EDITORIAL MR

ISSN 3045-7629

ENERO
FEBRERO

AÑO
2026

SEGURIDAD

Fran Medina Cruz
Francisco Javier Gonzales Fuentes
Carlos G. Barrett
Gregorio Duro
Mercedes Escudero Carmona
Iván Cantalapiedra
Emilio Piñeiro
Rosa Fernández
Carlos Serrano
Abraham Santana
Alina Rubio
Elena de la Parte
Carlos Miguel Ortiz
Jonatthan Hermida Sosa
Carlos E Pérez Barrios

Edición propiedad de @MetroRisk, asociación

@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.

LA SEGURIDAD EN MOVIMIENTO: UNA DEUDA NORMATIVA DEL TRANSPORTE PÚBLICO MODERNO

Metro Risk

Fran Medina Cruz
Director de MetroRisk

La seguridad en el transporte público masivo sigue siendo una de las grandes paradojas del sistema de protección contemporáneo. Cada día, millones de personas se desplazan en trenes, metros, ferris y aviones, compartiendo espacios cerrados, en movimiento, con alta densidad de ocupación y una característica determinante: durante el trayecto no pueden abandonar el entorno si perciben peligro. Son espacios de tránsito, pero también espacios de confinamiento temporal, donde el riesgo tiene un comportamiento propio, diferente al de un edificio, una calle o un evento. Y, sin embargo, el marco normativo español continúa aplicando modelos de seguridad diseñados para entornos estáticos, como si el movimiento no alterase la naturaleza del riesgo.

Mientras que los eventos deportivos o culturales están obligados a contar con vigilantes de seguridad por razones de aforo, concentración y riesgo, el transporte masivo, que reúne esos mismos factores de forma permanente, no dispone de una regulación específica que exija vigilancia profesional especializada en tránsito. No se trata de una ausencia de seguridad, sino de una ausencia de especialización normativa. La Ley de Seguridad Privada regula la vigilancia de recintos, bienes y eventos, pero no reconoce la vigilancia en movimiento como un entorno operativo propio, pese a que la complejidad de un tren en marcha, un barco navegando o un avión en vuelo exige competencias radicalmente distintas.

En tránsito, el riesgo no es puntual ni localizado: evoluciona con el trayecto, se desplaza, cambia de forma y se ve amplificado por la imposibilidad de escape. Un conflicto menor puede escalar rápidamente, una situación de ansiedad puede contagiar al resto del pasaje y una emergencia exige respuestas inmediatas en condiciones limitadas de evacuación. Estos escenarios requieren formación en gestión de conflictos en espacios confinados, psicología de masas, reducción del pánico, intervención no violenta, lectura anticipada del comportamiento humano y coordinación instantánea con centros de control y fuerzas públicas. Sin embargo, estas competencias no están exigidas normativamente, ni reguladas de forma homogénea, ni reconocidas como especialidad profesional dentro de la seguridad privada.

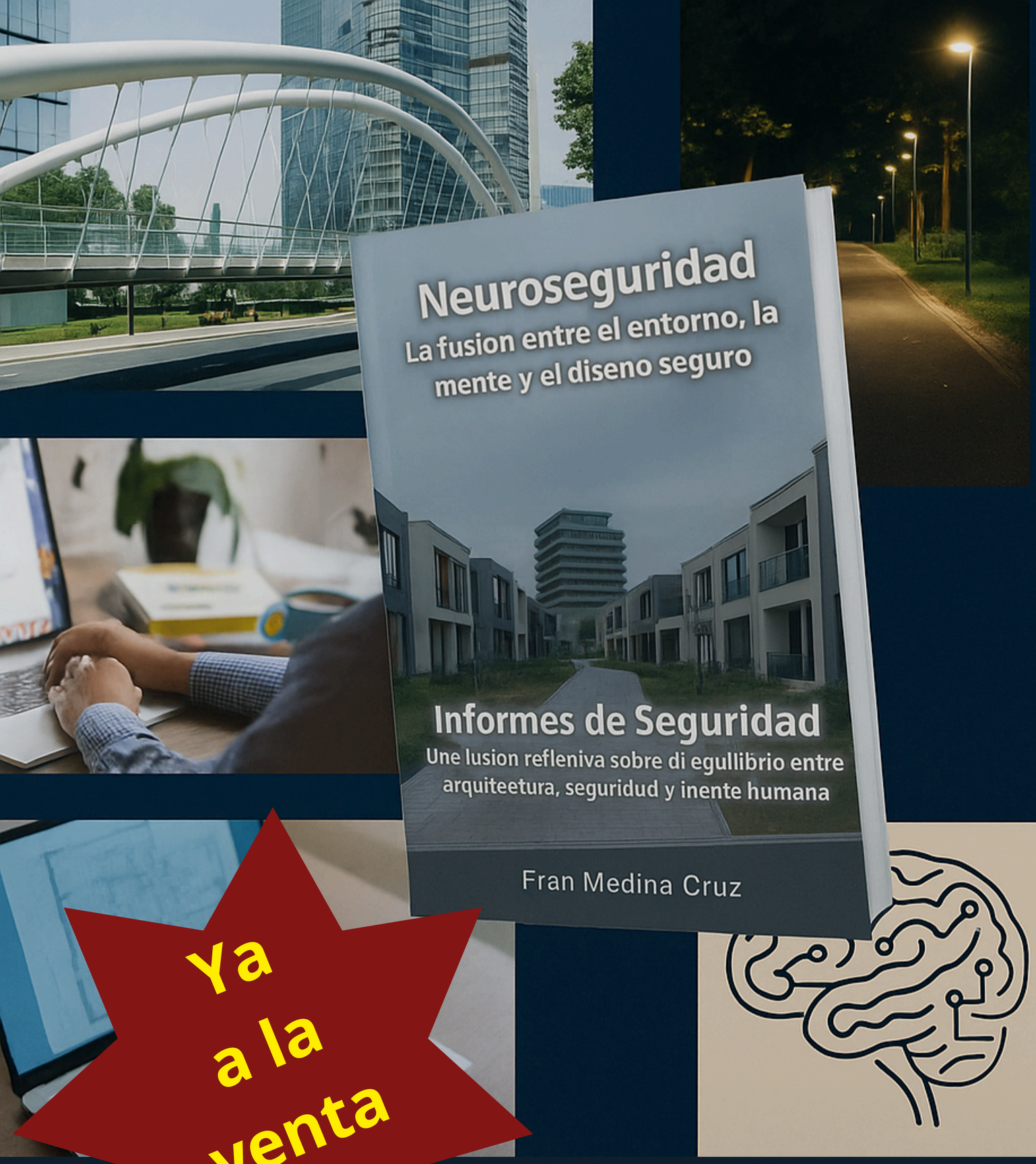
El modelo actual se apoya fundamentalmente en tecnología, protocolos y fuerzas de seguridad pública, lo cual es necesario, pero insuficiente. La seguridad moderna no se basa solo en la detección, sino en la prevención; no solo en la respuesta, sino en la anticipación. Y ahí la presencia humana especializada resulta insustituible. Un vigilante formado específicamente para operar en entornos de tránsito actúa como sensor preventivo, como estabilizador conductual y como primer interviniente, reduciendo incidentes antes de que se conviertan en problemas mayores y descargando operativamente a las fuerzas públicas de actuaciones que no requieren intervención policial.

Otros países europeos y asiáticos ya han comprendido esta realidad y han creado cuerpos o especialidades específicas para el transporte, integrando seguridad humana, tecnología y procedimientos en un solo sistema. España, pese a disponer de una de las redes ferroviarias más extensas de Europa y de infraestructuras de transporte de primer nivel, sigue sin dar ese paso. No por falta de necesidad, sino por inercia normativa. El resultado es un sistema eficaz desde el punto de vista técnico, pero incompleto desde el punto de vista humano y preventivo.

Desde la perspectiva de la seguridad por diseño y la neuroseguridad, el transporte no puede concebirse únicamente como infraestructura, sino como experiencia. El cerebro humano necesita referencias visibles de orden, control y protección, especialmente en entornos cerrados y en movimiento. La percepción de seguridad no es un elemento secundario: condiciona el comportamiento, reduce el estrés, previene reacciones desproporcionadas y mejora la convivencia. Un vigilante especializado en tránsito no es solo una figura disuasoria; es un modulador del comportamiento colectivo, un elemento de calma y un factor clave en la resiliencia del sistema de transporte.

La creación de una normativa específica que regule la vigilancia de seguridad en tránsito, con formación obligatoria, competencias definidas y protocolos claros de coordinación, no sería un exceso regulatorio, sino una evolución lógica y necesaria del sistema de protección de personas e infraestructuras críticas. Aportaría prevención real, mayor eficiencia, mejor percepción de seguridad, profesionalización del sector y una respuesta más rápida y ordenada ante incidentes. En un contexto donde la movilidad es esencial para la vida económica y social, seguir ignorando esta realidad es una oportunidad perdida.

A todos los afectados, y familiares del accidente ferroviarios en Córdoba. Mis condolencias y fuerzas para afrontarlo.



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

Disponible ahora

Fran Medina Cruz

MRConsulting

Ya a la venta

NEUROSEGURIDAD

El equilibrio entre la mente, el entorno y la seguridad

La seguridad no solo se construye, también se siente.

Fran Medina Cruz · MRConsulting

LA PSICOSOCIOLOGÍA DE LA SEGURIDAD: EL FACTOR HUMANO COMO EJE DEL RIESGO Y LA PROTECCIÓN

Metro Risk

Edición propiedad de @MetroRisk, asociación

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

Los entornos marcados por la incertidumbre, la complejidad y la convergencia de riesgos, físicos, tecnológicos, reputacionales y sociales, la seguridad ya no puede entenderse únicamente desde una perspectiva técnica o normativa. Cada vez resulta más evidente que el factor humano es tanto el principal activo como una de las mayores vulnerabilidades de cualquier sistema de seguridad. Es en este punto donde la psicosociología de la seguridad adquiere un papel central.

¿Qué entendemos por psicosociología de la seguridad?

La psicosociología de la seguridad analiza cómo los comportamientos individuales y colectivos, las percepciones del riesgo, las dinámicas de grupo, la cultura organizativa y el contexto social influyen directamente en la eficacia de las medidas de seguridad. No se trata solo de cómo reaccionan las personas ante una amenaza real, sino de cómo interpretan el riesgo, cómo toman decisiones bajo presión, cómo interiorizan (o no) los procedimientos y cómo el entorno social condiciona su conducta. En seguridad, la percepción del riesgo suele ser más determinante que el riesgo objetivo

La percepción del riesgo: entre la normalización y el miedo

Uno de los principales problemas en la gestión de la seguridad es la distorsión de la percepción del riesgo. En muchos entornos laborales se produce una normalización del peligro: “nunca ha pasado nada”, “esto siempre se ha hecho así”, “no es para tanto”. Esta banalización genera relajación, incumplimiento de protocolos y resistencia a las medidas preventivas. En el extremo contrario, encontramos entornos dominados por el miedo, donde la sobreestimación del riesgo provoca bloqueos operativos, estrés crónico y pérdida de eficacia. La psicosociología permite equilibrar ambos extremos, ajustando la comunicación y las medidas al contexto real.

Cultura de seguridad: mucho más que normas y procedimientos La cultura de seguridad no se implanta por decreto. No basta con manuales, protocolos o planes de autoprotección si estos no son comprendidos, aceptados e interiorizados por las personas. Una cultura de seguridad sólida se basa en:

- Liderazgo visible y coherente.
- Comunicación clara y bidireccional.
- Formación práctica y contextualizada.
- Participación activa de los trabajadores.
- Confianza y corresponsabilidad.

IntelForensic
G&F Soluciones

Desde la psicosociología, se analiza cómo influyen los estilos de liderazgo, las jerarquías informales, los conflictos internos o la presión productiva en el cumplimiento de las medidas de seguridad.

El comportamiento humano en situaciones críticas En situaciones de emergencia o crisis, el comportamiento humano rara vez responde al modelo racional que describen los planes. Aparecen reacciones como:

- Bloqueo o parálisis.
- Conductas imitativas.
- Búsqueda de figuras de autoridad.
- Toma de decisiones impulsivas.

Comprender estas reacciones permite diseñar planes más realistas, entrenamientos más eficaces y protocolos adaptados al comportamiento real de las personas, no al comportamiento idealizado.

Seguridad, estrés y riesgos psicosociales La seguridad también tiene un impacto directo sobre la salud mental y el bienestar. Turnos prolongados, vigilancia permanente, presión por el error cero, exposición continuada a amenazas o conflictos generan riesgos psicosociales que, paradójicamente, pueden aumentar la inseguridad. Un profesional de seguridad fatigado, estresado o desmotivado es más propenso al error, a la omisión y a la mala toma de decisiones. La psicosociología ayuda a integrar la prevención de riesgos psicosociales dentro de la estrategia global de seguridad.

El papel del Director de Seguridad El Director de Seguridad del siglo XXI no puede limitarse a gestionar medios y tecnologías. Debe ser también un gestor de conductas, percepciones y culturas organizativas. Esto implica:

- Entender la organización como un sistema social.
- Anticipar resistencias al cambio.
- Diseñar estrategias de concienciación eficaces.
- Mediar entre intereses operativos, humanos y estratégicos.

La seguridad eficaz es aquella que las personas comprenden, aceptan y hacen suya.

ESTIMADO LECTOR:
FELICES FIESTAS Y PROSPERO 2026
INVESTIGACIÓN PRIVADA.

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos G. Barrett
Gerente general en Spy Investigación & Barrett

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

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

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

Quieres saber que hace

- Saber dónde está
- Necesitas saber dónde va
- Con quién va acompañado/a

Buscas demostrar con fotografías / video que hace en su día a día

INVESTIGACIÓN PRIVADA para:

- Particulares
- Empresas
- Abogados

Discreción absoluta
Resultados reales
Atención personalizada

No dudes en llamar y consultar nuestra forma de trabajar y formalizar un presupuesto adecuado a tus necesidades.

Un equipo profesional cuestionará tus dudas y buscará las soluciones adecuadas a tu caso.

CONTACTA con nosotros a través de:
-Email : informacion@spyinvestigacion.com
-Tlf / Whatssap : +34 660 359 806
- **www.spyinvestigacion.com**

CARLOS G. BARRETT
Investigador Privado
Experto en Criminalística

Gregorio Duro
Tecnico en licitaciones y Proyectos

SOLUCIÓN POR SUSTITUCIÓN EN LAS OPERACIONES DE ANÁLISIS DE RIESGOS

Tras el paréntesis de las fiestas navideñas, retomo mi actividad en Metrorisk con energías renovadas y una motivación reforzada. Inicio esta nueva etapa con la ilusión de seguir aportando análisis, experiencias y contenidos de valor, manteniendo el compromiso con la mejora continua en el ámbito de la seguridad, la gestión del riesgo y la protección de personas e infraestructuras. Este comienzo de año se plantea como una oportunidad para afrontar nuevos retos desde una perspectiva actualizada y proactiva.

Solución por sustitución: simplificar el análisis de riesgos sin perder precisión En la gestión de riesgos, no siempre es posible conocer todos los datos con exactitud. Algunos parámetros son difíciles de medir, cambian con el tiempo o dependen de circunstancias externas que escapan al control de la organización. Ante esta incertidumbre, surge la solución por sustitución, una técnica que permite reemplazar variables complejas o inciertas por valores equivalentes confiables, manteniendo la coherencia y utilidad del análisis. Lejos de ser un simple atajo, esta práctica se basa en criterios técnicos sólidos y en la experiencia acumulada, asegurando que los riesgos evaluados sean realistas, comparables y útiles para la toma de decisiones estratégicas. El principio fundamental es sencillo: cuando un dato no está disponible o es demasiado complejo para calcularlo directamente, se busca un valor representativo que cumpla la misma función dentro del modelo de evaluación. Esto permite que el análisis continúe sin interrupciones y que los resultados se mantengan fiables y consistentes, proporcionando una base sólida para la gestión de riesgos en entornos dinámicos.

Cómo se aplica en la práctica La solución por sustitución se integra de manera natural en los modelos de riesgo dinámicos, donde la probabilidad de ocurrencia de un evento, la vulnerabilidad de los activos y la magnitud del impacto pueden variar con el tiempo. Esto es especialmente útil en sistemas de seguridad complejos, instalaciones críticas o procesos operativos con alta interdependencia entre factores.

A modo de ejemplo, imaginemos una planta industrial que está evaluando el riesgo de intrusión en un área sensible equipada recientemente con un sistema de control de accesos. La información precisa sobre la eficacia del nuevo sistema aún no está disponible, pero se necesita estimar la exposición para priorizar medidas adicionales. Aplicando la solución por sustitución, los responsables de seguridad pueden utilizar como referencia el comportamiento de sistemas similares en otras instalaciones. Esto permite continuar con el análisis, planificar acciones preventivas y evaluar la criticidad del riesgo sin comprometer la coherencia del estudio. Otro ejemplo se encuentra en activos complejos con múltiples vulnerabilidades interdependientes, como un centro de datos en el que varios sistemas de soporte eléctrico, climatización y seguridad están conectados.

Medir cada vulnerabilidad por separado podría resultar poco práctico y generar un exceso de complejidad en el cálculo. En este caso, se puede crear un parámetro equivalente que represente la vulnerabilidad global combinada lo que permite calcular el riesgo total de forma más clara y compararlo con otros escenarios y priorizar acciones preventivas de manera efectiva. Además, la sustitución puede aplicarse para evaluar impactos difíciles de cuantificar, como efectos reputacionales o pérdidas indirectas. Al transformar estos impactos complejos en un valor representativo, se puede integrar la información en matrices de riesgos, simulaciones de escenarios y modelos probabilísticos, manteniendo la consistencia del análisis global.

Ventajas de la solución por sustitución La principal ventaja de esta técnica es que reduce la complejidad del análisis sin sacrificar la precisión, permitiendo evaluar riesgos de manera rápida y eficiente, incluso en entornos inciertos o con información incompleta. Esto facilita la priorización de acciones, la planificación de medidas preventivas y la toma de decisiones estratégicas fundamentadas. Otro beneficio importante es la claridad en la comunicación. Los resultados derivados de la sustitución permiten que responsables y equipos de seguridad comprendan la exposición real y la criticidad de cada escenario, incluso cuando los cálculos subyacentes son complejos, lo cual facilita la mejora y la coordinación interna, facilita la gestión de recursos y permite una respuesta más efectiva ante posibles amenazas

No obstante, la técnica requiere criterio y conocimiento del contexto. Sustituir un parámetro sin fundamentos sólidos puede conducir a sobreestimaciones o subestimaciones del riesgo, afectando la eficacia de las medidas preventivas. Por eso, los valores sustitutos deben elegirse con base en datos confiables, referencias de experiencias previas y comprensión profunda de la operación y los riesgos asociados.

Un enfoque estratégico y cercano Más allá de su función técnica, la solución por sustitución tiene un valor estratégico significativo. Permite que los sistemas de gestión de riesgos sean flexibles, adaptativos y capaces de responder a cambios rápidos en el entorno. Al integrarse con análisis de interdependencias, simulaciones de escenarios y modelos probabilísticos, proporciona resultados fiables y comparables que permiten planificar medidas preventivas y correctivas de manera eficiente. A modo de ejemplo se puede contemplar una empresa de logística que evalúa el riesgo de interrupciones en la cadena de suministro y en la que algunos proveedores son nuevos y no existen datos históricos sobre su desempeño. Mediante sustitución, se puede utilizar como referencia el comportamiento promedio de proveedores similares. Esto permite estimar la exposición general y priorizar acciones preventivas, como contratos de respaldo o inventarios de seguridad, sin retrasar la planificación ni comprometer la validez del análisis. Por ello, la solución por sustitución no es solo un recurso técnico: es una herramienta que combina rigor y practicidad, acercando el análisis de riesgos al día a día de quienes toman decisiones y permitiendo abordar la incertidumbre con resultados confiables, claros y útiles. Su aplicación mejora la gestión estratégica y asegura que las decisiones sobre prevención y mitigación se basen en análisis sólidos, incluso cuando algunos parámetros son difíciles de medir o desconocidos.

Deseo expresar mi más sincero agradecimiento a Metrorisk por la difusión mensual de artículos de carácter técnico, cuyo compromiso constante no solo enriquece el conocimiento del sector, sino que también mantiene un espacio de reflexión y actualización profesional.

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.

CONTROL DE ACCESO: MÁS ALLÁ DE LA CERRADURA BAJO LAS NORMAS ISO 22341 Y 22341-2 CPTED

Tradicionalmente, el control de acceso se ha visto como un componente tecnológico, destacando los lectores de tarjetas y con datos biométricos, principalmente. Sin embargo, las normas ISO 22341 y 22341-2 de la Metodología Prevención del Delito Mediante el Diseño Ambiental CPTED (por sus siglas en inglés), definen directrices proponiendo que la seguridad y protección de activos deben ser indisociables del entorno, operando de forma orgánica en cada rincón del diseño." en el entorno físico para influir en el comportamiento humano y reducir las oportunidades delictivas

LOS PILARES DE CPTED APLICADOS AL CONTROL DE ACCESO: Para que un control de acceso sea efectivo según la norma, debe cumplir con cuatro principios fundamentales:

- Vigilancia Natural: el diseño debe permitir que los usuarios legítimos vean y sean vistos. Un control de acceso no debe crear puntos ciegos, escondites o lugares trampa.
- Control Natural de Accesos: utilizar elementos físicos (setos, cambios de nivel, diseño de senderos) para canalizar a las personas hacia puntos de entrada específicos controlados.
- Refuerzo Territorial: definir claramente qué es espacio público, semiprivado y privado para que los intrusos se sientan "fuera de lugar".
- Mantenimiento y Gestión: un sistema de acceso deteriorado envía una señal de falta de control, esto basado en la Teoría de las Ventanas Rotas.

ISO 22341-2 CPTED: EL MARCO OPERATIVO: Mientras que la primera parte de la norma establece los conceptos generales, la ISO 22341-2 profundiza en las metodologías de evaluación y la implementación técnica. Es decir, mientras que la parte 1 de la norma se centra en los conceptos, definiciones y principios teóricos de CPTED, la parte 2 establece el "cómo" se deben ejecutar las acciones en el terreno.

ESTRATEGIAS DE IMPLEMENTACIÓN DE CONTROLES DE ACCESO: Bajo esta visión, el control de acceso se divide en tres capas de intervención:

Capa de Control	Elementos Sugeridos por ISO 22341-2	Objetivo
Organizativa	Personal de seguridad, protocolos de registro.	Gestión del flujo humano.
Tecnológica	Biometría, Sistema de Video vigilancia con analítica, cerraduras inteligentes.	Verificación de identidad y registro.
Física (Diseño)	Paisajismo de seguridad, iluminación, cercados y/o barreras estéticas.	Disuasión psicológica y barrera física.

El Proceso de Evaluación de Riesgos: La norma enfatiza que no existe una solución única. El control de acceso debe nacer de un análisis previo que incluya:
1. Análisis del entorno social: entender quiénes transitan la zona.
2. Identificación de vulnerabilidades físicas: detectar rutas de escape o accesos no autorizados fáciles, entre otras.
3. Definición de perímetros: crear zonas de transición que preparen al usuario para el control de identidad.

Beneficios de la Integración ISO CPTED: La adopción de este enfoque no solo mejora la seguridad, sino que también optimiza la experiencia del usuario:

- Reducción del sentimiento de inseguridad: Un entorno bien diseñado se siente seguro sin parecer una prisión. La norma promueve que el usuario sepa siempre dónde está y hacia dónde puede ir.

1. Señalética de Orientación: mapas y letreros claros que reduzcan la desorientación.
2. Líneas de Visión Despejadas: eliminar el efecto "túnel" o esquinas ciegas donde el usuario siente que puede ser emboscado.
3. Transparencia: uso de materiales que permitan ver qué hay al otro lado de una puerta o muro antes de cruzarlo.

La reducción del sentimiento de inseguridad es uno de los objetivos centrales de la ISO 22341 CPTED, ya que la norma reconoce que un espacio puede ser estadísticamente seguro pero percibirse como peligroso, lo que ahuyenta a los usuarios legítimos y termina facilitando el crimen real.

- Eficiencia Operativa: Bajo el enfoque de la ISO 22341 no solo busca que el sistema de seguridad funcione, sino que lo haga de manera fluida, con el menor costo de recursos posible y sin entorpecer la función principal de la instalación, ya sea un hospital, una oficina o un centro comercial. Los elementos clave para lograr eficiencia operativa integrando CPTED y tecnología, son:

1. Automatización de procedimientos.
2. Reducción de falsas alarmas (análisis predictivo).
3. Optimización del recurso humano.
4. Gestión del flujo y wayfinding.
5. Recolección de datos para la toma de decisiones.

- Valorización del Activo: Los edificios al canalizar el flujo de personas de forma natural, reducen las falsas alarmas. Es el argumento económico definitivo para implementar la ISO 22341 CPTED.

6. Reducción del riesgo reputacional y legal.
7. Optimización de primas de seguros.
8. Longevidad de las instalaciones y bajo deterioro.
9. Plusvalía de las instalaciones.

En el sector inmobiliario y corporativo, la seguridad ya no se ve como un gasto necesario, sino como una mejora de capital que incrementa el valor de una propiedad en el mercado.

IONIQ SEGURIDAD: EXPERIENCIA, PERSONAS Y DIVULGACIÓN COMO BASE DE UN PROYECTO DIFERENTE

Metro Risk

Iván Cantalapiedra.Director de Seguridad.
CEO IONIQ Seguridad

La fundación de una empresa de seguridad privada no debería responder a una oportunidad puntual, sino a una convicción profesional construida con el tiempo. En mi caso, IONIQ Seguridad nace tras una trayectoria prolongada en el sector de más de 25 años, habiendo ocupado puestos de Dirección de Seguridad en empresas usuarias, de mando intermedio en empresas del sector, y por supuesto como personal operativo, Vigilante de Seguridad, lo que me permitió conocer la seguridad desde una visión global y realista desde todos los puntos de vista -trabajador-cliente-empresa

Esa experiencia me ayudó a identificar tanto las fortalezas del sector como aquellas áreas claramente mejorables.

Con el objetivo de ofrecer a mis clientes un servicio más especializado, cercano y verdaderamente integral, decidí dar un paso adelante y fundar **IONIQ Seguridad.**

Una empresa creada desde la experiencia **IONIQ Seguridad** se concibe desde el inicio como un proyecto basado en la gestión profesional de la seguridad, la planificación, la prevención y la adaptación a cada cliente.

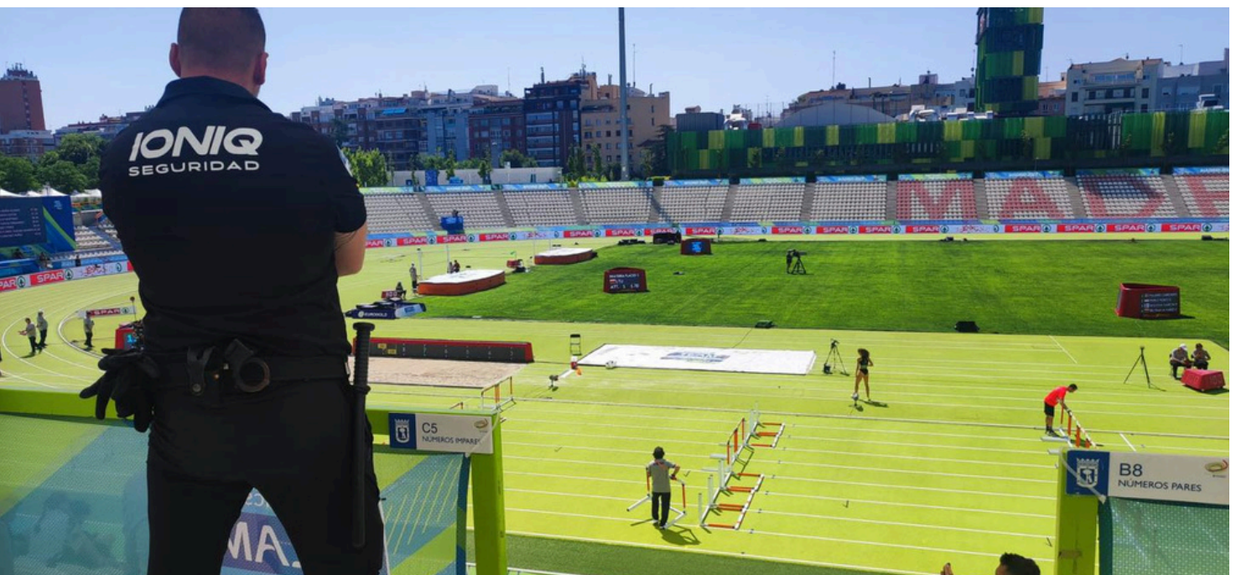
Entendemos que no existen soluciones universales y que cada entorno requiere un análisis específico de riesgos y una respuesta adecuada. La empresa nace también con la vocación de integrar correctamente distintos servicios, aportando valor añadido a los clientes a través de una dirección técnica sólida y una visión estratégica de la seguridad.

El vigilante como eje del sistema

Uno de los principios fundamentales de **IONIQ Seguridad** es el trato al vigilante. Desde el primer momento tuve claro que el personal de seguridad es la base real del servicio y que su motivación influye directamente en la calidad del trabajo que se presta.

En **IONIQ** apostamos por un trato profesional, cercano y respetuoso, por la comunicación directa y por el apoyo constante al vigilante en su labor diaria. Creemos firmemente que un vigilante contento presta un servicio excelente y que, además, se convierte en nuestra mejor publicidad, tanto por la imagen que proyecta como por lo que transmite de la empresa.

La seguridad empieza por las personas, y solo cuidando a los profesionales se puede ofrecer un servicio de calidad.



Divulgación y acercamiento del sector a la sociedad

Hace algo más de tres años decidí iniciar una labor paralela de divulgación sobre la seguridad privada con un objetivo claro: acercar el sector a la sociedad y poner en valor una profesión muchas veces desconocida o infravalorada.

A través de la creación de contenido divulgativo en Redes Sociales como Tiktok, Instagram y Youtube -@directordeseguridad- he buscado:

- Explicar qué es realmente la seguridad privada y cuál es su función.
- Recordar a los profesionales conceptos básicos que, con el tiempo, pueden haberse olvidado.
- Resolver dudas habituales tanto de vigilantes como de usuarios y clientes.
- Contribuir a una mayor cultura de seguridad en general.

La divulgación es una herramienta poderosa para mejorar la percepción del sector, dignificar la profesión y fomentar buenas prácticas. Una sociedad que entiende la seguridad es una sociedad más segura.

Un proyecto con visión de futuro. IONIQ Seguridad no nace para ser una empresa más, sino para aportar una visión moderna, responsable y humana de la seguridad privada donde la experiencia, la dirección técnica, la prevención y las personas ocupan un lugar central.

La seguridad del presente y del futuro se construye con conocimiento, profesionalidad y compromiso. Esa es la base sobre la que se fundó **IONIQ Seguridad** y la que sigue marcando nuestro camino. La seguridad privada no necesita más discursos, sino proyectos coherentes, profesionales comprometidos y una sociedad que entienda su importancia.

IONIQ Seguridad nace desde esa convicción: hacer seguridad con criterio, con respeto y con personas que creen en lo que hacen

VISIÓN
COMPLIANCE
Metro Risk
Edición propiedad de @MetroRisk, asociación

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

De Darwin a la IA: Evolución, Entornos VUCA-BANI y el Nuevo Paradigma del Compliance y Liderazgo

Desde los tiempos de Charles Darwin, sabemos que la supervivencia no depende de ser el más fuerte o el más inteligente, sino de quien mejor se adapta. En el entorno empresarial actual, esta premisa se ve reforzada por la disrupción tecnológica, el auge de la Inteligencia Artificial (IA) y el paso de los entornos VUCA a BANI. Hoy, no basta con "resistir" al cambio; necesitamos liderarlo y convertirlo en ventaja competitiva. En este ensayo, exploraré cómo la IA, el compliance y el liderazgo ético se han vuelto fundamentales para la evolución de las organizaciones. Mi propósito no es debatir si la IA generará cambios —eso ya ocurre—, sino cómo integrar esta transformación sin sacrificar la confianza, la integridad y el propósito que distinguen a las empresas sostenibles.

1. Del entorno VUCA al BANI: la incertidumbre intensificada Durante años, el acrónimo VUCA (Volatility, Uncertainty, Complexity, Ambiguity) describió la volatilidad y la complejidad del mundo de los negocios. Sin embargo, los últimos tiempos —marcados por crisis globales, aceleración digital y cambios estructurales— han hecho insuficiente este término. Surge así BANI (Brittle, Anxious, Nonlinear, Incomprehensible), que capta con mayor fuerza la fragilidad y la imprevisibilidad del momento actual.

- Brittle (Frágil): Nada es realmente estable; grandes corporaciones pueden derrumbarse por crisis repentinas.
- Anxious (Ansioso): El exceso de información y la velocidad del cambio saturan tanto a directivos como a empleados, generando parálisis o toma de decisiones impulsivas.
- Nonlinear (No Lineal): Un suceso pequeño puede desencadenar consecuencias desproporcionadas.
- Incomprehensible (Incomprensible):

La abundancia de datos puede, paradójicamente, dificultar la toma de decisiones estratégicas. En este mundo BANI, la adaptación reactiva deja de ser suficiente. Las organizaciones necesitan anticiparse, cuestionar modelos de negocio tradicionales y, sobre todo, cultivar la resiliencia para responder con rapidez y criterio a las disrupciones constantes.

2. La IA como acelerador de la evolución empresarial La Inteligencia Artificial va más allá de ser una herramienta para automatizar procesos; se ha convertido en el nuevo gran motor evolutivo de las empresas. Hasta ahora, la competitividad se basaba principalmente en capital financiero, talento humano y estructuras organizativas. Hoy, emerge un cuarto pilar: el capital algorítmico. Organizaciones como OpenAI o Amazon han demostrado cómo la IA puede escalar modelos de negocio en meses, reconfigurando industrias enteras. Sin embargo, esta celeridad despierta interrogantes éticos: ¿dónde ubicamos la responsabilidad humana cuando la IA toma decisiones críticas? ¿Cómo evitar sesgos en algoritmos que procesan millones de datos al día? La respuesta no está en frenar la tecnología, sino en integrarla con un marco de compliance robusto, un liderazgo ético que actúe como "cerebro y conciencia", y una cultura organizacional que entienda la IA como palanca de crecimiento, no como sustituto de la reflexión humana

3. Un nuevo enfoque de compliance: de norma a ecosistema vivo El cumplimiento normativo ha pasado de ser una lista de requisitos legales a un ecosistema vivo que conecta regulación, ética, tecnología, estrategia y liderazgo. El viejo enfoque de compliance se limitaba a "evitar multas" o "reducir riesgos legales". En cambio, el compliance del futuro:

- Se anticipa a los riesgos: La evolución de las normas y la rápida obsolescencia de los modelos obliga a que la supervisión sea continua, no anual.
- Integra la IA: Los algoritmos ayudan a monitorizar procesos con una precisión y alcance imposibles para un equipo humano. Pero siempre con supervisión final de personas.
- Fomenta la cultura de la transparencia: Más que imponer reglas, se trata de construir un contexto donde cada miembro de la organización asuma la integridad como valor esencial.

Lejos de ser un "costo", el compliance se convierte en ventaja competitiva, pues inspira la confianza de inversores, clientes y colaboradores, tan necesaria en un entorno cada vez más volátil y desconfiado.

4. La ética como eje vertebrador. En un mundo BANI, la ética es la brújula que evita que la organización se desvanezca en medio de la incertidumbre. La mera eficiencia no basta; necesitamos asegurar que las innovaciones tecnológicas —especialmente la IA— respeten la dignidad humana, la equidad y la transparencia. "La ética no es un lujo, sino la columna vertebral que sostiene la credibilidad en cada decisión empresarial." Este enfoque va más allá de cumplir leyes: implica asumir la responsabilidad de que los algoritmos no perpetúen sesgos, de que las decisiones automatizadas sean auditables y de que la dirección mantenga la última palabra. Un líder ético no delega su conciencia en una máquina, sino que utiliza la IA como aliada para refinar su criterio.

5. Liderazgo transformacional: más allá del control, hacia la influencia En el pasado, el liderazgo se asociaba al poder jerárquico y al control centralizado. Sin embargo, en un entorno BANI, la clave está en la influencia, la inspiración y la creación de confianza. Los líderes que triunfarán son aquellos que combinan:

- Empatía: En un contexto ansioso y frágil, un líder debe saber escuchar, contener y guiar a su equipo.
- Visión crítica: La IA ofrece datos, pero el líder traza el propósito y define los límites éticos y estratégicos.
- Adaptabilidad: La capacidad de aprender y desaprender a gran velocidad, asumiendo que lo válido hoy puede no servir mañana.

Dejar atrás el liderazgo autoritario implica reconceptualizar el poder. La autoridad no radica en imponer órdenes, sino en inspirar compromisos que motiven a la gente a dar lo mejor de sí misma.

6. Convergencia total: IA, compliance y liderazgo El verdadero salto evolutivo sucede cuando la IA, el compliance y el liderazgo ético dejan de verse como “silos” y se convierten en un tejido estratégico único.

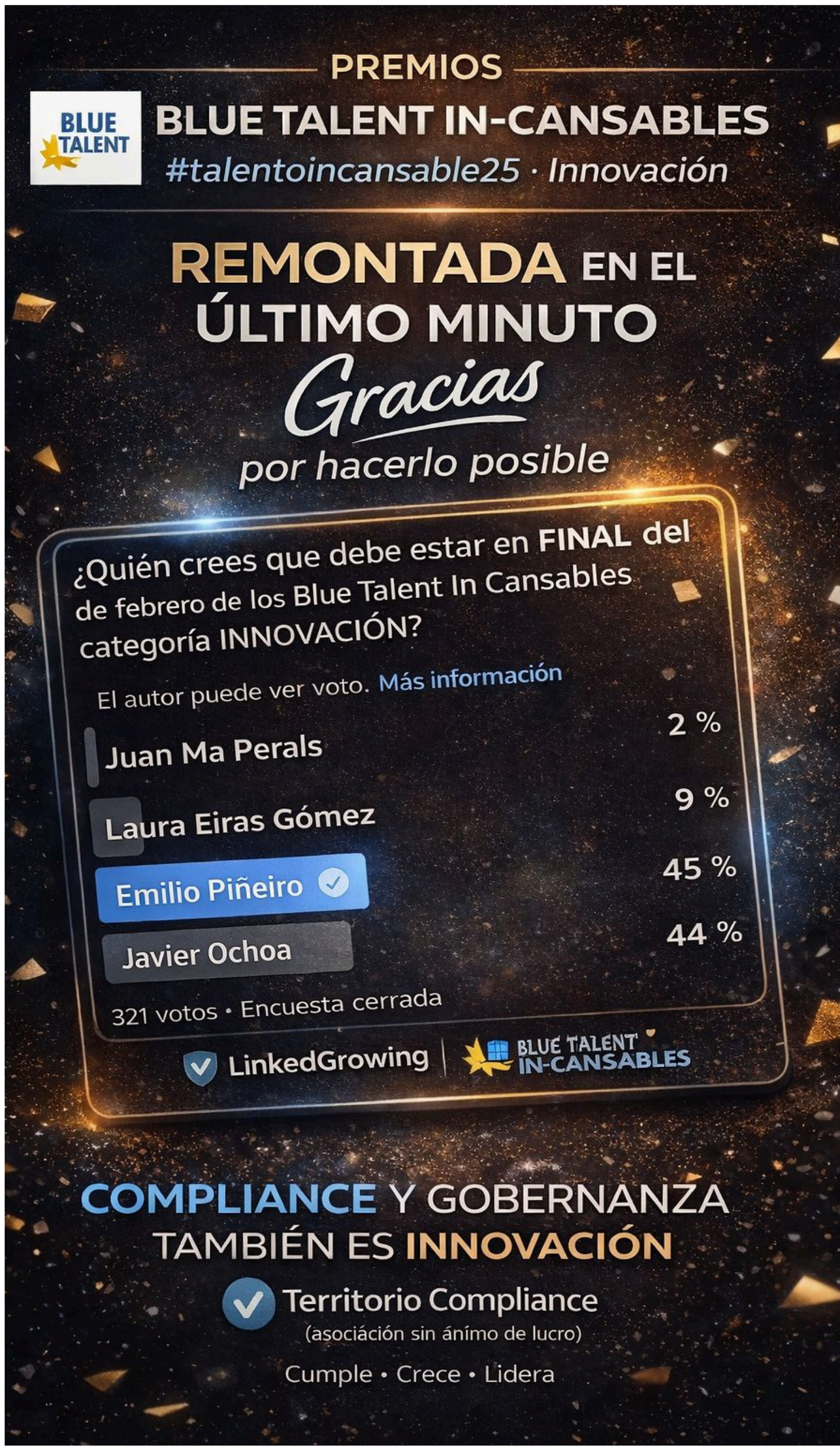
En esta convergencia:

- Compliance da coherencia, asegurando un ecosistema de transparencia y responsabilidad.
- La IA potencia la capacidad de análisis y la anticipación, pero sin anular el juicio humano.
- El liderazgo actúa como catalizador, orquestando la visión, la confianza y el compromiso ético.

Las organizaciones que entiendan esta integración no solo sobrevivirán, sino que definirán las nuevas reglas del juego. En un mercado ansioso por innovación, la diferenciación no se basa únicamente en productos o servicios, sino en la coherencia ética y en la calidad de la toma de decisiones. Ten presente que … Hoy, más que nunca, no podemos limitarnos a sobrevivir. Frente a las amenazas y oportunidades del entorno BANI, necesitamos transformarnos conscientemente, abrazando la IA con cautela y ambición, y erigiendo un compliance inteligente que sea referente de integridad.

La próxima era no se decide en un tablero de ajedrez, sino en la capacidad de construir puentes entre la ética y la innovación. La clave no es resistir el cambio, sino liderarlo con visión y compromiso.

Emilio Piñeiro
Consultor de cumplimiento normativo,
Compliance Officer,
Docente y Divulgador
Presidente de la Asociación Territorio Compliance



Joaquín Sampedro

Seguridad inteligente para vivir con confianza

SegurIA SOLUTIONS

Protegiendo el presente.
Anticipando el futuro.

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

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

La Metodología Joaquín Sampedro

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

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

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

LA SEGURIDAD PRIVADA FRENTE A UN RIESGO INVISIBLE

Metro Risk

Rosa Fernandéz

ASUNTO: RIESGOS

La seguridad privada española no afronta (sólo) un problema de falta de medios. Afronta un reto de madurez estratégica. En la era de la vigilancia inteligente, proteger ya no consiste solo en reaccionar ante el incidente, sino en evitar que el propio sistema se convierta en el punto débil. El sector de la seguridad privada en España se prepara para 2026 con una paradoja difícil de ignorar: nunca ha dispuesto de tanta tecnología avanzada y, al mismo tiempo, nunca ha estado tan expuesto a los riesgos derivados de su propio uso

Cámaras inteligentes, sistemas de analítica de vídeo, plataformas de gestión de incidencias, drones, dispositivos móviles y soluciones basadas en inteligencia artificial forman ya parte del día a día de muchas empresas de vigilancia. Sin embargo, la adopción tecnológica avanza a un ritmo muy superior al desarrollo de una cultura de gestión preventiva, de administración responsable del riesgo y de competencias reales en el personal que las opera.

El resultado es un modelo operativo cada vez más sofisticado en apariencia, pero estructuralmente frágil. La seguridad privada es uno de los sectores más regulados del mercado español. Habilitaciones, autorizaciones administrativas, inspecciones periódicas y un marco normativo detallado han generado durante años una sensación de control y estabilidad. Ese marco, sin embargo, ha sido interpretado por muchas organizaciones como un techo y no como una base. El cumplimiento de mínimos se ha convertido en el objetivo principal, desplazando a un segundo plano la gestión del riesgo, la anticipación de escenarios y la administración correcta de la tecnología. Este enfoque ha funcionado mientras los sistemas eran fundamentalmente pasivos. Pero deja de ser suficiente cuando la tecnología empieza a influir activamente en la toma de decisiones. La inteligencia artificial cambia la lógica del riesgo

La expansión de la inteligencia artificial en el ámbito de la vigilancia no es un escenario futuro: es una realidad operativa. Algoritmos que detectan comportamientos anómalos, sistemas que priorizan alertas, herramientas que sugieren actuaciones o clasifican situaciones ya están presentes en múltiples entornos

El problema no es la tecnología. El problema es cómo se gestiona y se administra su uso. En un sector tradicionalmente reactivo, donde la intervención se produce una vez ocurrido el incidente, la IA introduce una nueva capa de riesgo: el error ya no depende solo de la acción humana directa, sino de cómo se interpreta, se confía y se actúa sobre una recomendación automatizada. Y cuando ese error se materializa, la responsabilidad no se diluye: se concentra. Y la Responsabilidad es individual, no colectiva. El Responsable del Tratamiento es el que tiene que demostrar que cumple con la ley vigente. En 2026 se amplia el foco, con el RGPD ya no es suficiente, hay que tener un Cumplimiento 360º para estar al día en el marco normativo europeo, y aplicar la privacidad por defecto evaluando los riesgos y el impacto que puede suponer usar soluciones que incorporar Inteligencia Artificial

-El vigilante como operador digital sin red de protección suficiente
El vigilante de seguridad se ha convertido, de facto, en un operador digital. Maneja dispositivos, interpreta alertas automatizadas, utiliza aplicaciones móviles y gestiona información sensible en tiempo real. Sin embargo, esta evolución no ha venido acompañada, en muchos casos, de una gestión adecuada de competencias, de criterios claros de actuación ni de una comprensión real de los límites legales y operativos de la tecnología que utiliza.

El vigilante no decide qué sistemas se implantan ni bajo qué condiciones. Pero su actuación, correcta o incorrecta, recae finalmente sobre la empresa, que es quien administra el servicio y responde frente a terceros. En 2026, con sistemas capaces de registrar, trazar y reconstruir decisiones, justificar un error operativo será cada vez más complejo.

-El coste invisible de no gestionar preventivamente Desde la perspectiva de la gestión empresarial, la prevención sigue viéndose a menudo como un coste prescindible. La presión sobre márgenes, licitaciones ajustadas y competencia basada en precio refuerzan esta practica. Sin embargo, los costes reales del nuevo escenario no aparecen en el presupuesto inicial.

Se manifiestan después, en forma de reclamaciones, conflictos con clientes, inspecciones con efectos retroactivos, pérdida de contratos y deterioro reputacional. No gestionar preventivamente el uso de la tecnología no elimina el gasto: lo desplaza y lo amplifica.

¿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**

LA PROTECCIÓN COMERCIAL FRENTE AL ROBO INTERNO: PREVENCIÓN, CONTROL Y PROTOCOLOS DE ACTUACIÓN

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Serrano
Coordinador de Servicios

La protección comercial se ha convertido en un pilar estratégico para las empresas del sector retail, logístico e industrial. Aunque tradicionalmente el foco se ha puesto en el hurto externo, el robo interno representa uno de los mayores riesgos económicos, operativos y reputacionales para las organizaciones. Su correcta gestión exige protocolos claros, personal cualificado y una coordinación.

¿Qué entendemos por robo interno?

El robo interno hace referencia a cualquier sustracción, fraude o uso indebido de recursos llevado a cabo por personas que mantienen o han mantenido una relación laboral o profesional con la empresa: empleados, subcontratas, personal externo autorizado o incluso mandos intermedios. Este tipo de conductas suele ser más difícil de detectar que el hurto externo, ya que el autor conoce los procedimientos internos, dispone de acceso autorizado a zonas restringidas y sabe cómo evitar controles visibles. Importancia de la protección comercial en el robo interno

La protección comercial no se limita a la presencia de vigilantes. Incluye un enfoque integral basado en la prevención, la detección temprana, la investigación y la actuación proporcionada y legal. Un sistema eficaz permite reducir pérdidas económicas, proteger la imagen corporativa, evitar conflictos laborales innecesarios y garantizar la seguridad jurídica de la empresa. Marco legal: la Ley de Seguridad Privada La actuación frente al robo interno debe realizarse siempre dentro del marco legal establecido por la Ley 5/2014, de 4 de abril, de Seguridad Privada, que regula las funciones, límites y responsabilidades del personal de seguridad privada en España.

Esta ley establece, entre otros aspectos, las funciones del vigilante de seguridad en la protección de bienes y personas, la obligación de actuar con proporcionalidad, congruencia y oportunidad, la colaboración con las Fuerzas y Cuerpos de Seguridad y el respeto estricto a los derechos fundamentales, especialmente la intimidad, el honor y la protección de datos.

El papel clave de los departamentos de seguridad Los departamentos de seguridad son el eje vertebrador de la protección comercial moderna. Su función va mucho más allá de la supervisión operativa y debe incluir el análisis

www.seguridadyempleo.com

de riesgos específicos de robo interno, el diseño de protocolos de actuación, la coordinación con recursos humanos y asesoría jurídica, la supervisión de empresas de seguridad contratadas y la formación y concienciación del personal. La figura del Director o Jefe de Seguridad resulta esencial para garantizar que las actuaciones se ajusten a la legalidad y a los objetivos estratégicos de la empresa. Coordinación con las empresas de seguridad privada La colaboración entre el departamento de seguridad de la empresa cliente y la empresa de seguridad privada debe ser constante y estructurada. Una mala coordinación genera vacíos de responsabilidad, actuaciones improvisadas y riesgos legales innecesarios. Es fundamental que exista un servicio claramente definido, consignas escritas y actualizadas, canales de comunicación directos y procedimientos de reporte e incidencia.

El vigilante de seguridad en la protección comercial El vigilante de seguridad es la figura operativa clave en la detección del robo interno. Su labor debe basarse en la observación profesional, nunca en suposiciones o prejuicios. Entre sus funciones destacan el control de accesos y salidas, la vigilancia discreta de zonas sensibles, la detección de comportamientos anómalos, la comunicación inmediata de indicios al responsable del servicio y la intervención únicamente cuando exista causa legal suficiente. Protocolos de actuación ante el robo interno Un protocolo eficaz debe contemplar la detección de indicios objetivos, la comunicación interna al responsable designado, la verificación de los hechos evitando actuaciones precipitadas, la actuación ajustada a la legalidad y la correcta documentación mediante partes de incidencias detallados, objetivos y profesionales.

Prevención como herramienta estratégica La experiencia demuestra que la prevención es la medida más eficaz frente al robo interno. Entre las buenas prácticas destacan la formación continua en ética y seguridad, la existencia de protocolos claros y conocidos, la separación de funciones críticas, las auditorías internas periódicas y una presencia visible pero profesional de la seguridad

LA RESPONSABILIDAD DEL DIRECTOR DE SEGURIDAD DURANTE UNA CATÁSTROFE

Metro Risk

Edición propiedad de @MetroRisk, asociación

Abraham Santana Herrera
Director de seguridad. Perito

En el momento en que una catástrofe irrumpe, ya sea natural, tecnológica, sanitaria o social, la estructura formal de una organización se somete a una prueba extrema. Los procedimientos se tensionan, la cadena de mando se fragmenta, la información se vuelve confusa y el tiempo adquiere un valor crítico. Es precisamente en ese escenario donde la figura del Director de Seguridad deja de ser un gestor de sistemas para convertirse en un responsable estratégico de continuidad, protección y toma de decisiones bajo incertidumbre. Su función no es reactiva, es estructural; no se activa solo cuando ocurre el desastre, sino que se manifiesta como resultado de una planificación previa correctamente integrada en el gobierno de la organización.

Durante una catástrofe, el Director de Seguridad asume la responsabilidad de coordinar la respuesta global de protección de personas, activos e información, actuando como nexo entre la dirección general, los equipos operativos y las autoridades externas.

Su posición en el organigrama no es operativa, sino directiva, lo que le permite disponer de visión transversal sobre recursos, vulnerabilidades y dependencias críticas. En organizaciones maduras, el Director de Seguridad forma parte del comité de crisis y reporta directamente a la alta dirección, porque sus decisiones afectan de manera inmediata a la vida de las personas, a la reputación corporativa y a la viabilidad del negocio.

A diferencia de otros responsables funcionales, el Director de Seguridad trabaja con escenarios de baja probabilidad y alto impacto, donde el error no es corregible y el margen de improvisación es mínimo. En una catástrofe, su rol se centra en activar los planes de autoprotección, continuidad y contingencias, priorizar objetivos de protección, garantizar la evacuación o confinamiento de personas, asegurar la integridad de instalaciones estratégicas y mantener la operatividad de los sistemas críticos. Pero, sobre todo, su responsabilidad principal es evitar el colapso organizativo, manteniendo la estructura de mando, la coherencia de la información y la disciplina operativa cuando el entorno tiende al caos.

Dentro del organigrama, el Director de Seguridad actúa como figura de estabilización, capaz de traducir el riesgo en decisiones ejecutables. Su conocimiento previo del negocio, de las personas y de los procesos le permite evaluar rápidamente qué puede detenerse, qué debe continuar y qué debe protegerse a toda costa. Esta capacidad no se improvisa: se construye a través de análisis de riesgo, simulacros, auditorías, planes de resiliencia y una relación constante con todos los departamentos de la empresa. Cuando la catástrofe ocurre, el Director de Seguridad no pregunta qué hacer: ya lo sabe, y su obligación es hacerlo ejecutar.

La coordinación externa es otro de los pilares de su responsabilidad. En una emergencia real, la organización deja de ser un ente aislado y pasa a integrarse en un sistema de respuesta mayor, donde intervienen fuerzas de seguridad, servicios de emergencia, protección civil, autoridades locales y organismos reguladores. El Director de Seguridad es el interlocutor natural con estas entidades, el responsable de proporcionar información fiable, de canalizar órdenes y de garantizar que la actuación de la empresa se alinee con los planes públicos de emergencia. Su legitimidad para hacerlo nace de su posición en el organigrama y de su preparación técnica, no de la improvisación.

En grandes empresas, además, su papel se extiende a la gestión de la comunicación interna de seguridad, evitando el pánico, los rumores y las decisiones individuales no coordinadas. La forma en que una organización comunica durante una catástrofe puede ser tan decisiva como la propia respuesta operativa. Por ello, el Director de Seguridad actúa también como regulador del comportamiento colectivo, asegurando que las personas sepan qué hacer, cuándo hacerlo y a quién obedecer, incluso en escenarios de alta tensión emocional.

La responsabilidad del Director de Seguridad durante una catástrofe no termina cuando el incidente se controla. Tras la emergencia, lidera la fase de análisis, reconstrucción y aprendizaje, evaluando fallos, actualizando planes y fortaleciendo la resiliencia futura. En este sentido, su función no es solo proteger, sino garantizar que la organización salga reforzada, con procesos más sólidos y una cultura de seguridad más madura.

Entender al Director de Seguridad como un cargo secundario o meramente técnico es un error que solo se hace visible cuando ya es demasiado tarde. En una catástrofe, este profesional se convierte en uno de los pocos roles capaces de aportar orden, coherencia y continuidad en medio de la incertidumbre. No es un gestor de alarmas ni un supervisor de vigilantes; es un arquitecto de la resiliencia organizativa, y su lugar natural está en el núcleo de la toma de decisiones estratégicas de cualquier empresa que aspire a sobrevivir a lo imprevisible.

CÓMO ACTÚAN LAS COMPAÑÍAS DE SEGUROS ANTE UNA CATÁSTROFE

Metro Risk

Edición propiedad de @MetroRisk, asociación

Alina Rubio de las Casas
Experta en Seguros Generales

Quien nunca ha vivido una catástrofe desde dentro del sector asegurador suele pensar que la respuesta de una compañía de seguros se limita a pagar siniestros. La realidad es muy distinta. Cuando ocurre una catástrofe, un terremoto, una inundación, un incendio masivo, una pandemia, un apagón generalizado o un colapso tecnológico, lo que se activa no es un simple proceso de tramitación, sino una maquinaria compleja de gestión del riesgo, continuidad operativa y protección financiera del sistema. Para una aseguradora, una catástrofe no es solo un evento que genera pérdidas, es un test de solvencia, confianza y resiliencia.

En el primer momento, la prioridad absoluta de una compañía es mantener su capacidad operativa. Si la aseguradora no puede seguir funcionando, no puede cumplir su función social ni contractual. Por eso, antes incluso de analizar daños, se activan los planes de continuidad de negocio, se protege a los empleados, se asegura la integridad de los sistemas de información y se establecen canales de comunicación alternativos. La catástrofe no detiene la obligación de responder; al contrario, la multiplica.

Paralelamente, se pone en marcha la estructura de gestión de siniestros catastróficos, que no funciona como una tramitación ordinaria. Se despliegan equipos especializados, se refuerzan centros de atención, se habilitan procedimientos simplificados y se toman decisiones de alcance masivo, porque en una catástrofe el tiempo es tan importante como el dinero. La rapidez en la respuesta no es solo un servicio al cliente: es una medida de contención del impacto social y económico. Cada día de retraso en una indemnización es un día más de bloqueo para una familia, una empresa o una comunidad entera.

Uno de los aspectos menos visibles, pero más críticos, es la gestión del equilibrio entre solvencia y respuesta. Las aseguradoras operan con modelos actuariales que prevén eventos extremos, reaseguros internacionales y provisiones técnicas diseñadas precisamente para estos escenarios. Cuando la catástrofe se produce, esos modelos se ponen a prueba en tiempo real. Las decisiones no pueden ser impulsivas: deben garantizar que se atienda al mayor número de afectados posible sin comprometer la estabilidad futura de la entidad. Por eso, cada actuación está medida, auditada y alineada con criterios regulatorios muy estrictos.

Al mismo tiempo, las compañías trabajan en coordinación constante con administraciones públicas, consorcios, reaseguradoras y autoridades supervisoras. La catástrofe rompe la frontera entre lo privado y lo público, y obliga a construir una respuesta conjunta. En muchos países, como en España con el Consorcio de Compensación de Seguros, esta colaboración es clave para cubrir riesgos extraordinarios que el mercado privado no puede asumir en solitario. En esos momentos, el seguro deja de ser un producto y se convierte en infraestructura financiera de emergencia.

Pero hay algo que diferencia a una aseguradora sólida de una simplemente solvente: la forma en que acompaña al asegurado. En una catástrofe, las personas no necesitan solo dinero, necesitan orientación, claridad y sensación de respaldo. Por eso, las compañías más avanzadas priorizan la comunicación transparente, la empatía en la atención y la simplificación de procesos. Resolver no es solo indemnizar, es ayudar a reconstruir, a reabrir, a volver a la normalidad lo antes posible.

Una vez superada la fase más crítica, comienza un trabajo menos visible pero esencial: el análisis. Cada catástrofe deja lecciones, datos, fallos y nuevas variables de riesgo. Las aseguradoras revisan modelos, actualizan tarifas, redefinen coberturas y ajustan criterios de suscripción. Así es como el sector aprende, evoluciona y se prepara para el siguiente evento, porque en gestión del riesgo no existe el "nunca más", solo el "mejor preparados".

Desde dentro del seguro, una catástrofe no se vive como un fracaso del sistema, sino como la razón misma de su existencia. El seguro está diseñado para responder cuando todo lo demás falla. Y su verdadera función no es evitar el desastre, sino impedir que el desastre destruya el tejido económico y social. Esa es la responsabilidad silenciosa que asumimos cada vez que ocurre lo impensable

GALINDO BENLLOCH

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

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

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

Unidad de acción

CIERRA EL CÍRCULO CON GALINDO BENLLOCH

FORMACIÓN

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

PREVENCIÓN

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

Para más información visita **galindobenlloch.com** o escríbenos a gestion@galindobenlloch.com

MAS VALE PREVENIR QUE LAMENTAR

Metro Risk

Edición propiedad de @MetroRisk, asociación

Elena de la Parte

El inicio de este 2026 nos ha recordado de la forma más dolor dolorosa que la seguridad nunca es producto del azar. El siniestro en la discoteca "Le Constellation", que ha fulminado con la vida de más de 40 jóvenes no es un simple infortunio, sino el resultado de una quiebra sistemática de la Prevención De Riesgos Laborales. (PRL). En la organización de eventos y protocolos. << Año Nuevo, Vida nueva. Si se carece de control e inspección y estas se omiten la tragedia se admiten>> << Bengala en mano. Inspección ausente. Brindis de hoy luto, para siempre>>

En la editorial de enero de 2026 la seguridad no admite pausas. Porque el fuego no entiende de calendarios. Desde esta editorial enviamos todas nuestras condolencias a todos los fallecidos y familias afectadas. D.E.P - R.I.P. Como advertí, en la editorial de diciembre de 2025, << Los invito a cerrar 2025 con la convicción de que solo una estrategia cohesionada, consciente y resiliente nos permitirá liderar el 2026. ¡Que tengan unas fiestas inspiradoras y un 2026 de integración total!>> Hoy ante esta tragedia de Crans-Montana, esa advertencia cobra un peso desgarrador. "Reflexionemos un poquitin sobre la importancia vital e insustituible de la protección humana". Iniciamos este 2026 bajo un paradigma de seguridad que ya no permite la reactividad. El despliegue de los nuevos desafíos globales geopolíticos e internacionales nos obligan a transitar de una mentalidad de protección de activos hacia una soberanía operativa total. Este año no se trata de sobrevivir al cambio, sino de diseñar la arquitectura necesaria para liderar y sobrevivir.

La seguridad actualmente no es un departamento, es él; pulso, pulmón y el corazón de la organización. Tras haber blindado nuestras estructuras y demostrado nuestra capacidad de respuesta ante lo inevitable. Entramos en un ciclo donde la cohesión táctica y la conciencia del riesgo son las únicas divisas de valor. El liderazgo que este tiempo demanda es el que no se detiene, en el cumplimiento legal, sino que busca la excelencia en la prevención y en la integridad en la ejecución. La catástrofe acontecida el día 1 de enero 2026, en Suiza en 'Le Constellation', ha dejado un vacío y un gran duelo, en la vida de muchas familias.

Análisis Pericial. La investigación de la Fiscalía de Valais, confirma nuestras peores sospechas. El local operaba tras cinco años sin inspecciones de seguridad obligatorias. Este vacío administrativo permitió el uso de espuma acústica altamente inflamable en techos y la manipulación temeraria de bengalas en las botellas de champán en un espacio y recinto cerrado. Desde mi perspectiva pericial este caso invalida cualquier defensa de "inevitabilidad". Organización, institución u empresa. Ignora la trazabilidad documental y el fallo en los protocolos de evacuación. Estos parches y vulnerabilidades de alto riesgo derivaron en una estampida mortal, la responsabilidad penal por homicidio involuntario es la única vía de Justicia. "No podemos permitir que el beneficio económico opaque el deber de garante, es decir la premisa fundamental, es proteger a los clientes y cumplir con el deber de honestidad y transparencia. Cumpliendo con el bienestar social, los valores éticos o la responsabilidad pública-privada.

La narrativa institucional debe dejar constancia de que los hechos acontecidos superan cualquier medida de control razonable resultando técnica y operativamente imprevisibles. Resulta crítico por tanto sustentar nuestra defensa en una cultura de evidencia probatoria, que demuestre que se actuó bajo los más altos estándares de responsabilidad protegiendo la integridad jurídica de la organización ante posibles reclamaciones. Resulta vital evidenciar la inevitabilidad del suceso. Subrayando que éste se sitúa fuera de los límites de control de nuestras infraestructuras. La capacidad de defensa de la organización y demandas judiciales dependerá directamente de la solidez de sus registros. Demostrar que se ha cumplido con el deber de cuidado, no solo es una cuestión de ética, sino una estrategia de supervivencia legal fundamentada en pruebas objetivas. La seguridad es el único motor que permite la innovación y el crecimiento sostenible.

Que la tragedia de Crans Montana sea el último aviso en 2026, el compromiso con la vida debe ser absoluto. En este sentido la prevención de riesgos tendrá los siguientes pasos:

- Evaluación de las áreas de riesgo.
- Plan de reducción de riesgos.
- Monitoreo de los riesgos analizados
- Respuesta ante los riesgos.
- Reposición y recuperación.

En Suiza la prevención de riesgos y la seguridad no se rigen por una sola ley de paraguas como en otros países, sino que se asientan sobre dos pilares legales fundamentales que todo experto en seguridad debe conocer para operar con deontología profesional. En España, en eventos es necesario contar con personal de seguridad para garantizar que se cumplen las normas y reforzar la seguridad ante imprevistos. Los vigilantes de seguridad con o sin arma, trabajan en la vigilancia general de los locales y bienes en los que se organizan los eventos, protegiendo a las personas y a la propiedad de hechos delictivos o infracciones.

En España está registrado y documentado en;

- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Real Decreto 513/2017 que aprueba el Reglamento de
- Instalaciones de protección contra incendios.
- Código Técnico de la Edificación (CTE), Documento Básico
- Seguridad en caso de Incendio (SI).

Ante hechos de esta naturaleza, el personal de seguridad actúa en consecuencia cumpliendo con sus funciones y con la legislación vigente en materia de seguridad privada que responde a la Ley de 5/2014, de 4 de abril, de seguridad privada y Real Decreto 2364/1994 de 9 de diciembre, qué aprueba el Reglamento de Seguridad Privada. Los sistemas de protección contra incendios. Se suelen clasificar en protección pasiva y protección activa, y deben estar complementarios por medidas organizativas y de mantenimiento. Abarcan tanto los medios materiales como organizativos que permiten:

- Prevenir.
- Detectar.
- Controlar.
- Extinguir un incendio antes de que se propague y cause daños personales o materiales de consideración

1- Protocolos y procedimientos de actuación 1 -Planificación previa: es fundamental desarrollar protocolos específicos para cada instalación:

- Identificación de puntos críticos de corte de suministro.
- Formación del personal en técnicas de manipulación segura.
- Preparación de equipos y herramientas especializadas.

2- Coordinación durante la emergencia: La eliminación del combustible requiere acciones coordinadas:

- Comunicación clara entre equipos. • Secuenciación adecuada de las acciones.
- Monitorización constante de las condiciones.

Ejemplo práctico: En las instalaciones industriales, los planos de la instalación deben incluir claramente la ubicación de todas las válvulas de corte y puntos de aislamiento, con códigos de color según el tipo de fluido y copias de estos, planos que deben estar accesibles tanto para los equipos internos como para los servicios de emergencia externos.

3- Evaluación posterior: tras un incendio donde se haya utilizado este método, es importante:

- Revisar la efectividad de las acciones realizadas.
- Analizar posibles mejoras en los protocolos.
- Actualizar la formación del personal según las lecciones aprendidas.

Consejo profesional: Implementa un sistema de "tarjetas de aislamiento" para instalaciones complejas. Cada válvula o punto de corte debe tener una tarjeta numerada qué se recoge al activarla, permitiendo contabilizar rápidamente qué sistemas han sido aislados durante la emergencia.

Las Fases de los incendios
A= Alertar
P= Proteger
A= Avisar
G= Garantizar
A= Actuar Dar la alarma a uno mismo y a los demás. Llamar al 112.La evacuación.

Si estás capacitado y no hay riesgo. PAS. Proteger, Avisar y Socorrer. <> Prevención de Riesgos Laborales en Suiza: 1 La ley sobre el trabajo (ARG): Es la norma de referencia para la protección de la salud y la higiene. Se centra en las condiciones del entorno laboral; Iluminación, ruido ventilación ergonomía, CPTDE Neuroarquitectura, en la organización y optimización del tiempo, temporización y protección.

Cumplimiento. Obliga al; encargado, responsable, gerente, CEO, o el equipo de Primera Intervención, a tomar todas las medidas necesarias para proteger y custodiar la integridad física y psíquica de los trabajadores según el estado de la técnica.

2 La Ley Federal sobre el seguro de accidentes (UVG): Este es el Pilar técnico para la seguridad técnica y la prevención de siniestros e incidencias. El enfoque. Regula la prevención de accidentes laborales y enfermedades profesionales del organismo clave (SUVA).

La mayoría de las empresas están vinculadas a la (SUVA) La Caja Nacional de Suiza de seguro de accidentes, qué no solo asegura, sino que actúa como una autoridad inspectora. Es la normativa técnica específica que obliga a las empresas con ciertos niveles de riesgo a recurrir a especialistas en seguridad. “Desde mi rol en seguridad el punto crítico legal en este suceso no es solo la falta de inspecciones desde 2019, sino el incumplimiento de las ordenanzas de prevención de incendios (AEAI). En Suiza las normas de la (AEA)I, Asociación de establecimientos de seguro contra incendios son de cumplimiento obligatorio y establecen lo siguiente:
1. Mantenimiento. Los sistemas de detección de detención y extinción de incendios deben ser revisados periódicamente generalmente cada 1 o 2 años.
2. Carga de fuego. "La carga de fuego es uno de los parámetros fundamentales para determinar las medidas de protección necesarias según el Reglamento de Seguridad contra Incendios en los Establecimientos Industriales (RSCIEI)”. Real Decreto 2267/2004.

El uso de materiales inflamables en techos y paredes como ocurrió, en esta discoteca está estrictamente regulado y prohibido en locales de alta concurrencia si no son ignífugos. Nota pericial. En el marco legal suizo si se demuestra que la empresa ignoró estas normativas técnicas, el argumento de fuerza mayor o viabilidad cae por completo activando la responsabilidad penal de los administradores.

Prevención de riesgos laborales (SST) (PRL). En Suiza la seguridad en el trabajo se apoya en una estructura dual ley de trabajo y ley de seguros. Loí sur le Travail. Ley del Trabajo. Ley de seguro de accidentes. - (En idioma francés); Loi sur l'assurance - Accidents (LAA). - Loi sur le travail (LTR)- Ley del trabajo: 5 - Artículo 6: Establece la obligación general del empleador de tomar todas las medidas necesarias para proteger la salud física y psíquica de los trabajadores basándose en la experiencia y el estado de la técnica.
- Ordonnance 3 (OLT 3): Detalla las normas de higiene y ergonomía. El Artículo 2 Obliga a la prevención de riesgos (PRL) y a la preparación para emergencias.
- Loi sur l'Assurance-Accidentés (LAA).
Ley de seguro de accidentes : - Ley de seguro de accidentes. - (En idioma francés); Loi sur l'assurance -Accidents (LAA).
- Ley de seguro de accidentes. - (En idioma francés); Loi sur l'assurance -Accidents (LAA).
- Artículo 82. Es el artículo clave para la seguridad técnica. obliga al Organizador CEO y responsables en su caso a prevenir accidentes profesionales colaborando con organismos como la SUVA. - Directiva EKAS 6508 (msst): Obliga a las empresas con riesgos especiales a recurrir a especialistas para diseñar su sistema y protocolo de gestión y de seguridad.

Prevención y extinción de incendios. Suiza no tiene una ley de incendios única sino un sistema Inter cantonal vinculante: Normas AEAI, Asociación de establecimientos de seguro contra incendios. Son de obligado cumplimiento en todo el país.
Norma de protección contra incendios 1-15. Define los objetivos de producción evacuación segura y limitación de la propagación. Directiva 13-15 Materiales de construcción. Regula estrictamente, el uso de materiales inflamables.
En el caso que nos compite son; las bengalas o espumas acústicas de la discoteca en el incidente mencionado. Directiva 16-15 Vías de evacuación. Establecer dimensiones y señalización de las salidas de emergencia.

Organización de eventos y protocolos. La regulación de eventos es principalmente cantonal y municipal, pero se rige en: Loi sur les Auberges et Débits de Boissons (Ley de hostelería y hotelería). Cada cantón tiene su versión Ejemplo la ley del Balais o de Ginebra que exige: Aforo máximo. Este no puede cederse en ninguna circunstancia Planes de emergencia. Deben ser aprobados por la policía del comercio y los bomberos para obtener la licencia de explotación. La defensa basada en la “Inevitabilidad”, queda invalidada si se demuestra el incumplimiento del Art 82 (LAA) o las directivas (AEAI). La seguridad suiza, no es social es una responsabilidad penal directa de la gerencia.

El Código Penal suizo (CP):
recoge en los Artículos 117 Homicidio por negligencia
Artículo 125-Lesiones por negligencia

Ambos artículos son los que se aplican penalmente cuando los protocolos anteriores fallan como en la investigación actual del incendio acontecido. La única defensa jurídica inexpugnable ante un tribunal suizo es la capacidad de demostrar en los registros y auditorías vigentes. Qué se hizo todo lo técnicamente posible para prevenir el riesgo.

¿Esto ha ocurrido así?

En un ecosistema de amenazas en constante metamorfosis la seguridad deja de ser un perímetro estático para convertirse en el tejido vivo de la resiliencia organizacional. No se trata solo de resistir el impacto sino de evolucionar a través de él. Más allá de los protocolos y la vanguardia tecnológica. La seguridad es un compromiso ético y negociable, es la arquitectura invisible que sostiene la confianza en cada una de nuestras interacciones.

Es imperativo acreditar que el incidente trasciende en el radio de acción de la entidad derivado de factores exógenos e inevitables, Por consiguiente; la organización debe mantener una trazabilidad documental exhaustiva que certifique el cumplimiento diligente de sus obligaciones constituyéndose una defensa sólida e inexpugnable ante cualquier proceso de arbitraje o litigio legal.

Según fuentes oficiales, hemos leído en; prensa, redes sociales, comunicación vía digital y tv. El suceso fue originado por bengalas ubicadas en el interior de botellas de champán, velas y demás artículos festivos y peligrosos, y prohibitivos, en el interior de la discoteca, acontecido en Suiza, que fue por un proceso de deflagración. Es decir; es una combustión rápida con velocidad de propagación subsónica (menor que la velocidad del sonido). Produce ondas de presión y llamas. Después de esta deflagración se produce la detonación. Es una combustión extremadamente rápida, con velocidad de propagación supersónica (mayor que la velocidad del sonido). Genera una onda de choque destructivo. Los tipos de combustión existentes son los siguientes:

- 1. Combustión completa.
- 2. Combustión incompleta.
- 3. Combustión estequiométrica.
- 4. Combustión lenta u oxidación
- 5. Deflagración.
- 6. Detonación.

Decálogo 2026: Liderazgo y compromiso total con la seguridad.

- 1. Cultura de prevención activa: La seguridad no es un manual acumulando polvo en un estante es un proceso vivo que se respira en cada nivel de la organización desde el alta en dirección hasta la base operativa.
- 2. Diligencia debida como estándar: Cumplir la ley (LAA / LTr) Es el mínimo. La excelencia reside en anticipar el riesgo antes de que se convierta una cifra estadística o un titular trágico de prensa
- 3 Trazabilidad documental inexpugnable: Lo que no está registrado no existe Mantener una auditoría constante de inspecciones y protocolos es nuestra única defensa real ante la justicia.
- 4 Inversión en resiliencia. El presupuesto en seguridad no es un gasto es la prima de seguro que garantiza la continuidad del negocio y la protección de la reputación institucional.
- 5. Responsabilidad no delegable. El liderazgo asume la seguridad como un compromiso ético penal y personal. Delegar la tarea no significa eximirse de la responsabilidad de supervisión.
- 6. Capacitación continua y crítica. Ante un escenario de amenazas que evolucionan como el uso de las nuevas tecnologías TIC e IA. La formación y la concienciación debe ser constante técnica y cada vez más rigurosa.
- 7. Soberanía de datos e información. Proteger nuestros activos digitales es tan crítico como blindar nuestras estructuras físicas la seguridad es un concepto actualmente 360º.
- 8. Gestión de la evidencia. En caso de crisis la transparencia y la disponibilidad de datos probatorios son los que diferencian a una organización responsable de una negligente.
- 9. Protocolos de respuesta inmediata. No basta con saber qué hacer Hay que haberlo entrenado. La capacidad de reacción Y actuación tiene que ser innata. La velocidad de reacción es el factor determinante entre un incidente controlado y una catástrofe y tragedia incontrolada.
- 10 Compromiso con la integración total. Sólo una estrategia donde la seguridad y el CPT de esté integrado en el ADN de cada proyecto nos permitirá liderar este 2026 con autoridad y confianza.

Este decálogo no es una sugerencia es nuestro pacto de integridad para el año 2026 en un mundo donde lo inevitable puede suceder nuestra única respuesta válida es la preparación absoluta avancemos este 2026 con la determinación de ser el estándar de seguridad que el futuro exige.

Consejo profesional. Al diseñar la protección contra incendios para un CPTED, considera no solo la sala principal sino también los espacios técnicos auxiliares, o canalizaciones de; cables, falsos suelos y techos, donde muchos incendios se inician y propagan antes de ser detectados en la sala principal.

La seguridad de las personas siempre debe ser la prioridad. Si las circunstancias lo permiten antes de utilizar métodos de sofocación que puedan reducir el oxígeno en un espacio, asegúrate de que todas las personas han sido evacuadas. En el sistema de extinción de incendios: <>

<< La trazabilidad y el conocimiento técnico son nuestra única defensa real: son el puente que separa un conato mitigado a tiempo de una catástrofe que el calendario nunca podrá olvidar.>>

LA FALSA SENSACIÓN DE SEGURIDAD EN EL USO DE DRONES: CUANDO LA TECNOLOGÍA EXISTE, PERO NO SE INTEGRA

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Miguel Ortiz

La irrupción de los drones (UAS) en el ámbito de la seguridad privada ha sido rápida y, en muchos casos, poco reflexiva. Lo que comenzó como una herramienta puntual para apoyo visual se ha convertido en un elemento casi imprescindible en determinados entornos: vigilancia perimetral, supervisión de eventos multitudinarios, protección de infraestructuras críticas o apoyo a rondas de seguridad

Sin embargo, esta expansión ha traído consigo un riesgo menos visible pero especialmente relevante desde el punto de vista de la gestión del riesgo: la falsa sensación de seguridad. Disponer de drones, licencias y equipos avanzados no garantiza una mayor protección si estos sistemas no están correctamente integrados en los procedimientos, en el factor humano y en el marco normativo que los regula. La seguridad no falla por falta de tecnología, sino por exceso de confianza en ella. Drones incorporados como elemento simbólico de seguridad En no pocas organizaciones, el dron se ha convertido en un símbolo de modernidad y control. Su presencia transmite una imagen de vigilancia avanzada tanto a clientes como a usuarios finales. No obstante, esta visibilidad puede ocultar carencias importantes en la planificación real de su uso.

El dron se adquiere, se registra como operador, se forma a uno o varios pilotos y se da por resuelta la necesidad. Pero sin una definición clara de escenarios operativos, criterios de activación y responsabilidades, el UAS queda relegado a un uso ocasional, improvisado o meramente disuasorio. Desde el punto de vista normativo, esta aproximación es especialmente peligrosa. La normativa europea y nacional exige que toda operación esté justificada, evaluada y ejecutada conforme a unos parámetros concretos. Volar “porque se puede” o “porque está disponible” no es un criterio operativo válido y puede derivar en incumplimientos graves. El marco normativo: un pilar ignorado en la percepción de seguridad Uno de los factores que más contribuyen a la falsa sensación de seguridad es el desconocimiento —o la infravaloración— del marco normativo que regula el uso de drones. El Reglamento (UE) 2019/947, junto con su aplicación por parte de AESA en España, establece un enfoque basado en el riesgo. Esto implica que no todas las operaciones son iguales ni pueden tratarse como rutinarias. Categoría operacional, entorno, tipo de vuelo, personas expuestas y finalidad del uso son elementos que deben analizarse antes de cada operación. Cuando la normativa se percibe como un obstáculo y no como una herramienta de gestión del riesgo, se generan prácticas peligrosas:

- Operaciones fuera del escenario autorizado
- Uso del dron en entornos urbanos sin análisis previo
- Falta de coordinación con otras entidades
- Deficiencias en la protección de datos

Cumplir la normativa no es una carga administrativa; es una medida preventiva esencial.

Carlos Miguel Ortiz
Delegado Regional
Comunidad Autónoma de Madrid
Piloto remoto UAS certificado EASA
Instructor-examinador UAS certificado RITRAC

Ritrac International UAS professional services worldwide RUPSW

Correo electrónico: cmiguel@ritrac.eu
Móvil/Whatsapp: +34 685040875
Sitio web: https://ritrac.eu
Plataforma formación: https://remotepilot.online
Reuniones telemáticas: http://webex.ritrac.eu

Planes de autoprotección desconectados de la operación UAS

El plan de autoprotección debería ser el documento que articule todos los medios de seguridad disponibles. Sin embargo, en muchos casos, el dron aparece de forma testimonial, sin una integración real. No se definen con precisión los supuestos en los que se autoriza el vuelo, ni los límites operativos, ni la relación con otros sistemas como CCTV, control de accesos o seguridad física. Tampoco se contemplan escenarios de fallo: pérdida de señal, incidente aéreo o conflicto con terceros. Esta desconexión genera una ilusión de cobertura: el dron está contemplado en el plan, pero no está preparado para actuar de forma eficaz y segura cuando la situación lo exige.

Formación y entrenamiento: más allá de la certificación Otro de los grandes malentendidos en el uso de drones en seguridad es confundir certificación con capacitación operativa. Obtener la titulación como piloto es un requisito indispensable, pero claramente insuficiente. La operación en entornos de seguridad exige:

- Conocimiento del contexto operativo
- Capacidad de toma de decisiones bajo presión
- Coordinación con equipos terrestres
- Dominio de los límites legales de la captación de imágenes

Sin entrenamiento continuo, simulacros y evaluación de errores, el dron se convierte en un recurso frágil, dependiente de la improvisación del momento. La normativa, además, exige que el operador mantenga la competencia, lo que refuerza la necesidad de un enfoque formativo continuo.

P**rivacidad y protección de datos: el riesgo invisible**

La captación de imágenes aéreas introduce un riesgo adicional que a menudo se subestima: la protección de datos personales. En entornos urbanos o eventos, el dron puede captar información sensible de personas no relacionadas con la operación de seguridad. La ausencia de protocolos claros sobre:

- Finalidad de la grabación
- Conservación de imágenes
- Acceso a los datos
- Información a los afectados

No solo supone un incumplimiento normativo, sino que expone a la organización a riesgos legales y reputacionales que pueden superar cualquier beneficio operativo del vuelo. La falsa sensación de seguridad aparece cuando se cree que el valor preventivo del dron justifica cualquier uso de la imagen, lo cual es un error grave

La integración humana: el eslabón crítico La tecnología aérea no sustituye al criterio humano. El dron debe integrarse en una cadena de mando clara, con responsabilidades definidas y protocolos de actuación precisos.

¿Quién autoriza el vuelo? ¿Quién interpreta la información obtenida? ¿Quién decide la actuación posterior? Sin respuestas claras a estas preguntas, el dron genera información que no siempre se traduce en acción, o peor aún, en decisiones erróneas

Auditar la seguridad real: cuando el dron deja de ser decorativo

Evaluar la eficacia del uso de drones exige ir más allá de comprobar registros y licencias. Una auditoría realista debería analizar:

- **Coherencia entre análisis de riesgos y operaciones UAS**
- **Adecuación normativa de cada escenario**
- **Nivel de entrenamiento real del personal**
- **Integración con el resto de sistemas de seguridad**
- **Gestión de errores e incidentes Solo cuando estas variables están alineadas puede afirmarse que el dron aporta seguridad real y no una simple apariencia de control.**

Conclusión:

Del dron como gadget al dron como herramienta de gestión del riesgo Los drones son una herramienta potente, pero también exigente. Su valor en seguridad no reside en su presencia, sino en su uso responsable, planificado y legal.

La falsa sensación de seguridad surge cuando se confunde disponer de tecnología con estar preparados.

En un entorno normativo cada vez más estricto y en escenarios operativos complejos, el dron solo suma cuando se integra de forma coherente en la gestión global del riesgo.

En seguridad, como en aviación, la confianza excesiva es siempre un factor de riesgo

Carlos Miguel Ortiz
Delegado Regional
Comunidad Autónoma de Madrid
Piloto remoto UAS certificado EASA
Instructor-examinador UAS certificado RITRAC

Ritrac International UAS professional services worldwide RUPSW

Correo electrónico: cmiguel@ritrac.eu
Móvil/Whatsapp: +34 685040875
Sitio web: https://ritrac.eu
Plataforma formación: https://remotepilot.online
Reuniones telemáticas: http://webex.ritrac.eu

ESTABLECIMIENTO DE LOS TRES CANALES DE COMUNICACIÓN MILITAR: UN MODELO DE RESILIENCIA PARA LA SEGURIDAD CORPORATIVA GLOBAL.

Metro Risk

Edición propiedad de @MetroRisk, asociación

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

En el ámbito castrense, donde el caos y la incertidumbre son variables constantes, la eficacia de la comunicación no se delega al azar; se diseña meticulosamente como un sistema nervioso jerárquico y redundante. El procedimiento estandarizado 150-LDR-5010 del Ejercito de los Estados Unidos de América, "Establecer los Tres Canales de Comunicación", elaborado para operaciones de combate a gran escala, constituye un tratado avanzado sobre gestión de la información bajo presión extrema. Su relevancia, sin embargo, trasciende el campo de batalla, ofreciendo un marco estructural profundo y directamente transferible al desafío contemporáneo de la seguridad corporativa en un entorno empresarial globalizado, digital y perpetuamente amenazado.

La esencia del modelo militar reside en la segmentación disciplinada de los flujos de información en tres canales interdependientes: el canal de mando, el canal del personal y el canal técnico. El primero representa la columna vertebral de autoridad, la vía vertical por la cual descienden las órdenes estratégicas y asciende la información crítica.

En el ecosistema corporativo, este canal se materializa en la cadena de reporte ejecutivo durante una crisis, siendo el conducto exclusivo para decisiones que definen el rumbo de la organización frente a un ciberataque, un desastre operativo o una crisis reputacional. Paralelamente, el canal del personal opera en los planos horizontal y vertical entre funciones homólogas, facilitando la coordinación táctica y el soporte especializado.

Su analogía empresarial son las redes de comunicación entre departamentos entre el equipo legal y el de relaciones públicas, o entre seguridad física y ciberseguridad que deben actuar al unísono para contener un incidente, compartiendo inteligencia y recursos sin saturar al mando central. Finalmente, el canal técnico conecta a los especialistas, aquellos cuyo expertise permite el funcionamiento mismo de los sistemas. En la empresa, este es el dominio del centro de operaciones de seguridad (SOC), los administradores de infraestructura crítica o los equipos de cumplimiento normativo, que requieren un diálogo fluido y técnicamente preciso para restaurar servicios o implementar contramedidas.

La genialidad operativa del marco, no obstante, no radica solo en la segmentación, sino en los principios que lo sustentan. El imperativo de que "la información correcta llegue con prontitud a las personas correctas" es un antídoto contra la sobrecarga informativa y la fuga de datos, exigiendo una claridad predefinida sobre qué se comunica, a quién y por qué medio.

Más crucial aún es el principio de resiliencia codificado en la doctrina PACE (Primary, Alternate, Contingency, Emergency), que rechaza la peligrosa dependencia de un solo canal. Exige la preconfiguración de vías alternativas y de emergencia, un concepto que toda corporación debería aplicar a sus comunicaciones críticas, asumiendo que, en el momento de mayor necesidad, el canal principal estará comprometido o colapsado.

Complementariamente, el concepto de "crosstalk" autorizado la comunicación lateral directa entre mandos subordinados para agilizar decisiones tácticas sin escalar burocráticamente ofrece una lección poderosa en agilidad organizacional. Se trata de empoderar a los equipos de primera línea de seguridad con protocolos que les permitan coordinarse autónomamente dentro de un marco de reglas claro, acelerando drásticamente la contención de brechas mientras la dirección se enfoca en la estrategia global.

La transferencia práctica de este modelo al dominio corporativo implica un ejercicio de diagnóstico y reingeniería. Los líderes en seguridad (CISO) y continuidad del negocio deben comenzar por cartografiar exhaustivamente los flujos de comunicación existentes para incidentes críticos, identificando dónde existen, se solapan o, más preocupantemente, faltan los equivalentes a los canales de mando, personal y técnico. Sobre este mapa, es imperativo definir responsabilidades con precisión militar: quién se comunica con quién, en qué circunstancias y a través de qué medios (aplicando el modelo PACE para cada escenario). Posteriormente, la cultura de resiliencia debe cimentarse mediante simulacros regulares que, de manera realista, degraden o nieguen los canales de comunicación primarios como un ataque de denegación de servicio a los servidores de correo o la caída de la red interna forzando a los equipos a operar con sus protocolos alternativos y de emergencia. Solo a través de esta práctica deliberada se revelarán las fallas y se robustecerá la confianza en el sistema. La rigurosidad del procedimiento 150-LDR-5010 no es una reliquia de la jerarquía castrense, sino el producto de lecciones aprendidas en entornos de auténtica consecuencia. Para la corporación moderna, navegando en un paisaje de amenazas híbridas donde un ataque cibernético, una crisis logística y un desafío reputacional pueden converger en horas, adoptar un enfoque tan estructurado para las comunicaciones de seguridad deja de ser una opción académica para convertirse en un imperativo de supervivencia. Implementar este "sistema nervioso" tripartito, cimentado en la disciplina de la diseminación, la redundancia del plan PACE y la agilidad del crosstalk controlado, construye una capacidad organizacional distintiva: la de mantener la claridad, el control y la capacidad de decisión precisamente cuando el entorno opera para robárselos. En última instancia, la lección militar más valiosa para la seguridad corporativa es que la comunicación eficaz bajo presión no surge espontáneamente; se diseña, se practica y se institucionaliza como la piedra angular de la resiliencia.

SIN SEGURIDAD DEL ESTADO NO HAY TRANSICIÓN, NI GOBERNABILIDAD, NI REPÚBLICA

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Enrique Perez Barrios
Director General de GLOBAL SECURITY ACADEMY USA

En clave política

Una mirada necesaria para países que han perdido su piso institucional

Cuando un país pierde su piso institucional, denunciar la crisis ya no es suficiente ni el cambio político puede seguir siendo una consigna abstracta. Se requiere, con urgencia, un plan claro, una ruta coherente y la voluntad de reencontrarse con quienes poseen los valores, la experiencia y el compromiso republicano indispensables para reconstruir el país y sus instituciones, sean venezolanos del mundo civil, militar o policial.

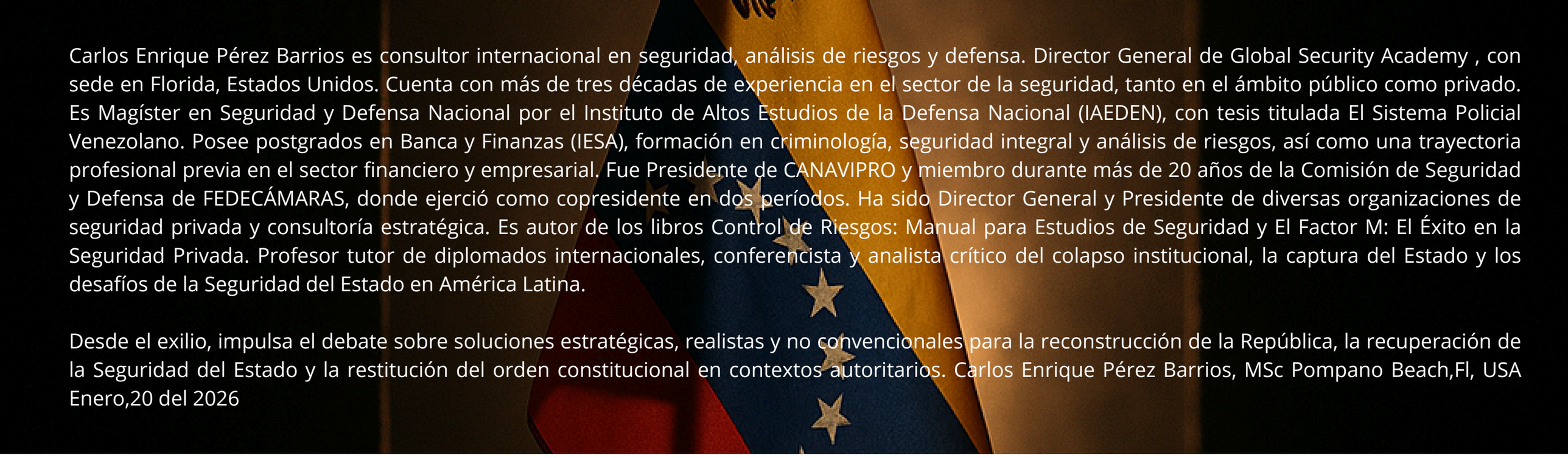
La Seguridad del Estado suele ser presentada como un concepto lejano, técnico o reservado a especialistas. Sin embargo, para sociedades que han vivido el colapso de sus instituciones, la Seguridad del Estado deja de ser una abstracción y se convierte en una necesidad vital, directamente vinculada con la libertad, la convivencia, la justicia y la posibilidad misma de reconstruir la República. Tal como he sostenido en trabajos anteriores y en la entrevista realizada por la periodista Raquel Marcano, no es posible hablar seriamente de transición democrática, recuperación económica o reconciliación nacional cuando el Estado ha perdido su capacidad básica de protegerse a sí mismo y a sus ciudadanos. A ello se suma una carencia aún más grave: la ausencia de una ruta clara y coherente que indique a los venezolanos hacia dónde se dirige el país y bajo qué principios se pretende reconstruirlo

La urgencia de una ruta clara y un plan nacional
En contextos de colapso institucional prolongado, la incertidumbre se convierte en una forma adicional de violencia social. Millones de ciudadanos no solo padecen inseguridad, pobreza o exilio, sino también la falta de un horizonte político creíble. Venezuela necesita, de manera urgente e inmediata, la presentación de una ruta nacional, un plan explícito que oriente a la sociedad sobre el proceso de recuperación del Estado, sus etapas, riesgos y responsabilidades.

La Seguridad del Estado cumple aquí un rol central: no solo protege, sino que ordena, orienta y da sentido estratégico a la reconstrucción nacional. Sin un plan claro, la seguridad se fragmenta; sin seguridad, el plan es inviable. Ambos elementos deben avanzar de manera inseparable.

¿Qué entendemos por Seguridad del Estado?
La Seguridad del Estado puede definirse, en términos sencillos, como la capacidad integral de una Nación para preservar su existencia, su soberanía, su estabilidad institucional y la seguridad de su población, frente a amenazas internas y externas. No se limita a lo militar ni a lo policial. Es un sistema amplio donde confluyen instituciones legítimas, normas claras, liderazgo político responsable y respaldo social. En un Estado democrático, la Seguridad del Estado está al servicio de la Nación y se ejerce dentro del marco de la ley. En un Estado capturado o autoritario, ese concepto se pervierte: la seguridad deja de proteger a la sociedad y pasa a proteger al régimen, incluso a costa de los derechos humanos y la legalidad.

Cuando se pierde el piso institucional
Un país pierde su piso institucional cuando las reglas dejan de ser predecibles, las instituciones dejan de cumplir su función y la ley se aplica de manera selectiva. En ese contexto, la Seguridad del Estado entra en una fase crítica. El Estado deja de ser garante del orden constitucional y se convierte en un actor más dentro de un escenario de confrontación política, corrupción estructural y penetración criminal. Las consecuencias son profundas: fragmentación del territorio, expansión del crimen organizado, debilitamiento de la soberanía, migración masiva y pérdida de confianza interna y externa. La inseguridad deja de ser solo ciudadana y se convierte en inseguridad estratégica.



Carlos Enrique Pérez Barrios es consultor internacional en seguridad, análisis de riesgos y defensa. Director General de Global Security Academy , con sede en Florida, Estados Unidos. Cuenta con más de tres décadas de experiencia en el sector de la seguridad, tanto en el ámbito público como privado. Es Magíster en Seguridad y Defensa Nacional por el Instituto de Altos Estudios de la Defensa Nacional (IAEDEN), con tesis titulada El Sistema Policial Venezolano. Posee postgrados en Banca y Finanzas (IESA), formación en criminología, seguridad integral y análisis de riesgos, así como una trayectoria profesional previa en el sector financiero y empresarial. Fue Presidente de CANAVIPRO y miembro durante más de 20 años de la Comisión de Seguridad y Defensa de FEDECÁMARAS, donde ejerció como copresidente en dos períodos. Ha sido Director General y Presidente de diversas organizaciones de seguridad privada y consultoría estratégica. Es autor de los libros Control de Riesgos: Manual para Estudios de Seguridad y El Factor M: El Éxito en la Seguridad Privada. Profesor tutor de diplomados internacionales, conferencista y analista crítico del colapso institucional, la captura del Estado y los desafíos de la Seguridad del Estado en América Latina.

Desde el exilio, impulsa el debate sobre soluciones estratégicas, realistas y no convencionales para la reconstrucción de la República, la recuperación de la Seguridad del Estado y la restitución del orden constitucional en contextos autoritarios. Carlos Enrique Pérez Barrios, MSc Pompano Beach,Fl, USA Enero,20 del 2026

Ambitos donde la Seguridad del Estado es indispensable

En primer lugar, el ámbito político e institucional. Sin instituciones legítimas, independientes y operativas, no puede existir Seguridad del Estado. La captura del poder judicial, la anulación del control parlamentario y la manipulación de los procesos electorales destruyen la base del Estado de Derecho.

En segundo término, el ámbito de la defensa y la fuerza pública. Las fuerzas armadas y policiales deben responder a la Constitución y al interés nacional, no a una parcialidad política ni a redes criminales. Su profesionalización y despolitización son condiciones esenciales para cualquier proceso de reconstrucción.
Un tercer ámbito es el de la seguridad interna y ciudadana. La proliferación de grupos armados irregulares, mafias y economías ilegales es siempre una señal inequívoca del fracaso de la Seguridad del Estado. Recuperar el monopolio legítimo de la fuerza es una tarea estratégica.

También resulta clave el ámbito económico y estratégico. La corrupción sistémica, el colapso productivo y la dependencia de actividades ilícitas debilitan al Estado y lo hacen vulnerable. No hay Seguridad del Estado posible en un país económicamente capturado. Finalmente, el ámbito internacional. Un Estado sin seguridad interna ni institucional pierde credibilidad y capacidad de apoyo externo. En cambio, una estrategia clara de reconstrucción de la Seguridad del Estado puede convertirse en un factor de respaldo político y cooperación internacional.

Llamar a quienes nunca debieron ser excluidos

Un componente frecuentemente ignorado en los debates sobre reconstrucción nacional es el capital humano y moral con el que cuenta el país, tanto dentro como fuera de sus fronteras. Venezuela dispone de un inmenso contingente de ciudadanos formados, con valores, principios morales y convicciones republicanas, que han sido apartados, forzados al exilio o tratados como si no existieran.
La reconstrucción de la Seguridad del Estado exige volver a llamar al servicio activo, en el sentido republicano del término, a estos venezolanos. No se trata de revancha ni de improvisación, sino de reintegración institucional, de aprovechar experiencia, formación y compromiso ético para recuperar capacidades hoy inexistentes o severamente debilitadas.
Excluir a quienes han demostrado lealtad a la Constitución y a la República no solo es injusto, sino estratégicamente irresponsable. Ningún país se reconstruye dejando fuera a quienes pueden y quieren contribuir a hacerlo.

Capacidades necesarias para reconstruir la Seguridad del Estado

Restablecer la Seguridad del Estado no es un acto inmediato ni un decreto político. Requiere desarrollar capacidades reales: capacidad institucional para diseñar políticas públicas serias; capacidad estratégica para identificar amenazas y priorizarlas; capacidad operativa en fuerzas de defensa, policía e inteligencia profesionalizadas; y, de manera transversal, una capacidad ética orientada a romper con la impunidad y la corrupción.

Igualmente indispensable es la conducción civil democrática del sector seguridad. Sin control político legítimo, la seguridad se desvirtúa y termina generando nuevas formas de inestabilidad**.**

Objetivos estratégicos

Los objetivos de la Seguridad del Estado en un país que busca reconstruirse deben ser claros para la ciudadanía: garantizar la supervivencia del Estado y la Nación; restablecer el orden constitucional; proteger a la población frente a amenazas criminales; crear condiciones de estabilidad para la recuperación económica y social; y recuperar la confianza nacional e internacional.
La transparencia y la claridad son fundamentales para generar legitimidad social.

Desde el punto de vista estratégico

Un país que ha perdido su piso institucional, como Venezuela, no puede hablar seriamente de seguridad ciudadana sin antes reconstruir su Seguridad del Estado. Pretender invertir el orden de las prioridades sólo conduce a políticas fragmentadas y a nuevos fracasos. La Seguridad del Estado constituye la columna vertebral que permite reconstruir la República, recuperar sus instituciones, proteger efectivamente a la población, asegurar una transición política real y garantizar la gobernabilidad futura. Solo después de cumplir estas etapas será posible avanzar hacia una estabilización duradera que permita retornar a un sistema político auténticamente democrático.

Ese sistema hoy no existe: fue sustituido por una estructura de poder criminal, represiva y asociada a economías ilícitas, que desnaturaliza al Estado y anuló la República.
De allí que la discusión sobre la Seguridad del Estado no sea ideológica ni teórica. Es una necesidad estratégica inmediata. Sin Seguridad del Estado no hay transición posible; sin transición segura no hay gobernabilidad; y sin gobernabilidad no hay democracia que pueda sostenerse en el tiempo. Reconstruir la Seguridad del Estado es, en consecuencia, el primer acto responsable para recuperar el país y devolverle a los ciudadanos un futuro posible.

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/

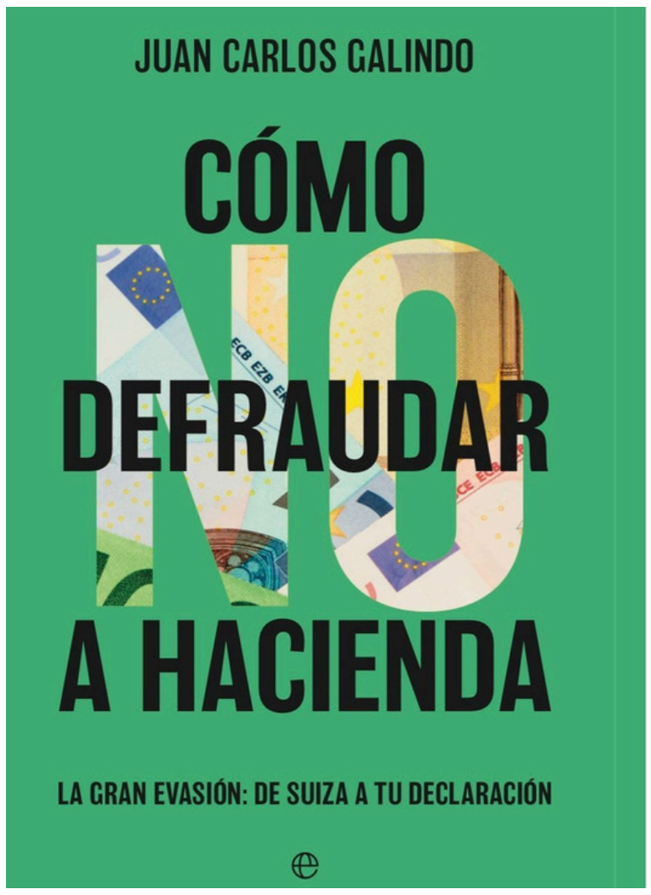
AGENDA

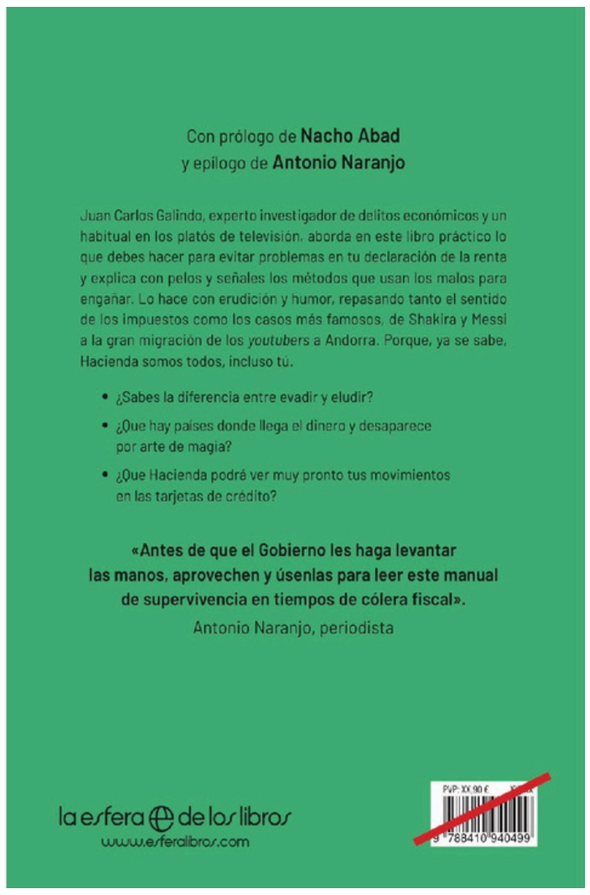
Metro Risk

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