inteligencia Artificial; cada patrón, es un reflejo de su ética: el movimiento de cada jugador es un suspiro de su ciberseguridad.

No estamos vaticinando el futuro, estamos diseñando tu nueva realidad competitiva: un mundo donde cada dictamen. no solo es un 300% más volátil, convirtiéndose un 100% más justa y segura. La IA ha dejado de ser una promesa, para convertirse en el motor de una transformación empresarial sin precedentes, pero para que éste motor no se gripe en mitad del ascenso corporativo. Debemos construirlo sobre dos pilares maestros: la ética y la ciberseguridad de vanguardia. Como bien sabemos en nuestra editorial de METRORISK. la palabra tiene poder, pero el algoritmo tiene impacto

El diccionario de la nueva era. Para navegar con maestría en este paradigma, es vital que compartamos la misma clave de cifrado. A menudo, la terminología técnica levanta muros que parecen infranqueables, pero en esencia, estamos hablando de conceptos profundamente humanos. Al igual, que el ritmo del tecleado de mis dedos al escribir en este mismo instante. —Ética: son las normas de lo bueno y lo malo, es decir lo permitido y lo prohibido. —Sesgo algorítmico: un trato injusto o discriminatorio automatizado por el sistema. Recordando mis lecturas inspiradoras recuerdo y cito al escritor _Franz Kafka, para advertir que, sin una supervisión humana, el algoritmo corre el riesgo de penetrar en nuestra realidad y como un camaleón en plena metamorfosis. Transformándose en un tribunal invisible, donde el individuo es sentenciado sin pruebas verídicas. Para combatir esta opacidad, es premisa fundamental una: resiliencia técnica inquebrantable y una asertividad ética que nos permita cuestionar la lógica del dispositivo.

Asegurando que el Big Data y la integridad del dato, no sea sacrificada en el altar de la eficiencia. —Deep Fakes: contenidos falsos ultra-realistas, que desafían nuestra percepción de la realidad. —Caja negra: algoritmos de funcionamiento opaco que debemos vigilar de cerca, para evitar decisiones arbitrarias. —RGPD (GDPR): nuestra Ley de protección de datos; es el escudo que garantiza que la privacidad no sea nunca una moneda o cripto moneda de cambio.

Blindando el Algoritmo. estrategias proactivas. Para que la IA no comprometa la Attack Surface Management de tu organización, es vital gestionar la seguridad con la ética desde el diseño. Aquí te comparto mis trucos, para que tu implementación sea impecable:

- Higiene de datos en Sandboxing. Antes de lanzar cualquier modelo, utiliza laboratorios de pruebas (en máquinas y entornos aislados) , para observar cómo reacciona la IA ante datos corruptos o ataques externos.
- Red Teaming Ético: No esperes al desastre. Realiza simulaciones de ataque para intentar “engañar” a tu propia IA, ante datos o metadatos .Si logras que revele datos sensibles, habrás parcheado mitigado, sellar y cerrado la brecha antes que el atacante.



- Auditoría de cajas negras: utiliza herramientas de IA explicable (XAI). Si no puedes explicar el proceso lógico de una decisión, tu sistema es vulnerable a una inyección de comandos maliciosos. Malware
- Cifrado Homomórfico: el truco definitivo de los expertos; permite que la la procese información mientras esta permanece cifrada. El sistema aprende “a ojos vendados”: es la victoria final de la técnica: obtener la respuesta sin haber tenido que revelar nunca, el secreto que la custodia, blindándote así contra cualquier filtración

La analogía del dominó: una coreografía de precisión Permíteme que te cuente esto como si fuera el clímax de una novela de suspense: imagina la ciberseguridad y la IA como dos fuerzas en una partida de dominó, dentro de nuestro castillo. La ciberseguridad es una mano cálida, amistosa y experta que coloca cada ficha con precisión milimétrica. asegurándose de qué estén alineadas y protegidas de interferencias externas; es la barrera física que previene que piezas maliciosas entren en juego. La ética, en su rol, es la dirección del desplome. Si la IA es el impulso inicial que derriba la primera pieza, la ética asegura que la caída sea constructiva y cree un patrón de valor.

Hacia un horizonte sostenible El marco legal “no es un freno” a la innovación, es nuestra guía de navegación. Mientras la Unión Europea lidera con el RGPD y organismos. como OpenAI o APeople establecen hojas de ruta éticas, la meta empresarial permanece nítida con el objetivo de proteger los derechos digitales, mientras escalamos el éxito empresarial. La implementación de la IA requiere criterios de integridad y transparencia para lanzar la ciberseguridad a un “estatus férreo”; sólo así lograremos que cada línea de código, sea un eslabón irrompible en la defensa de nuestro Big Data, transformando ese océano de información en un activo blindado, frente a la volatilidad del entorno digital

<< El futuro no se escribe sólo; lo programamos nosotros con responsabilidad. En este tablero donde las fronteras digitales definen la nueva soberanía. La ciberseguridad es la diplomacia silenciosa que evita el colapso de las naciones. Tu red no es sólo networking, es el puente levadizo de un castillo digital en constante metamorfosis, adaptándose, para resistir los asedios de la era cuántica. La partida de dominó ha iniciado a escala global e internacional, un solo sesgo es la pieza que inicia el derrumbe.

FATIGA DEL OPERADOR UAS: EL RIESGO HUMANO DEL QUE NADIE HABLA

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Carlos Ortiz
Ritrac Drones

Durante la última década, el crecimiento del sector UAS ha sido vertiginoso. Nuevas plataformas, sensores cada vez más sofisticados, sistemas automáticos de evitación, inteligencia artificial aplicada al vuelo y una narrativa dominante que repite una idea tranquilizadora: la tecnología ha reducido el riesgo. Sin embargo, esa afirmación solo es parcialmente cierta.

Porque mientras la tecnología ha avanzado a gran velocidad, la gestión del factor humano ha quedado peligrosamente rezagada. En el centro de toda operación con drones —por automatizada que sea— sigue existiendo una figura clave: el operador. Y es precisamente ahí donde se esconde uno de los riesgos más ignorados, menos medidos y peor gestionados del sector: la fatiga del operador UAS.

La ilusión de control en tierra. A diferencia de la aviación tripulada, el operador UAS trabaja desde tierra, en un entorno que transmite seguridad: una silla, pantallas, un mando, una carpa o una sala de control. No hay vibraciones, no hay fuerzas G, no hay cabina cerrada ni ruido constante. Esta aparente comodidad genera una ilusión de bajo esfuerzo que es profundamente engañosa. El operador UAS no sufre tanto una fatiga física como una fatiga cognitiva sostenida, resultado de mantener durante largos periodos:

- Atención constante y sin pausas reales
- Vigilancia pasiva prolongada
- Interpretación simultánea de datos visuales, telemétricos y contextuales
- Toma de decisiones críticas con información incompleta
- Responsabilidad legal directa sobre cada acción

Todo ello, además, con la presión implícita de que “no debería pasar nada”

La carga cognitiva: el enemigo que no aparece en los manuales En muchas operaciones profesionales, el operador UAS no está “pilotando” activamente. Está supervisando sistemas automáticos, corrigiendo pequeñas desviaciones y esperando que algo rompa la normalidad. Ese estado de espera activa es uno de los mayores generadores de fatiga mental conocidos. Obliga al cerebro a mantenerse alerta sin estímulos claros, lo que provoca:

- Descenso progresivo de la atención
- Automatización mental de decisiones
- Pérdida de sensibilidad ante alertas
- Reducción de la capacidad de reacción

Cuando finalmente aparece una anomalía, el operador debe pasar en segundos de un estado pasivo a uno altamente reactivo. Y ese salto cognitivo, bajo fatiga, es donde se cometen los errores



La monotonía como factor de riesgo operativo En seguridad, vigilancia perimetral, control de eventos o supervisión de infraestructuras, la monotonía es parte del trabajo. Paradójicamente, cuanto más “tranquila” es una operación, mayor es el riesgo latente. La monotonía:

- Reduce la percepción del riesgo real
- Fomenta el exceso de confianza
- Incrementa la dependencia de los sistemas automáticos
- Disminuye la conciencia situacional

Cuando todo funciona durante horas, el cerebro asume que seguirá funcionando. Y cuando deja de hacerlo, la respuesta ya no es óptima

Fatiga acumulada: el problema estructural. La mayoría de los incidentes UAS no se explican por una mala decisión aislada, sino por fatiga acumulada. Una suma de factores que rara vez se analizan juntos:

- Turnos prolongados sin pausas cognitivas
- Operaciones encadenadas en distintos entornos
- Escasez de personal cualificado
- Presión del cliente o del mando operativo
- Responsabilidad legal constante y personal

En muchos entornos profesionales UAS, no existen límites claros de carga operativa, ni herramientas reales para evaluar cuándo un operador ha superado su umbral cognitivo seguro. El operador puede “aguantar”, pero su rendimiento ya no es el mismo





Errores pequeños, consecuencias reales La fatiga rara vez provoca fallos espectaculares. Provoca errores sutiles, acumulativos, difíciles de detectar:

- Reacciones tardías ante alertas del sistema
- Mala interpretación de altura, distancia o velocidad
- Decisiones excesivamente conservadoras o innecesariamente arriesgadas.
- Fallos de comunicación con equipos en tierra
- Pérdida progresiva de conciencia situacional

Tras el incidente, el diagnóstico suele ser rápido y cómodo: error humano. Pero esa etiqueta genérica evita la pregunta importante: ¿por qué ese operador estaba en ese estado?

El protocolo I'M SAFE: una barrera que incomoda El protocolo I'M SAFE es una herramienta clásica en aviación tripulada para la autoevaluación del estado psicofísico del piloto antes de una operación. En el ámbito UAS, cuando existe, suele aplicarse de forma superficial. Y sin embargo, bien utilizado, es una de las mejores defensas contra la fatiga y el error humano.

Adaptado a operaciones UAS, el I'M SAFE obliga al operador a evaluar seis áreas críticas: Illness (Enfermedad) Dolores leves, infecciones, cefaleas o malestar general afectan directamente a la atención sostenida.

En operaciones UAS, donde la carga es principalmente cognitiva, este factor es determinante. Medication (Medicación) Antihistamínicos, analgésicos, relajantes musculares o incluso suplementos pueden alterar reflejos y toma de decisiones. Su impacto suele subestimarse. Stress (Estrés) Presión operativa, conflictos laborales, urgencias artificiales o problemas personales influyen directamente en la gestión del vuelo. Estar en tierra no elimina el estrés. Alcohol Más allá del consumo directo, los efectos residuales (fatiga, lentitud cognitiva) son un factor real, especialmente en operaciones tempranas. Fatigue (Fatiga) El elemento más ignorado. No se trata solo de horas de sueño, sino de fatiga mental acumulada, monotonía y ausencia de pausas reales. Emotion / Eating (Emoción / Alimentación) Estados emocionales alterados, hambre o deshidratación reducen la capacidad cognitiva y aumentan la irritabilidad y el error.

El verdadero problema: qué pasa cuando alguien dice “no”. El I'M SAFE no falla por el protocolo en sí. Falla cuando:

- No es vinculante
- No está respaldado por la organización
- Penaliza al operador que decide no volar
- Se percibe como una debilidad y no como profesionalidad

Si un operador UAS no puede detener una operación por motivos psicofísicos sin consecuencias, el riesgo ya no es individual: es sistémico.

Caso operativo: el incidente anunciado Operación nocturna de vigilancia perimetral. Tercer turno consecutivo del mismo operador. Vuelo automatizado, sin incidencias previas. Tras casi una hora de operación, aparecen interferencias leves.

El sistema avisa. El operador reacciona tarde. Corrección insuficiente. Pérdida de enlace. Aterrizaje de emergencia fuera del área prevista. Investigación interna. Conclusión: error humano. Lo que no aparece en el informe:

- Dos noches de descanso deficiente
- Estrés previo al turno
- Ausencia de briefing real
- I'M SAFE cumplimentado como trámite

El dron funcionó correctamente. El sistema organizativo, no

Medidas incómodas, pero necesarias Gestionar la fatiga del operador UAS implica asumir decisiones que no siempre gustan:

- Límites claros de carga operativa por operador
- Rotación real de funciones
- Pausas cognitivas planificadas
- Uso real del I'M SAFE como herramienta de decisión
- Cultura organizativa que respalde parar una operación

La seguridad UAS no se mejora añadiendo tecnología. Se mejora protegiendo al ser humano que toma decisiones cuando algo falla

El error no empieza en el mando, empieza en el sistema Si el sector UAS quiere madurar, profesionalizarse y ganar legitimidad, debe aceptar una verdad incómoda: El factor humano sigue siendo el eslabón más frágil porque es el menos protegido. Mientras la fatiga del operador sea un tabú, los incidentes seguirán repitiéndose y los informes seguirán señalando a la persona en lugar del sistema. Cuando un operador cansado comete un error, no es una sorpresa. Es una consecuencia previsible. Y mirar hacia otro lado también es una decisión operativa



LA SEGURIDAD PRIVADA EN EL PUERTO DE ALGECIRAS

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Rafael Ortega Quintana

Un pilar esencial y siempre los grandes olvidados.

El Puerto de Algeciras es uno de los enclaves marítimos más importantes de España y Europa, tanto por el movimiento de mercancías como por el constante tránsito de pasajeros hacia destinos como Ceuta y Tánger. Sin embargo, dentro de este engranaje fundamental para la economía y la conectividad marítima, existe un colectivo imprescindible que sostiene gran parte de la seguridad diaria y que, pese a su esfuerzo constante, sigue siendo uno de los “grandes olvidados”: la Seguridad Privada

Los vigilantes de seguridad desempeñan un papel clave en la vigilancia y protección de infraestructuras críticas del puerto, actuando como un complemento y apoyo a las Fuerzas y Cuerpos del Estado. FCSE. Contribuyendo a mantener el orden y garantizando la seguridad en puntos estratégicos del recinto portuario.

Seguridad en embarques y zonas de tránsito de pasajeros. La seguridad privada desarrolla diariamente funciones esenciales en las zonas de embarque de pasajeros y vehículos con destino a Ceuta y Marruecos, manteniendo la vigilancia preventiva, controlando accesos autorizados y actuando para evitar situaciones de riesgo. Su labor resulta clave para garantizar que el tránsito de viajeros y la logística, se realice con normalidad, especialmente en zonas donde la concentración de personas y vehículos requiere una presencia constante.

Control y vigilancia del tráfico pesado Otra de las áreas más exigentes del puerto es el Parking de Transporte Pesado, donde se concentra a diario un gran volumen de camiones. La Seguridad Privada desempeña aquí un trabajo indispensable para mantener el orden y la organización, apoyando en la gestión del flujo de transportistas y evitando incidencias. En zonas como la terminal EVOS, donde la actividad logística es continua y donde también prestan servicio compañeros de seguridad privada, los vigilantes realizan una labor constante de vigilancia y control, asegurando el correcto funcionamiento del entorno y reforzando la seguridad en todo el recinto.

Protección de terminales y de contenedores e infraestructuras estratégicas. En las terminales de contenedores, la seguridad privada cumple una función vital, protegiendo instalaciones de alto valor estratégico, supervisando zonas sensibles y evitando accesos no autorizados. Su trabajo se centra en la prevención y en garantizar que la operativa diaria se realice con seguridad, protegiendo tanto mercancías como infraestructuras.

Garantizar la seguridad del buque Uno de los aspectos más importantes del trabajo de seguridad privada en el Puerto de Algeciras, es su papel en la seguridad del buque, garantizando que las condiciones de protección se cumplan y que el entorno del embarque se mantenga bajo control. Se trata de una labor discreta, pero esencial, que contribuye directamente a la seguridad marítima y al correcto desarrollo de las operaciones portuarias.



La OPE: máxima exigencia y responsabilidad. Durante la Operación Paso del Estrecho (OPE), el puerto de Algeciras se convierte en uno de los puntos con mayor tránsito de Europa. En esas fechas la presión operativa aumenta notablemente, con miles de personas y vehículos concentrándose en el puerto para cruzar hacia el norte de África. En este contexto, la seguridad privada realiza un esfuerzo extraordinario, reforzando su presencia en los puntos críticos, garantizando la seguridad del embarque y colaborando activamente para que el operativo se desarrolle con orden y eficacia.

Un trabajo imprescindible que merece reconocimiento La seguridad en el Puerto de Algeciras es una parte esencial del engranaje diario del recinto portuario. Su labor, basada en la vigilancia, la prevención y la protección de infraestructuras y buques, permite que el puerto mantenga su actividad con seguridad durante todo el año, especialmente, en operaciones de gran magnitud como la OPE. Por ello, es importante que se reconozca el papel de este colectivo, que cada día demuestra compromiso, profesionalidad y dedicación en unos de los entornos más exigentes del país.

“Enviar un agradecimiento a la compañera Elena Parte y a Metrorisk, por poder participar, con mi artículo en esta Editorial. Gracias por la oportunidad de dar visibilidad a nuestro trabajo de seguridad privada día a día, en Algeciras”

Por, **Rafael Ortega Quintana**

ADP 3-90: LA ESENCIA DE LA OFENSIVA Y LA DEFENSIVA EN LA DOCTRINA TÁCTICA DEL EJÉRCITO

Metro
Risk

Edición propiedad de @MetroRisk, asociación

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

En el ámbito de las operaciones militares terrestres, la existencia de un marco doctrinal sólido no solo es necesaria, sino que constituye la base sobre la cual se construye la victoria. El manual ADP 3-90, titulado *Offense and Defense* y publicado por el Departamento del Ejército de los Estados Unidos en julio de 2019, representa uno de los pilares fundamentales de ese marco. Lejos de ser un mero compendio de reglas, este documento profundiza en la naturaleza dual del combate, explorando la compleja interacción entre el arte y la ciencia de la táctica para resolver los problemas que impone el campo de batalla moderno.

Para comprender la profundidad de este manual, es esencial partir de la base de que la táctica es, ante todo, la resolución de un problema. Un comandante se enfrenta a una situación única moldeada por el enemigo, el terreno y sus propias tropas, y debe aplicar un juicio experto para emplear sus medios de manera efectiva. Este proceso se apoya en el análisis de las variables de misión, conocidas por el acrónimo METT-TC, que consideran la misión específica, las características del enemigo, las particularidades del terreno y las condiciones meteorológicas, las tropas y el apoyo disponibles, el tiempo disponible y las consideraciones civiles. Sobre este análisis, se articulan las funciones de combate movimiento y maniobra, inteligencia, fuegos, sostenimiento, protección y mando de la misión que deben sincronizarse para generar una superioridad operativa sobre el adversario.

El corazón del ADP 3-90 reside en su tratamiento de las dos formas fundamentales de la acción táctica: la ofensiva y la defensiva. La ofensiva se presenta como el medio principal para imponer la voluntad propia al enemigo, buscando su destrucción o la conquista de un objetivo decisivo.

Se caracteriza por la audacia, la concentración de poder de combate en el momento y lugar críticos, la sorpresa y un ritmo implacable que desborde la capacidad de reacción enemiga. Dentro de este paraguas, el manual distingue operaciones como el movimiento de contacto, cuyo fin es desarrollar la situación; el ataque, que puede ser hasty o deliberado según el tiempo de planificación; y las fases de explotación y persecución, diseñadas para capitalizar el éxito y aniquilar a un adversario en retirada. Por otro lado, la defensiva es conceptualizada no como una postura pasiva, sino como una fase de preparación para la futura ofensiva.

Sus propósitos incluyen ganar tiempo, desgastar al enemigo, retener terreno clave o concentrar fuerzas en otro lugar. Una defensiva exitosa se construye sobre la preparación del terreno, la seguridad de las posiciones, la capacidad de desgastar al atacante y la flexibilidad para adaptarse.

El manual detalla sus dos formas principales: la defensa de área, que se enfoca en negar al enemigo el acceso a terreno específico mediante un despliegue en profundidad, y la defensa móvil, que sacrifica terreno para atraer al enemigo a una trampa donde una reserva poderosa lo destruya mediante un contraataque decisivo.



Más allá de estas dos caras de la moneda, el ADP 3-90 otorga una importancia crítica a las operaciones que permiten y conectan la ofensiva y la defensiva. Se trata de las operaciones de habilitación, entre las que se incluyen el reconocimiento para obtener información, las operaciones de seguridad para proteger a la fuerza principal, el movimiento de tropas, y maniobras complejas como el relevo en el lugar o el paso de líneas, que permiten mantener la continuidad del combate. Finalmente, el manual subraya que la guerra es un flujo constante, por lo que la capacidad de transitar de la ofensiva a la defensiva y viceversa de manera rápida y ordenada constituye una de las habilidades más críticas para cualquier comandante, marcando a menudo la diferencia entre un éxito efímero y una victoria estratégica duradera.



CONSEJO PARA LA RECONSTRUCCIÓN DE VENEZUELA.

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Carlos Enrique Perez Barrios
Director General de GLOBAL
SECURITY ACADEMY USA

En clave política

Entre la oportunidad y el peligro de la cohabitación.

Hoy existe en Venezuela una situación totalmente nueva e inesperada. La Administración de los Estados Unidos está dominando el panorama político, luego de ejecutar una extraordinaria operación militar policial, que trajo como resultado la captura de Nicolás Maduro Moros y de su esposa Cilia Flores, ambos representantes del sistema criminal que impera en Venezuela. Sin embargo, es necesario precisar algo fundamental para no caer en errores de apreciación estratégica: no ocurrió una ruptura estructural del poder.

No cayó el sistema. No se produjo una transición formal. Lo que existe hoy es un reacomodo bajo presión externa, donde el aparato de control sigue operando, aunque obedeciendo, a duras penas, directrices emanadas desde Washington. ¿Qué escenario enfrenta la administración norteamericana luego de ese importante 3 de enero del 2026? La operación realizada el 3 de enero no busca conquistar el territorio, ni tampoco invadir a otro país. Sus objetivos son varios pero podríamos resumirlos en:

- Control estratégico del hemisferio occidental, Latinoamérica en particular.
- Cercar, bloquear y anular el tráfico de narcóticos hacia los Estados Unidos.
- Procurar un cambio de un régimen criminal para cuando las condiciones lo permitan, transitar hacia un sistema político democrático que no existe en Venezuela.
- Crear un ambiente que permita el pleno desarrollo de las actividades sociales, políticas y económicas, que generen un cambio positivo para todos los venezolanos.

Todo esto es plausible y llena de esperanza a todo un pueblo, secuestrado por el régimen por lo menos durante 30 años, aunque germinado antes de eso. Pero aquí surge el primer gran peligro estratégico: la cohabitación. Si el régimen, aún golpeado y parcialmente descabezado, logra mantenerse operando dentro de un esquema tutelado, sin desmontaje institucional profundo, lo que se estaría construyendo no es una transición, sino una legitimación progresiva del sistema que destruyó la República. La historia comparada demuestra que cuando estructuras criminales comparten espacios sin ser depuradas, utilizan el tiempo para reorganizarse, infiltrar procesos, dividir liderazgos y recuperar capacidad de maniobra.



¿Cómo se piensa evolucionar a un sistema político que genere estabilidad, seguridad en todos los sentidos y progreso?

La mano que mece la cuna, esta especie de "protectorado" que ejerce los Estados Unidos en Venezuela, está implementando acciones que persigan los objetivos, en un ambiente de desmantelamiento gradual del régimen criminal, de la manera más pacífica posible. Sin embargo, se mantiene la estructura del régimen operando, amenazando con acciones contundentes, de no cumplir con los pedidos del gobierno americano y, que a todas luces se desarrolla con una lentitud asombrosa, que se torna absolutamente peligrosa para lograr en el corto plazo el necesario cambio.

¿Puede entonces pensarse que esa lentitud no es neutra? Cada día que pasa sin ruptura real, se fortalece a las redes que sobreviven dentro del aparato del Estado. Cada semana que transcurre sin depuración institucional, le da oxígeno a actores que saben cómo ganar tiempo, cómo mover recursos, cómo infiltrar decisiones y cómo manipular narrativas.

El tiempo atenta contra la Administración Trump y sus planes, a la vez que le da oxígeno a los actores del régimen a continuar en el poder, sembrando incertidumbre, terror, censura, carencia de justicia y dignidad y mucho menos respeto a los derechos humanos y ciudadanos. Existe además un elemento que no puede ignorarse: la ventana política en los Estados Unidos no es infinita. Si la actual Administración pierde mayoría legislativa en próximos procesos electorales, el respaldo político puede debilitarse, las prioridades pueden cambiar y la presión puede diluirse. El régimen lo sabe. Su estrategia histórica ha sido resistir hasta que el contexto internacional cambie.



Carlos Enrique Pérez Barrios Magíster en Seguridad y Defensa Nacional por el Instituto de Altos Estudios de la Defensa Nacional (IAEDEN). Tesis “El Sistema Policial Venezolano”.

Consultor internacional y Director General de Global Security Academy (GLOSECA), con sede en Florida, Estados Unidos. Autor de los libros “Control de Riesgos: Manual para Estudios de Seguridad” y “El Factor M: El Éxito en la Seguridad Privada”, profesor tutor en diplomados internacionales, conferencista y analista en temas de seguridad del Estado, defensa nacional y reconstrucción institucional.

Si esa es la situación actual y la visión a corto plazo, ¿cómo podemos convertir esas buenas intenciones en logros a mediano y a largo plazo? En otros artículos que he publicado en redes y en revistas de Iberoamérica, y en entrevistas realizadas, he opinado que estamos ante un enemigo que está siendo subestimado en su potencial, capacidad política y financiera y que sabe cómo ganar tiempo para su sobrevivencia.

Mientras tanto, se mantiene una actitud represiva. Siguen los presos políticos en prisión, no se respetan los derechos humanos y continúan apresando a otros, generando la terrible autocensura. Ante esta realidad en mi opinión debe operar una RUPTURA con el régimen criminal lo antes posible, no una cohabitación administrada, no una convivencia funcional, no un acuerdo táctico que termine consolidando lo que se prometió desmontar.

Solo una ruptura permitirá iniciar una reconstrucción del país y una reinstitucionalización de todo el Estado, todo esto teniendo como pilar fundamental el ejercicio del poder para lograr la necesaria Seguridad del Estado, de la cual he hablado en artículos y entrevistas anteriormente. Para que esto sea posible si debe existir una protección por parte de los Estados Unidos, ya que sin ellos sería imposible ejecutar ningún programa. Pero esa protección no puede sustituir la conducción nacional.

Para el momento en que se produzca esa RUPTURA con toda la estructura del régimen, propongo que desde ya nos vayamos organizando conformando un grupo de talentos venezolanos, dispuestos a trabajar en la reconstrucción del país.

UNA PROPUESTA CONCRETA: “UN CONSEJO DE RECONSTRUCCIÓN DEL PAÍS”

Ante la actual coyuntura histórica que vive Venezuela, se propone la conformación de un Consejo para la Reconstrucción del País, integrado por profesionales con trayectoria, solvencia moral y reconocimiento sectorial. Esta consulta tendrá como propósito identificar nombres de venezolanos con experiencia en áreas estratégicas (seguridad, defensa, justicia, economía, inteligencia, institucionalidad, derechos humanos, entre otras), que puedan contribuir a un proceso de reinstitucionalización nacional. No se trata de cuotas partidistas, sino de legitimidad profesional y credibilidad institucional. Ignorar ese capital humano sería un error estratégico. Su participación será confidencial.

¿Cómo pienso hacer realidad este proyecto? Es necesario lograr la participación de todos aquellos miembros de todos los sectores del país, y para ello, a través de una encuesta mundial (ya que muchos de los cerebros venezolanos están exiliados en diferentes partes del mundo).

Se pedirá proponer nombres de aquellas personas, que en su valiosa opinión personal y profesional y moral, puedan formar parte de ese Consejo. No se trata de cuotas partidistas. Se trata de legitimidad sectorial. Se trata de reconstruir desde la credibilidad interna de cada institución.

¿A quiénes se les debe hacer llegar ese cuadro de postulaciones al Consejo Nacional de Reconstrucción Nacional? Existe una autoridad supranacional que está dirigiendo el proceso de cambio, y es a esa Administración de los EEUU que se le hará llegar este cuadro de méritos, de manera tal que no se subestime ese ejército de talento venezolano, de patriotas calificados profesional y académicamente, y con un alto valor moral, que estén dispuestos a asumir su responsabilidad en tan titánico reto.

En mi opinión, no se podrá ejercer a distancia el gobierno que apoya nuestra nación para rescatar y conseguir el verdadero camino a un Sistema de Gobierno Democrático, en un ambiente de seguridad, estabilidad y progreso. Sin ruptura no hay reconstrucción.

Sin depuración no hay República. Sin talento nacional incorporado no hay sostenibilidad. Y sin comprensión del factor tiempo, podemos perder la oportunidad histórica que hoy aún está abierta.

**Carlos E. Pérez Barrios,
MSc Pompano Beach, Florida, USA
2026**

**Blog controlatuseguridad.blogspot.com
email: carloseperezbarrios@gmail.com
Linkedin: Carlos Enrique Pérez Barrios I
instagram: @cperezbarrios
Whatsapp: +1 (754) 581-7101**

ADECUACION E IMPLEMENTACION DE ARMAS NO LETALES PARA LOS CUERPOS DE SEGURIDAD DE LATINOAMERICA COMO LAS PISTOLAS TASER.

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Salvador Romani.
Consultor de Seguridad
Instructor Certificado de Pistolas Taser

En américa latina el uso de PISTOLAS TASER para los cuerpos de seguridad policiales, han sido un gran éxito en minimizar el uso de armas de fuego con consecuencias fatales, en gran medida ya que los policías tienen como primera opción poder capturar a los delincuentes haciendo debido uso de sus armas no letales como lo son las PISTOLAS TASER las cuales les brindan capacidad defensiva ante las criminalidad en las calles y así pueden realizar sus labores de seguridad y prevención con excelentes resultados .

El uso de pistolas taser como arma no letal esta en crecimiento ya que países como: Alemania, Arabia Saudita , Australia , Canada, España, Finlandia , Francia, Reino Unido , Suiza, Suecia, Chile, Colombia, Brasil y Bolivia han adoptado esta valiosa herramienta para sus cuerpos policiales.

En Venezuela su uso para los cuerpos de seguridad policiales, no ha sido adecuados e implementados por regulaciones como la fiscalía, ya que a futuro se espera que esta valiosa herramienta de seguridad policial pueda ser tomada en cuenta para la prevención y seguridad de los cuerpos policiales. Como instructor certificado de pistolas taser y consultor de seguridad he observado que sería excelente la adecuación para las empresas de seguridad privadas y vigilancia como una magnifica herramienta para ser usada por los funcionarios de estas empresas después de recibir una inducción del uso de pistolas taser , solo faltaría ser aprobada por el estado venezolano y así poder contar con esta excelente herramienta de seguridad no letal. Como consultor de seguridad y asesor de seguridad de empresas recomiendo esta valiosa herramienta de seguridad para ser adoptadas por más países en sus cuerpos policiales y a futuro en Venezuela también a las empresas de seguridad y vigilancia las cuales bajarían sus costos operativos adquiriendo estos equipos.

Las pistolas Taser son armas eléctricas no letales que usan descargas de alto voltaje y bajo amperaje para causar inmovilización neuromuscular temporal, generando contracciones musculares que incapacitan al objetivo sin causar la muerte, aunque presentan riesgos y requieren entrenamiento y protocolos estrictos debido a su potencial de causar daño indirecto (como caídas) o efectos graves en personas con problemas cardíacos, siendo una herramienta intermedia entre la fuerza no letal y la letal para las fuerzas policiales.

¿Qué te hace una pistola taser? Los dispositivos de energía TASER utilizan corriente eléctrica para incapacitar temporalmente a una persona generando inmovilización neuromuscular (INM). El concepto de INM es simple: Cuando se despliega un dispositivo de energía TASER y se conecta con el cuerpo, envía una señal a los músculos para que se flexionen.

¿Qué alcance tiene una pistola taser? Es eficaz hasta 7,6 metros mediante el disparo de dos dardos unidos a sendos cables eléctricos, que transmiten los pulsos desde el arma hasta el agresor, si bien también funciona por contacto.



La experiencia policial con las pistolas Taser es mixta: son vistas como herramientas menos letales que reducen lesiones a sospechosos y agentes al inmovilizar temporalmente, facilitando el control en conflictos, pero también generan preocupación sobre su uso desproporcionado, posibles riesgos para la salud mental y la necesidad de protocolos estrictos de entrenamiento y supervisión para evitar impactos negativos en comunidades vulnerables y mantener la confianza pública



Salvador Romani
PRESIDENTE

*Servicios Ejecutivos
de Escoltas V.I.P.*

Celular Contacto: 0414-261.94.01
E-mail: escoltas805@gmail.com - salvador.romani@gmail.com
www.usmarshalsecurity.com.ve

EL INSTRUCTOR DE TIRO EN SEGURIDAD

Metro
Risk

Edición propiedad de @MetroRisk, asociación

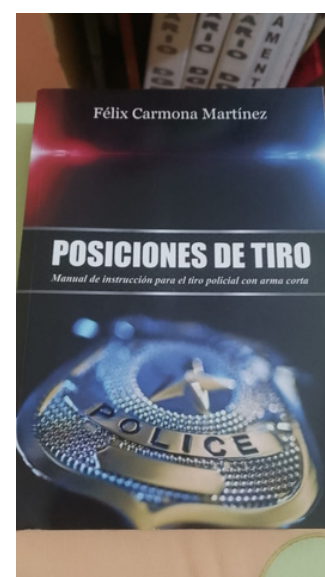
RAFAEL SOLER PENADÈS

En el ámbito que engloba a la seguridad privada, el uso responsable y controlado de las armas de fuego, en la prestación de todos los servicios armados, tanto en vigilantes de seguridad, vigilantes de explosivos, escoltas privados, guardas rurales de campo, incluyendo los ejercicios de prácticas de tiro, tanto semestrales y anuales en los vigilantes de seguridad, vigilantes de explosivos y guardas rurales de campo, trimestrales en el caso de los escoltas privados e incluso obtención de armas tipo c para nuevas licencias y prácticas de tiro en las academias, para el mismo curso de vigilantes y escoltas, constituye una competencia crítica que debe desarrollarse bajo estándares estrictos de legalidad, ética y seguridad

Dentro de este marco, el instructor de tiro desempeña un papel fundamental y esencial en la formación, evaluación y supervisión del personal habilitado. Su función no solo se limita a enseñar técnicas básicas de disparo, posiciones de tiro Weaver (la más adaptada para tiro de precisión y aconsejable siempre realizar el tiro en simple acción), recordemos que la realización de tiro de precisión se realiza a 25 metros de distancia desde la línea de tiro, hasta la línea del blanco, posición de tiro crouch (una de las mejores para tiro instintivo, ya que con ella se reduce silueta, muy importante en poca distancia), recordemos que el tiro instintivo se realiza a unos 10 metros con las 2 siluetas o posición rodilla suelo etc...etc..., sino que abarca la planificación de los ejercicios, según normativas vigentes, la prevención de riesgos, la corrección de conductas inseguras, verificación de documentación en vigor, tanto en el D.N.I, la T.I.P, licencias de armas tipo C e incluso a partir de 55 años, cada 2 años el visado de la revisión médica, algo a tener en cuenta y la consolidación de una cultura profesional orientada a la seguridad, etc.

Los ejercicios de tiro son actividades de alto riesgo potencial que exigen una dirección experta, clara y decisiva. Por ello, la presencia del instructor de tiro garantiza que la instrucción, se realice conforme a la normativa vigente y a los protocolos de seguridad, protegiendo tanto a los participantes como a terceros. Este artículo analiza de manera sistemática las principales funciones del instructor de tiro en la seguridad privada durante todos los ejercicios prácticos e inclusive me atrevería a decir mucho antes de acceder a la galería de tiro. Una de las responsabilidades fundamentales del instructor de tiro es el cumplimiento y la correcta aplicación del marco legal que regula el uso de armas en la seguridad privada. Esto incluye conocer la legislación nacional y autonómica, las órdenes ministeriales y los reglamentos específicos (reglamento de armas) que establecen, los requisitos de formación, las condiciones de los campos y galerías de tiro (exteriores o interiores, por la extracción de gases) y las obligaciones del personal armado.

El instructor actúa como garante del respeto a estas normas durante los ejercicios. Antes de iniciar cualquier práctica, verifica que los participantes estén debidamente uniformados, solo portando el material de dotación, en el caso de vigilantes de seguridad, explosivos y guardas rurales de campo y de escoltas de particular y discreto, pero todos ellos habilitados, que las armas, junto sus guías y munición, sean las autorizadas y que las instalaciones cumplan las condiciones técnicas y de seguridad exigidas. De este modo, el instructor no solo forma, sino que también supervisa el estricto cumplimiento de la legalidad.



La planificación es una función clave del director e instructor de tiro en dicho ejercicio. Cada sesión debe responder a objetivos formativos claros, adaptados al nivel de experiencia del personal y a las competencias que se desean reforzar. El director diseña el ejercicio correspondiente a dicho ejercicio, ya que puede tratarse del ejercicio anual de vigilantes de seguridad, semestral para todos los que presten servicio armados o en el caso del escolta con cambio de arma y ejercicio realizando los mismos con arma semiautomática del 9mm, ya teniendo en cuenta factores como el número de participantes (máximo línea de 30, pero cada 10 vigilantes un instructor), el tiempo disponible (siendo series de precisión 3 minutos por serie o instintivo 3 segundos por serie), el tipo de arma (vigilantes de seguridad arma de repetición, revolver cal.38 y escopeta de repetición cal.12/70 (en el caso de blindados) y guardas rural de campo, siendo la más usual la carabina de repetición cal.22, aunque puede solicitar a guardia civil el utilizar armas cortas de repetición como el revolver cal. 38) y las medidas de seguridad necesarias.

Ya se habla de la figura del director, porque de entre los instructores uno realizará toda la labor y máxima responsabilidad de todo el ejercicio de tiro, la del director de tiro, el resto de instructores darán apoyo al director, pero solo existe una voz directiva: la del director de tiro.

Asimismo, organiza la secuencia de los ejercicios para favorecer un aprendizaje progresivo y seguro. Esto implica establecer turnos, delimitar zonas de seguridad, definir las órdenes que se utilizarán durante la práctica y prever posibles contingencias. Una planificación adecuada reduce riesgos y optimiza el aprovechamiento formativo de la sesión.

POSICIONES DE TIRO

Manual de instrucción para el tiro policial con arma corta

La función más crítica del director e instructor de tiro es la seguridad. Durante los ejercicios, su atención se centra en detectar y prevenir accidentes y corregir de inmediato cualquier conducta que pueda suponer un peligro (inclusivo si se detectara y, muy importante, algún participante que no se encontrase en buenas condiciones para realizar las prácticas de tiro).

El director de tiro recuerda y refuerza de manera constante las normas básicas de seguridad, entre algunas de las más importantes que la boca de fuego del arma siempre se encuentre encarada a los blancos, nunca girarse con el arma y siempre que no se haga fuego, dedo fuera del disparador, es muy importante que todo se hable con un tono claro y decisivo para ser comprendidas y respetadas por todos los participantes y por supuesto si se observase alguna anomalía o incumplimiento de dichas normas apreciando que pone en riesgo o que pueda crear algún accidente por dicho incumplimiento, nunca dudar de parar el ejercicio de tiro y en caso de estar la supervisión de la guardia civil, informar de lo sucedido y apartar a dicha persona de la línea de tiro haciendo entrega cualquier instructor de su arma y cartuchería al delegado o jefe de seguridad de dicha empresa, la cual se encuentra el arma guiada.

Si fuese un ejercicio de prueba, que normalmente la guardia civil es de obligación presencial en los ejercicios de calificación, segundo semestre de vigilantes de seguridad, vigilantes de explosivos, guardas rurales de campo y segundo trimestre, cuarto trimestre de escoltas, fuera de estos ejercicios solamente en los de entrenamientos sin estar la guardia civil presente, el directo de tiro tiene la autoridad necesaria para detener el ejercicio de forma inmediata.

Esta capacidad de intervención rápida es esencial para preservar la integridad física de las personas y la seguridad del entorno. Y nunca olvidarse de los servicios médicos, si no se encuentran en las instalaciones, se puede adelantar en teórica, explicar todos los ejercicios a desarrollar, pero nunca repartir armas, ni munición, ya que siempre quedarán custodiadas por los escoltas de las empresas en representación física del jefe o delegado de seguridad de dicha empresa.

El instructor de tiro cumple una importante función pedagógica. Su labor consiste en transmitir conocimientos técnicos de manera clara, estructurada y adaptada al perfil de los profesionales o en el caso de las academias, al alumnado. Durante los ejercicios de tiro, observa el desempeño individual y colectivo, identifica errores comunes y ofrece correcciones orientadas a mejorar la seguridad y la eficacia. Por mucho que el primer semestre de vigilantes de seguridad, vigilantes de explosivos y guarda rural de campo y primer y tercer trimestre de escoltas sean ejercicios de práctica y entrenamiento, siempre hay que aconsejar, aunque no sean los ejercicios de calificación, que no bajen la guardia, se empleen a fondo, para que en los ejercicios de calificación mejoren el resultado.

Más allá de la técnica, el instructor fomenta actitudes profesionales como la disciplina, la responsabilidad y el autocontrol. Estas cualidades son especialmente relevantes en la seguridad privada, donde el uso de la fuerza debe ser siempre proporcional y justificado. El instructor contribuye así a la formación integral del personal. Otra función relevante es la evaluación del rendimiento durante los ejercicios de tiro. El instructor valora el grado de cumplimiento de los objetivos formativos, el respeto a las normas de seguridad y la evolución de cada participante. Esta evaluación permite detectar necesidades de refuerzo o reciclaje formativo.

El seguimiento posterior a las prácticas también forma parte de su labor. A partir de los resultados observados, el instructor puede proponer mejoras en los programas de formación, ajustar los ejercicios futuros y recomendar acciones correctivas cuando sea necesario. De este modo, la instrucción se convierte en un proceso continuo de mejora. El instructor de tiro en seguridad privada debe actuar con un alto sentido de la ética profesional. Su ejemplo influye directamente en el comportamiento del personal a su cargo. La imparcialidad, el respeto y la coherencia entre lo que se enseña y lo que se practica refuerzan la credibilidad del instructor y la eficacia de la formación.

Asimismo, el director e instructor de tiro asume una responsabilidad directa sobre el desarrollo seguro de los ejercicios. Esta responsabilidad implica tomar decisiones prudentes, priorizar la seguridad sobre cualquier otro objetivo y promover una cultura de prevención dentro de la organización. La función del instructor de tiro en la seguridad privada durante los ejercicios de tiro es compleja y multidimensional. Su papel abarca el cumplimiento del marco legal, la planificación de las prácticas, la prevención de riesgos, la formación técnica y ética, y la evaluación continua del personal, dependiendo a su vez, en casos de una incidencia, bajo la presencia y supervisión del instructor de tiro, el profesional que encuentre, comunique la incidencia con el arma a 45 grados y dedo fuera del disparador y evaluar la incidencia -en mi caso siempre he intentado que sea el vigilante o escolta- intente solventar la incidencia bajo las órdenes remitidas, para que ellos al final en situaciones reales sepan solventar posibles incidencias que les puedan pasar.

De esta forma también se enseña a que los profesionales de la seguridad se motiven y se encuentren más seguros poco a poco de ir conociendo más a fondo el manejo de un arma en una interrupción e intentar solventarla como se encuentren en esa situación, sin instructor de tiro.

Gracias a su intervención, los ejercicios de tiro se desarrollan en condiciones controladas y seguras, contribuyendo a la capacitación responsable del personal armado. En definitiva, el instructor de tiro es una figura clave para garantizar que la seguridad privada ejerza sus funciones con profesionalidad, legalidad y respeto a la seguridad de todos. Un arma es segura, si quien la porta, es una persona bien formada

RAFAEL SOLER PENADÈS

ARQUITECTURA INTEGRAL DE SEGURIDAD: DE LA FRAGMENTACIÓN OPERATIVA A LA GOBERNANZA ESTRUCTURAL DEL RIESGO

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Edison Cadena Ayala Presidente AIMCSE Ecuador

He observado durante años que muchas organizaciones no carecen de inversión en seguridad; carecen de arquitectura; donde existen controles, protocolos y tecnología, pero no siempre existe un diseño que los articule con los objetivos estratégicos.

En infraestructuras críticas esta fragmentación resulta particularmente evidente: seguridad física desconectada de la ciberseguridad, análisis de riesgos aislado del gobierno corporativo y decisiones operativas que no dialogan con el apetito de riesgo institucional. Este enfoque reactivo es insuficiente frente a amenazas híbridas y entornos volátiles.

La norma ISO 31000 establece que la gestión del riesgo debe integrarse en la gobernanza y en todos los procesos organizacionales. De igual forma, ISO 18788 subraya la necesidad de sistemas de gestión coherentes y auditables en operaciones de seguridad. El modelo Enterprise Security Risk Management (ESRM) promovido por ASIS International refuerza esta integración al vincular seguridad con objetivos estratégicos y protección de activos críticos (ASIS, 2019).

El riesgo no es un elemento aislado que simplemente se “identifica”; es la resultante dinámica entre amenazas, vulnerabilidades e impactos, evaluada en función de consecuencias para el negocio. Su tratamiento exige análisis estructurado, priorización y métricas verificables.

Desde esta perspectiva, la Arquitectura Integral de Seguridad se articula en tres niveles interdependientes:

- Primero, el fundamento estratégico: contexto organizacional, gobierno corporativo y definición explícita del apetito de riesgo.
- Segundo, el núcleo analítico: evaluación técnica de amenazas, vulnerabilidades y consecuencias.
- Tercero, las capas de protección: controles físicos, tecnológicos, humanos, procedimentales y de inteligencia, diseñados bajo el principio de defensa en profundidad.

En sectores como energía, transporte o salud, donde la interrupción impacta directamente a la sociedad, la fragmentación no es solo ineficiencia; es exposición estratégica. La evolución disciplinar exige pasar de la acumulación de controles a un diseño coherente que permita anticipar, adaptar y sostener la resiliencia organizacional. La seguridad, cuando carece de arquitectura, es presencia.

Cuando se integra bajo gobernanza, se convierte en sistema.

Edison Cadena Ayala



Bibliografía:

- **ASIS International. (2019). Enterprise Security Risk Management Guideline. ASIS.**
- **International Organization for Standardization. (2015). ISO 18788:2015 Management system for private security operations. ISO.**
- **International Organization for Standardization. (2018). ISO 31000:2018 Risk management — Guidelines. ISO.**

Arquitectura Estratégica de Seguridad

Protección de Activos bajo
Estándares Internacionales

ISO 18788 / Gestión Integral de Riesgos / Seguridad Corporativa

Edison Cadena Ayala

sein

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
- Geopolítica.
- Seguros de Embarcaciones Recreo.
- Grafología,
- Documentoscopia,
- Grafopsicopatología Criminal y Forense.
- Due Diligence (Debida Diligencia).

www.oterotrillogabinetepericial-andaluciaceuta.es/

SERVINT-SEGUR

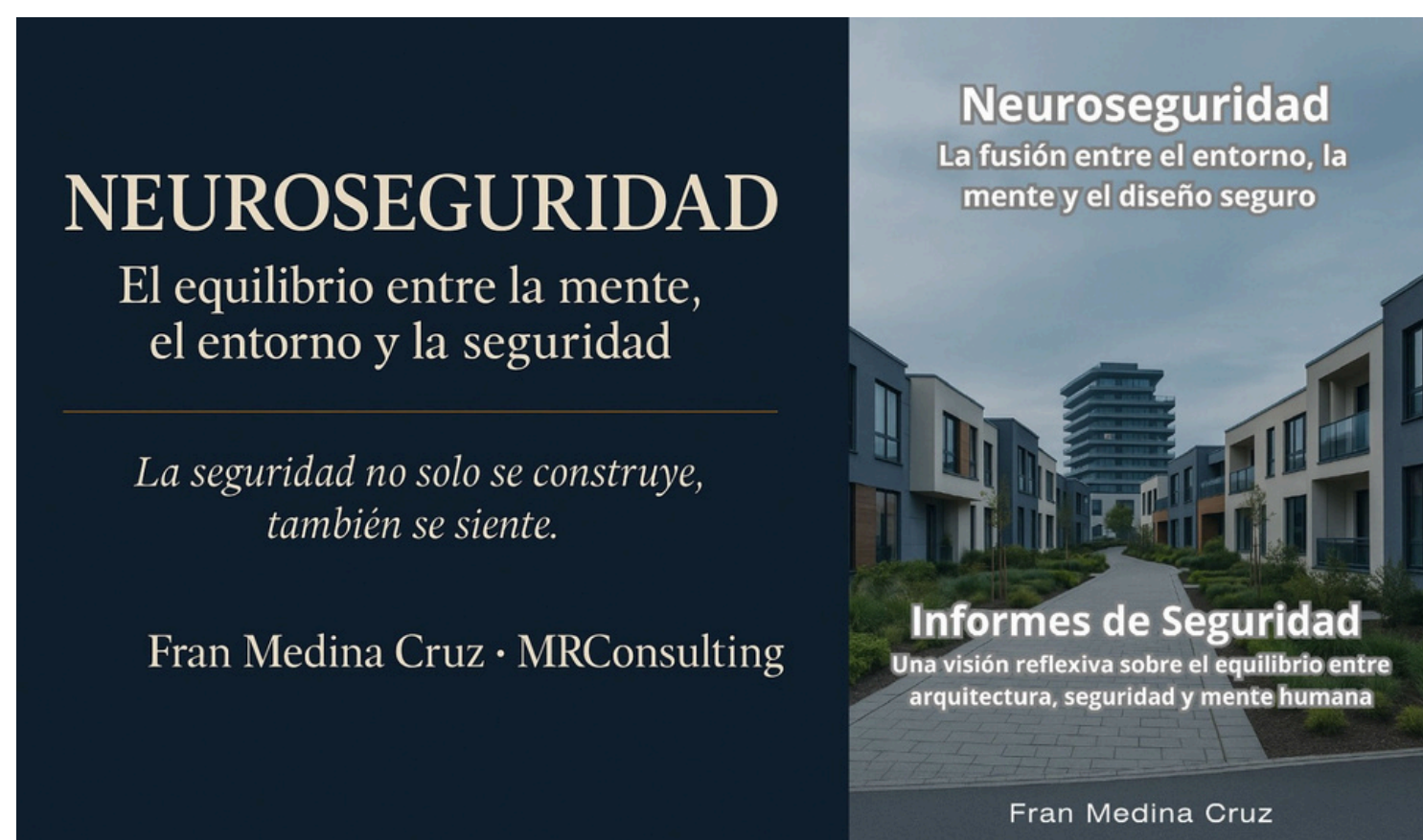
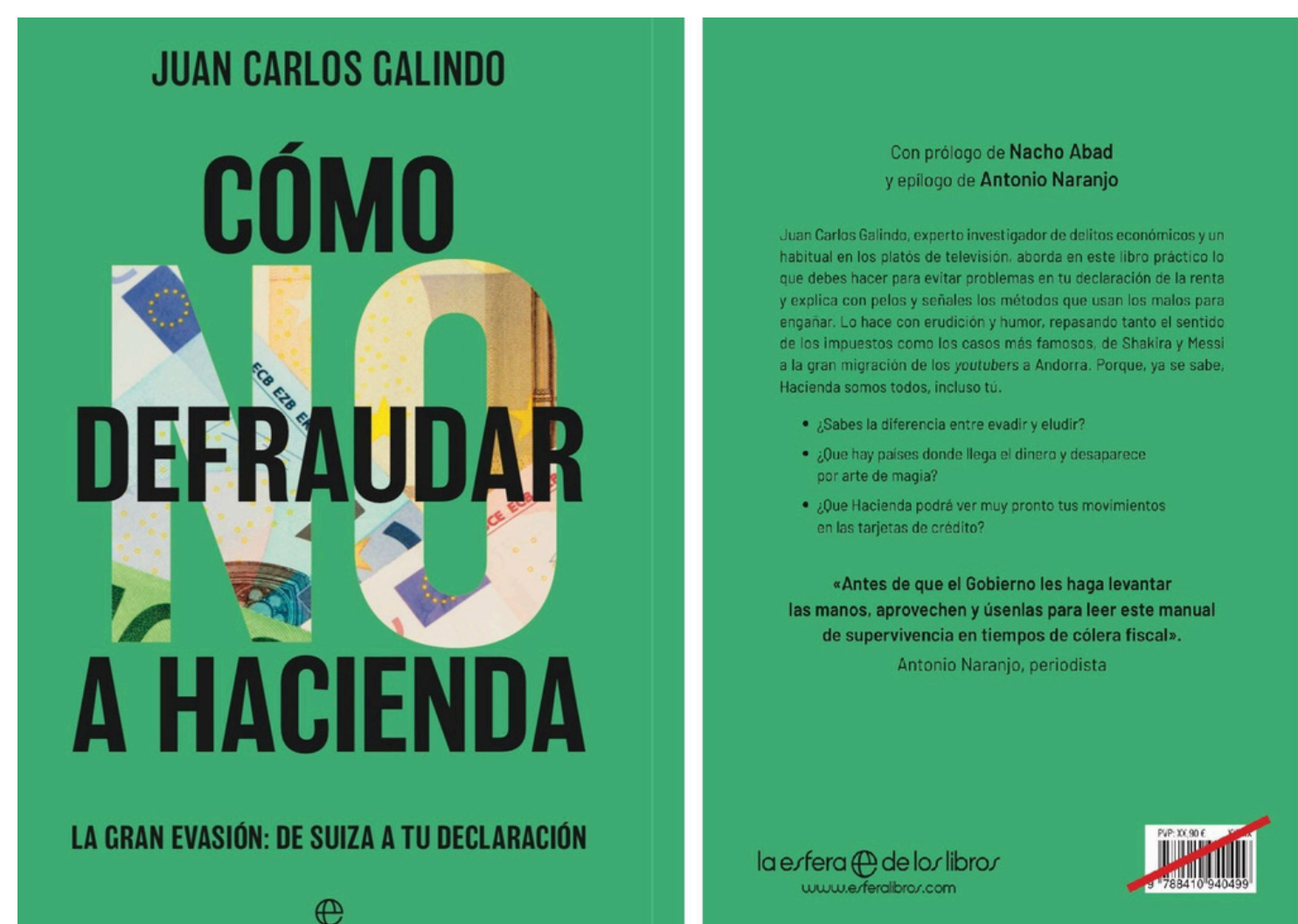
AGENDA

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