EDITORIAL MR

ISSN 3045-7629

MAYO
JUNIO

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
Antonio Pérez Cala
Jonatthan Hermida Sosa
Carlos E. Pérez Barrios
Eduardo Reyes
Edison Cadena Ayala

@Metrorisk.es

ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

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 pais o región.

¿SE PUEDE CREAR UNA COOPERATIVA DE VIGILANTES DE SEGURIDAD EN ESPAÑA?

Metro Risk

Fran Medina Cruz
Director de MetroRisk

Sí, se puede. La forma jurídica de cooperativa no está prohibida dentro del marco de la Ley 5/2014 de Seguridad Privada. Pero esa posibilidad no implica que sea fácil ni automática. La ley no distingue entre una cooperativa y una empresa tradicional cuando se trata de exigir responsabilidades, controles o garantías operativas.

¿Basta con que los vigilantes se asocien y contraten a un director de seguridad?

No. Ese es solo el punto de partida. La cooperativa tendría que convertirse, en la práctica, en una auténtica empresa de seguridad. Eso significa obtener autorización administrativa, inscribirse en el registro correspondiente y demostrar ante el Ministerio del Interior que dispone de estructura real, capacidad operativa y control efectivo del servicio.

¿Es clave la figura del director de seguridad?

Sí, absolutamente. El director de seguridad no es una figura decorativa ni contractual. Debe ejercer una dirección real, con autoridad sobre la operativa, los procedimientos y el control del servicio. Sin esa figura plenamente integrada y con poder efectivo, la estructura no sería viable.

¿Dónde está entonces la dificultad?

En la propia naturaleza de la cooperativa. La seguridad privada no es un sector donde la toma de decisiones pueda diluirse o repartirse sin control. Requiere mando claro, disciplina operativa y responsabilidad perfectamente definida. La Administración, a través de la Unidad Central de Seguridad Privada, exige saber quién decide, quién ordena y quién responde ante cualquier incidente.

¿Puede una cooperativa cumplir con ese nivel de exigencia?

Sí, pero solo si deja de funcionar como una cooperativa clásica en lo operativo. Tendría que adoptar una estructura jerárquica real, con mando definido, protocolos estrictos y una dirección efectiva que no dependa de decisiones asamblearias en el día a día. En ese momento, aunque jurídicamente sea una cooperativa, funcionalmente será una empresa de seguridad convencional.

¿Entonces merece la pena intentarlo?

Depende del enfoque. Si la cooperativa se plantea como un modelo idealista basado en igualdad operativa entre socios, probablemente fracasará en la fase de autorización. Si se plantea como una empresa sólida con estructura profesional, control y dirección clara, entonces sí puede ser viable.

¿Recomendación final al mercado de la seguridad privada?

El sector no necesita más formas jurídicas, necesita más rigor. Antes de pensar en cómo organizarse, hay que entender qué exige realmente la seguridad privada: control, responsabilidad y profesionalización. Cualquier modelo que no garantice eso desde el diseño, no es una alternativa, es un riesgo.

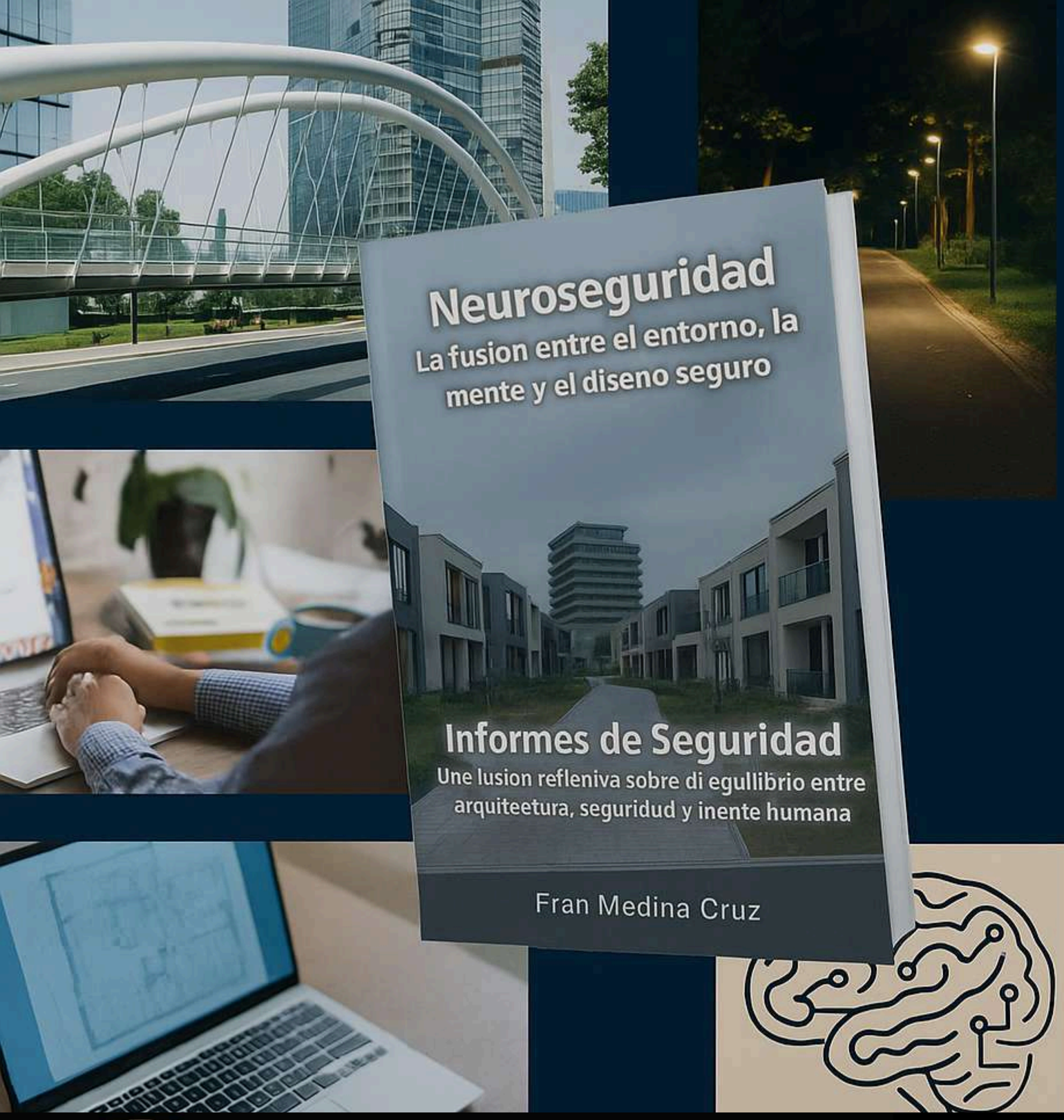
RESUMIENTDO:.

¿Se puede crear una cooperativa de vigilantes de seguridad? Sí. ¿Es viable sin estructura empresarial real? No.

La seguridad privada no admite modelos difusos: exige dirección efectiva, control operativo y responsabilidad clara. Si una cooperativa quiere operar en este sector, debe comportarse como una empresa de seguridad plenamente estructurada y alineada con la Ley 5/2014 de Seguridad Privada. Todo lo demás no es innovación, es inviabilidad regulatoria.

En términos prácticos, el mercado debe entender que la forma jurídica no sustituye al modelo operativo. La Administración, a través del Ministerio del Interior, no evalúa intenciones, evalúa capacidad real de control, mando y respuesta ante riesgos. Por eso, cualquier iniciativa que pretenda introducir modelos alternativos en seguridad privada debe partir de un principio básico: primero estructura, después forma. Sin ese orden, no hay proyecto viable, solo una idea sin recorrido.

Fran Medina

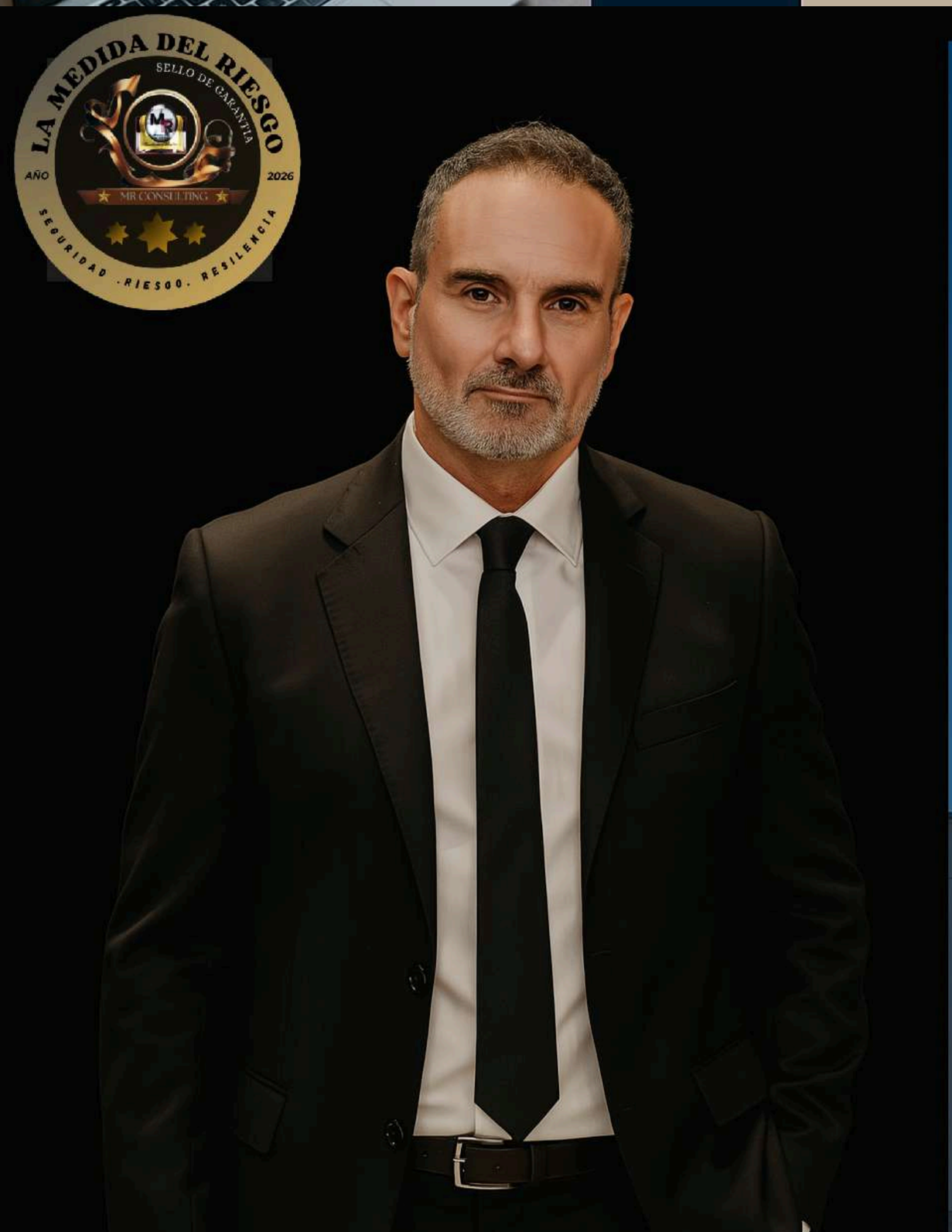


Una nueva visión sobre la seguridad: el equilibrio entre mente, entorno y diseño urbano

Disponible ahora

Fran Medina Cruz

MRConsulting



EL NUEVO PARADIGMA DE LA SEGURIDAD CORPORATIVA: RETOS ESTRATÉGICOS PARA EL DIRECTOR DE SEGURIDAD DEL SIGLO XXI

Metro Risk

Edición propiedad de @MetroRisk, asociación

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

En un entorno global caracterizado por la incertidumbre, la aceleración tecnológica y la interconexión de riesgos, la Seguridad Corporativa ha dejado de ser una función meramente operativa para consolidarse como un eje estratégico dentro de las organizaciones. Este cambio de paradigma no solo redefine el papel del Director de Seguridad, sino que amplía su ámbito de actuación más allá del marco tradicional de la Seguridad Privada.

Hoy, la seguridad ya no puede entenderse como un conjunto de medidas aisladas destinadas a proteger activos físicos. Se trata de un sistema integral de gestión del riesgo que abarca dimensiones físicas, digitales, humanas, reputacionales y geopolíticas. En este contexto, el Director de Seguridad se posiciona como un actor clave en la toma de decisiones empresariales.

De la seguridad reactiva a la inteligencia estratégica El modelo tradicional, basado en la reacción ante incidentes, ha sido superado por un enfoque preventivo y predictivo. La inteligencia corporativa se convierte en una herramienta esencial para anticipar amenazas, analizar tendencias y apoyar la estrategia empresarial. Los Directores de Seguridad deben integrar capacidades de análisis de información, gestión de fuentes abiertas (OSINT), evaluación de riesgos emergentes y elaboración de escenarios prospectivos. Ya no basta con proteger; es necesario comprender el entorno y adelantarse a él.

La convergencia de riesgos: un enfoque transversal Uno de los principales retos es la gestión de riesgos de forma integrada. La fragmentación entre seguridad física, ciberseguridad, compliance, riesgos laborales o continuidad de negocio genera ineficiencias y vulnerabilidades. El nuevo paradigma exige una visión holística donde el Director de Seguridad actúe como coordinador de diferentes áreas:

- Ciberseguridad: la protección de la información y los sistemas críticos.
- Compliance y buen gobierno: adaptación a marcos normativos cada vez más complejos.
- Gestión de crisis y continuidad de negocio: preparación ante escenarios disruptivos.
- Protección de personas: incluyendo riesgos psicosociales y nuevas amenazas.
- Seguridad reputacional: especialmente en un entorno dominado por la inmediatez digital.

Esta transversalidad implica trabajar en estrecha colaboración con otras direcciones (IT, Legal, Recursos Humanos, Operaciones), rompiendo silos organizativos.

I**mpacto de la tecnología:** oportunidad y riesgo La transformación digital es, al mismo tiempo, un facilitador y un generador de nuevas amenazas. Tecnologías como la inteligencia artificial, el Internet de las Cosas (IoT), el big data o los sistemas de videovigilancia avanzada están redefiniendo la seguridad. El reto para el Director de Seguridad es doble:

1. Aprovechar estas tecnologías para mejorar la eficiencia y la capacidad de anticipación.
2. Gestionar los riesgos asociados, como ciberataques, vulnerabilidades sistémicas o el uso indebido de datos.

Además, surge la necesidad de abordar aspectos éticos y legales relacionados con la privacidad, el tratamiento de datos y la automatización de decisiones.

El factor humano: el eslabón más crítico A pesar del avance tecnológico, el factor humano sigue siendo el elemento más vulnerable y, al mismo tiempo, más valioso. La cultura de seguridad dentro de las organizaciones se convierte en un pilar fundamental. El Director de Seguridad debe impulsar programas de concienciación, formación y sensibilización que involucren a todos los niveles de la empresa. La seguridad ya no es responsabilidad exclusiva de un departamento, sino un compromiso colectivo.

El factor humano: el eslabón más crítico A pesar del avance tecnológico, el factor humano sigue siendo el elemento más vulnerable y, al mismo tiempo, más valioso. La cultura de seguridad dentro de las organizaciones se convierte en un pilar fundamental. El Director de Seguridad debe impulsar programas de concienciación, formación y sensibilización que involucren a todos los niveles de la empresa. La seguridad ya no es responsabilidad exclusiva de un departamento, sino un compromiso colectivo.

Entorno geopolítico y riesgos globales Las tensiones geopolíticas, los conflictos internacionales, el terrorismo, el crimen organizado o las crisis energéticas impactan directamente en la actividad empresarial. La seguridad corporativa debe incorporar una visión global.

Esto implica:

- Monitorizar riesgos país.
- Evaluar cadenas de suministro.
- Proteger operaciones internacionales.
- Preparar planes de contingencia ante escenarios complejos.

El Director de Seguridad se convierte así en un analista del entorno global, con capacidad para traducir riesgos macro en decisiones operativas. Nuevas exigencias regulatorias El marco normativo evoluciona constantemente, especialmente en ámbitos como protección de datos, ciberseguridad, resiliencia operativa o sostenibilidad (ESG). El reto no es solo cumplir la normativa, sino integrarla en la estrategia corporativa. La seguridad se convierte en un elemento de valor añadido, capaz de generar confianza en clientes, inversores y stakeholders.

El Director de Seguridad como líder estratégico Todos estos cambios configuran un perfil profesional diferente. El Director de Seguridad del futuro deberá combinar competencias técnicas con habilidades directivas:

- Visión estratégica.
- Capacidad de comunicación e influencia.
- Liderazgo transversal.
- Gestión del cambio.
- Pensamiento crítico y analítico.

Ya no se trata únicamente de gestionar la seguridad, sino de dirigirla como una función clave para la resiliencia y la competitividad empresarial. Conclusión: hacia una seguridad integrada y sostenible

El nuevo paradigma de la Seguridad Corporativa exige una transformación profunda en la forma de entender, gestionar y liderar la seguridad. Los retos son múltiples y complejos, pero también representan una oportunidad única para posicionar al Director de Seguridad como un elemento central en la gobernanza corporativa.

En un mundo donde los riesgos son cada vez más interdependientes, la seguridad deja de ser un coste para convertirse en una inversión estratégica. Aquellas organizaciones que comprendan esta realidad estarán mejor preparadas para afrontar el futuro

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

MEDIOS DE COMUNICACIÓN E INVESTIGACIÓN PRIVADA: UNA ALIANZA SILENCIOSA EN LA BÚSQUEDA DE LA VERDAD

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos G. Barrett
Gerente general en Spy Investigación & Barrett

En una sociedad donde la información circula a gran velocidad y donde la reputación, la seguridad y la transparencia se han convertido en activos estratégicos, la relación entre los medios de comunicación y la investigación privada adquiere una relevancia cada vez mayor.

Aunque tradicionalmente ambas disciplinas han operado en ámbitos distintos, lo cierto es que comparten un objetivo esencial: obtener información verificada, contrastar hechos y esclarecer situaciones complejas.

El valor de la investigación profesional

La figura del detective privado continúa siendo una de las profesiones más desconocidas y, al mismo tiempo, más necesarias dentro del ámbito de la investigación civil y corporativa. Su trabajo no se basa en la especulación, sino en la obtención legal de pruebas, el análisis de conductas y la verificación objetiva de hechos.

Desde investigaciones internas en empresas, fraudes, fugas de información o bajas laborales simuladas, hasta asuntos relacionados con patrimonio, competencia desleal o riesgos reputacionales, el detective privado aporta una capacidad de análisis especializada difícilmente sustituible.

En un contexto donde abundan rumores, filtraciones y contenidos manipulados, la investigación profesional aporta algo fundamental: evidencia.

Medios de comunicación: responsabilidad y rigor

Los medios de comunicación, por su parte, desempeñan un papel esencial como transmisores de información y garantes del interés público. Sin embargo, la inmediatez digital ha incrementado el riesgo de difundir contenidos incompletos o insuficientemente contrastados.

Es aquí donde la investigación privada puede convertirse en un apoyo técnico relevante para determinadas líneas informativas, especialmente en asuntos corporativos, económicos o relacionados con la seguridad.

La combinación entre periodismo e investigación especializada permite construir relatos más sólidos, sustentados en documentación, observación y análisis profesional.

Una sociedad que exige transparencia

Empresas, instituciones y ciudadanos exigen cada vez más claridad y protección frente a amenazas invisibles: fraude interno, espionaje industrial, manipulación de información o conflictos reputacionales.

CARLOS G. BARRETT
Investigador Privado
Experto en Criminalística

En este escenario, tanto el periodismo responsable como la investigación privada cumplen una función esencial dentro del equilibrio democrático y empresarial.

Ambos sectores comparten una misma exigencia:

- rigor,
- discreción,
- ética profesional,
- y capacidad de verificar antes de afirmar.

Más allá del estereotipo

La figura del detective privado ha evolucionado enormemente en las últimas décadas. Hoy hablamos de profesionales especializados en inteligencia corporativa, análisis digital, ciberinvestigación y obtención legal de información estratégica.

Del mismo modo, los medios de comunicación modernos necesitan cada vez más apoyarse en procesos de validación sólidos para mantener la confianza pública. Porque en una era dominada por la sobreinformación, la verdadera diferencia no está en acceder a los datos, sino en saber distinguir qué información es real, útil y demostrable. Y para ello, la investigación profesional sigue siendo una herramienta imprescindible.

Edición propiedad de @MetroRisk, asociación

Gregorio Duro
Tecnico en licitaciones y Proyectos

CONCEPTO DE SOLUCIONES SEPARABLES (I)

La creciente complejidad de los entornos de seguridad exige superar los enfoques estáticos tradicionales de análisis de riesgos y avanzar hacia modelos capaces de describir su evolución en el tiempo. En este contexto, el concepto matemático de las soluciones separables ofrece una base metodológica sólida para representar el riesgo como una magnitud dinámica, influida tanto por su estado actual como por factores externos como la amenaza, la vulnerabilidad o la capacidad de respuesta.

Este enfoque permite descomponer el comportamiento del sistema en componentes analizables de forma independiente, facilitando la comprensión de cómo se generan, evolucionan y pueden mitigarse los riesgos. A partir de esta perspectiva, es posible desarrollar modelos más precisos, predictivos y operativos, alineados con las necesidades actuales de la gestión de la seguridad.

Fundamento matemático y conceptual

El empleo de las soluciones separables dentro del cálculo aplicado al análisis de riesgos constituye una herramienta especialmente útil para modelizar la evolución dinámica de escenarios de seguridad complejos. Frente a los enfoques tradicionales, basados en matrices estáticas de probabilidad e impacto, este planteamiento permite entender el riesgo como una magnitud que cambia continuamente en el tiempo en función de variables clave como la vulnerabilidad, la amenaza y la capacidad de respuesta.

En este contexto, las soluciones separables —propias del ámbito de las ecuaciones diferenciales— permiten descomponer el comportamiento del riesgo en componentes independientes, facilitando su análisis cuando la evolución del sistema depende, por un lado, del estado actual del propio riesgo y, por otro, de factores externos que evolucionan con el tiempo. Este enfoque introduce una visión más realista del riesgo, al incorporar efectos como la acumulación, la inercia o la influencia del entorno operativo.

Formulación y lógica del modelo

La lógica del modelo parte de considerar que el riesgo no es una variable aislada, sino el resultado de la interacción entre distintos factores que pueden evolucionar de manera diferenciada. Así, el riesgo puede aumentar cuando se incrementan las amenazas o las vulnerabilidades, y disminuir cuando se refuerzan las medidas de control o la capacidad de respuesta. Las soluciones separables permiten tratar estas influencias de forma estructurada, separando el efecto del estado interno del sistema (nivel de riesgo existente) del efecto de las condiciones externas (entorno, amenazas, recursos disponibles).

Este tipo de modelización facilita el análisis porque permite estudiar cómo cada componente influye en la evolución global del riesgo, y cómo determinadas combinaciones de factores pueden generar comportamientos de crecimiento, estabilidad o reducción. Además, posibilita la construcción de modelos predictivos que anticipan la evolución del riesgo bajo diferentes escenarios operativos.

Ejemplo práctico aplicado a seguridad

Para ilustrar su aplicación, puede considerarse una instalación industrial con un nivel inicial de riesgo moderado, en la que durante un periodo determinado las condiciones externas permanecen relativamente estables.

En este contexto, el riesgo tenderá a evolucionar en función del equilibrio entre la presión de la amenaza y la eficacia de las medidas de control existentes. Si, por ejemplo, se produce una reducción del personal de seguridad o una relajación de los procedimientos operativos, el sistema experimentará una tendencia al incremento del riesgo, que además puede acelerarse con el tiempo debido a la acumulación de vulnerabilidades no corregidas. Por el contrario, si se refuerzan los controles, se incrementa la vigilancia o se implementan mejoras técnicas, el riesgo tenderá a disminuir de forma progresiva.

Este tipo de comportamiento permite identificar escenarios de crecimiento sostenido del riesgo —que requieren intervención urgente— o situaciones de estabilización y control —que indican una gestión eficaz—. Lo relevante es que el modelo no solo describe el nivel de riesgo en un momento dado, sino su evolución, lo que facilita anticipar cuándo se alcanzarán niveles críticos y actuar con antelación.

Aplicación limitaciones operativa, ventajas y Desde una perspectiva operativa, la aplicación de soluciones separables en el análisis de riesgos permite comprender mejor fenómenos como la acumulación progresiva de vulnerabilidades, la propagación de amenazas o la eficacia de las medidas de mitigación a lo largo del tiempo. Asimismo, facilita la integración con datos reales procedentes de sistemas de seguridad, como la frecuencia de incidencias, los tiempos de respuesta o la disponibilidad de recursos, lo que permite ajustar los modelos a la realidad operativa.

Entre sus principales ventajas destacan la capacidad de anticipación, la mejora en la toma de decisiones y la optimización de recursos, al permitir identificar no solo dónde existe riesgo, sino cómo y cuándo evolucionará. Sin embargo, este enfoque también presenta limitaciones: no todos los sistemas pueden modelizarse de forma separable, la calidad del análisis depende de la fiabilidad de los datos disponibles y de la correcta interpretación de los resultados, y en entornos altamente complejos puede ser necesario recurrir a metodologías más avanzadas.

En conjunto, las soluciones separables constituyen una base sólida para desarrollar modelos de análisis de riesgos más dinámicos, predictivos y adaptativos, alineados con las necesidades actuales de la seguridad. En el próximo número de Metrorisk, abordaré este enfoque de una manera menos sistemática y desde un punto de vista práctico.

Deseo expresar mi sincero reconocimiento a Metrorisk por su labor en la difusión mensual de artículos técnicos. Su compromiso no solo proporciona contenido de gran valor, sino que también consolida un espacio permanente de estudio y actualización para los profesionales del sector.

Gregorio Duro Navarro
Licitaciones y Proyecto

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

ARQUITECTURA DE LA PREVENCIÓN: CÓMO EL DISEÑO CPTED Y LA ISO 22341 REDEFINEN LA SALUD Y SEGURIDAD LABORAL

Introducción:

La violencia laboral es uno de los riesgos psicosociales con mayor impacto sobre la salud, la dignidad y el bienestar del trabajador. Tanto la norma internacional ISO 45003:2021 como la regulación mexicana NOM-035-STPS-2018 la reconocen explícitamente como un factor que debe ser identificado, analizado y prevenido por las organizaciones, en el marco más amplio de los sistemas de gestión de la seguridad y salud en el trabajo.

Sin embargo, el abordaje tradicional de la violencia laboral suele limitarse a protocolos administrativos —políticas, denuncias, capacitación, mecanismos de queja— sin intervenir sobre la dimensión que más condiciona su aparición: el entorno físico donde se desempeña el trabajo. Es ahí donde la metodología CPTED, formalizada por la ISO 22341, ofrece un marco operativo específico para incidir sobre las condiciones espaciales, ambientales y socio-urbanas que facilitan o, por el contrario, dificultan, la materialización de la violencia.

El presente documento es parte de una investigación profunda en tres niveles: el tratamiento que la ISO 45003 hace de la violencia laboral; el tratamiento detallado que le otorga la NOM-035-STPS-2018; y la forma en que CPTED incide sobre este riesgo psicosocial mediante mecanismos preventivos concretos y verificables.

La violencia laboral en la ISO 45003:2021: Marco general de la norma: La ISO 45003:2021, titulada Gestión de la seguridad y salud en el trabajo — Seguridad y salud psicológicas en el trabajo — Directrices para la gestión de los riesgos psicosociales, es la primera norma internacional que ofrece orientación práctica específica sobre la gestión de los riesgos psicosociales en el trabajo. Diseñada para utilizarse junto con la ISO 45001:2018, define el riesgo psicosocial como la combinación de la probabilidad de exposición a peligros de naturaleza psicosocial relacionados con el trabajo y la severidad del daño que estos pueden provocar.

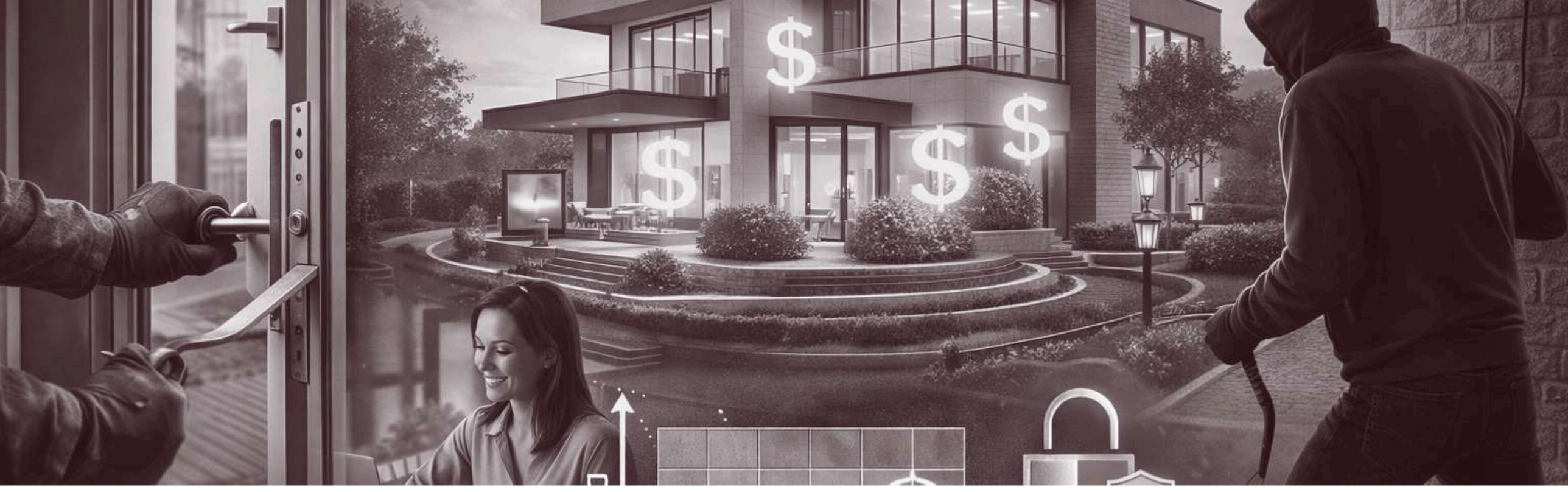
Clasificación de los peligros psicosociales: La ISO 45003 organiza los peligros psicosociales en tres grandes ámbitos:

- 1. Aspectos relacionados con la organización del trabajo: cargas de trabajo, control sobre la tarea, jornadas, comunicación, claridad de roles.
- 2. Factores sociales en el trabajo: relaciones interpersonales, liderazgo, apoyo social, conflictos, comportamientos inaceptables, violencia y acoso.
- 3. Ambiente de trabajo, equipos y tareas peligrosas: el entorno físico (iluminación, ruido, espacio, ergonomía) y la exposición a tareas con riesgo para la integridad personal

La violencia laboral como peligro psicosocial específico: Dentro de los factores sociales en el trabajo, la ISO 45003 identifica explícitamente la exposición a conflictos interpersonales, a situaciones de violencia, a comportamientos inaceptables como la discriminación, el acoso y la intimidación, así como la inadecuada gestión de los conflictos por parte de 1 la empresa. La norma reconoce que estos peligros pueden surgir tanto del interior de la organización (entre compañeros, jefes, subordinados) como desde el exterior (clientes, usuarios, terceros).

Adicionalmente, la norma incluye en la categoría de ambiente de trabajo y tareas peligrosas un grupo de actividades que por su naturaleza incrementan el riesgo de violencia: tareas con manejo de bienes valiosos, atención a clientes potencialmente conflictivos, situaciones de aislamiento geográfico, trabajo en zonas con alta criminalidad, atención al público sin control de accesos, y centros con numerosos puntos de entrada o sin vigilancia. Es relevante destacar que la ISO 45003 establece que la responsabilidad de la organización sobre la salud psicosocial no se limita a sus trabajadores directos: incluye también a otras personas bajo su control —contratistas, proveedores, visitantes— y exige integrar la gestión psicosocial en el ciclo PHVA (Planificar–Hacer–Verificar–Actuar) del sistema de gestión de SST

Medidas de control sugeridas: La ISO 45003 propone medidas estructurales para controlar el riesgo de violencia: políticas explícitas de cero tolerancia, mecanismos confidenciales de denuncia, formación específica del personal en reconocimiento de señales de violencia, planes de actuación ante incidentes, evaluación continua del clima organizacional y, de manera particularmente relevante para los fines de este documento, el diseño seguro del entorno laboral como medida preventiva primaria. Esta última disposición es la que permite la articulación operativa con la metodología CPTED.



Cómo incide CPTED sobre la violencia laboral: CPTED no actúa sobre el agresor: actúa sobre el entorno que permite o dificulta la agresión. Su lógica preventiva se basa en la teoría criminológica de la oportunidad, según la cual los actos violentos requieren la convergencia de tres elementos: un agresor motivado, una víctima vulnerable y un entorno permisivo. CPTED opera sobre el tercer elemento, modificando el espacio físico para reducir las oportunidades. Esta intervención se traduce en cinco mecanismos preventivos concretos que inciden de manera diferenciada sobre la violencia laboral.

Reducción del miedo al delito: incidencia psicosocial directa: El miedo al delito no requiere que el delito ocurra: basta con que el entorno transmita señales de inseguridad para que el trabajador entre en un estado de alerta sostenida. Este estado, prolongado en el tiempo, produce tres efectos psicosociales identificados tanto por la ISO 45003:

- Estrés ambiental crónico: activación fisiológica permanente del sistema de alarma, con consecuencias cardiovasculares, gastrointestinales e inmunológicas.
- Hipervigilancia: atención dividida entre la tarea y la exploración del entorno, con caída de la concentración, errores y accidentes laborales.
- Agotamiento emocional y burnout: desgaste psicológico que conduce al absentismo, la rotación de personal y, en casos severos, a trastornos de ansiedad y depresión como consecuencias de los riesgos psicosociales.

CPTED reduce estos efectos antes de que ocurra ningún incidente, mediante señales ambientales de control y cuidado: iluminación uniforme, espacios bien mantenidos, visibilidad recíproca, presencia de usuarios legítimos. Un entorno que se percibe como vigilado y cuidado disminuye la activación fisiológica del trabajador, aunque no desaparezcan los peligros objetivos.

Cinco estrategias que rediseñan la seguridad de cualquier centro de trabajo: La metodología CPTED se estructura en cinco principios aplicables a cualquier entorno construido — oficina, hospital, banco, parque industrial, comercio, escuela—:

• Vigilancia natural: iluminación, paisajismo y disposición arquitectónica que maximizan la visibilidad y eliminan puntos ciegos.

• Control natural de accesos: puntos claros de entrada y salida, barreras físicas y simbólicas que orientan el flujo de personas.

• Refuerzo territorial: límites claros entre lo público, lo semi-privado y lo privado para fomentar pertenencia y responsabilidad.

• Apoyo a la actividad: promoción de usos legítimos del espacio que desplazan los usos antisociales.

• Mantenimiento y gestión de la imagen: basada en la teoría de las ventanas rotas, donde un entorno cuidado disuade conductas delictivas.

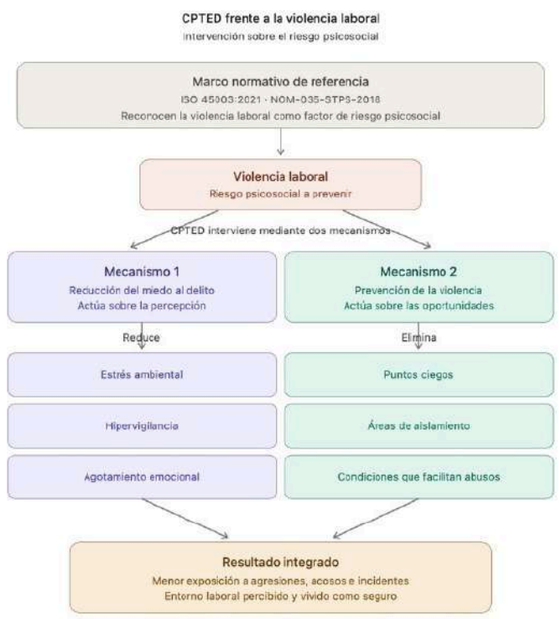
La segunda generación de CPTED suma además cohesión social, cultura comunitaria, conectividad y capacidad de umbral, expandiendo el enfoque hacia las dimensiones psicosociales del entorno.

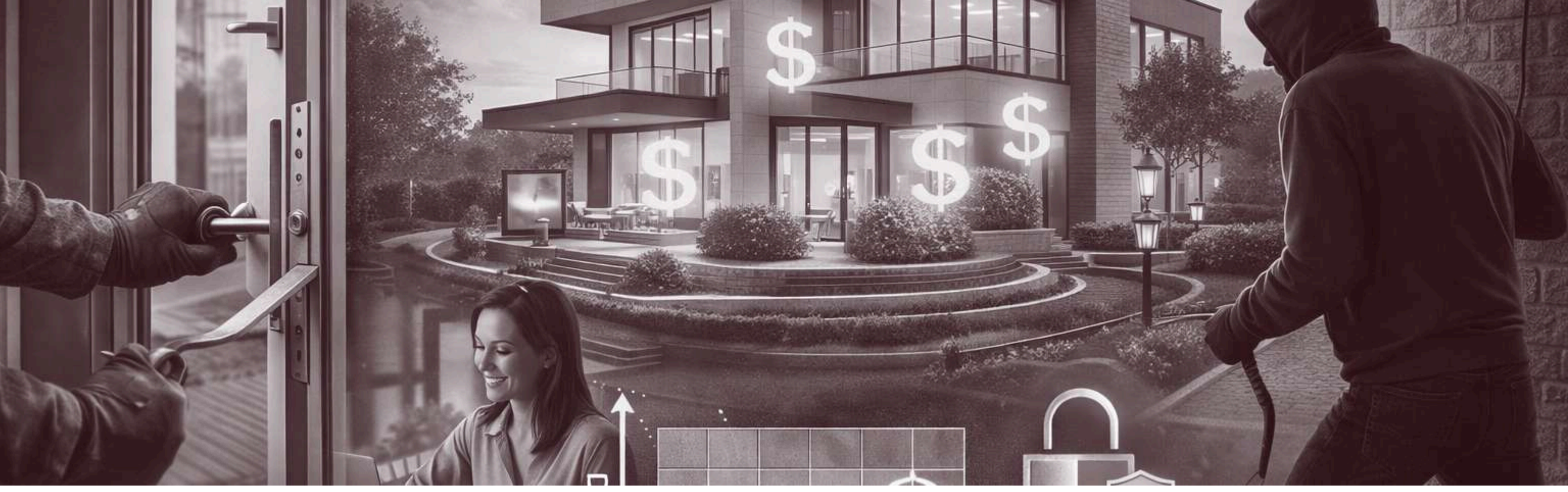
Los trabajadores más expuestos: cuando el entorno es el verdadero peligro La investigación identifica sectores donde la convergencia entre CPTED y SST resulta crítica:

- Trabajadores de comercio minorista, banca y servicios, expuestos a violencia externa.
- Personal sanitario, educativo y de atención al público, expuesto a violencia de clientes y usuarios.
- Personal de transporte, logística y distribución, expuesto al entorno urbano y sus riesgos.
- Personal de seguridad privada y vigilancia, expuesto por definición al riesgo socio-urbano.
- Trabajadores de parques industriales, naves logísticas y centros de distribución, expuestos a delitos contra el patrimonio y la persona en accesos, estacionamientos y perímetros

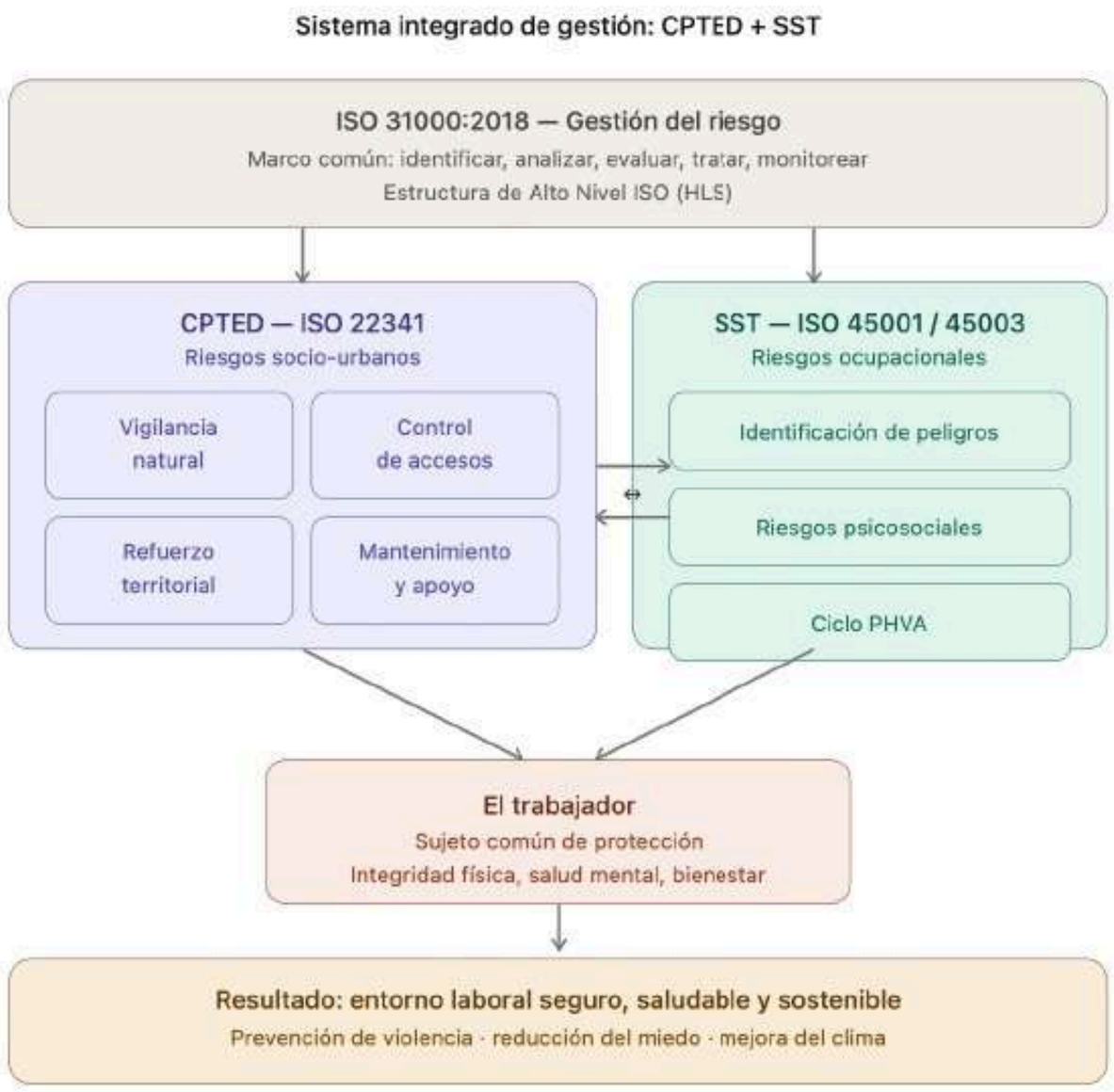
Seis convergencias de alineación entre CPTED y la SST: El estudio establece seis ejes de alineación entre CPTED y la SST, que sustentan su integración como un único sistema de gestión:

- Convergencia normativa: ambos sistemas operan bajo los principios de gestión del riesgo de ISO 31000 y comparten la Estructura de Alto Nivel de ISO.
- Convergencia del objeto protegido: el trabajador y los usuarios del espacio construido son el sujeto común de protección.
- Convergencia preventiva: CPTED actúa en los niveles superiores de la jerarquía de controles, eliminando peligros en origen mediante el diseño.
- Convergencia psicosocial: la reducción del miedo al delito y la prevención de la violencia mitigan los riesgos identificados por ISO 45003.
- Convergencia metodológica: el proceso CPTED de tres etapas es homólogo al ciclo PHVA (Planificar–Hacer–Verificar–Actuar) de ISO 45001.
- Convergencia estratégica: la filosofía de “seguridad por diseño” de CPTED es coherente con el enfoque proactivo y de mejora continua de ISO 45001.

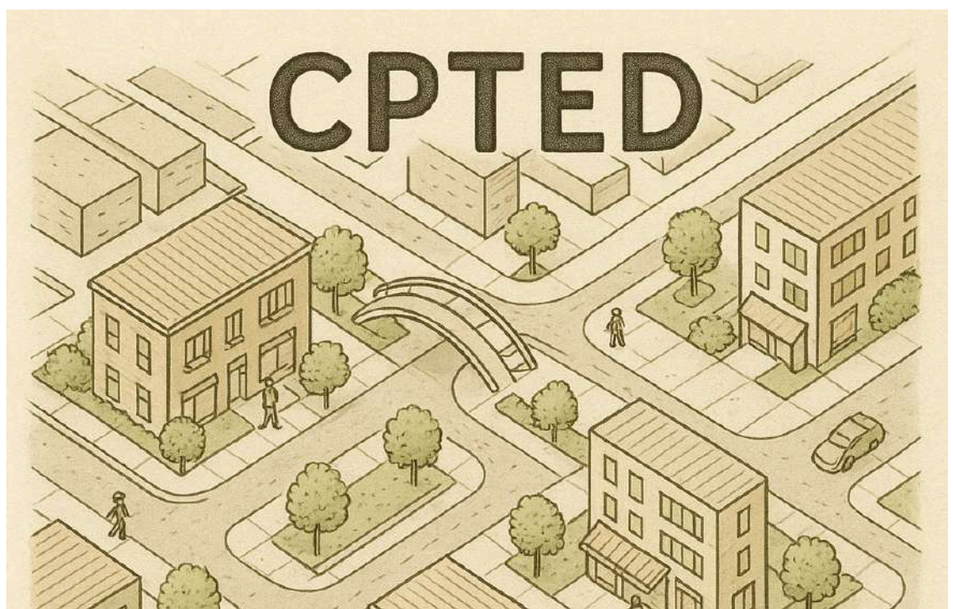




Cuando el diseño previene la violencia: el factor psicosocial La ISO 45003 reconoce la violencia laboral como un factor de riesgo psicosocial. CPTED interviene directamente sobre este riesgo a través de dos mecanismos: • Reducción del miedo al delito: menos estrés ambiental, menos hipervigilancia y menos agotamiento emocional en entornos percibidos como inseguros. • Prevención de la violencia externa e interna: el diseño ambiental reduce las oportunidades de agresiones, acosos e incidentes al eliminar puntos ciegos, áreas de aislamiento y condiciones que facilitan conductas abusivas.



Elaboración: Dra. Mercedes Escudero Carmona



Dónde se aplica: del perímetro al trayecto in-itinere1: La integración CPTED–SST abarca todo el centro de trabajo y va más allá:

- Perímetro y accesos, con iluminación y diferenciación de zonas público/privado.
- Estacionamientos y zonas de circulación vehicular.
- Áreas comunes interiores, lobbies y rutas de evacuación.
- Puestos de atención al público, con diseño que permita huida en caso de agresión.
- Almacenes, bodegas y zonas de carga, con segregación de accesos.
- Entorno urbano inmediato, incluyendo el trayecto in-itinere y la coordinación con autoridades locales.

Beneficios medibles: lo que gana la organización

- Reducción de la accidentalidad y de los incidentes de violencia en el trabajo.
- Disminución del ausentismo y de las bajas por riesgo psicosocial.
- Mejora del clima organizacional y del sentido de pertenencia.
- Reducción de primas de seguros por siniestralidad.
- Cumplimiento integrado de ISO 45001, ISO 45003, ISO 22341 y la ISO 31000.
- Fortalecimiento de la reputación corporativa y la responsabilidad social empresarial.
- Optimización de la inversión en seguridad: diseño ambiental preventivo frente a tecnología reactiva

El centro de trabajo del futuro se diseña, no se reacciona: La conclusión técnica es contundente: el Sistema de Gestión de Riesgos Socio-Urbanos CPTED no es una actividad paralela ni subsidiaria al sistema de SST, sino un componente estructural que lo enriquece y completa. Especialmente en la prevención de la violencia laboral, la mitigación del riesgo psicosocial y la protección de trabajadores expuestos al contexto socio-urbano. La recomendación final es clara: las organizaciones deben implementar un sistema integrado donde la SST (ISO 45001 + ISO 45003) y CPTED (ISO 22341) operen articuladas bajo la gobernanza común de la ISO 31000, con auditorías, indicadores y planes de mejora conjuntos.

Esta integración convierte al centro de trabajo en un espacio que, además de cumplir con la normativa laboral, se concibe y opera como un entorno de vida y de actividad humana diseñado desde su origen para la seguridad, la salud, la productividad y el bienestar integral de quienes lo ocupan, en línea con el Objetivo de Desarrollo Sostenible No. 11 de las Naciones Unidas.

“Diseñar el espacio es diseñar la seguridad: el entorno donde se trabaja determina la salud de quien trabaja.”
Dra. Mercedes Escudero Carmona

¿QUÉ ESPERA REALMENTE UN CLIENTE DE LA SEGURIDAD PRIVADA?

Metro Risk

Edición propiedad de @MetroRisk, asociación

Iván Cantalapiedra.Director de Seguridad.
CEO IONIQ Seguridad

Cuando una empresa contrata un servicio de seguridad privada, no está adquiriendo únicamente la presencia de un vigilante o la instalación de un sistema tecnológico. Lo que realmente busca es algo mucho más profundo: tranquilidad, control y confianza.

Sin embargo, en muchas ocasiones existe una desconexión entre lo que el cliente espera y lo que realmente recibe. Entender esta diferencia es clave para mejorar el sector y ofrecer un servicio verdaderamente profesional.

La seguridad como necesidad, no como trámite

Para el cliente, la seguridad no es un fin en sí mismo, sino un medio para proteger su actividad. Ya sea una empresa, una instalación o un evento, lo que busca es minimizar riesgos y garantizar la continuidad de su negocio. El problema surge cuando la seguridad se plantea como un trámite o una obligación, en lugar de abordarse como un servicio estratégico adaptado a cada necesidad. En esos casos, el cliente percibe que el servicio no aporta valor real.

Tranquilidad: el objetivo principal

El cliente necesita saber que su instalación está protegida, que existen protocolos claros y que, ante cualquier incidente, habrá una respuesta eficaz. Esa tranquilidad no se consigue únicamente con presencia física, sino con organización, supervisión y capacidad de reacción. En IONIQ Seguridad, entendemos que esa confianza se construye desde la gestión diaria del servicio, cuidando cada detalle y manteniendo una supervisión y seguimiento constante.

Profesionalidad y actitud

La profesionalidad del personal de seguridad influye directamente en la percepción del servicio. La imagen, la actitud y la implicación del vigilante marcan la diferencia. Un profesional motivado y bien dirigido transmite seguridad. Por el contrario, la falta de implicación genera dudas sobre la eficacia del servicio. Por ello, es fundamental no solo seleccionar bien al personal, sino también cuidarlo, formarlo y dirigirlo adecuadamente.

Comunicación: el factor determinante

Uno de los aspectos más valorados por los clientes es la comunicación. Saber qué está ocurriendo en su servicio —incidencias, actuaciones o posibles riesgos— genera control y confianza. La falta de información provoca inseguridad, incluso cuando el servicio se está prestando correctamente. Informar, reportar y mantener contacto no es un añadido, es parte esencial del servicio.

Adaptación y asesoramiento

Cada cliente es diferente, y por tanto, cada servicio lo es también. Sin embargo, todavía es frecuente encontrar soluciones estándar que no responden a la realidad de cada entorno. El cliente espera que la empresa de seguridad actúe como un asesor profesional, capaz de detectar riesgos, proponer mejoras y adaptar el servicio con el tiempo. En IONIQ Seguridad trabajamos bajo esa premisa, entendiendo cada servicio como único y en evolución constante.

Más allá del precio

Aunque el coste es un factor importante, no suele ser el único determinante. Muchos clientes valoran la calidad, la estabilidad del servicio y la confianza que les genera. Cuando la seguridad se reduce únicamente a una cuestión económica, se pierde eficacia, motivación y, en consecuencia, resultados.

El cliente de seguridad privada no busca simplemente cumplir con una necesidad, sino sentirse protegido y respaldado. Espera profesionalidad, comunicación, implicación y una gestión real del servicio. La diferencia entre un servicio que cumple y uno que realmente aporta valor está en los detalles, en la dirección y en las personas que lo hacen posible. Porque al final, la seguridad no se mide solo por lo que se ve, sino por la confianza que genera.

IONIQ SEGURIDAD

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

UNA CAUSA TE TRANSFORMA

Porque esto no va de "cumplircumplir".

- Ni de tachar checks.
- Ni de aparentar cultura o innovación

(ni ponerlo bonito en en un PowerPoint.)

Va de algo mucho más serio:
cuando trabajas la causa, el sistema se ordena.

- Y cuando el sistema se ordena, **el resultado aparece**.

Y ahí está nuestra causa.

La digo sin adornos, porque
no se necesita ningún maquillaje:

"Democratizamos el cumplimiento normativo
y la innovación ética en la era de la IA."

Uffff...son muchas cosas...

- Es una postura.
- No es un claim.
- No es un slogan.
- Así, como suena.
- No es una frase bonita.
- Es una responsabilidad.

Porque democratizar el **cumplimiento** significa, en la práctica:

- que la protección no sea un privilegio,
- que la ética no sea un póster,
- que la cultura no sea cosmética, y
- que la IA no se "tenga"... sino que se gobierne.

Lo que he defendido hoy es simple
(y a la vez, se que es incómodo en ocasiones):

Los resultados importan. Claro.
Pero el resultado es el "**qu**é".
La causa es el "**por qu**é".

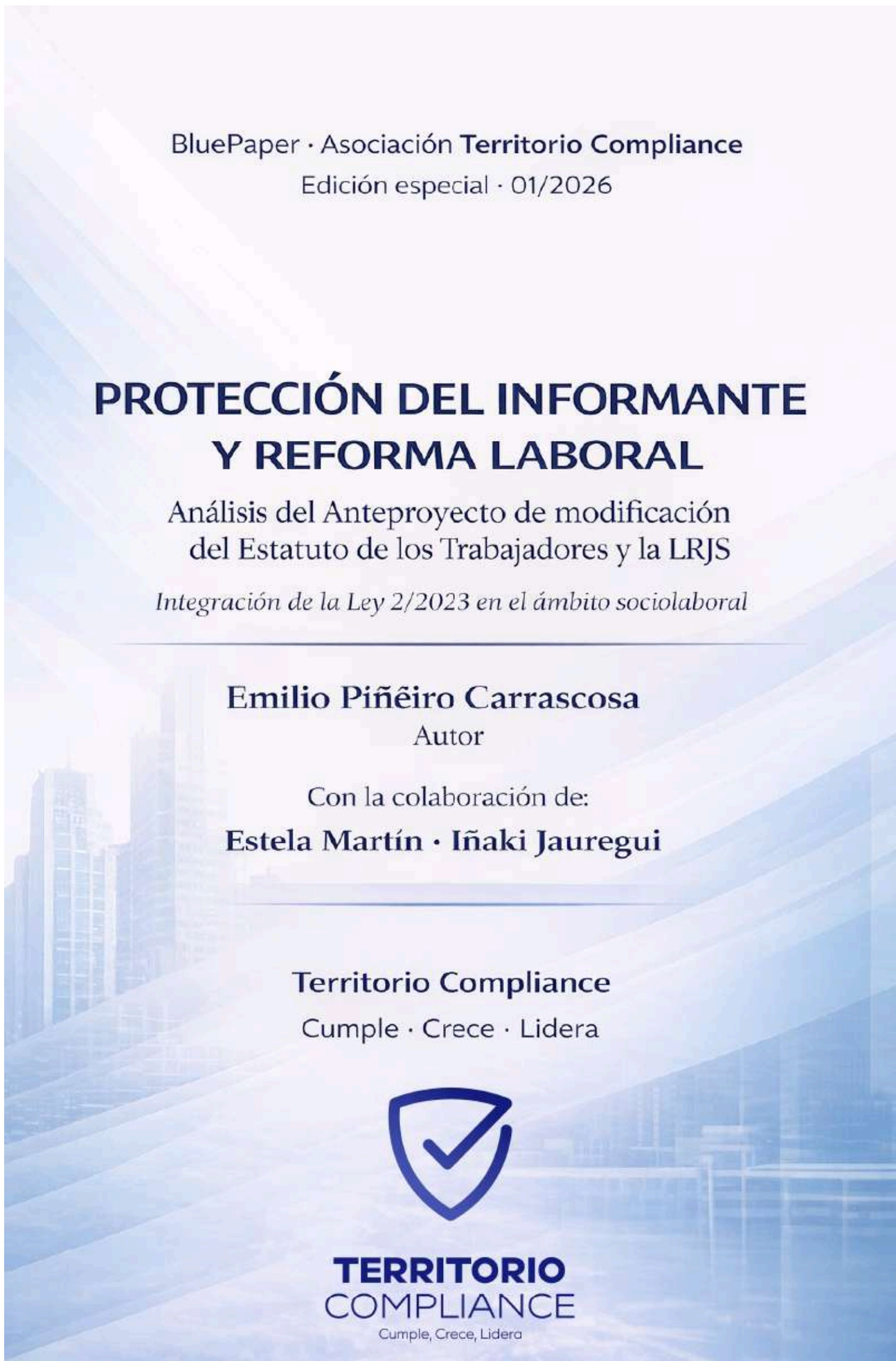
Y cuando el "por qué" es sólido,
el "qué" deja de depender de la épica...
y empieza a depender del sistema y personas.

Este lunes me quedo con una certeza,
una comunidad alineada en una causa no busca impacto.

Simplemente "lo fabrica".

Y hora te pregunto, de verdad,

¿Crees que en las **organizaciones** se está trabajando la causa...
o solo se están persiguiendo **resultados**/**objetivos**?

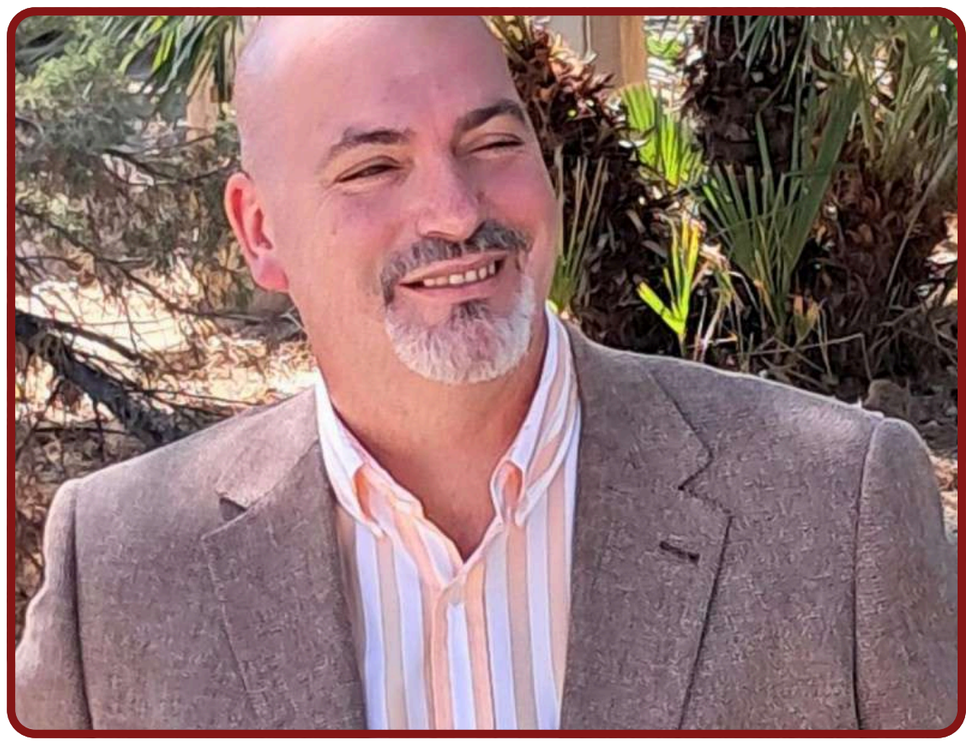


LA SEGURIDAD NO DEBERÍA DISEÑARSE DESDE EL PRODUCTO, SINO DESDE LAS PERSONAS

Metro Risk

Edición propiedad de @MetroRisk, asociación

Joaquín Sampedro
Diseñador de Arquitectura de Seguridad
Seguridad por Diseño



El sector residencial está cambiando. Los edificios ya no se entienden solo como espacios construidos, sino como lugares donde las personas viven, se relacionan, trabajan, reciben visitas, usan zonas comunes y buscan sentirse tranquilas. En ese contexto, la seguridad empieza a ocupar un lugar distinto. Ya no se trata únicamente de instalar sistemas al final de una obra, sino de pensar desde el inicio cómo debe funcionar un edificio para ser cómodo, seguro y fácil de gestionar. Joaquín Sampedro, consultor en Seguridad Inteligente aplicada al Real Estate, defiende una visión sencilla: la tecnología es importante, pero nunca debería estar por encima de las personas.

¿Cómo ve el momento actual de la seguridad aplicada al Real Estate residencial? Creo que estamos en un momento de cambio. Durante mucho tiempo, la seguridad se ha entendido como una parte técnica del proyecto: control de accesos, cámaras, videoporteros, cerraduras, alarmas… Todo eso sigue siendo necesario, pero ya no es suficiente. El Real Estate residencial ha evolucionado mucho. Hoy hablamos de vivienda colectiva, Build to Sell, Build to Rent, Flex Living, coliving, senior living, villas o comunidades residenciales de alto nivel. Son proyectos con formas de uso muy diferentes, con más servicios, más zonas comunes y más perfiles de usuario. Por eso creo que la seguridad tiene que pensarse antes. No al final, cuando ya está todo decidido. Hay que entender cómo va a vivir una persona ese edificio, cómo va a entrar, cómo va a recibir visitas, cómo se van a gestionar los accesos, qué zonas son compartidas, qué necesita el operador y qué experiencia se quiere ofrecer. Para mí, la seguridad no debería diseñarse desde el producto, sino desde las personas.

¿Qué significa diseñar seguridad desde las personas? Significa que antes de hablar de tecnología hay que hablar de uso. A veces empezamos por la solución: qué lector ponemos, qué cámara, qué cerradura o qué aplicación. Y para mí la primera pregunta debería ser otra: qué necesita realmente la persona que va a vivir ahí. Un residente quiere entrar a su casa sin complicaciones. Quiere recibir a alguien de forma sencilla. Quiere usar el garaje, las zonas comunes o los servicios del edificio con naturalidad. Y también quiere sentirse tranquilo, sin tener la sensación de estar pasando controles todo el tiempo. La tecnología tiene que ayudar a eso. Si la tecnología complica la vida, algo no está bien planteado.

¿Qué papel juega la seguridad en la experiencia residencial? Juega un papel muy importante, aunque muchas veces no se vea. Cuando un edificio está bien resuelto, la seguridad casi no se nota. Todo fluye. El acceso es cómodo, los recorridos son claros, las zonas comunes están bien ordenadas, los permisos funcionan, las visitas se gestionan sin problema y el operador tiene control sin molestar al usuario. Eso genera confianza. Y en residencial la confianza es fundamental. Una vivienda no es solo un activo inmobiliario. Para quien vive allí, es su casa. Por eso la seguridad debe acompañar, no imponerse.

Habla mucho de seguridad por diseño. ¿Cómo lo explicaría de forma sencilla? Lo explicaría así: pensar la seguridad cuando todavía se puede decidir. Cuando un proyecto está en fase de diseño, hay muchas decisiones que pueden ayudar muchísimo: dónde se sitúan los accesos, cómo se separan las zonas públicas de las privadas, cómo entra un visitante, cómo accede mantenimiento, cómo se gestiona el garaje, dónde están las zonas comunes o cómo se resuelven los recorridos. Si eso se piensa tarde, normalmente toca corregir con tecnología. Y ahí aparecen soluciones que funcionan, sí, pero que a veces generan más fricción de la necesaria. La seguridad por diseño busca evitar eso. No se trata de llenar el edificio de sistemas, sino de hacer que el propio edificio ayude a vivir mejor y con más confianza.

¿Cuáles son los errores más habituales en este tipo de proyectos? El primero es llegar tarde. Se piensa en seguridad cuando el proyecto ya está muy avanzado o cuando la obra está prácticamente definida. El segundo es pensar que más tecnología significa más seguridad. No siempre es así. A veces se instalan muchos sistemas, pero no están bien conectados entre sí o no responden a la operativa real del edificio. Otro error es olvidarse de la gestión diaria. Un edificio no termina el día que se entrega. Hay altas y bajas de usuarios, visitas, proveedores, mantenimiento, incidencias, reservas de espacios comunes… Todo eso hay que poder gestionarlo bien. Y también diría que a veces se piensa poco en el usuario final. Si una solución es incómoda, la gente acaba buscando atajos. Y cuando hay atajos, la seguridad pierde fuerza.

¿Cómo cambia el enfoque entre Build to Sell y Build to Rent? Son modelos distintos y eso afecta mucho. En Build to Sell, la seguridad forma parte de la percepción de calidad del proyecto. El comprador no solo valora la vivienda, también valora cómo entra al edificio, cómo se siente en las zonas comunes, qué privacidad tiene, cómo se resuelve el garaje o qué sensación de tranquilidad transmite el conjunto. En Build to Rent, además de la experiencia del residente, pesa mucho la operación. Hay rotación, gestión continua, servicios, incidencias, proveedores, mantenimiento y necesidad de controlar permisos de forma ágil. En ambos casos, la seguridad debe estar bien pensada, pero no se puede aplicar la misma receta a todos los proyectos. Cada edificio tiene su lógica y su forma de vida.

Joaquín Sampedro

Seguridad inteligente para vivir con confianza

SegurIA SOLUTIONS

Protegiendo el presente.
Anticipando el futuro.

¿Qué papel deben jugar el software y el hardware? Los dos son importantes, pero cada uno tiene su sitio. El hardware tiene que ser fiable. Cerraduras, lectores, cámaras, videoporteros, sensores o automatismos deben funcionar bien y estar bien elegidos. Pero la experiencia la ordena cada vez más el software. La gestión de usuarios, permisos, horarios, visitantes, proveedores, incidencias o zonas comunes depende mucho de cómo se conectan y se gestionan todos esos elementos. Para mí, el hardware debe estar al servicio de la experiencia. No al revés.

¿Qué importancia tiene que los sistemas sean escalables e interoperables? Muchísima. Un edificio cambia con el tiempo. Puede cambiar el operador, pueden aparecer nuevos servicios, nuevas aplicaciones, nuevas necesidades de gestión o nuevas exigencias normativas. Si el sistema nace cerrado o demasiado rígido, el edificio queda limitado. Por eso creo que hay que pensar en soluciones que puedan crecer, integrarse y adaptarse. No por moda tecnológica, sino por sentido práctico. Un activo residencial debe poder evolucionar sin tener que rehacerlo todo cada pocos años.

¿Hacia qué tipo de proyectos está orientando ahora su trabajo? Mi enfoque está especialmente orientado al Real Estate residencial contemporáneo: vivienda colectiva, Build to Sell, Build to Rent, Flex Living, coliving, senior living, villas y comunidades residenciales de alto nivel. Son proyectos donde la seguridad influye mucho en cómo se vive el edificio. Y también en cómo se gestiona. Me interesan especialmente los proyectos donde se entiende que la seguridad no es solo una partida técnica, sino una parte de la experiencia residencial. Cuando se trabaja desde esa mirada, las soluciones suelen ser más sencillas, más coherentes y más útiles.

¿Cómo resumiría su forma de entender la seguridad inteligente? Diría que la seguridad bien diseñada debe dar confianza sin hacerse protagonista. No se trata de que el edificio parezca más tecnológico. Se trata de que funcione mejor. Que sea cómodo, claro, seguro y fácil de gestionar. La tecnología tiene que estar ahí, pero sin imponerse. Tiene que acompañar la vida diaria. Al final, diseñar seguridad también es diseñar convivencia. Y en un edificio residencial, eso es clave.

Contacto
Pza. Los Luceros 7-9
03003 Alicante, España
hola@seguriasolutions.com
965 52 87 22+34 616 02 06 59

SEGURIDAD PRIVADA EN 2026: EL RIESGO YA NO ESTÁ EN LA PUERTA

Metro Risk

Rosa Fernandéz

ASUNTO: RIESGOS, TECNOLOGÍA Y CUMPLIMIENTO

Durante años, el sector de la seguridad privada ha vivido relativamente cómodo en un modelo casi estático: proteger accesos, vigilar perímetros, controlar flujos.

Hoy, ese modelo sigue vendiéndose. Pero ya no describe lo que realmente está en juego. El riesgo ha cambiado de lugar. Y, en muchos casos, sigue buscándose donde ya no está. Mientras parte del sector continúa centrado en cámaras, controles físicos o dispositivos visibles, el entorno operativo se ha desplazado hacia escenarios mucho más complejos: eventos masivos, entornos industriales hiperconectados, polígonos logísticos con actividad 24/7, instalaciones donde conviven personas, sistemas automatizados y flujos de datos en tiempo real.

Es aquí donde está ocurriendo el cambio. Y no tiene que ver con instalar más tecnología. Tiene que ver con entender qué está pasando dentro de esos entornos. Tiene que ver con aplicar la inteligencia operativa y la capacidad analítica de quienes intervienen en las operaciones de vigilancia. Por ejemplo, en un concierto multitudinario, la cuestión ya no es solo controlar accesos o evitar altercados.

Es gestionar —y analizar— información en tiempo real: movimientos de masas, patrones anómalos, puntos de congestión, comportamientos que anticipan incidentes. En una fábrica o en un entorno de industria 4.0, el riesgo no entra por la puerta principal. Se desplaza por sistemas interconectados, por accesos mal gestionados, por decisiones operativas tomadas sin comprender el impacto que pueden tener sobre la continuidad del negocio o la seguridad de los datos.

En un polígono industrial, el problema ya no es únicamente quién entra o sale. Es qué ocurre dentro, qué información se genera, cómo se gestiona y quién tiene realmente el control.

El problema ya no es la falta de información. Es la saturación. Datos, alertas, registros, recomendaciones. Todo ocurre al mismo tiempo. Todo parece relevante. Y, sin embargo, la mayoría no lo es. Ahí empieza el verdadero trabajo. Y también los errores. Uno de los más frecuentes es creer que la tecnología ha resuelto la parte difícil. Pero…no la ha resuelto. La ha desplazado. Y, además, no solo han cambiado los riesgos de lugar o su tipología, sino que el cliente también ha cambiado.

El cliente actual es un cliente que sabe que la seguridad ahora no es solo operativa, así que si tu empresa se dedica a la seguridad, ponte las pilas y centra el foco en todo lo que el cliente necesita o demanda, sin pedírtelo expresamente:

- -Capacidad de interpretación, no solo de vigilancia: que no se limite a “estar”, sino a entender qué está pasando en sus instalaciones, detectar patrones anómalos y poder explicarlos con claridad.
- -Integración real entre seguridad física, digital y normativa: que tus servicios no vayan por carriles separados. Quiere una visión única de riesgo que conecte accesos, sistemas, datos, personas y cumplimiento legal.
- -Trazabilidad de todo lo que haces en su nombre: registros claros, auditables y ordenados de actuaciones, decisiones, incidentes y respuestas. Si algo pasa, quiere poder reconstruir el “quién, qué, cuándo y por qué” (puede que se lo exija a su vez su sistema de compliance)
- -Equipos formados de verdad, no solo habilitados: ya no basta con que tengan TIP. Quiere saber qué formación continua reciben, en qué están actualizados (tecnología, RGPD, NIS2, ENS, IA, procedimientos) y cómo se evalúa su criterio.-Capacidad de reducir mi exposición, no solo de reaccionar a incidentes: que tu propuesta incluya prevención, análisis de señales débiles, recomendaciones de mejora y medidas para evitar sanciones, brechas y decisiones mal documentadas.
- -Criterio profesional demostrable: protocolos claros, pero también margen para decidir con sentido.-Explicaciones, no solo informes: si algo falla, necesita una empresa capaz de explicar qué ha ocurrido, por qué y qué va a cambiar para que no se repita. No quiere excusas técnicas, quiere responsabilidad.
- -Un enfoque basado en señales previas, no solo en incidentes consumados: trabajar de forma proactiva, no reactiva, sobre lo que precede al problema: aforos, flujos, comportamientos, anomalías, correlación de eventos. Poder demostrarle al cliente que identificas señales y que sabes leer antes de que estalle.
- -Compromiso con la evaluación continua: que acepten ser medidos: KPIs, revisiones periódicas, lecciones aprendidas, mejora continua. La seguridad que no se deja evaluar no es confiable.

Es decir, el cliente actual no pide —solo— más cámaras ni más presencia. Pide más criterio, más integración y más capacidad de explicar lo que está pasando antes de que sea noticia, o de que ocurra.

.

¿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 ﷺ 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

ZONAVIGILADA.NET

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

EL GRAN PROBLEMA DE LAS PRÁCTICAS EN SEGURIDAD PRIVADA (SEAD0112)

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Serrano
Coordinador de Servicios Grupo Sureste

Realidad operativa vs. teoría formativa

"El sistema está bien planteado sobre el papel... pero cuando entra en la operativa real, aparecen los problemas."

En mi experiencia como coordinador de servicios, la gestión de alumnos en prácticas del certificado SEAD0112 se ha convertido en uno de los mayores retos operativos del sector. No se trata solo de formación: se trata de encajar esa formación dentro de servicios reales, con clientes reales y responsabilidades reales.

Problema de ubicación

Uno de los principales problemas es la proximidad del alumno al servicio. Las academias necesitan ubicar al alumno para completar el certificado, mientras que la empresa tiene que adaptarlo a servicios ya establecidos. Esto genera retrasos, ineficiencias y, en muchos casos, alumnos que no pueden comenzar prácticas.

Las 88 horas de prácticas

El sistema exige 88 horas obligatorias, algo que en la práctica supone una carga importante. Los servicios no están diseñados para formación, sino para cumplir funciones operativas. Esto provoca saturación tanto en el servicio como en el personal.

El papel del vigilante tutor

El vigilante de seguridad es quien realmente forma al alumno. Sin embargo, no recibe incentivos ni preparación específica para ello. Esto genera rechazo en muchos casos y dificulta la integración del alumno.

Carga para la empresa

La empresa debe coordinar con el cliente, adaptar el servicio y hacer seguimiento del alumno Todo esto sin afectar al funcionamiento normal del servicio. Es una gestión constante que muchas veces no se valora

Falta de retorno

Muchos alumnos no continúan en la empresa tras las prácticas. Esto hace que las empresas cuestionen la utilidad de seguir colaborando en estos programas

Impacto en las academias

Las academias están acumulando alumnos que no pueden realizar prácticas. Esto genera retrasos en certificaciones y presión en el sistema formativo. .

www.seguridadyempleo.com

Reflexión final operativa El modelo formativo necesita adaptarse a la realidad del sector. La formación debe alinearse con la operativa real para ser efectiva

El Boletín Oficial del Estado (BOE) del pasado 29 de abril de 2026 ha publicado una resolución judicial de gran importancia para el sector de la seguridad privada. El Tribunal Supremo, mediante su sentencia núm. 1281/2025, ha fallado a favor de los trabajadores al anular las tablas salariales del año 2021 de la empresa Alcor Seguridad, SL, por no estar debidamente adaptadas al Convenio Colectivo Estatal de las empresas de seguridad.

LA INTELIGENCIA ARTIFICIAL Y EL NUEVO DIRECTOR DE SEGURIDAD

Metro Risk

Edición propiedad de @MetroRisk, asociación

Abraham Santana Herrera
Director de seguridad. Perito

Durante años, la figura del Director de Seguridad estuvo asociada a planos, cámaras, protocolos, vigilantes y capacidad de reacción. Su trabajo consistía en supervisar, coordinar y responder ante amenazas visibles. Pero el entorno cambió. Y con él, también cambió la naturaleza del riesgo

Hoy, las amenazas ya no siempre atraviesan una puerta. Muchas veces llegan a través de datos, patrones invisibles, comportamientos anómalos o decisiones que pasan desapercibidas hasta que el daño ya se ha producido. En medio de ese escenario aparece una herramienta capaz de transformar por completo la forma de entender la seguridad: la inteligencia artificial.

El nuevo Director de Seguridad ya no se limita a observar. Ahora interpreta, predice y anticipa.

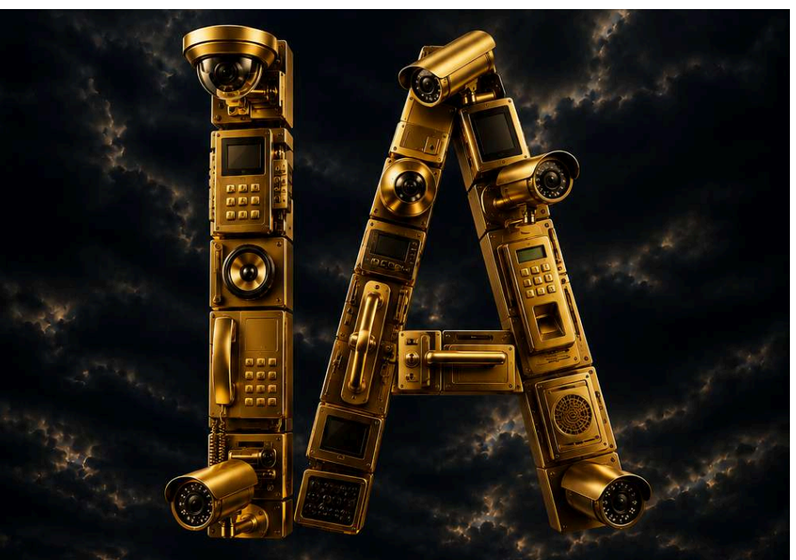
La IA ha comenzado a ocupar un espacio decisivo dentro de la seguridad corporativa moderna. Sistemas capaces de analizar miles de imágenes en segundos, detectar movimientos inusuales, identificar patrones de comportamiento o correlacionar incidencias que antes quedaban aisladas están redefiniendo el concepto de protección.

Pero la verdadera revolución no está únicamente en la tecnología. Está en la capacidad humana de dirigirla correctamente.

Porque la inteligencia artificial no sustituye al Director de Seguridad. Lo potencia.

Un profesional especializado puede utilizar la IA para convertir datos dispersos en inteligencia útil. Puede detectar vulnerabilidades antes de que se conviertan en incidentes, optimizar recursos, automatizar auditorías y comprender el comportamiento operativo de un activo con una precisión nunca antes vista.

En un centro comercial, por ejemplo, la IA puede analizar flujos de personas, detectar acumulaciones anómalas o identificar situaciones potencialmente conflictivas. En un hotel, puede ayudar a reconocer patrones relacionados con accesos indebidos, riesgos internos o comportamientos asociados a fraude. En infraestructuras críticas, puede cruzar variables operativas y generar alertas predictivas antes de que exista una amenaza evidente.

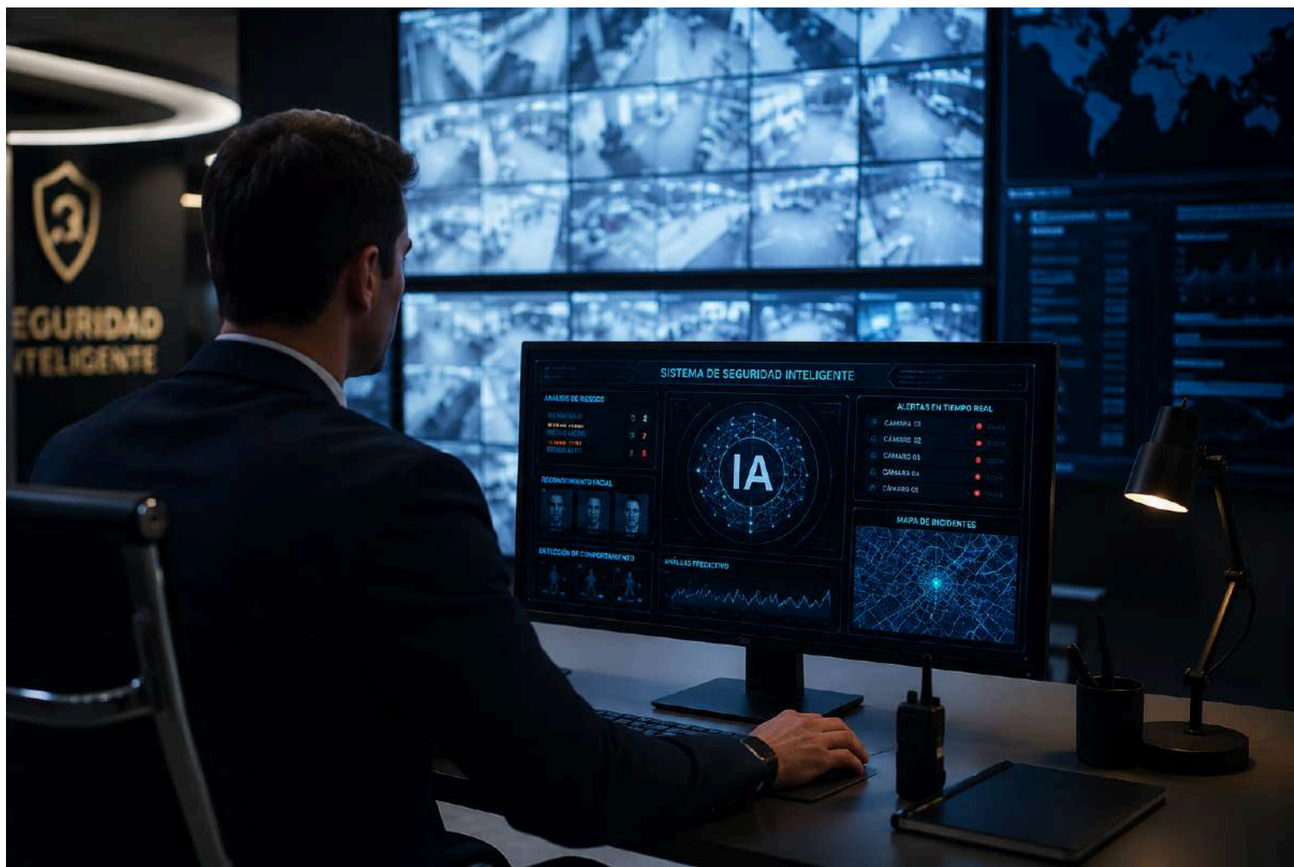


La seguridad deja entonces de ser reactiva para convertirse en preventiva. Sin embargo, la incorporación de inteligencia artificial también exige algo fundamental: criterio.

La tecnología por sí sola no entiende el contexto humano, jurídico o estratégico de cada situación. La IA puede detectar una anomalía, pero sigue siendo el Director de Seguridad quien debe interpretar el riesgo real, valorar el impacto y decidir cómo actuar. Ahí reside la diferencia entre acumular tecnología y construir una verdadera cultura de seguridad.

El Director de Seguridad del futuro será, en gran parte, un gestor de inteligencia. Un profesional capaz de integrar tecnología, análisis de riesgos y visión estratégica en un mismo ecosistema. Ya no bastará con conocer sistemas físicos de protección. Será necesario comprender datos, automatización, análisis predictivo y comportamiento digital.

La inteligencia artificial no ha llegado para reemplazar la experiencia humana. Ha llegado para exigir un nivel más alto de preparación, visión y liderazgo. Y quizá ahí se encuentre el mayor cambio de todos. Porque el nuevo Director de Seguridad no será quien más cámaras controle. Será quien mejor comprenda el riesgo antes de que ocurra.



EL SEGURO DE SALUD, EL MÁS BARATO. -YO CASI NO VOY AL MÉDICO.

Metro Risk

Alina Rubio de las Casas
Experta en Seguros Generales

En seguridad privada ocurre exactamente lo mismo que con los seguros: muchas decisiones se toman pensando únicamente en el coste inmediato y no en el riesgo real al que uno está expuesto.

Empresas, hoteles, comercios o grandes activos suelen contratar "lo mínimo necesario", convencidos de que nunca ocurrirá nada relevante. Menos vigilancia, menos auditorías, menos control técnico… hasta que aparece el incidente que demuestra que la seguridad no se mide el día que todo funciona, sino el día que algo falla.

El día que hace falta

La conversación empezó como empiezan muchas otras: buscando ahorrar.

"Ponme el seguro de salud más barato. Yo casi no voy al médico."
La frase parecía lógica. Incluso razonable. Al fin y al cabo, nadie quiere pagar por algo que apenas utiliza. Y quizá ahí es donde comienza una de las mayores contradicciones alrededor de los seguros: valorar su coste únicamente cuando todo va bien.

Porque esa misma idea, casi sin darse cuenta, termina extendiéndose a todo lo demás.

La cobertura de vida se reduce "a lo justo para la hipoteca".
La baja laboral parece innecesaria "porque nunca pasa nada".
El negocio "siempre ha funcionado sin problemas".
Y hablar de decesos siempre resulta incómodo… hasta que deja de serlo.

Cada decisión, por separado, parece pequeña. Sensata incluso. Pero juntas construyen otra realidad: la de una protección cada vez más ligera, más frágil y más vulnerable precisamente el día que realmente importa.

Y es entonces cuando se entiende el verdadero valor de un seguro.
No cuando se firma.
No cuando se paga.
Sino cuando hace falta utilizarlo.

Porque un seguro no debería medirse por lo barato que resulta mientras duerme en un cajón, sino por la tranquilidad que aporta cuando la vida cambia sin avisar.
A veces habrá que aumentar coberturas.
Otras veces ajustarlas.
Y en ocasiones simplemente mantenerlas.

Pero siempre entendiendo que protegerse no consiste en pagar menos, sino en estar preparado para el momento en que todo aquello que parecía improbable deja de serlo.

Como ocurre con un buen vino, hay cosas cuyo valor solo se comprende cuando llega el momento de descorcharlas.

"El seguro de salud, el más barato. Yo casi no voy al médico."

Eso me dijo un asegurado la semana pasada.

Le entiendo.
Si no usas algo, no quieres pagar de más por ello.

El problema empieza cuando esa misma lógica se aplica a todo lo demás:

→ "Vida, solo para cubrir la hipoteca."
→ "Baja laboral… nunca he estado de baja."
→ "En mi negocio nunca ha pasado nada."
→ "Decesos… mejor cambiamos de tema."

Una a una, cada decisión parece sensata.
Sumadas cuentan otra historia.

Ir recortando coberturas hasta que la póliza pesa poco en la cuenta…
y también el día que hace falta.

Un seguro vale lo que cubre el día que se necesita.
Ni un euro más. Ni uno menos.

A veces toca subir la cobertura.
A veces toca bajarla.
Y otras toca dejarla como está.

Porque un seguro, como un buen vino, solo se entiende cuando llega el momento de descorcharlo.

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

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

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

Unidad de acción

CIERRA EL CÍRCULO CON GALINDO BENLLOCH

FORMACIÓN

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

PREVENCIÓN

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

DETECCIÓN

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

INVESTIGACIÓN

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

SEGURIDAD INTEGRAL

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

EL HARDENING DE SERVIDORES WEB: FUNDAMENTOS Y BUENAS PRÁCTICAS

Metro Risk

Elena de la Parte

"En el mundo del código, un servidor sin 'hardening' es como una caja fuerte de alta tecnología instalada en una habitación con la puerta de cristal: por mucha seguridad que tenga la combinación, el soporte que la sostiene es frágil por definición."

La seguridad de una infraestructura digital comienza, inevitablemente, en sus cimientos. Un servidor mal configurado se convierte rápidamente en el eslabón más débil, sin importar qué tan robustas sean las aplicaciones que aloje. El proceso metódico para mitigar estos riesgos es lo que conocemos como Server Hardening.

Este no es una tarea puntual de "instalar y olvidar", sino un compromiso continuo con la resiliencia del sistema, guiado por tres pilares que transforman una máquina expuesta en una fortaleza:

- 1. Mínimo Punto de Exposición (MPE): Se trata de la economía de recursos. Si tu servidor es un escaparate web, no tiene sentido dejar puertas traseras abiertas para servicios innecesarios como la impresión (CUPS) o archivos compartidos (Samba). Menos servicios activos significan menos vectores de ataque.
- 2. Mínimo Privilegio Posible (MPP): Los procesos deben vivir en "jaulas" de permisos. Un ejemplo práctico: Imagina que el proceso de Apache es un bibliotecario; su función es entregarte el libro que pides, pero bajo ninguna circunstancia debe tener las llaves maestras para cambiar las cerraduras del edificio (acceso root). Si un atacante logra engañarlo, el daño se limitará a los estantes, protegiendo la estructura del sistema operativo.
- 3. Defensa en Profundidad (DP): Seguridad en capas. La protección nunca debe depender de un solo muro, sino de una serie de obstáculos donde cada medida refuerza a la anterior sin asfixiar la operatividad del servidor

Aplicación Práctica: Checklist de Hardening El hardening se materializa en acciones que cierran brechas antes de que sean explotadas:

- Gestión de Acceso: Controlar con lupa quién entra y cómo.
- Minimización de Huellas: No des pistas. Revelar que usas "Apache 2.4.6 en CentOS" es entregarle al atacante el manual de instrucciones para vulnerar.
- Parcheo y Backups: El mantenimiento preventivo y la capacidad de restaurar el sistema son tus mejores seguros de vida

El Riesgo de lo "Predeterminado" Confiar en las configuraciones por defecto es un error común. Estas suelen estar diseñadas para ser "amigables" y fáciles de usar, no para resistir un ataque en producción. El hardening es el paso necesario para pasar de una configuración estándar a una arquitectura consciente del riesgo.

Hardening Específico: Apache y NGINX

- En Apache: Es vital deshabilitar la indexación de directorios (Options-Indexes) para que nadie pueda curiosear tus archivos, y asegurar que el servicio corra bajo usuarios con permisos limitados.
- En NGINX: El rate limiting es clave para frenar ataques DDoS. Ajustar los timeouts (por ejemplo, bajarlos de 300 a 60 segundos) puede ser la diferencia entre un servidor que sigue dando servicio y uno que colapsa ante conexiones lentas.

Seguridad Avanzada: SSL/TLS y WAF El transporte de datos debe ser un túnel blindado. Es imprescindible forzar TLS 1.2 o 1.3 y desterrar protocolos obsoletos. Finalmente, añadir un WAF (como ModSecurity) funciona como un filtro inteligente: inspecciona el tráfico en tiempo real para bloquear inyecciones SQL o ataques XSS antes de que lleguen siquiera a procesarse. ***<< Implementar estas prácticas eleva drásticamente la barrera para cualquier atacante. Un servidor endurecido garantiza que la integridad de tus servicios no sea una cuestión de suerte, sino el resultado de un diseño robusto y profesional>>.***

"Al final del día, el hardening no es una limitación para el administrador, sino su mayor declaración de cuidado: es el arte silencioso de construir sistemas que no solo funcionan, sino que resisten."

LICITACIONES PÚBLICAS EN SEGURIDAD

Metro Risk

Edición propiedad de @MetroRisk, asociación

Antonio Pérez Cala
Director de Seguridad
Vocal Presidente de ADISPO Andalucía

¿Calidad o Precio? He ahí la disyuntiva que condiciona.

Las licitaciones públicas en el sector de la seguridad privada constituyen uno de los ámbitos contractuales más sensibles de la administración. Sin embargo, el análisis sistemático de los pliegos publicados en España y en el conjunto de la Unión Europea revelan una tendencia preocupante. El precio continúa siendo el criterio dominante en la adjudicación de contratos de vigilancia, a pesar de que la normativa vigente, en particular la Ley de Contratos del Sector Público (LCSP) establece la obligatoriedad de la valoración multicriterio.

Existente una brecha real entre el marco legal y la práctica de contratación, se ha realizado para este artículo, una comparativa con los modelos de referencia europeos y latinoamericanos, y se podría proponer un conjunto de medidas concretas orientadas a garantizar que la calidad de los servicios de seguridad sea el eje principal de la contratación pública. La contratación de los servicios de seguridad privada por parte de organismos públicos, administraciones, hospitales, universidades, infraestructuras críticas, etc. Implica una responsabilidad directa sobre la integridad de personas, bienes e información sensible. No se trata de adquirir material de oficina, se trata de contratar personas formadas, motivadas y equipadas para realizar su labor, PROTEGER lo que más importa.

El escenario de la realidad del mercado es muy diferente. Los presupuestos disponibles, a veces la ausencia de parte de criterios técnicos vinculantes y la mala cultura de por qué no decirlo, el precio más bajo como señal de eficiencia, han convertido licitaciones de seguridad en una carrera hacia el mínimo. El resultado es predecible: empresas que reducen costes, pero ¿dónde? Pues en formación, buscar lo más barato para que forme a su personal, medios materiales de baja calidad y en la retribución del personal para poder ofertar precios no se produciría normalmente, al estar las licitaciones condicionando a las empresas a retribuir a sus empleados a convenio nacional, pero buscarían otro tipo de ahorro; esto ocurre y los datos lo confirman, porque el sistema lo permite.

Como curiosidad, un servicio de limpieza puede admitir mayor margen de optimización de costes que un servicio de seguridad, y en la mayoría de los casos, ambos compiten frecuentemente bajo los mismos criterios de adjudicación, ignorando que el error en un vigilante de seguridad tiene consecuencias que ninguna auditoría económica posterior puede reparar.

Aunque todos conocemos que, La LCSP prohíbe la adjudicación al precio como único criterio en contratos de servicios y suministros con prestaciones de carácter intelectual,

- Obliga a incluir criterios cualitativos y a que el precio no sea desproporcionadamente dominante.
- Regula las ofertas anormalmente bajas, estableciendo la obligación de solicitar justificación antes de descartarlas o aceptarlas.
- La Ley 5/2014 de Seguridad Privada establece estándares mínimos de formación y medios para las empresas del sector. En la práctica real podemos encontrar, que en los pliegos de condiciones presentan
- Criterios técnicos en su mayoría subjetivos, difícilmente ponderables y con frecuencia, definidos de forma tan genérica que no discriminan entre ofertas.
- En las mesas de contratación, se carece en muchos casos, de especialización suficiente para valorar adecuadamente parámetros técnicos de seguridad privada.
- Las ofertas económicamente ventajosas, se interpreta en la práctica, como la más económica dentro de unos umbrales formalmente cumplidos.
- El mecanismo de baja temeraria se aplica de forma inconsistente, permitiendo la entrada de propuestas inviables (ya que pueden demostrar las empresas que no lo es para ellas) luego generan conflictos en la ejecución del contrato.

Podrías consultar un ejemplo de cómo Dinamarca, ha desarrollado el modelo MEAT (Most Economically Advantageous Tender) con mayor consistencia que la media europea.

La contratación de servicios de seguridad en instalaciones públicas incorpora invariablemente criterios como la ratio de personal certificado, el índice de rotación de plantilla, la antigüedad media de la empresa y la trazabilidad de los incidentes gestionados, de este modelo e l precio raramente supera el 40% de la puntuación total. Eso sí, no podemos mirar en la zona iberoamericana, para tomarlas como ejemplo, ya que en esos países por regla general solo se tiene en cuenta el precio.

Como propuestas de mejoras, se podría comenzar creando, Comités técnicos independientes que evalúen las ofertas; Auditorías post-contrato con publicación de resultados en páginas oficiales; Penalizaciones económicas por incumplimiento de calidad y una Formación obligatoria para los componentes de las mesas de contratación en seguridad privada.

Conclusiones:

El precio no es el enemigo, pero tampoco puede ser el árbitro.

- Si algo queda claro tras este análisis es que el sistema actual no está roto por accidente, sino por inercia, la buena noticia es que la inercia se rompe.
- El marco legal ya está ahí, la LCSP, la Ley 5/2014, lo que falta es voluntad de aplicarlo con rigor, y eso depende de personas, no de leyes nuevas.
- La seguridad privada no es un producto o mercancía básica, es una profesión.
- Normalizar esta distinción en las mesas de contratación es un cambio cultural que, una vez que empieza, no tiene marcha atrás.
- El modelo MEAT danés, donde el precio raramente supera el 40% de la puntuación, no es utopía, es burocracia bien aplicada. Si funciona en un país europeo con normativa similar a la nuestra, puede funcionar aquí. Solo hace falta un pliego bien redactado y una mesa de contratación que sepa leerlo.
- Comités técnicos independientes, auditorías post-contratos con resultados públicos, formación obligatoria para las mesas.
- Estas no son ideas abstractas, son pasos perfectamente ejecutables. Y cuando alguien las pone por escrito con este nivel de detalle, es cuestión de tiempo que alguien con poder de decisión las lea

MÁS ALLÁ DEL CAMPO DE BATALLA

Metro Risk

Edición propiedad de @MetroRisk, asociación

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

Cómo la Medicina Táctica TCCC está Revolucionando la Seguridad Civil y Empresarial en LATAM La mentalidad de "parar la hemorragia" ya no es exclusiva de los soldados. En una región donde la violencia y los accidentes laborales exigen respuestas inmediatas, el estándar TCCC (Tactical Combat Casualty Care) se está consolidando como el nuevo pilar de la seguridad en Latinoamérica

Durante décadas, los protocolos de primeros auxilios en entornos civiles y empresariales se basaron en esperar a los servicios de emergencia. Sin embargo, la creciente complejidad de la seguridad en Latinoamérica desde la alta peligrosidad en operaciones policiales hasta los riesgos en industrias extractivas ha demandado un cambio de paradigma. La solución ha llegado de la mano de los protocolos militares, específicamente del TCCC, que está transformando la manera en que salvamos vidas fuera del campo de batalla.

La "Zona Roja" Corporativa: Aplicando Lecciones de Guerra. El TCCC no es un simple curso de primeros auxilios; es un sistema de protocolos diseñado para evitar las tres principales causas de muerte prevenible en un trauma: hemorragia masiva, obstrucción de la vía aérea y neumotórax a tensión . En el entorno empresarial latinoamericano, especialmente en sectores como la minería (Perú, Chile, Colombia), el petróleo (Brasil, Ecuador, Venezuela) o la seguridad privada (México, Centroamérica), el "combate" se asemeja a entornos de alto riesgo. Accidentes laborales graves, incidentes con maquinaria pesada o incluso asaltos violentos en zonas de alto tránsito ya no son gestionados con la mentalidad pasiva del "esperar y ver".

La adopción del TCCC en estos entornos implica dotar a los jefes de seguridad y supervisores de torniquetes tácticos, apósitos hemostáticos y la habilidad de realizar descompresión torácica con aguja. Este es el verdadero cambio de paradigma: pasar de ser "primer respondedor" a ser "socorrista táctico", capaz de operar bajo amenaza activa o en entornos hostiles para estabilizar al paciente in situ .

Capacitación Masiva: El Efecto "AMISTAD" y "Relámpago". La rápida adopción de esta doctrina en la región no es casualidad. Ejercicios combinados como AMISTAD (Paraguay, Perú) y Relámpago de los Andes (Colombia) han servido como catalizadores. La colaboración entre el Comando Sur de EE.UU. y las fuerzas locales está filtrando el conocimiento táctico a los cuerpos de policía, bomberos y servicios de emergencia civil. El caso de Paraguay en 2024 es paradigmático. Agentes de la Policía Nacional recibieron entrenamiento TCCC y horas después lo aplicaron exitosamente, salvando la vida de un hombre que había sufrido una herida grave por arma blanca en el cuello, aplicando presión directa antes de que llegara la ambulancia. Esta transferencia de conocimiento está creando una "masa crítica" de personal civil capacitado para intervenir en los "minutos de oro" antes de la evacuación.

Latinoamérica como Laboratorio de Innovación Táctica. A diferencia de los entornos clínicos estériles de Estados Unidos o Europa, Latinoamérica ofrece un entorno operativo complejo que está forzando la evolución del TCCC. Organizaciones como CIMATO (Comité Iberoamericano de Medicina Táctica y Operativa) están liderando la adaptación de estos protocolos a nuestras realidades. ¿Por qué es relevante esto para la seguridad empresarial? Porque los estándares internacionales genéricos fallan en la selva amazónica, la altura de Potosí o las calles congestionadas de Ciudad de México. La integración de la telemedicina, el uso de drones para el envío de desfibriladores o torniquetes, y la creación de "cursos híbridos" (virtuales + prácticos) están haciendo la formación más accesible y escalable para las corporaciones que operan en áreas remotas de la región.

Seguridad Empresarial: Un Imperativo de Negocio. Para las empresas en LATAM, implementar estándares TCCC en sus departamentos de Salud Ocupacional y Seguridad Industrial ya no es un "plus", sino una necesidad de debida diligencia. La violencia laboral (robos, tomas de rehenes) y los accidentes de tránsito de alto impacto son riesgos latentes. Un empleado que se desangra en 3 minutos mientras se espera una ambulancia que tarda 15 es un riesgo legal y de reputación que las empresas no pueden permitirse. La implementación de botiquines tácticos y la certificación en TCCC para el personal de seguridad privada mitiga significativamente este riesgo. El TCCC está rompiendo el "cerco militar". Estamos asistiendo a una "tactificación" de la respuesta civil en Latinoamérica. Los protocolos que salvaron vidas en Irak y Afganistán hoy se enseñan a policías en Paraguay, bomberos en Guatemala y enfermeros en Santa Lucía. Para el sector empresarial, la lección es clara: la próxima generación de la seguridad no se medirá solo por la cantidad de cámaras o guardias, sino por la capacidad real de salvar una vida cuando el caos ocurre. Adoptar la medicina táctica es, en esencia, adoptar una cultura de resiliencia y preparación extrema, adaptada a la realidad más exigente de América Latina.

Autor: Jonatthan Hermida
S. SAPPC, SFPC, ISOC, DAS, CPO, GER, CRASE.
PARAMEDICO TACTICO -TCCC
Seguridad Corporativa Integral
HERMIDA SEGURIDAD S.A.S

SEGURIDAD DEL ESTADO VS SEGURIDAD DEL GOBIERNO: LA FRONTERA INVISIBLE.

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Enrique Perez Barrios
Director General de GLOBAL SECURITY ACADEMY USA

En clave política

En el debate contemporáneo sobre seguridad, Estado y gobernabilidad, existe una confusión conceptual que, lejos de ser inocente, tiene profundas implicaciones institucionales: la tendencia a equiparar la Seguridad del Estado con la Seguridad del Gobierno porque existe una frontera invisible entre la protección nacional y el control del poder. Esta confusión no es simplemente semántica. En contextos, como en el caso de Venezuela, donde las instituciones han sido debilitadas, politizadas o capturadas, la redefinición del concepto de seguridad se convierte en una herramienta fundamental de poder. Y es precisamente allí donde comienza a difuminarse una frontera esencial para cualquier democracia funcional: la diferencia entre proteger a la Nación y proteger al poder.

La Seguridad como función estructural del Estado La Seguridad del Estado no es un componente operativo más dentro del aparato institucional. Es una función estructural de carácter permanente, diseñada para garantizar la existencia misma del Estado como organización política, jurídica y territorial. Su lógica no depende del ciclo político ni de los cambios de gobierno. Por el contrario, su esencia es la continuidad.

En un Estado institucionalmente sano, la Seguridad del Estado está orientada a:

- Garantizar la soberanía nacional frente a amenazas externas
- Preservar la integridad del orden constitucional
- Mantener la estabilidad institucional del sistema democrático
- Proteger los derechos fundamentales de los ciudadanos
- Y asegurar la continuidad funcional del Estado en el tiempo

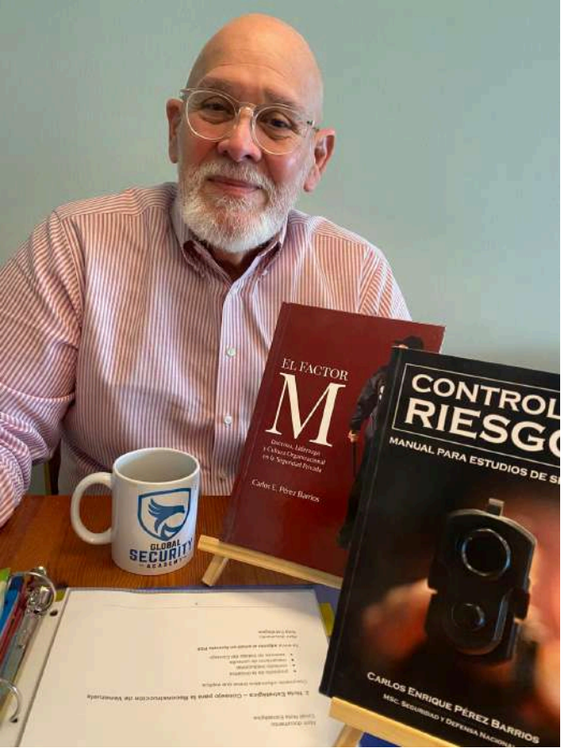
Esto implica un principio clave: la seguridad del Estado no pertenece a un gobierno, sino a la Nación en su conjunto. Por ello, su naturaleza debe ser técnica, institucional, profesional y, sobre todo, no partidista. En su diseño ideal, la Seguridad del Estado también cumple una función de equilibrio interno, ya que no solo enfrenta amenazas externas, sino que puede identificar desviaciones institucionales que comprometan la estabilidad del propio sistema. En este sentido, su lógica superior es clara: proteger al Estado incluso frente a posibles abusos del poder que lo administra temporalmente.

La Seguridad del Gobierno: una función legítima pero subordinada La Seguridad del Gobierno responde a una lógica distinta. Su objetivo es garantizar la protección de quienes ejercen el poder político en un momento determinado, así como la estabilidad operativa del aparato gubernamental. Esto incluye la protección de autoridades, infraestructuras críticas de gobierno y la continuidad administrativa del Estado en su dimensión ejecutiva. En sistemas democráticos funcionales, esta forma de seguridad es necesaria. Ningún gobierno puede operar sin mecanismos de protección adecuados. Sin embargo, su naturaleza es claramente distinta: es temporal, circunstancial y dependiente del ciclo político. Su legitimidad no proviene de su autonomía, sino de su subordinación al interés superior del Estado. El problema comienza cuando esta relación se invierte.

El punto de ruptura: cuando la Seguridad deja de ser institucional y se vuelve funcional al poder En contextos de deterioro institucional, captura del Estado o concentración del poder, la Seguridad del Gobierno puede comenzar a expandir su influencia más allá de su función original. Este proceso suele ser progresivo y no necesariamente explícito. Se manifiesta cuando la seguridad deja de operar como un mecanismo técnico y comienza a actuar como un instrumento de preservación del poder político. En ese punto, ocurre una transformación crítica:

- El objeto de protección deja de ser la Nación y pasa a ser el gobierno
- Las prioridades de seguridad dejan de ser estratégicas y se vuelven políticas
- La neutralidad institucional se debilita
- Y la seguridad comienza a interpretarse como un mecanismo de control interno

Este cambio altera profundamente la arquitectura del Estado, porque introduce una lógica de protección selectiva del poder en lugar de protección universal del sistema institucional



La captura institucional del concepto de Seguridad Uno de los fenómenos más complejos en estos contextos es la captura del concepto mismo de seguridad. Las instituciones no desaparecen, pero cambian de función. La seguridad deja de ser un sistema de protección del Estado y comienza a operar como un sistema de gestión del riesgo político.

Esto se expresa en varias dinámicas estructurales:

- La inteligencia se reorienta hacia el monitoreo interno de actores políticos y sociales
- La disidencia comienza a ser interpretada como amenaza potencial
- Los mecanismos de seguridad se integran a dinámicas de control político
- Y el ciudadano pasa a ser percibido no como sujeto de derechos, sino como variable de riesgo

En este punto, la seguridad deja de ser un bien público y comienza a funcionar como un instrumento de preservación del poder

El entorno criminal y la distorsión de la Seguridad En algunos contextos, esta transformación no ocurre únicamente por razones políticas, sino también por la interacción entre el poder estatal y estructuras de criminalidad organizada. Cuando el Estado es capturado o infiltrado por redes de corrupción estructural, economías ilícitas o actores criminales, la seguridad se reconfigura aún más profundamente.

En estos escenarios:

- Las instituciones pueden ser utilizadas para proteger intereses ilegales
- La inteligencia puede ser desviada hacia la protección de redes de poder
- La fuerza pública puede ser instrumentalizada para fines no institucionales
- Y el sistema de seguridad pierde su función de neutralidad

Aquí, la Seguridad del Estado no solo es sustituida por la Seguridad del Gobierno, sino en algunos casos por la Seguridad del régimen o del sistema de poder real.

Esto genera una distorsión estructural más profunda: el Estado deja de ser árbitro y se convierte en actor dentro de redes de poder.

Las terribles consecuencias institucionales de la confusión Las implicaciones de esta confusión son profundas y afectan directamente la calidad del sistema político e institucional. En primer lugar, el ciudadano pierde su posición central dentro del sistema de seguridad. En lugar de ser el objeto principal de protección, pasa a ser un sujeto observado, gestionado o condicionado, tal como cualquier delincuente.. En segundo lugar, la disidencia política pierde su carácter legítimo dentro del sistema democrático y comienza a ser tratada como un problema de seguridad, como organizaciones criminales. En tercer lugar, el sistema de seguridad pierde su función de equilibrio institucional y se convierte en un mecanismo de preservación del poder. Finalmente, el Estado pierde capacidad de distinguir entre amenazas reales a la Nación y riesgos percibidos desde la lógica del poder.

El dilema fundamental del Estado moderno Toda arquitectura institucional de seguridad se enfrenta a una pregunta central: ¿Está diseñada para proteger a la Nación o para proteger a quienes gobiernan la Nación? La respuesta a esta pregunta define la naturaleza del sistema político porque cuando la seguridad protege al Estado, el sistema tiende al equilibrio institucional, mientras que cuando la seguridad protege al gobierno, el sistema tiende a la concentración del poder. Cuando la seguridad es capturada por estructuras políticas o criminales, el Estado pierde su función original

Las evidentes diferencias La diferencia entre Seguridad del Estado y Seguridad del Gobierno no es un debate técnico, sino un principio estructural que define la calidad de una democracia. En un Estado funcional, la Seguridad del Gobierno está subordinada a la Seguridad del Estado. En un Estado distorsionado, esa relación se invierte o lo que es peor aún, la Seguridad del Estado desaparece como concepto y como práctica, y esa inversión no es menor: redefine la relación entre poder, instituciones y ciudadanía. Recuperar esta distinción no es solo una tarea académica o doctrinal. Es una condición indispensable para cualquier proceso serio de reconstrucción institucional

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

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

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.

SEGURIDAD Y FACILITACIÓN EN LA AVIACIÓN CIVIL: LA NUEVA VISIÓN DE LA SEGURIDAD.

Metro Risk

Edición propiedad de @MetroRisk, asociación

Eduardo Reyes
Gerente de Aseguramiento de Calidad, Seguridad Ocupacional

Seguridad y Facilitación son dos términos que, hasta hace no mucho tiempo, entraban en conflicto en la aviación. La Facilitación en términos simples, tiene que ver de manera directa con uno de los principales atributos del transporte aéreo: la velocidad, es decir, se trata de que los procesos de entrada y salida de aeronaves, pasajeros, equipaje y carga hacia o desde un aeropuerto, sean ágiles considerando por ejemplo, en caso de los pasajeros, los procesos de check-in, abordaje, migración, aduanas y por supuesto seguridad, y hablo de aquella en los puntos de inspección de pasajeros, llamada Seguridad de la Aviación Civil (AVSEC Aviation Security).

El Anexo 9 del Convenio de Chicago de la Organización de la Aviación Civil Internacional (OACI), establece los requerimientos hacia los Estados Contratantes (países), con relación a temas de Facilitación (tales como los visados de entrada a un país, certificados de vacuna, documentos de viaje, manejo de pasajeros deportados y no admisibles entre muchos otros), inclusive recomienda que los trámites de un vuelo internacional de origen no excedan 60 minutos desde que el pasajero se presenta en el mostrador de check-in hasta que aborda su aeronave ni de 45 minutos a la llegada de un vuelo internacional desde que desembarca de la aeronave hasta que sale del aeropuerto.

Por otro lado, el Anexo 17, establece los requerimientos de Seguridad de la Aviación Civil que deben cumplir los Estados Contratantes contra los actos de interferencia ilícita (terrorismo, sabotaje, utilización de aeronaves como armas, entre otros). Por años, la Seguridad de la Aviación Civil ha sido una barrera para la Facilitación y viceversa, lo que debe ser claro, es que, ante cualquier controversia, debe prevalecer la seguridad, más en estos tiempos en donde con mayor rapidez van surgiendo nuevas amenazas. Actualmente, la Seguridad de la Aviación Civil y la Facilitación se ven como un binomio que trabaja de manera armónica (AVSEC-FAL), eso no ha sido para nada sencillo, ya que anteriormente los procesos de inspección de pasajeros eran muy tardados y tediosos, por ello, la razón de presentarnos con 2 o hasta 3 horas de antelación a la salida de nuestro vuelo. Actualmente, el uso de nuevas y más avanzadas tecnologías de inspección y detección han logrado disminuir de manera sustancial los tiempos de procesamiento de pasajeros y su equipaje de mano, equipaje facturado y de la carga a través de los puntos de inspección, esto ha permitido que la aviación siga manteniendo su atributo de velocidad, sin embargo sigue habiendo excepciones, pues será necesaria una revisión manual de la persona (cacheo) y/o de su equipaje cuando exista sospecha que porta algún objeto prohibido o peligroso, o cuando en el aeropuerto exista un nivel de amenaza que justifique, aplicar medidas de seguridad extraordinarias que generalmente van dirigidas a inspeccionar de manera más minuciosa a una mayor cantidad de pasajeros de manera aleatoria. La Seguridad de la Aviación Civil y la Facilitación van muy de la mano, un documento fraudulento puede ser utilizado por un terrorista para ingresar a la zona estéril del aeropuerto haciéndose pasar por un pasajero con un nombre y/o una nacionalidad diferente, o los pasajeros insubordinados, que en la mayoría de las veces además de generar incomodidad a los demás pasajeros, afectan el itinerario del vuelo, por regreso del avión al aeropuerto para desembarcar a dicho pasajero, el cual si no se gestiona de manera adecuada, podría representar una amenaza para la seguridad.

En cuanto al perfil del personal de seguridad en los aeropuertos, también ha tenido que adaptarse y evolucionar con un enfoque de servicio y respeto a los Derechos Humanos, sin perder de vista que su prioridad es y será la prevención de actos de interferencia ilícita. Por los aeropuertos transitan cualquier cantidad de pasajeros de todas nacionalidades, razas y creencias, es muy importante que el personal que efectúa la inspección, conozca los protocolos para cada tipo de pasajero, por ejemplo, pedir a una mujer islámica que se levante el niqab para ver su rostro y hacer la identificación positiva o a un hombre que practica el Sijismo que se retire el turbante puede ser ofensivo e inaceptable, pueden hacerse revisiones en privado o utilizando algún equipo de inspección que evite un mal momento al pasajero sin que demerite la efectividad de la inspección. Saludar al pasajero y sonreírle en el punto de inspección, solicitar su autorización para que se le haga una revisión manual a su persona y a sus pertenencias y explicarle la razón, colocarse guantes de látex para evitar contaminar las pertenencias del pasajero (además de proteger las manos del inspector ante cualquier sustancia que pueda causarle algún daño o infección), son protocolos básicos que se deben impartir en la capacitación inicial.

Para la carga aérea es algo similar, existen certificaciones como CTPAT, OEA, BASC, ISO 28001 y algunas propias de la industria aeronáutica que establecen medidas de seguridad en la cadena de suministro. Los métodos de inspección de carga también han tenido mejoras sustanciales para hacer el proceso mucho más expedito y confiable, equipos de rayos X, EDS (Explosives Detection System), ETD (Explosives Trace Detection) entre otras tecnologías.

La figura de Agente Acreditado de Carga y de Embarcador Conocido como entidades que cumplen con procedimientos de seguridad documentados e implementados, son muy importantes para mantener la cadena de custodia de los embarques desde que salen de la planta de producción hasta que llegan al aeropuerto. En algunos países como Estados Unidos, existe la figura de CCSF (Certified Cargo Screening Facility), que son entidades certificadas por la autoridad para inspeccionar la carga, por ejemplo, una empresa certificada como CCSF puede inspeccionar sus productos desde que salen de sus instalaciones y ya no ser sujetos a otra inspección por parte de la aerolínea cuando llegan al aeropuerto, reduciendo sustancialmente los tiempos de procesamiento.

El ACAS (Air Cargo Advance Screening) funciona de manera similar al APIS (Advance Passenger Information System) para los pasajeros, es decir, antes de que la carga se suba a la aeronave, la autoridad de seguridad del país de destino (Transportation Security Administration en caso de Estados Unidos), mediante una evaluación de riesgos, determina si esta se puede subir o no a la aeronave o debe ser sujeta a una segunda inspección más detallada.

Medidas como las anteriores contribuyen a que se mantenga ese equilibrio entre seguridad y Facilitación.

El futuro presenta nuevos retos, tiempos de procesamiento de pasajeros, equipajes y carga mucho más expeditos y seguridad más eficiente, lo cual solamente se puede lograr con el apoyo de tecnologías más avanzadas, personal altamente calificado y procedimientos bien establecidos. La Seguridad de la Aviación Civil seguirá evolucionando con miras de hacer a la industria más segura pero también más consciente en temas de servicio y Derechos Humanos, anticiparnos a lo que viene simple y sencillamente ya es una exigencia para poder subsistir en una industria altamente demandante por su relevancia económica y comercial a nivel mundial, pero también para continuar manteniendo sus dos principales atributos: seguridad y velocidad que le dan una ventaja competitiva respecto a otros modos de trasporte.

Les invito a leer mi libro "Sistema de Gestión de Seguridad integral" en donde podrán encontrar mayor información al respecto. Disponible en:

https://alfaomega.com.mx/producto/sistema-de gestion-de-seguridad-integral/#/ y en las principales librerías

PROFESIONALIZAR LA SEGURIDAD MÁS ALLÁ DEL CONOCIMIENTO Y HACIA LA VALIDACIÓN DEL CRITERIO

Metro Risk

Edición propiedad de @MetroRisk, asociación

Edison Cadena Ayala
Presidente AIMCSE Ecuador

Durante años, y debido a la falta de oferta y aval académico, el sector seguridad ha luchado por alcanzar un reconocimiento profesional equivalente al nivel de responsabilidad que realmente asume. Proteger personas, activos críticos, información sensible o infraestructuras estratégicas implica tomar decisiones bajo presión, interpretar escenarios complejos y gestionar riesgos que cambian constantemente. Sin embargo, en muchos casos, la conversación sobre profesionalización ha terminado reducida únicamente a la acumulación de certificados, horas de capacitación o aprobaciones memorísticas

El conocimiento es indispensable, pero por sí solo no garantiza competencia. Conocer conceptos, definiciones o metodologías puede permitir aprobar una evaluación; demostrar criterio es lo que verdaderamente permite responder de forma adecuada frente a escenarios reales. En seguridad, donde una decisión puede impactar directamente la continuidad operativa, la integridad de las personas o la resiliencia organizacional, la diferencia entre saber y comprender resulta crítica. La norma ISO/IEC 17024 establece que los sistemas de certificación de personas deben orientarse a garantizar competencias verificables y consistentes en relación con funciones específicas (ISO, 2012). Esto implica que una certificación profesional no debería limitarse a validar memoria técnica, sino capacidad de análisis, interpretación, toma de decisiones y aplicación práctica del conocimiento.

La competencia profesional no se construye únicamente desde la teoría; se consolida mediante experiencia, criterio y responsabilidad. En el ámbito de la seguridad, esta distinción adquiere aún mayor relevancia. Las amenazas contemporáneas son dinámicas, híbridas y cambiantes. Ningún procedimiento puede prever absolutamente todos los escenarios, y ningún manual reemplaza completamente la capacidad humana de evaluar contexto, anticipar consecuencias y adaptar respuestas. Allí es donde el criterio profesional se convierte en un activo estratégico. Hablar de profesionalización no significa desacreditar la formación técnica ni minimizar el valor del estudio. Por el contrario, implica reconocer que el verdadero propósito de una certificación debería ser fortalecer la confianza en las capacidades reales del profesional. Cuando una certificación valida competencias, también valida ética, madurez operativa y responsabilidad frente al riesgo.

El desafío actual no es emitir más certificados; es asegurar que estos representen verdaderamente la capacidad de proteger, gestionar y decidir en entornos complejos. La profesionalización sostenible del sector dependerá menos de la acumulación de credenciales y más de la capacidad de demostrar desempeño, criterio y coherencia profesional.

Porque en seguridad, memorizar información puede permitir responder preguntas; pero es el criterio lo que realmente permite proteger organizaciones, personas y entornos críticos.

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.**

Figura 1. Evolución conceptual de la certificación profesional en seguridad

Comparación entre un modelo centrado únicamente en conocimiento y un enfoque orientado a competencias y criterio profesional.

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
- Geopolitica.
- Seguros de Embarcaciones Recreo.
- Grafologia,
- Documentoscopia,
- Grafopsicopatologia Criminal y Forense.
- Due Diligence (Debida Diligencia).

www.oterotrillogabinetepericial-andaluciaceuta.es/

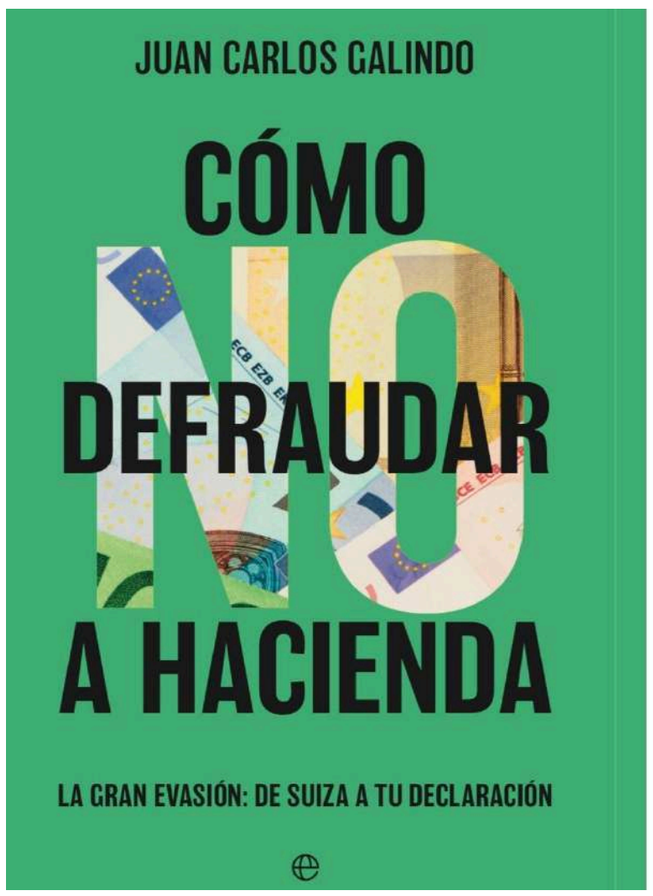
AGENDA

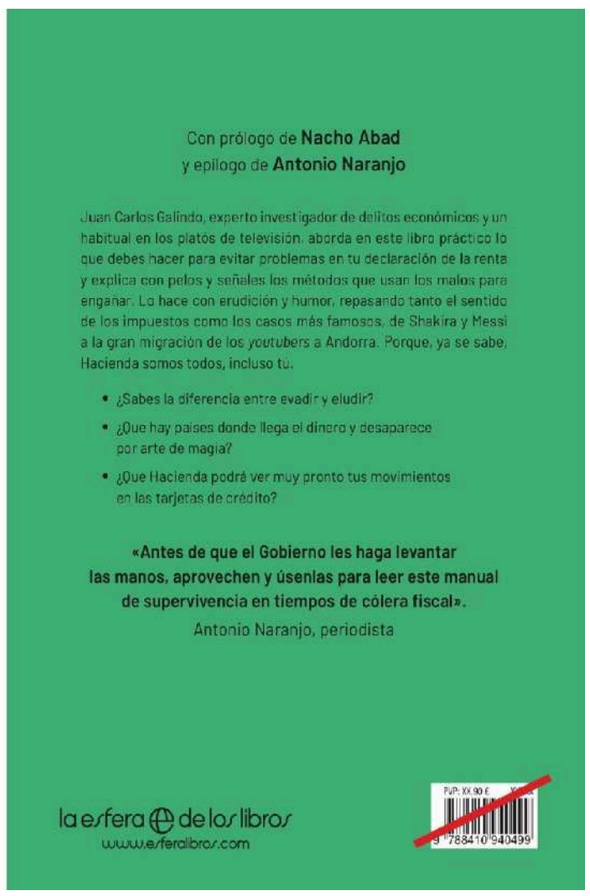
Metro Risk

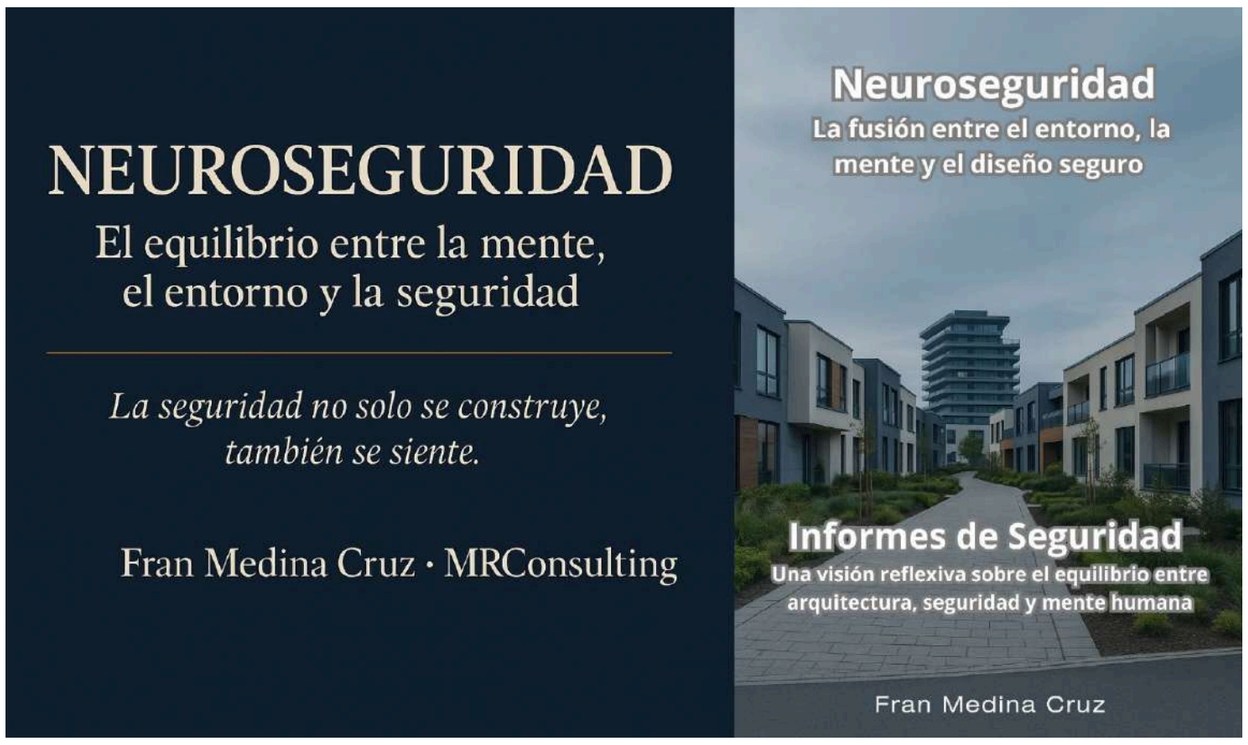
Edición propiedad de @MetroRisk, asociación

RADIO

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







Metrorisk

Proyecto Asociativo

www.metrorisk.es