EDITORIAL MR

ISSN 3045-7629

NOVIEMBRE

AÑO 2025

Edición propiedad de @MetroRisk, asociación

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

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.

EL FUTURO DE LA SEGURIDAD

Metro Risk

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz
Director de MetroRisk

El futuro de la seguridad no puede construirse sobre los mismos cimientos que el pasado, porque el mundo actual se enfrenta a riesgos mucho más complejos, globales e interconectados. La profesión de la seguridad debe asumir una transformación profunda si quiere responder a los desafíos de una sociedad cada vez más tecnológica, más vulnerable y más dependiente de la confianza en sus sistemas. En esta evolución, la clave no está solo en la tecnología, sino en las personas que la gestionan, en su preparación, en sus condiciones laborales y en el reconocimiento real de su papel dentro del entramado social y económico.

La seguridad del futuro exige mejores condiciones laborales, un entorno más justo y profesionalizado, y un modelo que incentive el crecimiento de quienes dedican su vida a proteger a los demás. El profesional de la seguridad debe contar con recursos, estabilidad y formación que le permitan desarrollar su labor con eficacia y orgullo. Formar, especializar y motivar no son lujos, sino necesidades estratégicas.

La formación avanzada en áreas como la ciberseguridad, la protección crítica, la inteligencia preventiva o el diseño ambiental seguro, debe ser la base sobre la que construir una nueva generación de profesionales capaces de anticipar las amenazas y actuar con criterio, no solo reaccionar ante ellas. Al mismo tiempo, las empresas y las instituciones deben disponer de un marco normativo más coherente y actualizado, adaptado a un mundo global y digital en el que los riesgos no reconocen fronteras. No es posible mantener estructuras rígidas en un entorno que se transforma constantemente.

La normativa debe evolucionar para dar respuesta a la realidad híbrida de la seguridad actual, combinando la prevención física y la tecnológica, y estableciendo estándares internacionales que garanticen la calidad, la trazabilidad y la interoperabilidad de los servicios. La fiscalización y las auditorías también deben dar un salto cualitativo. No basta con auditar los números, hay que evaluar la esencia: la gestión de recursos humanos, la aplicación de protocolos, la respuesta operativa, la ética profesional y la eficiencia en el servicio. Las auditorías normativas y de gestión deben convertirse en instrumentos de mejora continua, que ayuden a las empresas a crecer, a corregir desequilibrios y a elevar el nivel de exigencia del sector.

El futuro de la seguridad se apoya igualmente en la tecnología, pero no como un fin en sí misma, sino como una herramienta de apoyo al criterio humano. Drones, sensores inteligentes, sistemas de vigilancia predictiva e inteligencia artificial son aliados poderosos, pero su eficacia depende del conocimiento, la ética y la capacidad analítica de los profesionales que los manejan. La tecnología amplifica la seguridad solo cuando se usa con formación y responsabilidad. Así pues, la seguridad del mañana será el reflejo del compromiso que hoy asumamos con la profesionalidad, la dignidad y la excelencia.

Requerirá de una sociedad que entienda su valor, de empresas que la gestionen con responsabilidad y de profesionales que encuentren en ella un camino de desarrollo y estabilidad. Porque en un mundo en constante cambio, donde las amenazas se transforman y multiplican cada día, quizás la pregunta más importante que debamos hacernos sea esta: **¿estamos realmente preparados para construir una seguridad a la altura de los tiempos que vienen?**

UN BUEN DISEÑO DE SEGURIDAD ES VIVIR SEGURO DESDE EL PRIMER PLANO

Un informe de seguridad especializadó analiza la vivienda en su conjunto:

- ✓ Arquitectura y accesos
- ✓ Enforno y urbanización
- ✓ Iluminación y paisajísmo

Con ello se anticipan riesgos y se convierten los espácios en **entornos seguros**, funcionales y sostenibles

FRAN MEDINA CRUZ

Consultor y Asesor en Seguriidad por Diseno

Especialista CPTED y BREEAM

MRConsulting

Sequridad inteligente pare viviendas de alto standing

LA DIRECCIÓN DE SEGURIDAD Y SU RELACIÓN CON LA COMPLIANCE

Metro Risk

Edición propiedad de @MetroRisk, asociación

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

La creciente complejidad normativa, la globalización de los riesgos y la exigencia de transparencia han impulsado la integración de nuevos modelos de control interno, entre los que destaca el Compliance. En este contexto, la Dirección de Seguridad se posiciona como un actor clave no solo en la protección física o tecnológica, sino también en la garantía del cumplimiento normativo que afecta a la seguridad corporativa y a la responsabilidad penal de las organizaciones.

La función del Director de Seguridad

El Director de Seguridad, conforme a la Ley 5/2014 de Seguridad Privada, es responsable de planificar, dirigir e inspeccionar los recursos destinados a la seguridad de la entidad. Su papel, tradicionalmente operativo, ha evolucionado hacia una función estratégica que incluye la protección de la información, la continuidad del negocio, la gestión de crisis y la prevención del fraude. Hoy, su misión se amplía a la gestión de la seguridad integral, alineada con los principios del Compliance.

El Compliance: cultura de cumplimiento y control

El Compliance, o cumplimiento normativo, es un sistema de gestión que busca garantizar que la organización, sus directivos y empleados actúan conforme a la ley y a los valores éticos corporativos. Desde la reforma del Código Penal español (LO 1/2015), la existencia de un modelo de prevención eficaz puede eximir de responsabilidad penal a la persona jurídica.

Convergencia entre Seguridad y Compliance

La relación entre Dirección de Seguridad y Compliance es estructural, ya que ambos comparten la misma filosofía preventiva basada en la gestión del riesgo. El Director de Seguridad y el Compliance Officer deben coordinarse bajo un marco común de Enterprise Risk Management (ERM) para evitar duplicidades y reforzar los controles.

Puntos de convergencia principales:

- Gestión del riesgo (físico, tecnológico y legal).
- Protección de la información (RGPD, ENS, ISO 27001).
- Investigación interna y canales de denuncia.
- Prevención del fraude y la corrupción.
- Formación y cultura de seguridad y cumplimiento.

El modelo de seguridad como parte del sistema de Compliance.

Integrar la seguridad dentro del sistema de Compliance refuerza la eficacia y credibilidad del modelo preventivo. Normas como la UNE 19601:2017 y la ISO 31000:2018 promueven la integración transversal de todas las áreas críticas, entre ellas la seguridad corporativa.

Conclusión

La sinergia entre Dirección de Seguridad y Compliance representa la evolución natural de la gestión del riesgo. El Director de Seguridad deja de ser un mero gestor operativo para convertirse en un agente estratégico del cumplimiento y la integridad corporativa. Integrar ambos enfoques fortalece la gobernanza, protege la reputación de la empresa y fomenta una cultura organizativa ética y sostenible.

Bibliografía recomendada

- Ley 5/2014, de Seguridad Privada.
- Ley Orgánica 1/2015, de reforma del Código Penal.
- UNE 19601:2017 – Sistemas de gestión de Compliance penal.
- ISO 31000:2018 – Gestión del riesgo.
- ISO 27001:2022 – Seguridad de la información.

INVESTIGACIÓN PRIVADA ANTE EL AUGE DE LAS BAJAS LABORALES FRAUDULENTAS

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos G. Barrett
Gerente general en Spy Investigación & Barrett

Son las nueve de la mañana y, como cada día, las consultas comienzan antes de que el café termine de prepararse. Abogados y clientes privados llaman para conocer el estado de investigaciones en curso: casos que, en su mayoría, tienen un elemento en común, las bajas laborales fraudulentas.

Este fenómeno se ha convertido en uno de los principales desafíos para pequeñas y medianas empresas en España. Según profesionales del sector, existen compañías donde el porcentaje de trabajadores de baja puede superar el 50% del total de la plantilla, un índice insostenible para la rentabilidad del negocio. Esta situación, aseguran, es producto de un marco legal que favorece ampliamente al trabajador, dejando al empresario en una posición vulnerable.

En respuesta, muchos despachos de detectives privados afirman estar saturados. Más del 50% de los servicios solicitados están relacionados con bajas laborales. Entre todas ellas, las de carácter psicológico, como ansiedad o depresión, son las más difíciles de detectar. Los investigadores destacan que, al tratarse de dolencias poco visibles, resulta complejo para las mutuas verificar la veracidad del cuadro clínico. Con el objetivo de esclarecer estos casos, la labor del detective privado se ha vuelto indispensable. Las pesquisas pueden incluir vigilancia en las inmediaciones del domicilio del investigado y seguimientos puntuales que permitan observar actividades incompatibles con la baja médica. Por ejemplo, la ingesta de alcohol, que podría interferir con la medicación prescrita.

El incumplimiento de indicaciones profesionales puede derivar en la revocación de la baja e incluso en despido procedente. La jurisprudencia respalda estas investigaciones. Existen múltiples sentencias que avalan la actuación empresarial cuando se demuestra fraude. Asimismo, los detectives señalan que, en ocasiones, descubren a trabajadores desempeñando labores remuneradas en otras compañías mientras mantienen una baja activa, situación sancionable de inmediato.

Los despachos especializados en investigación privada aseguran que estas prácticas son recurrentes. Los patrones de conducta suelen repetirse y, cuando el empresario detecta anomalías intermitentes, suele recurrir al detective como último recurso.

A nivel político, el fenómeno pone en evidencia una gestión deficiente del sistema. Los casos fraudulentos no solo afectan a la economía empresarial, sino que eclipsan la situación de trabajadores que realmente necesitan procesos de recuperación legítimos, generando gasto adicional a las mutuas y al sistema de salud.

Desde el Ministerio del Interior, únicamente los detectives privados acreditados están facultados para realizar este tipo de investigaciones, que requieren rigor jurídico y una presentación sólida ante el juez. El informe pericial es, en definitiva, la herramienta que respalda cualquier decisión disciplinaria. La jornada del investigador es extensa, y rara vez se parece a la imagen cinematográfica del espionaje.

Detrás de cada caso hay horas de análisis previo, verificación de datos y redacción exhaustiva. Al finalizar el día, algunos profesionales admiten disfrutar del trabajo bien hecho acompañados de un buen vino y, en ocasiones, un puro, como recompensa al esfuerzo invertido.

Mientras el debate continúa, el sector de investigación privada se consolida como un aliado crucial para empresas que buscan protegerse del fraude laboral en un entorno legal cada vez más complejo

CARLOS G. BARRETT
Investigador Privado
Experto en Criminalística

LA ASOCIACIÓN ESPAÑOLA DE AUDITORES DE SEGURIDAD COGE IMPULSO

Metro Risk

Edición propiedad de @MetroRisk, asociación

José Ignacio Olmos Casado
Presidente AEAS

En los últimos meses la Asociación Española de Auditores de Seguridad (AEAS) ha retomado su actividad con nuevas incorporaciones dentro de la Junta Directiva. Se pretende aumentar el número de actividades y seguir reforzando el papel del auditor de seguridad en todos los proyectos de consultoría y en sus múltiples campos de actividad.

En las próximas semanas los socios recibirán información actualizada con las próximas actividades a desarrollar, detalle de las novedades de funcionamiento y estructura de trabajo de la Asociación. Además, firmaremos una serie de convenios con distintos colectivos y asociaciones al objeto de beneficiar a nuestros socios.

Como hemos comentado en ocasiones precedentes AEAS pretende ser un foro donde profesionales de prestigio tengan un lugar de encuentro, tanto para la defensa de sus intereses como para su formación continua. He de resaltar que nuestra Asociación nace claramente con esta vocación, y no con el ánimo de ser mayoritaria; así, el ingreso debe ser aprobado por la Junta Directiva tras examinar la competencia y trayectoria profesional del candidato, no siendo esta una asociación al uso, y en la que la T.I.P. de director de seguridad no es más que el punto de partida, pero absolutamente insuficiente si no va acompañada de experiencia en proyectos de consultoría acreditables para el ingreso dentro de nuestro colectivo profesional.

Nuestro objetivo seguirá siendo contribuir a la mejora de la seguridad integral, prestigiar la figura del auditor y defender los intereses de nuestros asociados

Gregorio Duro
Tecnico en licitaciones y Proyectos

MÁQUINAS DE SOPORTE VECTORIAL (SVM) EN EL ENTORNO DEL ANÁLISIS DE RIESGOS

En el artículo de este mes, quiero desarrollar un interesante concepto enfocado a las operaciones de análisis de riesgos. El concepto concreto, las Máquinas de Soporte Vectorial (SVM, por sus siglas en inglés), son una clase de algoritmos de aprendizaje supervisado que han demostrado ser altamente efectivas en la clasificación y regresión de datos complejos.

Aunque originalmente fueron diseñadas para tareas de clasificación matemática, las SVM se han adaptado paulatinamente al entorno del análisis de riesgos físicos, donde la capacidad de modelar relaciones no lineales y manejar grandes volúmenes de datos es de suma importancia. Esta adaptabilidad se ha convertido en una herramienta esencial en la predicción y evaluación de riesgos, optimizando la toma de decisiones y la gestión de la seguridad física.

Fundamento de las SVM en el análisis de riesgos.

Las SVM funcionan encontrando el hiperplano óptimo que separa las diferentes clases de datos en el espacio de características. En el contexto del análisis de riesgos físicos, este hiperplano puede ser interpretado como la frontera de clasificación entre eventos de riesgo y no riesgo, o entre niveles de severidad del impacto. Dado que muchos eventos físicos no siguen relaciones lineales simples, las SVM pueden aplicar el denominado truco del núcleo (kernel trick), que transforma los datos a un espacio de mayor dimensión para hacer posible una separación lineal, clasificación permitiendo una más precisa de riesgos complejos. Por ejemplo, en el caso de un análisis de riesgos de un evento de incendio forestal, las características del sistema, como la temperatura, humedad, velocidad del viento y tipo de vegetación, pueden ser las variables de entrada. Las SVM aprenderán a identificar patrones entre estos factores y clasificarlos como "zona de riesgo" o "zona segura". La ventaja de este enfoque es que las SVM pueden modelar de forma precisa los límites complejos entre estas clases, especialmente cuando las interacciones entre variables son no lineales.

Aplicación de las SVM en la predicción de riesgos físicos.

En el análisis de riesgos físicos, las SVM pueden ser utilizadas para predecir la probabilidad de ocurrencia de eventos adversos y evaluar su impacto. Su capacidad para manejar datos multidimensionales y modelar relaciones no lineales resulta esencial para escenarios donde las variables involucradas son numerosas y tienen interacciones complejas.

Por ejemplo, en un análisis de riesgo de inundación por condiciones atmosféricas adversas, las SVM pueden integrarse con datos geográficos, climáticos e históricos. Las variables de entrada podrían incluir la altitud, historial de precipitaciones y pico de lluvias, condiciones del suelo, temperatura y humedad entre otros. Las SVM, al analizar datos de eventos pasados, pueden identificar patrones que predicen la probabilidad de inundación bajo condiciones específicas y clasificarlas en categorías como "riesgo bajo", "riesgo moderado" o "riesgo alto". En este caso, el kernel de la SVM sería clave para transformar el conjunto de datos en un espacio de características que permita identificar las fronteras no lineales entre las zonas de inundación y las zonas seguras.

Manejo de la incertidumbre y evaluación del impacto

Uno de los aspectos más valiosos de las SVM en el análisis de riesgos físicos es su capacidad para trabajar con incertidumbre. Las SVM no solo proporcionan una clasificación binaria o categórica, sino que, mediante la técnica de márgenes suaves (soft margins), pueden manejar situaciones donde los datos no son perfectos o precisos. Esta capacidad de modelar incertidumbre es crucial en el análisis de riesgos, donde las predicciones siempre tienen un grado de imprecisión.

Incertidumbre en la predicción de riesgos

En escenarios complejos, como la predicción de incendios forestales, la probabilidad de que ocurra un incendio puede depender de variables que presentan un alto grado de incertidumbre, como los cambios climáticos imprevistos o comportamientos humanos aleatorios. Las SVM permiten que el modelo haga predicciones incluso cuando los datos no son completamente consistentes, asignando un margen de confianza que puede ser interpretado como la "certeza" de la predicción. Esto es suma importancia para la toma de decisiones precisas sobre la implementación de medidas preventivas.

Evaluación del impacto

Además de la clasificación de riesgo, las SVM pueden ser adaptadas para evaluar el impacto de los eventos de riesgo, mediante la regresión. La regresión con SVM permite estimar variables continuas, como el daño potencial en caso de incendio, inundación o robo, proporcionando un modelo que no solo predice si ocurrirá un evento, sino también la magnitud del impacto. Por ejemplo, en un escenario de inundación, la regresión de SVM podría predecir la altura del agua o la cuantía de los daños a la infraestructura, lo que ayuda a priorizar las áreas de intervención y a asignar recursos de manera más eficiente.

Desarrollo actual

La adaptación de las Máquinas de Soporte Vectorial (SVM) al análisis de riesgos físicos ha permitido una revolución en la forma de gestionar y predecir eventos adversos, como incendios, inundaciones, robos e intrusiones. Su capacidad para manejar relaciones no lineales, clasificar grandes volúmenes de datos e incorporar incertidumbre en las predicciones las convierte en una herramienta esencial en la evaluación y mitigación de riesgos. Si bien su implementación plantea algunos desafíos, como la necesidad de un preprocesamiento adecuado de los datos y una alta capacidad computacional en escenarios complejos, sus ventajas en términos de precisión y capacidad de generalización hacen que las SVM sean una de las opciones más precisas en el campo del análisis de riesgos físicos.

Me gustaría agradecer a Metrorisk la generosa contribución mensual de artículos técnicos, los cuales considero un valioso esfuerzo de divulgación además de jugar un papel fundamental en el avance y la expansión del conocimiento en nuestro sector. Estos artículos fomentan el análisis crítico de nuevas metodologías, impulsan el fortalecimiento de la cultura de gestión de riesgos y aportan ejemplos prácticos, enfoques innovadores y reflexiones que enriquecen tanto las tareas cotidianas como la toma de decisiones estratégicas en un entorno cada vez más complejo y dinámico.

Gregorio Duro Navarro
Licitaciones y Proyecto

SECCIÓN

PREVENCIÓN DEL CRIMEN. CPTED

Metro Risk

Edición propiedad de @MetroRisk, asociación

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

AUDITORÍA CPTED: ASEGURANDO LA SEGURIDAD POR DISEÑO CON ISO 22341 Y EL RIGOR DE ISO 19011:2018

La Prevención del Delito Mediante el Diseño Ambiental (CPTED) es una estrategia proactiva para reducir la oportunidad delictiva. La norma ISO 22341:2021 (Directrices para la prevención del delito mediante el diseño ambiental) proporciona el marco técnico para implementar CPTED. Sin embargo, para garantizar que esta implementación sea sistemática, objetiva y conduzca a la mejora continua, es crucial aplicar las directrices de auditoría establecidas en la ISO 19011:2018 (Directrices para la auditoría de los sistemas de gestión).

En esta ocasión describo cómo llevar a cabo una auditoría CPTED integrando los requisitos técnicos de la ISO 22341 con los principios y el proceso de auditoría de la ISO 19011.

I. Fundamentos de la Auditoría CPTED:

1. Criterios de Auditoría (ISO 22341:2021): La auditoría se centra en la conformidad con los lineamientos de la ISO 22341, que se dividen en dos conceptos principales:

-Estrategias Físicas (Primera Generación):

- o Vigilancia natural.
- o Control de acceso natural.
- o Refuerzo territorial.
- o Imagen y gestión/mantenimiento.
- o Apoyo a la actividad.
- o Endurecimiento del sitio/objetivo.

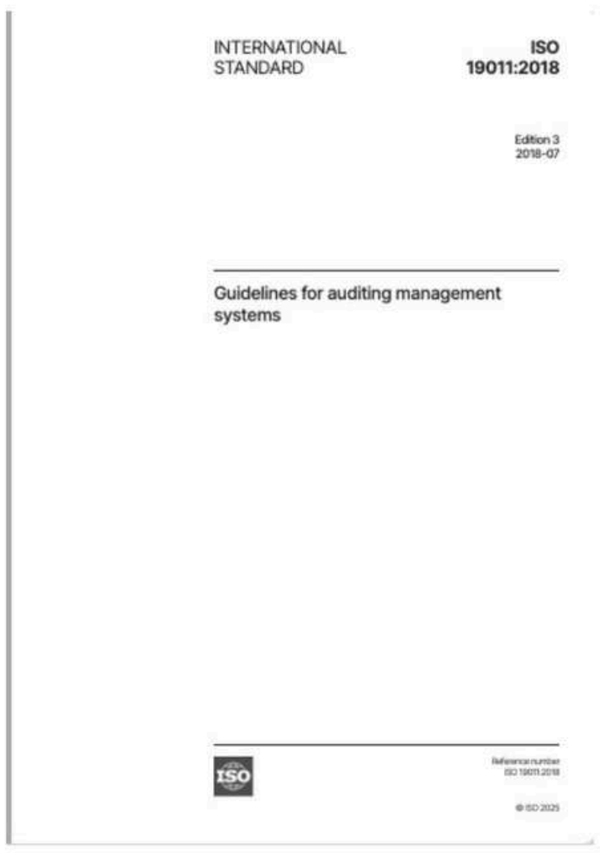
-Estrategias Sociales (Segunda Generación):

- o Cohesión social.
- o Conectividad social.
- o Cultura comunitaria.
- o Capacidad de umbral.

2. Principios de Auditoría (ISO 19011:2018): La conducta y el trabajo del auditor y del equipo deben regirse por los siete principios de la ISO 19011 para garantizar conclusiones pertinentes y fiables:

- Integridad: actuar con honestidad, diligencia y responsabilidad.
- Presentación imparcial: informar con veracidad y exactitud (los hallazgos deben reflejar objetivamente la conformidad con ISO 22341).
- Debido cuidado profesional: aplicar diligencia y juicio en la planificación y realización.
- Confidencialidad: proteger la información sensible (ej. detalles de vulnerabilidades de seguridad).
- Independencia: ser objetivo y libre de sesgos en la actividad que se audita.
- Enfoque basado en la evidencia: los hallazgos se sustentan en registros, declaraciones o hechos verificables.
- Enfoque basado en riesgos: considerar los riesgos y oportunidades durante la planificación y ejecución, concentrando el esfuerzo en áreas críticas de riesgo delictivo.

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


INTERNATIONAL STANDARD

ISO 19011:2018

Edition 3
2018-07

Guidelines for auditing management systems

ISO

II. El Proceso de Auditoría: Alineado a la ISO 19011: El proceso de auditoría CPTED debe seguir las fases del ciclo PHVA (Planificar-Hacer Verificar-Actuar) definidas por la ISO 19011.

1. Planificación de la Auditoría: Este es el momento de aplicar el Enfoque Basado en Riesgos (ISO 19011)

Etapa	Actividades Clave	CPTED/ISO 22341 Relevancia
Objetivos y Alcance	Determinar qué se auditará (ej. solo el diseño físico de un nuevo proyecto o también la gestión social de un área existente).	Los objetivos deben incluir verificar la aplicación del proceso CPTED (planificación, diseño, gestión del sitio) de ISO 22341.
Riesgos del Programa	Identificar riesgos que puedan afectar la auditoría (ej. falta de acceso a áreas críticas, sesgo del auditor interno).	Aplicar el Enfoque Basado en Riesgos para priorizar las zonas de la instalación con mayor riesgo de delincuencia.
Criterios y Equipo	Definir los criterios (ISO 22341) y seleccionar el equipo auditor con la competencia adecuada en CPTED.	El auditor debe tener capacidad de interpretar los principios CPTED en el entorno físico y social.
Plan de Auditoría	Detallar fechas, métodos, y áreas de enfoque.	Priorizar la revisión del Análisis del Riesgo de Delincuencia previo (que debe seguir la ISO 31000).

2. Realización de la Auditoría**:** El equipo auditor aplica los principios de Independencia y Debido Cuidado Profesional.

-Reunión de apertura: presentar el plan y confirmar la disponibilidad de recursos.
-Recopilación de evidencias: se realiza a través de:

- Inspección física: observación del entorno construido, verificando la implementación de las 6 estrategias físicas (ej. ¿Los setos permiten la vigilancia natural? ¿El alumbrado es adecuado?).
- Revisión documental: evaluación de planos, políticas de mantenimiento (gestión y mantenimiento de ISO 22341) y registros de incidentes (para validar el análisis de riesgo).
- Entrevistas: conversaciones con partes interesadas (arquitectos, gestores del sitio, usuarios, comunidad), para verificar las estrategias sociales.

-Generación de Hallazgos: contrastar la evidencia obtenida con los criterios de la ISO 22341. Los hallazgos se clasifican en Conformidades, No Conformidades (si se incumple un requisito clave de la ISO 22341) u Oportunidades de Mejora**.**

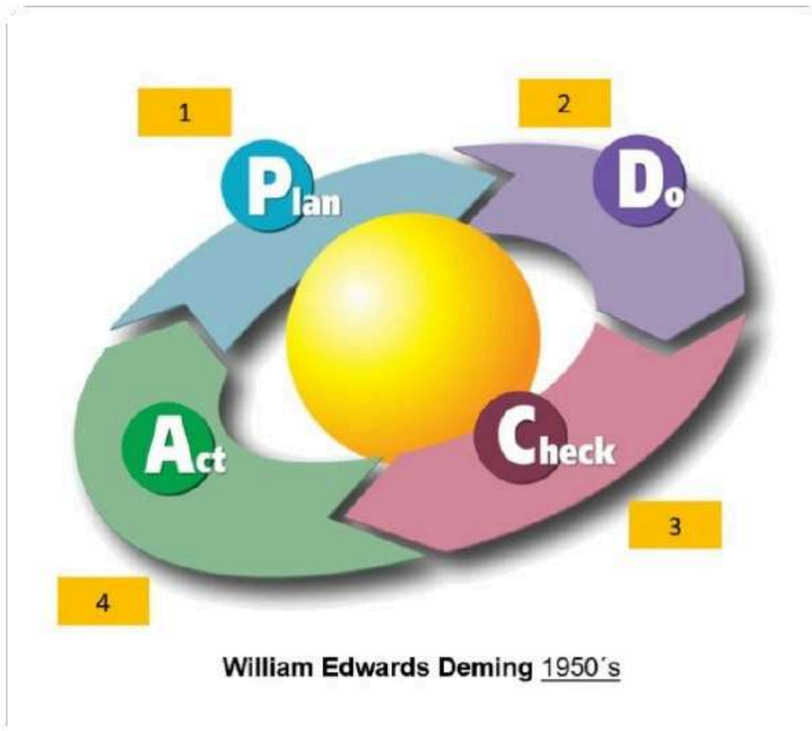
3. Informe: El principio de Presentación Imparcial es esencial.

- Preparación del informe: documentar las conclusiones de la auditoría y los hallazgos de manera veraz, exacta, objetiva y clara.
- Conclusiones CPTED: la conclusión principal debe ser sobre la adecuación, idoneidad y eficacia de las medidas CPTED implementadas para prevenir el delito y el temor al delito, en conformidad con la ISO 22341.
- Reunión de cierre: presentar los hallazgos y conclusiones a la dirección.

4. Seguimiento y mejora continua:

- Acciones correctivas: el auditado debe determinar y tomar acciones correctivas para eliminar las causas de las no conformidades (un requisito clave de cualquier Sistema de Gestión ISO).
- Revisión y mejora del programa: el equipo que gestiona el programa de auditoría (ISO 19011) debe revisar y mejorar continuamente el proceso de auditoría CPTED, asegurando que futuras auditorías sigan concentrándose en los riesgos de delincuencia más significativos.

III. El Rol de las Normas de Gestión La aplicación de la ISO 19011 garantiza que la auditoría CPTED sea más que una simple lista de verificación de diseño; se convierte en un proceso de evaluación rigurosa que asegura que el diseño ambiental está correctamente integrado en el Sistema de Gestión de la Seguridad y Resiliencia de la organización, promoviendo la eficacia a largo plazo de las medidas preventivas



William Edwards Deming 1950´s

Competencia del Auditor CPTED:

La ISO 19011:2018 (Cláusula 7) establece que el auditor debe poseer los conocimientos y habilidades necesarios para llevar a cabo la auditoría, y la persona que gestiona el programa de auditoría debe determinar la competencia requerida para los auditores de manera sistemática.

En el contexto de una auditoría CPTED/ISO 22341, la competencia requerida va más allá de la comprensión del proceso de auditoría e incluye una doble especialización: conocimiento de la seguridad física por diseño y dominio de los sistemas de gestión

1. Conocimiento y Habilidades Específicas del CPTED (ISO 22341) El auditor debe tener la capacidad de interpretar y evaluar la aplicación técnica de la ISO 22341 en el entorno construido. Esto incluye:
   - Fundamentos CPTED: comprensión profunda de las estrategias de CPTED de primera y segunda generación (vigilancia natural, refuerzo territorial, gestión/mantenimiento, cohesión social, etc.).
   - Análisis del entorno: habilidad para analizar planos, diseños urbanos y arquitectónicos, e identificar elementos que crean oportunidades de delito ("puntos ciegos", vegetación inadecuada, iluminación deficiente).
   - Gestión del riesgo de delincuencia: dominio de las metodologías de evaluación de riesgos delictivos (alineadas con ISO 31000), enfocadas en la interacción entre el delincuente, la víctima/objetivo y el entorno.
   - Legislación aplicable: conocimiento de los requisitos legales, reglamentarios y contractuales relevantes para el desarrollo urbano, construcción y seguridad

2. Atributos Personales y Habilidades de Auditoría: El auditor CPTED debe exhibir los atributos personales que sustentan los siete principios de auditoría de la ISO 19011:

Atributo Personal	Impacto en la Auditoría CPTED
Ético, honesto e íntegro	Actuar con discreción, especialmente al manejar información sobre vulnerabilidades críticas del diseño.
Mentalidad Abierta	Considerar ideas o puntos de vista alternativos, crucial en la evaluación de los factores **sociales** del CPTED (segunda generación).
Diplomático y Persuasivo	Interactuar eficazmente con diversas partes interesadas: arquitectos, ingenieros, personal de seguridad y miembros de la comunidad.
Perceptivo	Ser consciente y capaz de comprender las situaciones sutiles, especialmente durante la observación del uso real de los espacios.
Versátil	Adaptar el estilo de auditoría para evaluar diferentes entornos (edificios nuevos, espacios públicos, barrios existentes).
Independiente y Objetivo	Garantizar que el juicio sobre la efectividad del diseño CPTED no esté influenciado por intereses personales o de la organización auditada.
Decisivo	Ser capaz de llegar a conclusiones oportunas basadas en el nivel

La ISO 19011 enfatiza que la competencia de los auditores debe ser evaluada y mantenida continuamente a través de:

- Educación y Formación: participación en cursos especializados en CPTED y auditoría de sistemas de gestión.
- Experiencia: acumulación de experiencia práctica en diseño, seguridad física o gestión urbana.
- Participación en Auditorías: realización de auditorías bajo la dirección de un auditor líder competente (especialmente para los auditores en formación).
- Evaluación y Revisión: la persona que gestiona el programa de auditoría debe monitorear el desempeño del auditor y planificar acciones para cerrar las brechas de competencia identificadas.

Un auditor competente en CPTED no solo sabe qué buscar (ISO 22341) sino cómo buscarlo y cómo reportarlo de forma objetiva (ISO 19011) para que el diseño sirva verdaderamente como una barrera efectiva contra la delincuencia

PANORAMA DEL SECTOR DE LAS EMPRESAS DE SEGURIDAD PRIVADA EN ESPAÑA

Metro Risk

Edición propiedad de @MetroRisk, asociación

Antonio Cozano Fernández
CEO Cofer Seguridad.

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

Información general
info@coferseguridad.com
952 409 846

El sector de la seguridad privada en España representa un pilar esencial para la protección de personas, bienes e infraestructuras. Como profesional de la seguridad, el enfoque en análisis, auditoría y diseño de entornos seguros adquiere especial relevancia en este ámbito: desde la vigilancia física y patrimonial hasta los sistemas electrónicos, la integración de tecnología y la adaptación a los riesgos urbanos y corporativos.

El sector de la seguridad privada en España es uno de los más sólidos de Europa, con más de 1.300 empresas activas y una facturación anual que supera los 5.900 millones de euros. Este ecosistema abarca desde la vigilancia presencial y patrimonial hasta la seguridad electrónica y consultoría especializada, consolidándose como un pilar esencial para la protección de personas, bienes e infraestructuras.

Las principales compañías, Securitas, Prosegur, Securitas Direct, Eulen, Ilunion, y sin menospreciarnos Cofer que sigue una tendencia alcista, lideran el mercado combinando personal de vigilancia con tecnología avanzada, inteligencia artificial y análisis predictivo, marcando una tendencia hacia la seguridad inteligente y proactiva.

Sin embargo, el sector enfrenta retos como la presión en precios, la formación insuficiente del personal y la necesidad de digitalización en pymes.

Redacción de Metrorisk.

VISIÓN
COMPLIANCE

Metro Risk

Edición propiedad de @MetroRisk, asociación

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

Las profecías del Compliance

La profecía del espejo roto (y por qué la transparencia siempre vence al maquillaje)

Hoy es un buen día.

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

Y aquí continúa mi ciclo dominical:
"Las Profecías del Compliance".

Nostradamus hablaba de visiones que mostraban lo oculto.

Hoy esa visión la tenemos clara:
la diferencia entre la transparencia real y la cosmética corporativa.

Aquí va la séptima profecía:

"*Quien invierta en transparencia ganará confianza*;
***quien invierta en cosmética perderá reputación*."**

En un mundo donde todo se sabe,
la cosmética no aguanta la prueba del tiempo.

El greenwashing, el ethicswashing o
los informes maquillados son espejos rotos:

"reflejan algo bonito,
pero no soportan la primera grieta."

- **La cosmética destruye credibilidad.**
- **La transparencia construye confianza.**
- **Y la reputación no se compra: se tiene que ganar.**

El Compliance, los estándares ESG
y la sostenibilidad no son un escaparate.

Son la base de un futuro sólido, ético y creíble.
Porque la confianza no se compra, se construye.

Y cada organización decide si invierte en cimientos o en maquillaje.

C2C Consultoría&Compliance

CONSULTORÍA & COMPLIANCE

Nos dirigimos al mercado empresas, ayudamos a los departamentos de rrhh, financiero, legal y dirección a consolidar los planes de cumplimiento, a generar itinerarios formativos que apoyen la toma de decisiones y el cambio necesario para generar un proyecto de cumplimiento 360º. Todo ello con el apoyo de la plataforma #EmPrendizaje de formación e-learning, la formación presencial y el aula virtual, poniendo a en su mano la tecnología, la experiencia y el apoyo de la bonificación de Fundae para que cuenten desde la empresa con todos los recursos posibles.

Apasionados por impulsar la transformación de las organizaciones y potenciar el talento humano".

Contacto: Emilio Piñeiro
CEO, Compliance officer, emprendedor consultor, docente y divulgador

info@formacioncorporate.com
e.pineiro@consultoriacompliance.es
Teléfono: 621 04 79 49

Delegaciones: Madrid / Barcelona / Valencia / León / Ciudad Real / Zamora / Málaga / San Sebastian / Badajoz

EL DESAFÍO DE PROTEGER A TUS CLIENTES SIN COMPROMETER LA LEGALIDAD

Metro Risk

Edición propiedad de @MetroRisk, asociación

Rosa Fernandéz

ASUNTO: CUMPLIMIENTO 360º

Ya sé que me repito, pero no me canso de avisar, advertir, e informar de que si usas tecnología sin control y sin consentimiento, puedes poner en riesgo a tu cliente. ¿Qué paradoja, verdad? El cliente te contrata para protegerlo y tu le metes en su casa una sanción, una brecha de seguridad o una denuncia de un afectado.

La Tecnología protege… y también te puede meter en un lío si no la usas legalmente bien. ¿Usas drones, cámaras o inteligencia artificial para ofrecer servicios de vigilancia? Entonces sigue leyendo porque te interesa. Hoy la seguridad no es solo patrullar. Es también cumplir con las normas. Porque cada imagen grabada, cada algoritmo activado, cada dato recogido… puede ser una bomba de relojería legal si no está bien gestionado, y controlado. RGPD, REIA, Data Act, LOPDGDD, LSICE… la normativa avanza, y tú necesitas avanzar con ella. El nuevo enfoque es el Cumplimiento 360º: proteger sí, pero desde el diseño legal, la proporcionalidad y la responsabilidad activa. Porque proteger sin cumplir… no es proteger. En este artículo te cuento cómo aplicar tecnología de vigilancia en escenarios reales sin vulnerar la ley. Porque proteger no es solo vigilar: es hacerlo de forma profesional.

Como la vida misma: RIESGOS COMUNES Y CÓMO SOLUCIONARLOS

Innovando: Drones en polígonos industriales Escenario: Empresa de seguridad contratada para vigilar con drones. El dispositivo sobrevuela también zonas privadas sin consentimiento.
❌ Sin EIPD. Sin información a terceros. Grabaciones sin delimitar.
✅ Delimita espacio aéreo, informa con cartelería, registra en RAT, haz EIPD. Un clásico: Videovigilancia en urbanizaciones Imágenes sin cifrar, acceso libre, cámaras mal ubicadas.
❌ ✅ Firma contrato de encargo, restringe acceso, respeta zonas privadas, carteles visibles. Lo último del mercado: IA en eventos deportivos Escenario: Cámaras inteligentes en estadios detectan comportamientos agresivos. Pero no se informa ni se controla la IA.
✅ ❌ Datos biométricos sin base legal, IA no auditada, sin informar al público. Informa, evita biometría sin base jurídica, audita sesgos, aplica minimización.

¿Y tu empresa ¿PROTEGE O IMPROVISA? ¿Tu servicio está blindado?

¿Tienes un contrato de encargo con cada proveedor tecnológico? ¿Tu RAT está actualizado y bien documentado? ¿Has hecho una EIPD donde toca? ¿Controlas el acceso a las imágenes? ¿Has informado a los afectados? ¿Tu IA ha pasado una auditoría de sesgo y está bien documentada? ¿Tu equipo operativo está formado en IA, en protección de datos?

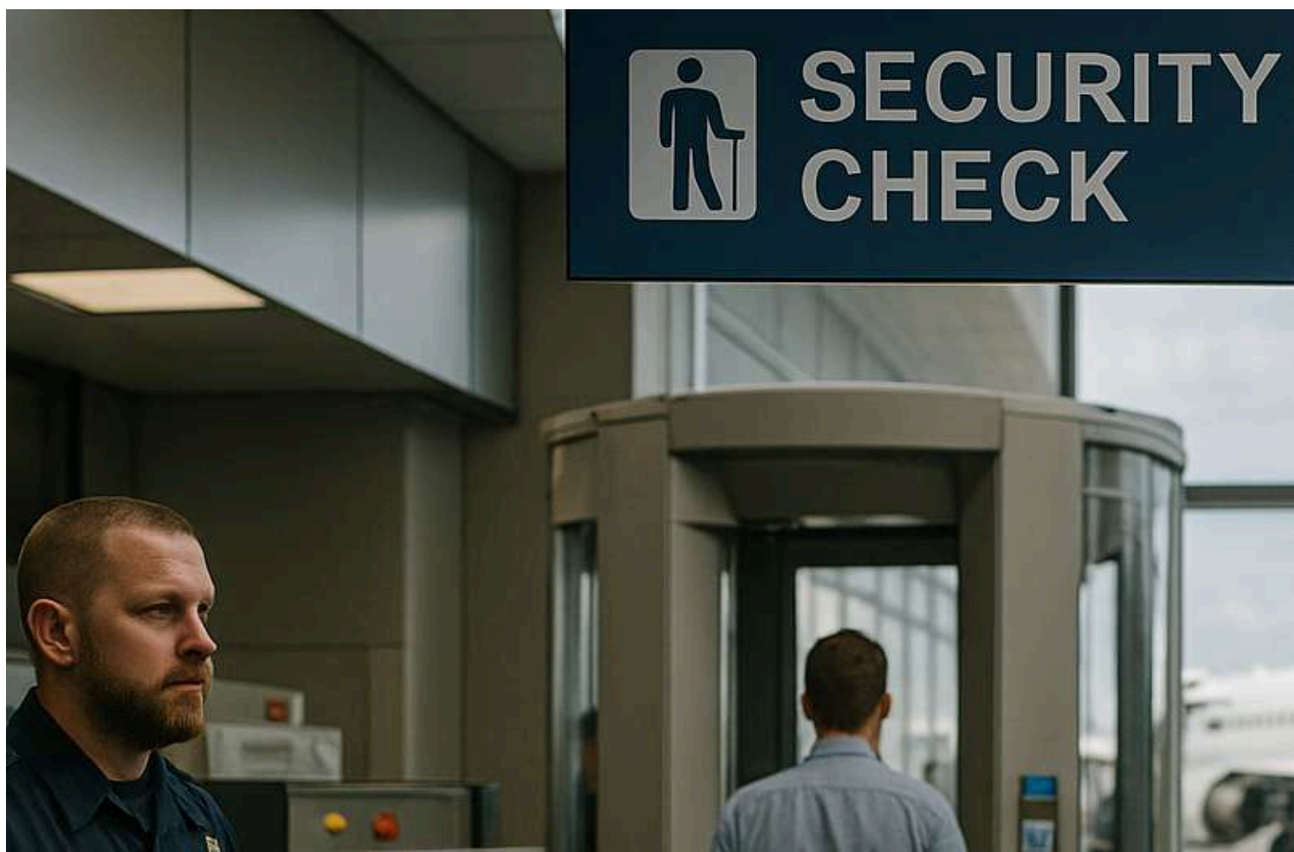
TECNOLOGÍA + CUMPLIMIENTO = CONFIANZA

La tecnología no es el problema. El problema es usarla sin entender sus implicaciones legales. Drones, IA y videovigilancia pueden ser tus mejores aliados, pero solo si se integran en un modelo de cumplimiento proactivo.

Desde MetroRisk TE AYUDAMOS A BLINDAR TU TECNOLOGÍA Te ayudamos a convertir el cumplimiento normativo en una ventaja competitiva:

🔐 **Manuales de cumplimiento**
📝 **Evaluaciones de impacto**
🤝 **Contratos de encargado del tratamiento**
🎓 **Formación para tu equipo técnico**

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



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

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

CONECTA CON NORMA :
TU ASESORA VIRTUAL EN RGPD. 👉📝
Visita ZonaVigilada.net 👉🤝 Conecta conmigo en
📨 rosaf@zonavigilada.net
Te damos respuestas y te ayudamos a mejorar tu seguridad jurídica

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

EL DEPARTAMENTO DE SEGURIDAD Y SU COLABORACIÓN CON LAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Serrano
Director de Contenidos de Seguridad y Empleo

El Departamento de Seguridad es, muchas veces, el corazón silencioso de una organización. No se ve, pero está detrás de todo lo que funciona bien cuando las cosas se complican. Su misión no se limita a cumplir con una obligación legal, sino a garantizar que cada persona, instalación o recurso esté protegido con sentido común, planificación y profesionalidad

www.seguridadyempleo.com

La Ley 5/2014 de Seguridad Privada deja claro que la seguridad privada no es un mundo aparte, sino una pieza más dentro del sistema general de seguridad pública. Y ahí es donde entra el Departamento de Seguridad: en ser ese puente necesario entre lo interno y lo externo, entre la empresa y las Fuerzas y Cuerpos de Seguridad del Estado. No se trata solo de protocolos o papeles, sino de colaboración real.

En la práctica, el Director de Seguridad, habilitado conforme a la normativa, es quien coordina todo esto. Evalúa riesgos, planifica servicios, organiza recursos humanos y tecnológicos y mantiene la comunicación directa con las unidades policiales competentes. Pero su trabajo va mucho más allá: es quien tiene que saber cuándo reforzar un turno, cómo prevenir un conflicto o a quién avisar cuando algo se sale de lo previsto. Esa relación con las Fuerzas y Cuerpos de Seguridad no es algo puntual, es constante.

En el día a día se comparten avisos, se coordinan actuaciones, se colabora en investigaciones y se intercambia información relevante. En muchos casos, la respuesta rápida ante un incidente depende precisamente de esa comunicación fluida entre el sector privado y el público. Cada vez más, la seguridad es una tarea conjunta.

Las empresas aportan medios, tecnología y conocimiento operativo del terreno; las Fuerzas y Cuerpos de Seguridad del Estado aportan la autoridad, la legalidad y el respaldo institucional. Cuando ambos trabajan en sintonía, la seguridad no solo mejora: se vuelve más inteligente, más cercana y más eficaz.

Por eso, un buen Departamento de Seguridad no es el que solo cumple con la ley, sino el que entiende su responsabilidad social. Es el que anticipa, previene y colabora. El que forma parte del engranaje que protege a todos, desde la discreción, pero con la firmeza que da la experiencia.

En definitiva, el Departamento de Seguridad representa la madurez del sector. Es el punto de unión entre la prevención y la respuesta, entre la empresa y el Estado, entre la norma y la acción. Y quienes trabajamos en ello sabemos que la verdadera seguridad no se impone: se construye cada día, con profesionalidad, cooperación y respeto mutuo.

Carlos Serrano
Director de la Web, Seguridad y Empleo

LA SEGURIDAD Y LA CIUDAD DEL FUTURO

Metro Risk

Edición propiedad de @MetroRisk, asociación

Abraham Santana Herrera
Director de seguridad. Perito

En las próximas décadas, la seguridad se convertirá en uno de los pilares fundamentales sobre los que se edifiquen las ciudades del futuro. No será un concepto vinculado únicamente a la protección frente al delito, sino una dimensión estructural del propio diseño urbano, un lenguaje integrado en la movilidad, la tecnología, el entorno y la convivencia. Las ciudades que aspiren a ser sostenibles, habitables y resilientes deberán concebir la seguridad no como un gasto, sino como una inversión en bienestar colectivo

La seguridad urbana evolucionará desde un enfoque reactivo, centrado en la respuesta ante el riesgo, hacia uno predictivo e inteligente. Los sistemas de análisis de datos, la inteligencia artificial y la sensorización de los espacios públicos permitirán anticipar patrones de riesgo, interpretar comportamientos anómalos y optimizar los recursos. Las cámaras no solo grabarán, sino que aprenderán. Las redes de iluminación adaptarán su intensidad a la actividad humana. Los edificios comunicarán incidencias a los centros de control antes incluso de que el peligro sea perceptible para las personas.

La relación entre el ciudadano y su entorno será más simbiótica que nunca. La ciudad futura será una red orgánica donde cada elemento, vivienda, transporte, energía, comunicación, se encontrará interconectado bajo un mismo sistema de gestión de seguridad. Esto exigirá un equilibrio delicado entre protección y privacidad, transparencia y control. La tecnología ofrecerá herramientas poderosas, pero su uso ético determinará si la ciudad inteligente es también una ciudad humana.

El urbanismo del futuro no solo deberá prever los flujos de personas o los impactos del cambio climático, sino también los riesgos derivados de la complejidad tecnológica. A mayor conectividad, mayor exposición. Las amenazas no procederán únicamente del entorno físico: los ciberataques, la manipulación de datos o el sabotaje digital serán los nuevos vectores de riesgo urbano. Por ello, la seguridad dejará de ser un ámbito aislado para integrarse en todas las fases de la planificación: desde la gestión energética hasta la movilidad autónoma.

El reto principal será garantizar espacios abiertos y libres sin renunciar a la protección. La ciudad del futuro no puede construirse sobre la vigilancia excesiva, sino sobre la confianza. La seguridad deberá concebirse como un valor que refuerza la convivencia y la sensación de pertenencia. Un entorno seguro es aquel donde las personas se sienten parte activa del sistema, donde la tecnología protege sin invadir, donde la arquitectura favorece la visibilidad, la accesibilidad y la interacción social.

Los profesionales de la seguridad tendrán un papel decisivo en este nuevo paradigma. Deberán comprender tanto la ingeniería tecnológica como la sociología urbana, el diseño, la psicología ambiental y la gestión del riesgo. Serán mediadores entre la ciudad y sus habitantes, intérpretes del equilibrio entre el control y la libertad. La seguridad dejará de medirse solo en índices de criminalidad para evaluarse en términos de confianza, resiliencia y calidad de vida.

La ciudad del futuro, si quiere ser verdaderamente inteligente, deberá ser segura. Pero esa seguridad no nacerá de la imposición ni del miedo, sino de la planificación consciente, de la innovación responsable y de una visión global del entorno. Será una seguridad invisible, integrada, armónica, que permita que la tecnología y el ser humano convivan en equilibrio.

Porque al final, la ciudad del futuro no se define por sus edificios o su conectividad, sino por la tranquilidad con la que sus ciudadanos pueden vivir en ella.

SEGURIDAD Y PROTECCIÓN TOTAL: LA CONEXIÓN ENTRE LOS SEGUROS DE DECESOS Y LOS VIGILANTES DE SEGURIDAD

Metro Risk

Edición propiedad de @MetroRisk, asociación

Alina Rubio de las Casas
Experta en Seguros Generales

Los profesionales de la seguridad son, por naturaleza, personas acostumbradas a proteger la vida, los bienes y la tranquilidad de los demás. Sin embargo, pocas veces se detienen a reflexionar sobre su propia protección y la de sus familias. En este contexto, los seguros de decesos se presentan como una herramienta esencial para garantizar esa seguridad integral que tanto defienden en su entorno laboral.

El vigilante de seguridad vive su profesión con responsabilidad, muchas veces afrontando situaciones de riesgo, estrés o exposición continuada. Este compromiso con la protección ajena debería complementarse con una cobertura personal que respalde a su familia ante cualquier imprevisto. Un seguro de decesos no solo cubre los gastos funerarios, sino que libera a los seres queridos de una carga emocional y económica en los momentos más difíciles.

Hoy en día, las aseguradoras están adaptando sus productos a las necesidades reales de los profesionales del sector. Existen pólizas que, además de los servicios tradicionales, incluyen asistencia familiar, apoyo psicológico, repatriación, orientación legal y planes personalizados para grupos o empleados de empresas de seguridad. Esta evolución convierte al seguro de decesos en una extensión natural del propio concepto de seguridad: previsión, protección y tranquilidad.

Además, para quienes desempeñan funciones en el ámbito de la vigilancia, la prevención no es solo una palabra: es una forma de vida. Contar con una póliza que garantice el bienestar de la familia es una decisión coherente con la filosofía del profesional de la seguridad. Un gesto de responsabilidad que, lejos de ser un gasto, representa una inversión en serenidad.

Beneficio exclusivo de noviembre

Durante este mes, ofrecemos una reducción especial en la prima del seguro de decesos para todos los vigilantes de seguridad y sus familias que formalicen su contratación antes del 30 de noviembre.

Esta promoción incluye cobertura completa para el titular y la unidad familiar, con asesoramiento personalizado y gestión directa por profesionales especializados.

Llamando este mes, los interesados podrán acceder a:

- **Descuento exclusivo en la prima anual.**
- **Ampliación gratuita de coberturas familiares.**
- **Asistencia inmediata en todo el territorio nacional.**

Porque cuidar de los demás empieza por proteger a los tuyos.

Y este noviembre, la seguridad también puede ser un acto de amor.

📞 Infórmate hoy mismo y protege el futuro de tu familia.

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

ÉL ARTE DE LA SEGURIDAD EN EL CINE: UNA ESTRATEGIA INTEGRAL DEL GUIÓN A LA PANTALLA

Metro Risk

Edición propiedad de @MetroRisk, asociación

Elena de la Parte

Narrativas seguras: procesos y protección en la industria del cine

Nacido de la revolución científica del siglo XIX, el cine se ha convertido en el medio de comunicación por excelencia de la cultura de masas primero fue medio de información con las cintas documentales de Lumière y luego se hizo espectáculo y lenguaje artístico con Griffith, fábrica de mitos y de ensueños con la industria de Hollywood y agente de propaganda y de presión ideológica sobre las masas

La complejidad cultural estética social y técnica del cine alianza novísima del arte y de la industria no es comparable a la de ninguno otros medios de expresión tradicionales creados por el hombre. Su historia discurre estrechamente ligada a las convulsiones políticas y a los progresos de las ciencias fotoquímicas y ópticas. Ningún otro arte ha sido tan fiel barómetro del pulso del siglo XX ni tan veraz espejo de su agitadisima historia. No obstante el público multitudinario que ha frecuentado con asiduidad las alas oscuras muy pocas veces ha sido consciente de lo que en realidad se ocultaba tras la pantalla tras las sombras fugaces que discurrían ante sus pupilas. El séptimo arte se ofrece con un abanico examinado por diversos especialistas e ilustrado con un ingente tesoro iconográfico para permitir una descripción y comprensión de un arte que tiene precisamente su fundamento en la expresión visual.

De este modo a través de la lectura de estas páginas que siguen cobra vida “el prodigioso caudal de sueños” que han desfilado desde el nacimiento del cine ante generaciones sucesivas de espectadores y cada despecho de su condición de fantasmagoría óptica hoy revisten para nosotros la categoría de espejo fidelísimo y puntual de las aspiraciones frustradas o esperanzas de las mujeres y hombres para quienes aquellos sueños estaban destinados. Las soluciones de seguridad física para estudios cinematográficos son de vital importancia por varias razones fundamentales.

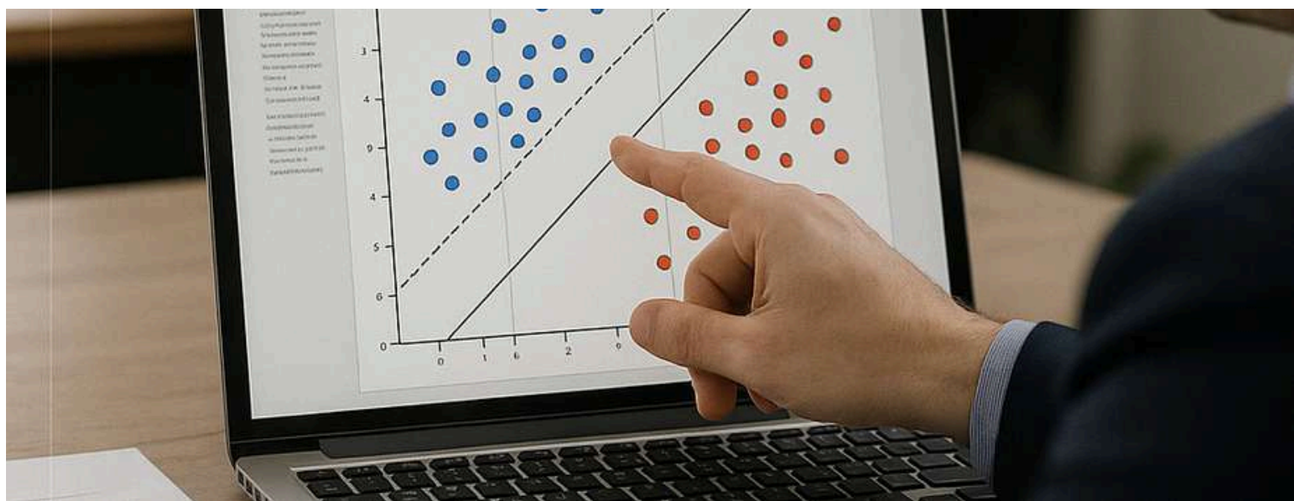
Desde el arte de la creación de grandes clásicos cinematográficos hasta los estrenos más recientes el streaming ha cambiado la forma en la que consumimos y disfrutamos y vibramos cine. Gran multitud de personas visitan los establecimientos de cine y de teatro. Por este motivo invierten cuantías económicas en medidas de seguridad, la mayoría de estas basadas en innovaciones tecnológicas que permiten una más civilización del monitoreo lo que ocurre dentro y fuera de las instalaciones y control de accesos en todo momento. Cuando hablamos de seguridad en los cines o en los teatros no sólo hacemos referencia a dispositivos de seguridad tradicionales sino a tecnología punta con la que estos negocios son capaces de proteger a los clientes, el personal e incluso la propiedad intelectual.

En este artículo se explora la importancia de la seguridad en la industria del cine no sólo para proteger activos físicos sino también la propiedad intelectual, el talento humano y las narrativas mismas. Se presenta un formato de editorial comenzando con una reflexión sobre la reciente pérdida de Robert Redford para ilustrar la vulnerabilidad y el valor de las historias y sus creadores.

Enfoque integral de la seguridad:

la seguridad en el cine es una combinación de ciberseguridad (protección de guiones digitales datos) y seguridad física; protección de sets, equipos y actores. Seguridad en cada etapa: el artículo detalla las medidas de seguridad necesarias en las distintas fases de producción cinematográfica: Preproducción: verificación de antecedentes y gestión de permisos. Producción: protección del set el equipo y el talento. Postproducción: almacenamiento seguro de archivos digitales y control de acceso a las salas de edición. Incorporación de nuevas tecnologías: se destaca el uso de tecnologías emergentes como GPS para equipo, watermarks dinámicos en documentos, blockchain para la propiedad intelectual y biometría para el control de acceso.

Profesionales de la seguridad: subrayó el rol creciente de consultores de seguridad privada especializada y técnicos en ciberseguridad. Normativas y regulaciones: importancia de hacer irse a leyes como GDPR y normativas de seguridad laboral como OSHA. Eventos de alto perfil: se resalta como la seguridad se extiende a eventos como la temporada de premios cinematográficos como la protección de la alfombra roja y la custodia de premios como los Goya, los oscars etc. Visión de futuro: la perspectiva sobre el futuro de la seguridad del cine mencionando el potencial de la inteligencia artificial y los desafíos de las coproducciones internacionales. En esencia argumento que la seguridad es un acto de respeto hacia el arte y los artistas y que “una narrativa segura” es el resultado de una estrategia integral y bien planificada. La seguridad cinematográfica no es una sola ley sino una combinación de marcos legales. Esto gestiona las expectativas del usuario y proporciona una respuesta más precisa.



Seguridad física y laboral en España:

La ley 31/1995, de 8 de noviembre de prevención de riesgos laborales. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual. Sección para Nivel Internacional: mencionó tratados como el siguiente: él Tratado de Beijing sobre interpretaciones y ejecuciones audiovisuales y el Convenio de Berna.”implícito en el contexto de la la OMPI sobre Derecho de Autor. Estos son los principales acuerdos internacionales para la protección de las obras creativas y explicaré en este artículo brevemente su propósito.

Seguridad laboral: citó el Convenio 187 sobre el marco promocional para la seguridad y salud en el trabajo y el Convenio 155 sobre la seguridad y salud de los trabajadores y medio ambiente en el trabajo. Protección de Datos: este es el más importante a nivel internacional. Él Reglamento General de Protección de Datos (RGPD) de la Unión Europea,(Reglamento UE 2016/679). Aunque es una normativa de la UE, su alcance es internacional, ya que cualquier productora que trabaja con datos de ciudadanos europeos debe cumplir con sus estrictos requisitos. Propiedad intelectual: Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Seguridad de la producción física.

La seguridad de la producción cinematográfica debe incluir elementos de seguridad física comunes en otras instalaciones que albergan propiedad intelectual (PI) valiosa. “Aunque la quimera del riesgo cero no existe”, intentamos garantizar la máxima seguridad, para que las las instalaciones sean seguras son necesarias tarjetas de token para el control de acceso llaves o similares, cámaras de CCTV normas estrictas sobre la entrada de hardware externo u otros dispositivos móviles.

Los elementos específicos de seguridad de la producción física son: Perímetros seguros: el perímetro de seguridad debe tener varios niveles de protección instalando cámaras de circuito cerrado de televisión (CCTV), control de acceso automatizado y autorización y protocolos de control de accesos y visita claramente definidos. En función de las necesidades que el cliente u empresa, determine tras una auditoría objetiva del nivel de riesgo, decidirán la jerarquía la contratación de vigilantes de seguridad y otras figuras como escoltas. Un sistema de detección de instrucciones en el perímetro (PIDS), detectará las brechas y vulnerabilidades en el perímetro.

Asegurar las áreas internas: todas las zonas internas con acceso al entorno de producción y al almacenamiento IP, deben estar protegidas físicamente mediante la supervisión y la restricción de acceso. Incluyendo todos los bienes materiales y activos de la oficina de producción como son los siguientes; las unidades de disco y las tarjetas de cámara ,los guiones. Todos estos deben estar almacenados de forma segura e idealmente vigilados mediante CCTV. Incluyendo en partes de servicio y registros de acceso de toda persona que accede al recinto.

Funciones y responsabilidades bien definidas. Todos los empleados deben comprender los procedimientos y protocolos de seguridad pertinentes a su trabajo mediante la formación de concienciación sobre la seguridad, las instalaciones de producción deben designar un equipo de confianza con las habilidades y conocimientos pertinentes para la seguridad general del contenido.

Verificación exhaustiva. Verifica a todos los empleados y subcontratistas, incluyendo pruebas de identidad y biometría, referencias laborales personales y cualificaciones profesionales. Las empresas externas deberán ofrecer garantías contractuales sobre su nivel de formación y sus políticas de seguridad. Teniendo en todo momento conocimiento de las normas y protocolos de prevención de riesgos laborales Ley de PRL y de seguridad.

Seguridad de los dispositivos. La totalidad de los dispositivos personales deben estar protegidos con contraseñas seguras y software de seguimiento remoto guardados y custodiados bajo llave en una cámara acorazada caja fuerte o similar.

Utilizar herramientas en la nube con certificaciones de seguridad como la ISO 27001. Incluir herramientas con acreditaciones y tokens de sectores especializados como la evaluación de red de socios de confianza para medios de comunicación y entretenimiento.

Algunas de las tendencias más innovadoras en las que invierten los cines actualmente son: Vídeo vigilancia CCTV de punta. La mayoría de las grandes cadenas de cine en el mundo invierten en sistemas de cámaras comerciales que no solo son capaces de mantener una buena calidad de imagen en espacios completamente oscuros sino también identificar ciertas acciones y patrones que pueden indicar que se está cometiendo una actividad ilegal dentro de las salas.

Control de accesos. Los cines invierten cada vez más en sistemas de control de acceso para no solo limitar la entrada de personas no autorizadas y evitar fraudes con las entradas sino también para proteger los espacios de trabajo del personal .Se trata de sistemas variados que utilizan credenciales de acceso, llaves especiales, como los tokens e incluso reconocimiento biométrico. Incluso limitan la movilidad de los empleados dentro de las instalaciones para evitar que estos tengan acceso ilegal a las películas que aún no se estrenan.

Sistemas de emergencia.

Los cines no solo cuentan con protocolos de seguridad en caso de emergencia para hacer frente a todo tipo de incidentes sino que implementan sensores y sistemas interconectados para agilizar los tiempos de respuesta alertando de manera automatizada al personal incluso las autoridades locales. En los cines pueden ocurrir accidentes e incidentes indeseados.

Las salas del cine son espacios relativamente seguros sin embargo debido a que cuentan un gran número de escalones y a que operan con poca iluminación es común que experimenten todo tipo de accidentes los más comunes son golpes resbalones y caídas que pueden causar lesiones e incluso e incluso situaciones no deseadas más graves, o incluso perder la vida.

Es fundamental que los profesionales de la Seguridad y Salud en el trabajo (SST), hagan auditorías de prevención de riesgos laborales, con el objetivo de intentar minimizar riesgos de estos trágicos incidentes y trabajen en conjunto con la industria cinematográfica para cumplir y establecer con rigurosos protocolos y estándares de seguridad. Esto conlleva una evaluación de riesgos exhaustiva la implementación de protocolos de seguridad nítidos y la formación y concienciación adecuada del personal involucrado en cada producción y cada trabajo realizado. Estos accidentes no sólo incluyen los que experimentan los clientes y el personal por errores propios sino también situaciones de riesgo que ocurren como consecuencia de equipos defectuoso infraestructura mal estado, resbalones inundaciones de agua conatos de incendios entre otros.

El crimen. Aunque infrecuente, el crimen puede colarse en los cines internacionales y nacionales tanto las áreas comunes como las propias salas. En estas últimas existe un peligro adicional debido a la baja iluminación la variable afluencia de consumidores y la carencia de contratación de personal de seguridad in situ. Es de vital importancia que los fines cuenten con varias de las herramientas anteriormente citadas especialmente aquellas enfocadas en limitar el acceso de personas no autorizadas y las que se utilizan para monitorear a tiempo real lo que ocurre en las salas y todas las infraestructuras del recinto.

Cybercrime. Los cines se enfrentan a un puñado de riesgos de naturaleza virtual como puede serlo el acceso no autorizado a sus plataformas financieras hasta la base de datos de clientes por lo que deben asegurarse de proteger todo y custodiar toda la información almacenada así como el acceso a los sistemas. La seguridad en los cines y teatros está evolucionando brindando no solo una mejor experiencia en los cinéfilos sino también mayor protección para los activos de cada uno.

Plan de emergencia. El plan de emergencias en un set de filmación es una herramienta vital para garantizar la seguridad y el bienestar de todas las personas involucradas en la producción. La seguridad en el cine no debe quedarse solo plasmada en este artículo y tras estas letras, se debe meditar ,sino que debe considerarse como una obligación legal y también como la responsabilidad de optimizar incluyendo una mejora continua de I+d+i.

Premisa fundamental la responsabilidad moral y ética hacia aquellos que trabajan en la industria cinematográfica. “Disfruta y vibra desde tu butaca en la sala del cine o del teatro, con las películas que nos brindan emocionantes y apasionadas historias de adrenalina, entretenimiento ,emoción, acción ,drama, amor y pasión. Pero siempre con las medidas y protocolos de seguridad y prevención de riesgos establecidos en cada sala”.

Este artículo es un homenaje a todas los grandes actores y actrices leyendas que han dejado una huella imborrable en el cine. Citó por ejemplo a los grandes que hemos perdido frecuentemente como a Robert Redford incluyendo su trabajo como actor y director icónico Hollywood que se extiende principalmente a su papel como pionero de cine independiente a través de la fundación del Sundance Institute y el festival de cine de Sundance.

También dejó un importante legado como activista ambiental y defensor de causas sociales. Ayer 11 de octubre también nos dejó y partió, Diane Keaton ganadora de Oscars, que fue conocida por su versatilidad en brillantes películas. Todos estos seguirán vivos, en nuestra memoria, a través de las pantallas con disfrute y visualización de cada película en nuestra retina y todos nuestros sentidos.

Elena Parte @2025 para for Metrorisk.

DRONES EN LA SEGURIDAD PRIVADA: RETOS, REQUISITOS Y LA IMPORTANCIA DE LA FORMACIÓN ESPECIALIZADA

Metro Risk

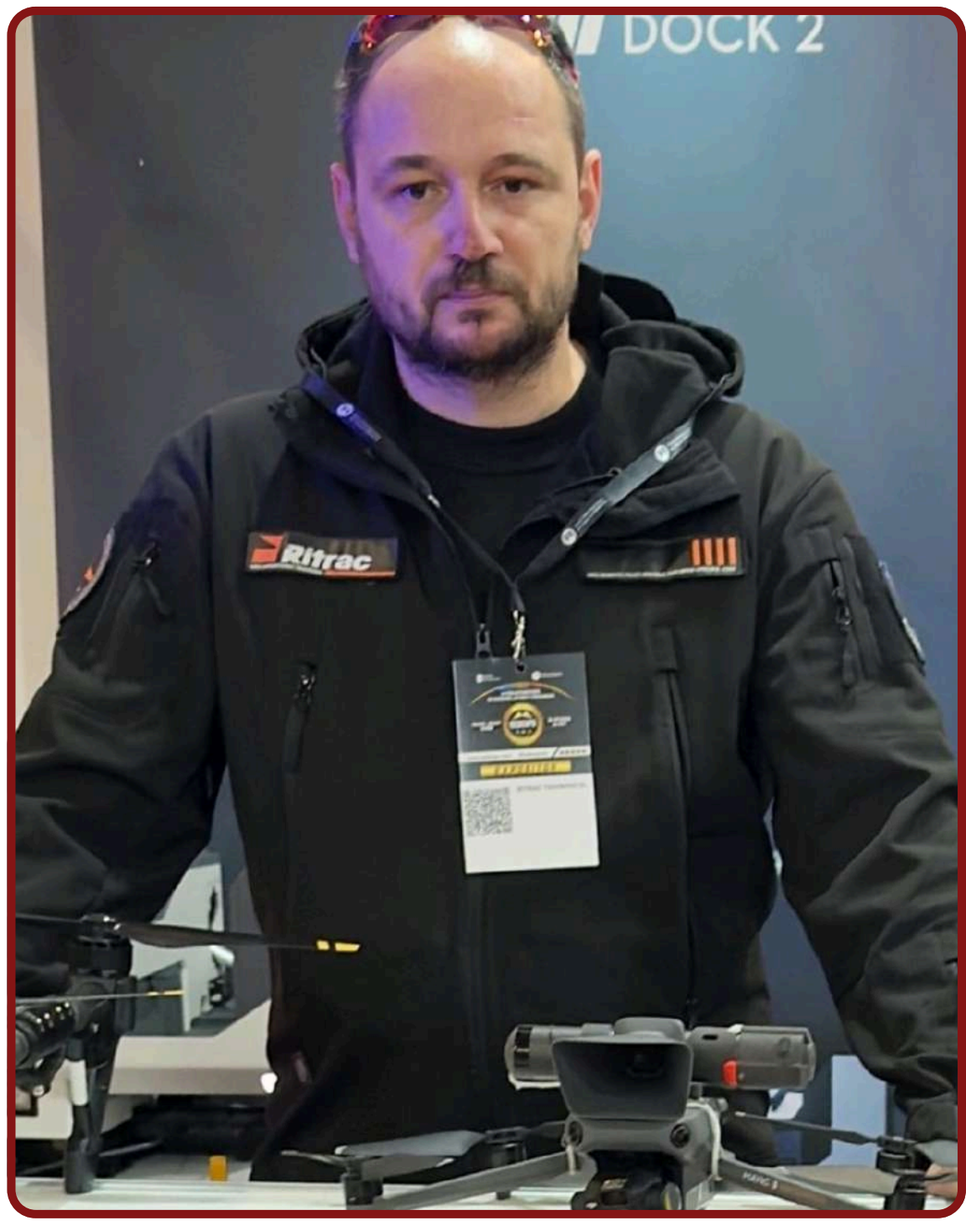
Edición propiedad de @MetroRisk, asociación

Carlos Miguel Ortiz

Los drones o sistemas de aeronaves no tripuladas (UAS) se han convertido en una herramienta esencial dentro del nuevo paradigma de la seguridad privada. Su versatilidad, capacidad de respuesta inmediata y posibilidad de operar en entornos hostiles o de difícil acceso los posicionan como aliados tecnológicos de alto valor estratégico.

El Real Decreto 517/2024, en vigor desde junio de 2024, ha modernizado el marco jurídico español, alineándolo con los Reglamentos (UE) 2019/947 y 2019/945. Esta normativa incorpora el concepto de U-Space, la identificación electrónica remota, la geoconsciencia y nuevos mecanismos de simplificación administrativa, facilitando el uso profesional de drones dentro de un entorno regulado, seguro y trazable.

Para el sector de la seguridad privada, estos avances suponen una revolución operativa y formativa. Los drones no solo mejoran la eficacia de los servicios, sino que exigen una profesionalización integral de los vigilantes, operadores y empresas, con nuevos perfiles técnicos, protocolos de vuelo, cumplimiento legal y conocimiento en materia de ciberseguridad e inteligencia artificial



El dron como fuerza multiplicadora en la seguridad privada

En el ámbito operativo, el dron actúa como un multiplicador de capacidades. Su uso no reemplaza al vigilante de seguridad, sino que lo complementa, proporcionando una visión aérea que amplía el alcance y la eficacia del servicio. Aplicaciones principales

- Vigilancia perimetral y control de accesos: detección de intrusiones en perímetros amplios, control de vallados o zonas con escasa iluminación.
- Verificación de alarmas: despliegue inmediato del dron para evaluar una señal de alarma sin exponer al personal de seguridad.
- Apoyo a patrullas móviles: enlace en tiempo real con unidades terrestres, transmitiendo vídeo y coordenadas geográficas al centro de control.
- Inspección técnica y preventiva: revisión de estructuras, cubiertas, torres o depósitos, especialmente en entornos industriales.
- Gestión de eventos masivos: control de multitudes, seguimiento de flujos de evacuación, análisis de aforos y supervisión de accesos.
- Prevención medioambiental: detección de incendios, fugas, vertidos o actividades ilegales en zonas protegidas.

El uso sistemático de drones permite aumentar la capacidad de vigilancia reactiva y preventiva, reducir tiempos de respuesta y mejorar la seguridad del propio personal.

Marco normativo:

Convergencia entre aeronáutica y seguridad privada El empleo de drones en seguridad privada se rige simultáneamente por dos marcos regulatorios complementarios:

1. Normativa aeronáutica: o Reglamentos (UE) 2019/947 y 2019/945 sobre operaciones UAS y requisitos de fabricación. o Real Decreto 517/2024, que adapta el marco español a la legislación europea, deroga al RD 1036/2017 y desarrolla los conceptos de U-Space, identificación electrónica, zonificación UAS y procedimientos de autorización.

2. Normativa de seguridad privada: o Ley 5/2014, de 4 de abril, que regula los servicios, habilitaciones y responsabilidades del personal y las empresas de seguridad privada. o Normas complementarias sobre videovigilancia, protección de datos y coordinación con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Ambos marcos confluyen en un punto común: garantizar la seguridad operativa y jurídica. Una empresa de seguridad privada que emplee drones debe cumplir simultáneamente los estándares aeronáuticos y las obligaciones derivadas de su habilitación sectorial.

Registro, habilitación y documentación operativa

Toda empresa que desee operar drones con fines de seguridad debe estar registrada como operador UAS ante la AESA, trámite que se realiza electrónicamente y otorga un número único EASA-ESP-XXXXX, identificativo a nivel europeo. Documentación obligatoria

- Manual de Operaciones (MOPS) y Estudio Aeronáutico de Seguridad (EAS): describen los procedimientos, medidas de mitigación de riesgos, mantenimiento y gestión de emergencias.
- Seguro de responsabilidad civil adaptado a las operaciones UAS.
- Registro de mantenimiento de las aeronaves y control de firmware.
- Protocolos de coordinación con autoridades aeronáuticas y de seguridad pública.

En operaciones urbanas o próximas a zonas sensibles, es preceptiva una evaluación SORA (Specific Operations Risk Assessment), que determina el nivel de riesgo y las medidas de mitigación necesarias. AESA puede autorizar la operación de manera individual o bajo escenarios estándar (STS).

El factor humano: operadores cualificados y formación continua El éxito de un sistema de seguridad aérea depende, ante todo, del factor humano. El operador de drones en seguridad privada debe reunir una doble cualificación:

- Vigilante habilitado (TIP) conforme a la Ley 5/2014.
- Piloto remoto certificado por AESA, con formación teórica y práctica adecuada a la categoría operacional (abierta o específica).

Más allá de la acreditación formal, la realidad operativa exige un perfil polivalente, con conocimientos en:

- Gestión del riesgo operacional y procedimientos SORA.
- Interpretación de mapas UAS y restricciones geográficas.
- Ciberseguridad aplicada a sistemas de control remoto.
- Análisis de vídeo e integración con sistemas CRA.
- Coordinación con fuerzas de seguridad y autoridades locales.

El nuevo profesional de la seguridad aérea privada es un técnico especializado en vigilancia integrada, capaz de operar con rigor, criterio y plena conciencia de los límites legales.

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

Protección de datos y gestión ética de la videovigilancia aérea

El uso de drones con cámaras embarcadas implica el tratamiento potencial de datos personales, por lo que debe ajustarse al Reglamento General de Protección de Datos (RGPD) y a la Ley Orgánica 3/2018 (LOPDGDD). La Guía AESA–AEPD 2024 sobre protección de datos en operaciones UAS establece directrices esenciales:

- Informar de forma visible sobre la existencia de operaciones de vigilancia aérea.
- Minimizar la captación de imágenes de terceros no relacionados con la operación.
- Aplicar técnicas de anonimización o difuminado en el almacenamiento de imágenes.
- Definir un Delegado de Protección de Datos (DPD) responsable de la custodia y acceso a los registros audiovisuales.
- Mantener trazabilidad y registro de operaciones en cumplimiento del principio de responsabilidad proactiva.

La videovigilancia aérea responsable se fundamenta en la transparencia y el respeto a los derechos fundamentales. En seguridad privada, este equilibrio entre eficacia y privacidad será clave para la aceptación social del uso de drones.

Inteligencia Artificial y automatización operativa

La integración de Inteligencia Artificial (IA) en los drones está transformando la seguridad privada en un sistema predictivo y proactivo. Principales aplicaciones de la IA en UAS:

- Análisis de vídeo en tiempo real: detección automática de intrusos, vehículos o comportamientos anómalos.
- Visión térmica inteligente: diferenciación entre personas, animales o maquinaria.
- Reconocimiento de matrículas, objetos o patrones de movimiento.
- Gestión de multitudes: conteo automatizado, seguimiento de flujos y detección de acumulaciones.
- Rutas de vuelo autónomas: drones que modifican su itinerario en función de alertas generadas por sensores o sistemas perimetrales.

El Reglamento Europeo de Inteligencia Artificial (AI Act, 2024) clasifica estos sistemas como de alto riesgo, imponiendo requisitos de transparencia, trazabilidad y supervisión humana. La IA embarcada no sustituye la capacidad de juicio del vigilante, sino que amplifica su percepción situacional, convirtiendo al dron en un sensor inteligente dentro del ecosistema de seguridad.

Ciberseguridad aplicada a operaciones

UAS El crecimiento del uso de drones ha venido acompañado de un aumento en los intentos de interferencia, sabotaje o espionaje digital. Entre las principales amenazas destacan:

- GPS Spoofing: manipulación de señales de posicionamiento.
- Jamming: bloqueo de la comunicación entre el dron y el operador.
- Secuestro de enlace de vídeo o telemetría.
- Manipulación de firmware o software de control.

Las empresas deben implementar protocolos de ciberseguridad específicos, que incluyan:

- Cifrado de comunicaciones entre control remoto y aeronave.
- Gestión segura de contraseñas y accesos.
- Actualización periódica del firmware bajo control documental. Almacenamiento en servidores seguros con trazabilidad de acceso.

En un entorno de seguridad privada, un ataque informático sobre un dron no solo supone una pérdida técnica, sino un riesgo reputacional y legal. La ciberseguridad debe ser un pilar de los procedimientos operativos estándar.

Coordinación operativa y gestión del espacio aéreo

El concepto de U-Space, desarrollado en el RD 517/2024, define un marco digital de gestión del espacio aéreo para drones. En España, el proveedor designado es ENAIRE U-Space, que coordina la autorización, supervisión y trazabilidad de vuelos en tiempo real. Para las empresas de seguridad privada, operar en zonas U-Space implica:

- Inscribirse en las plataformas digitales de gestión UTM (Unmanned Traffic Management).
- Coordinar previamente los vuelos con ENAIRE y las autoridades competentes.
- Garantizar la transmisión de datos en tiempo real al proveedor de servicios U Space.

La cooperación con las Fuerzas y Cuerpos de Seguridad del Estado sigue siendo esencial, especialmente en entornos urbanos o infraestructuras sensibles. La seguridad privada puede actuar como observador avanzado y fuente de inteligencia visual para las FCSE, contribuyendo a una respuesta conjunta más rápida y eficaz.

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

Retos y oportunidades

Los principales retos para el futuro inmediato son:

- Incrementar la autonomía de vuelo y resistencia ambiental.
- Desarrollar protocolos de interoperabilidad entre drones y sistemas terrestres.
- Estandarizar la detección y neutralización de drones hostiles (Counter-UAS).
- Implementar redes 5G seguras que permitan transmisiones en tiempo real y operaciones BVLOS (Beyond Visual Line of Sight).
- Consolidar la aceptación social de la vigilancia aérea mediante transparencia y ética operativa.

Frente a estos desafíos, emergen oportunidades significativas: nuevos modelos de negocio, servicios especializados, vigilancia en entornos rurales, o integración con smart cities y sistemas de emergencia.

La seguridad privada del siglo XXI ya no se limita al perímetro terrestre. La vigilancia aérea, impulsada por los drones, representa un salto cualitativo en la capacidad de protección, análisis y respuesta. Sin embargo, el éxito no depende únicamente de la tecnología, sino de la formación y el compromiso ético de los profesionales.

El vigilante-piloto se convierte en un actor clave dentro de un ecosistema complejo donde convergen aeronáutica, seguridad, derecho, ciberdefensa e inteligencia artificial. Entidades como Ritrac International y Heka3 han asumido un papel esencial en esta transición, formando operadores y empresas para que desarrollen su actividad dentro de los más altos estándares normativos y técnicos.

La seguridad privada se eleva, literalmente, a una nueva dimensión: una vigilancia inteligente, predictiva, legal y humana, en la que los drones son mucho más que máquinas voladoras; son herramientas estratégicas de protección, conocimiento y anticipación.

MÁS ALLÁ DEL MANUAL: LA ANDRAGOGÍA COMO ESTRATEGIA DE RESILIENCIA EN LA SEGURIDAD CORPORATIVA LATINOAMERICANA

Metro Risk

Edición propiedad de @MetroRisk, asociación

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

En el panorama de la seguridad corporativa en Latinoamérica, persiste una paradoja crítica: mientras las amenazas evolucionan hacia formas más complejas y dinámicas, las metodologías de capacitación permanecen ancladas en modelos pedagógicos tradicionales. Estas capacitaciones convencionales, estructuradas como monólogos unidireccionales centrados en el "qué hacer", han creado inadvertidamente una cultura de espectadores de protocolos. Este enfoque, que trata a los profesionales de la seguridad como recipientes vacíos a ser llenados con información estática, genera un cumplimiento superficial. El resultado es una fuerza laboral que ejecuta instrucciones sin una comprensión profunda de su propósito subyacente, lo que se traduce en respuestas mecánicas y vulnerabilidades latentes ante situaciones imprevistas, un lujo que las organizaciones modernas no pueden permitirse..

La Andragogía: Un Cambio de Paradigma hacia la Agencia Profesional La andragogía, la ciencia de cómo aprenden los adultos, emerge no como una simple alternativa metodológica, sino como un pilar estratégico para la seguridad integral. Su implementación representa una transformación cultural que trasciende la capacitación y se adentra en el territorio de la educación para la resiliencia. A diferencia del modelo obsoleto, la andragogía no se centra en la mera transferencia de conocimientos, sino en cultivar la capacidad de aplicación crítica. Se construye sobre la premisa de que los adultos aprenden mejor cuando el contenido es relevante, está contextualizado y respeta su acumulación de experiencias previas.

Este enfoque pivota del "qué" al "por qué" y al "cómo" en escenarios complejos. Fomenta un diálogo bidireccional donde las vivencias de los guardias, analistas y supervisores en el campo no son desestimadas, sino integradas para enriquecer y adaptar los procedimientos. La técnica, por tanto, deja de ser una lista de verificación estática para convertirse en un ejercicio vivo de análisis colaborativo de incidentes reales, simulaciones inmersivas que replican la presión operativa y la resolución colaborativa de problemas.

Retos en la Implementación del Modelo Andragógico

La transición hacia este modelo no está exenta de desafíos en el contexto latinoamericano. Entre los más significativos se encuentran:

Resistencia Cultural e Inercia Organizacional: Muchas organizaciones están acostumbradas a estructuras jerárquicas rígidas donde la obediencia se valora por encima del criterio. Fomentar un entorno donde se espera que los equipos cuestionen, analicen y propongan puede encontrar resistencia en todos los niveles.

Inversión en Desarrollo de Facilitadores: Este modelo requiere instructores que actúen como facilitadores y mentores, no como lectores de diapositivas. Formar a estos facilitadores en técnicas andragógicas exige una inversión inicial de tiempo y recursos.

Autor: Licenciado en Seguridad Pública y Criminología.
Jonatthan Hermida Sosa
www.hermidaseguridad.org

Medición del Retorno de la Inversión (ROI): Mientras que el cumplimiento de una capacitación tradicional es fácil de medir (se asistió o no, se aprobó un examen), cuantificar el impacto de un pensamiento crítico más agudo o una toma de decisiones más efectiva es un desafío métrico complejo.

Oportunidades para una Seguridad Transformadora

A pesar de los retos, las oportunidades que presenta la andragogía son transformadoras:

- Construcción de una Inteligencia Colectiva Activa: El modelo convierte a todo el equipo de seguridad en una red neuronal de la organización. Cada individuo se convierte en un sensor proactivo y un procesador de información, capaz de detectar anomalías y adaptar respuestas en tiempo real.

- Mayor Retención y Compromiso del Talento: Los profesionales de la seguridad, al sentirse valorados por su experiencia y criterio, desarrollan un sentido de propiedad y compromiso más profundo con la misión organizacional, lo que reduce la rotación y fortalece la cultura corporativa.

- Resiliencia Organizacional Auténtica: Las empresas dejan de depender de un manual y pasan a confiar en la agilidad mental y la capacidad de adaptación de sus equipos. Esta resiliencia es la única defensa sostenible contra un panorama de amenazas en constante evolución

De la Uniformidad a la Agencia Informada. El cambio de espectadores a protagonistas en la seguridad corporativa no es una mera actualización de técnicas; es una redefinición fundamental del rol del profesional de la seguridad. Mientras la capacitación tradicional busca uniformidad, la andragogía cultiva la agilidad mental y el compromiso profundo. Es la diferencia crucial entre tener un manual subutilizado y construir una capacidad orgánica de defensa. Para las organizaciones latinoamericanas que aspiran a una seguridad integral genuina, adoptar la andragogía no es una opción, sino un imperativo estratégico para convertir su primera línea de defensa en una fuerza consciente, proactiva y, sobre todo, protagonista de su propia resiliencia.

LA OPOSICION EN VENEZUELA BAJO PELIGRO DE MUERTE

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Enrique Perez Barrios
Director General de GLOBAL SECURITY ACADEMY USA

En clave política

Ser opositor en Venezuela: un camino lleno de riesgos y represión.
En la Venezuela actual, ser opositor al régimen encabezado por Nicolás Maduro no es solo una postura política: es un acto de resistencia que pone en riesgo la libertad, la integridad física y hasta la vida de quien se atreve a disentir. El país vive bajo un sistema que ha criminalizado la disidencia y transformado la persecución política en una política de Estado. Lo que alguna vez fue una democracia imperfecta se ha convertido en un régimen autoritario de corte totalitario, sostenido por el miedo, la censura y la violencia institucional. Nada distinto a otros gobiernos que se soportan en un entramado criminal que tiene como directriz central la implementación del terror. como ejemplos tenemos que recordar la Alemania del Nazismo con Adolfo Hitler, la Union Soviética de Stalin, la Italia fascista de Benito Musolini o la que impera en Corea del Norte

Un Estado represivo al servicio del poder. El Estado venezolano, que debería proteger los derechos y libertades de sus ciudadanos, ha sido transformado en un aparato represivo diseñado para garantizar la permanencia del régimen. Organismos como el Servicio Bolivariano de Inteligencia Nacional (SEBIN), la Dirección General de Contrainteligencia Militar (DGCIM) y las Fuerzas de Acciones Especiales (FAES) actúan como fuerzas de ocupación interna, realizando detenciones arbitrarias, allanamientos sin orden judicial, secuestros y ejecuciones extrajudiciales. Estos cuerpos no operan bajo supervisión judicial ni control parlamentario. Su obediencia es política, no institucional. Los informes de la Misión Internacional Independiente de Determinación de los Hechos de la ONU confirman que estas instituciones han sido utilizadas de manera coordinada para reprimir a la oposición, aplastar manifestaciones pacíficas y generar un clima de terror. La consecuencia es una sociedad silenciada y sometida, donde hoy se convive con un temor que genera una autocensura aterradora.

Detenciones arbitrarias y desapariciones forzadas. Hoy en Venezuela, la libertad personal es un privilegio frágil porque las detenciones arbitrarias se han vuelto un instrumento cotidiano de castigo político. Activistas, líderes estudiantiles, periodistas, defensores de derechos humanos e incluso ciudadanos que simplemente expresan una opinión crítica en redes sociales pueden ser arrestados sin orden judicial y permanecen incomunicados durante días o semanas y algunos por meses y año. Las desapariciones forzadas se usan como método de intimidación. Durante ese período de incertidumbre, los detenidos son interrogados bajo coacción, torturados o presionados para firmar declaraciones falsas. La práctica se repite con frecuencia alarmante y ha sido documentada en informes internacionales. La arbitrariedad se ha normalizado, y el mensaje es claro: cualquier voz disidente puede ser borrada temporal o permanentemente del mapa.

Tortura y tratos crueles. La tortura se ha institucionalizado como herramienta de control político. Las denuncias son múltiples y consistentes: descargas eléctricas, golpizas con objetos contundentes, asfixia con bolsas plásticas, aislamiento prolongado, privación del sueño, exposición a temperaturas extremas y amenazas de violación o daño a familiares. Estas prácticas buscan destruir psicológicamente a las víctimas y arrancar confesiones forzadas.

Los casos del concejal Fernando Albán, cuyo cuerpo fue arrojado desde un edificio del SEBIN tras ser torturado, y del capitán Rafael Acosta Arévalo, muerto bajo custodia militar, son apenas dos ejemplos visibles de un patrón mucho más amplio. Los centros de detención se han convertido en espacios de sufrimiento sistemático, violatorios del derecho internacional y de toda noción de humanidad.

Censura, vigilancia y control digital. El control informativo es otro de los pilares de la represión. Más de 400 medios de comunicación han sido clausurados o censurados, y las plataformas digitales son vigiladas y bloqueadas selectivamente. Internet se utiliza como herramienta de espionaje. El Estado, a través de mecanismos de monitoreo y empresas de telecomunicaciones controladas, rastrea la actividad en línea de periodistas, dirigentes políticos y usuarios comunes.

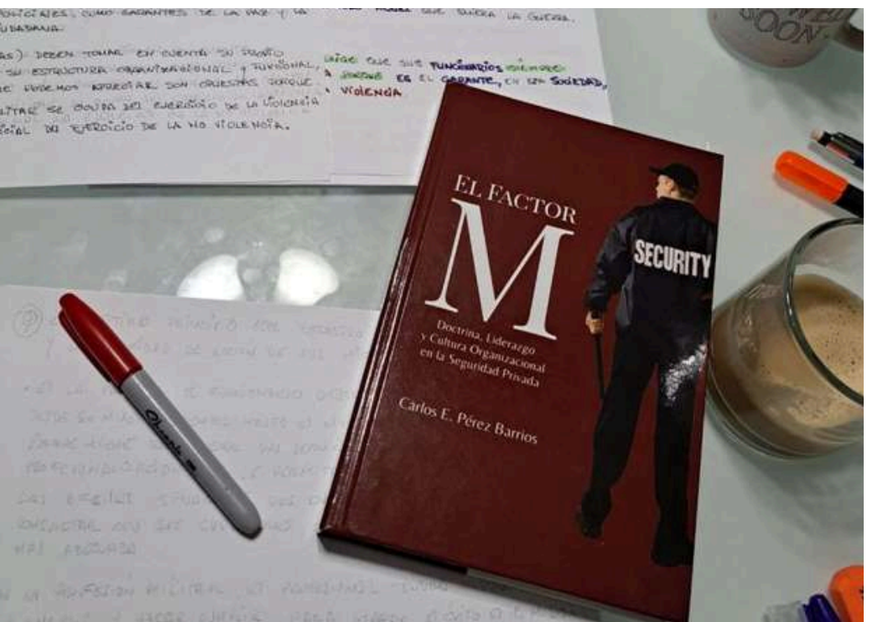
Los bloqueos de portales informativos, la persecución de tuiteros, los ataques cibernéticos a organizaciones civiles y la difusión de campañas de difamación desde cuentas automatizadas o vinculadas al gobierno son parte de una estrategia de control social. Con todo esto se busca aislar a los ciudadanos, manipular la información y destruir la credibilidad de la oposición. En este contexto, la verdad se convierte en un peligro y la mentira en un arma peligrosa en manos de un régimen criminal.

Amenazas físicas y hostigamiento Los colectivos armados, grupos paramilitares leales al régimen, desempeñan un papel clave en la represión. Actúan con total impunidad, atacando manifestaciones, agrediendo a periodistas y asaltando residencias de opositores. Estos grupos, organizados en barrios populares y coordinados con el aparato de inteligencia, siembran miedo mediante violencia selectiva. Las amenazas no se limitan al espacio público: muchos opositores son seguidos, fotografiados y acosados en sus hogares o lugares de trabajo. Los atentados físicos, los incendios intencionales y los "accidentes" provocados son tácticas para intimidar sin necesidad de procesos judiciales. El mensaje es inequívoco: quien desafía al poder pone en riesgo su vida y la de su familia.

Persecución familiar y profesional. La represión no termina con el individuo opositor. Los familiares suelen ser víctimas colaterales de la violencia del régimen tiránico. Son despedidos de sus empleos, amenazados, vigilados o directamente detenidos. En el ámbito profesional, los opositores son inhabilitados políticamente, expulsados de universidades, perseguidos laboralmente y excluidos de concursos públicos o privados.

Este hostigamiento busca quebrar el tejido familiar y económico de la oposición. El objetivo no es sólo castigar, sino aislar al disidente, destruir su entorno y eliminar su capacidad de resistencia. De esta manera, la represión se transforma en un mecanismo de aniquilación social que refuerza el control totalitario del régimen.

Exilio y persecución transnacional. Ante la persecución, miles de venezolanos han optado por el exilio forzado. Sin embargo, salir del país no garantiza seguridad. Muchos opositores tienen prohibición de salida, pasaportes anulados o se les impide embarcar en aeropuertos. Aquellos que logran escapar enfrentan la vida del refugiado: desarraigo, precariedad y constante miedo a la persecución transnacional. El régimen mantiene una política activa de hostigamiento contra líderes en el exilio mediante campañas de desinformación, difamación y vigilancia a través de embajadas o agentes encubiertos. Esta persecución fuera de las fronteras venezolanas evidencia la extensión del control autoritario más allá del territorio nacional.



Crímenes de lesa humanidad La represión en Venezuela cumple con los elementos establecidos en el Estatuto de Roma para calificar como crímenes de lesa humanidad: persecución por motivos políticos, encarcelamientos ilegales, tortura, desapariciones forzadas y ejecuciones extrajudiciales. La Misión de Determinación de los Hechos de la ONU ha afirmado que estas violaciones no son hechos aislados, sino una política de Estado diseñada y ejecutada por las más altas autoridades.

Los informes internacionales recomiendan la intervención de la Corte Penal Internacional para investigar y sancionar a los responsables. Mientras tanto, el régimen mantiene la negación, destruye evidencias y busca proyectar una falsa imagen de legalidad ante la comunidad internacional. La impunidad sigue siendo el motor que sostiene esta maquinaria de represión.

Ser opositor en Venezuela es enfrentarse a un sistema totalitario que ha institucionalizado el terror. No existen garantías jurídicas, ni independencia judicial, ni respeto por los derechos humanos. Cada ciudadano que se atreve a disentir se convierte en blanco de un aparato que persigue, tortura, encarcela y, en muchos casos, mata. La comunidad internacional tiene la responsabilidad moral y política de no ser indiferente ante esta tragedia. Documentar, denunciar y sancionar a los responsables son pasos imprescindibles para evitar que la represión continúe y que Venezuela recupere, algún día, su libertad. Mientras tanto, los opositores seguirán siendo los portadores del coraje en un país donde pensar diferente puede costar la vida

Servicios de Peritaje y Consultoría en Andalucía y Ceuta, España.
Due Diligence - Debida Diligencia, a Nivel Nacional como Internacional.

✓ Nuestro Compromiso, es Proporcionar Asesoramiento Experto en Peritajes, Consultoría y Due Diligence (Debida Diligencia),
para Apoyar a nuestros Clientes en el Ambito Legal y Técnico.

✓Para ofrecer el Máximo Servicio a Nuestro Clientes, y por el Valor que Ofrece el Servicio Consultora de Formación e Implementación de Arquitecturas y Proyectos de Seguridad.

Colaboramos con MR-CONSULTING.

Asesoramiento Técnico Especializado, para Situaciones legales y Técnicas:
En el Ámbito de la:
Seguridad Privada, Balística Forense.
Ciberseguridad, Inteligencia y Geopolitica.
Seguros de Embarcaciones Recreo.
Grafologia, Documentoscopia, Grafopsicopatologia Criminal y Forense.
Due Diligence (Debida Diligencia).

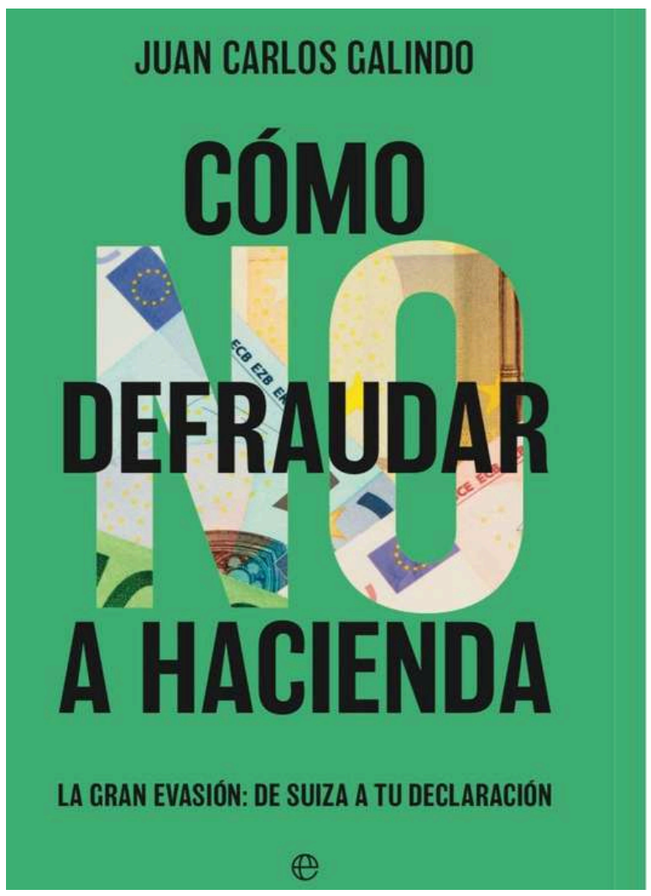
https://www.oterotrillogabinetepericial-andaluciaceuta.es/

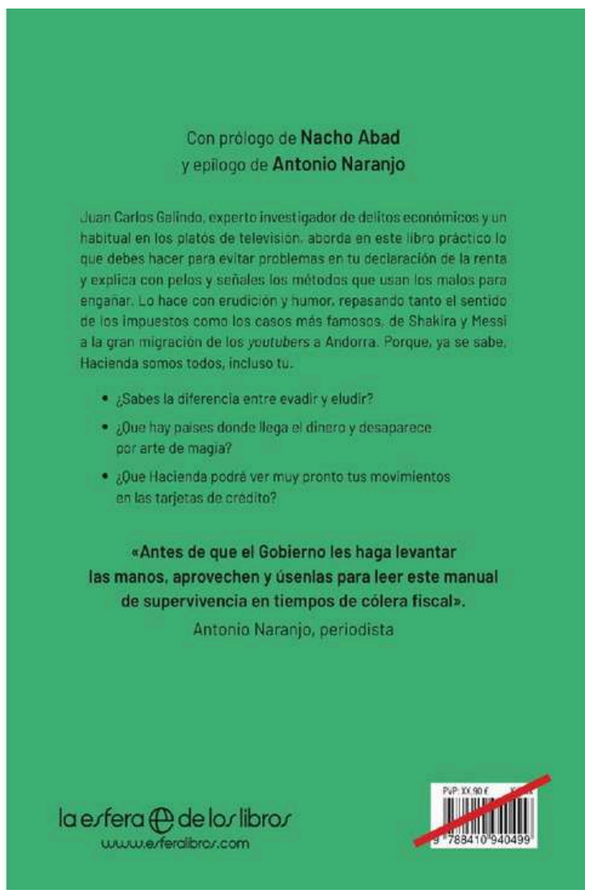
AGENDA

Metro Risk

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