

EDITORIAL MR



ISSN 3045-7629

JUNIO

**AÑO
2025**

Edición propiedad de @MetroRisk, asociación

SECUR

**Fran Medina Cruz
Gregorio Duro
Emilio Piñeiro
Abraham Santana**

**Francisco Javier Gonzales Fuentes
Mercedes Escudero Carmona
Adolfo M. Gelder
Alina Rubio**

**José Ignacio Olmos
Antonio Cozano Fernández
Rosa Fernández
Carlos Serrano
Elena de la Parte
Carlos Miguel Ortiz**

@Metrorisk.es

ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

Presidente:

D. Francisco Medina cruz

Vicepresidente Económico:

D. Abraham Santana Herrera

Vicepresidente Relaciones Institucionales:

D. Juan Carlos Galindo

Secretario General:

D. Emilio Piñeiro

Vocal Comunicación:

Dña. Elena González de la Parte

Vocal Temas Legales:

Dña. Rosa Fernández Fernández



MeTroRisk
Seguridad Patrimonial y CPTED

Editado por:

Fran Medina Cruz y Elena González de la Parte,
en Málaga, España

ISSN 3045-7629



COLABORADORES



PATROCINADO POR LAS FIRMAS



Los artículos aquí expuestos son respetados en su naturaleza lingüística de país o región.

SEGURIDAD DESDE EL DISEÑO. CPTED + EVALUACIÓN BREEAM SYB11

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz
Director de MetroRisk

Cómo integrar el diseño arquitectónico con estrategias CPTED y certificaciones BREEAM para crear entornos más seguros, sostenibles y exclusivos



Esta cuestión resume con contundencia uno de los principios fundamentales que guían la elaboración de los informes de seguridad MRConsulting: la seguridad no es un complemento, sino una obligación ética desde la fase de diseño.

Desde nuestra consultora, como expertos en seguridad por diseño (CPTED) y en la elaboración de informes adaptados al criterio SyB11 de BREEAM, advertimos de una tendencia preocupante: la proliferación de lo que denominamos viviendas vulnerables o crimipetas, espacios arquitectónicamente atractivos pero con deficiencias estructurales de seguridad que se integran desde la concepción del proyecto. Estas deficiencias no suelen ser advertidas por arquitectos ni promotores, pero sí por quienes se aprovechan de ellas: los delincuentes.

En España, se contabilizan más de 100.000 robos anuales en viviendas, la mayoría mediante forzamientos silenciosos de puertas y ventanas, aprovechando vulnerabilidades evitables si se hubieran considerado desde el origen del proyecto.

Nuestros informes no se limitan a identificar riesgos una vez ejecutado el diseño, sino que los anticipan:

- Analizamos los cuatro anillos de protección: perimetral exterior, zona de tránsito, perímetro envolvente y núcleo de habitabilidad.
- Proponemos medidas pasivas y activas de seguridad arquitectónica.
- Auditamos el entorno físico, la distribución espacial, y los accesos desde una visión integral y técnica, con base en normas europeas, CPTED y criterios BREEAM.

La seguridad no puede seguir siendo un elemento decorativo ni añadido tecnológico de última hora. MRConsulting defiende una arquitectura con conciencia preventiva, capaz de reducir el riesgo delictivo sin renunciar al diseño ni a la funcionalidad, promoviendo así entornos resilientes, habitables y protegidos.

Seguridad es diseño inteligente. Seguridad es previsión. Seguridad es valor añadido.



Un caso de éxito: Villa Ayantam Marbella

Un ejemplo real fue el caso de la Villa Ayantam, en Marbella, donde la aplicación de un informe de seguridad por diseño permitió alcanzar la máxima calificación SyB11 de BREEAM. Esto no solo facilitó su comercialización, sino que la convirtió en un referente técnico citado por medios especializados.

¿Por qué este informe importa?

Ofrece un diagnóstico profesional y certificado del nivel de protección real de una vivienda de lujo.- Mejora la puntuación BREEAM en los procesos de certificación ambiental.- Transforma la seguridad en una ventaja competitiva para promotoras y agencias inmobiliarias.

Conclusión

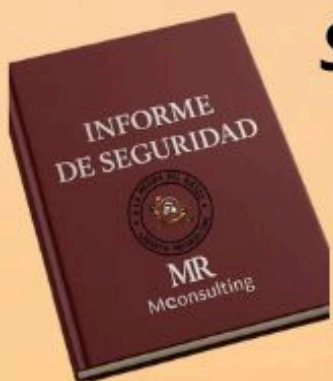
No se trata solo de construir espacios bellos, funcionales o sostenibles. Se trata de que esos espacios también sean seguros desde su concepción, como parte de un todo coherente y a la altura de quienes los habitarán

PROCESO DE INFORME DE SEGURIDAD



Porque no existe el lujo si carece de seguridad

- AUMENTA EL VALOR DESDE EL DISEÑO
- MEJORA SU CERTIFICACIÓN BREEAM
- REFUERZA LA CONFIANZA DEL COMPRADOR MÁS EXIGENTE
- REVALORIZA LA PROPIEDAD A ACTIVO DE ALTO ESTÁNDAR



Su Informe de Seguridad. Analizado, auditado y exclusivo

No se trata solo de construir espacios bellos, funcionales o sostenibles. Se trata de que esos espacios también sean seguros desde su concepción, como parte de un todo coherente y a la altura de quienes los habitarán.



MRConsulting

franmedina@mr-consulting.es
info@mr-consulting.es
www.mr-consulting.es

EL ROL DEL PERITO JUDICIAL EN SINIESTROS DURANTE EVENTOS PÚBLICOS

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

Cuando ocurre un siniestro en un evento público, ya sea un festival, concierto, feria, partido de fútbol o acto institucional, las consecuencias pueden ser trágicas: heridos, daños materiales, caos operativo, y sobre todo, una urgente necesidad de aclarar qué falló. Es entonces cuando cobra relevancia una figura fundamental: el perito judicial.

El perito judicial es un profesional con formación técnica y experiencia contrastada, designado por una de las partes o por el juez, para aportar conocimiento objetivo y especializado en un proceso judicial. Su misión en estos casos no es sólo reconstruir técnicamente los hechos, sino identificar causas, valorar medidas de prevención adoptadas, y determinar negligencias o fallos estructurales.



¿Qué analiza un perito judicial tras un siniestro?

1. Condiciones del recinto o entorno del evento
 - Vías de evacuación
 - Señalética
 - Capacidad del aforo
 - Existencia de planes de autoprotección
2. Diseño y ejecución de medidas de seguridad
 - Seguridad perimetral
 - Personal acreditado y procedimientos de control
 - Sistemas de emergencia (extintores, iluminación de emergencia, salidas)
 - Coordinación con cuerpos policiales y servicios médicos
3. Cronología y dinámica del siniestro
 - Secuencia de hechos según registros (vídeos, partes de incidencias, testigos)
 - Respuesta del personal de seguridad y primeros intervinientes
 - Actuación del organizador ante la crisis
4. Normativas aplicables
 - Ley de Espectáculos Públicos
 - Normativa autonómica o municipal
 - Reglamento de prevención de riesgos laborales
 - Normas UNE sobre seguridad estructural y evacuación

Funciones clave del perito judicial

- 🔧 Realizar una inspección ocular técnica, detallando las condiciones físicas del entorno y sus posibles deficiencias.
- 📄 Emitir un informe pericial claro, riguroso y comprensible por un juez, evaluando las causas del siniestro.
- 🌱 Vincular responsabilidades entre diseño, organización, ejecución y supervisión del evento.
- 🏛️ Comparecer en juicio para defender técnica y verbalmente sus conclusiones ante la sala.
- ⚖️ Actuar como asesor técnico imparcial en apoyo a la labor de jueces y fiscales.

¿Por qué su labor es tan importante?

Porque muchas veces, en los procesos judiciales, lo que se dirime no es sólo quién cometió un error, sino si las condiciones estructurales y organizativas eran razonablemente seguras. Y esa evaluación sólo puede realizarla alguien con conocimientos técnicos, normativos y experiencia práctica: el perito.

Su informe puede ser determinante para absolver o condenar, para justificar indemnizaciones o para evitar que tragedias similares se repitan. Actúa como el puente entre la técnica y la justicia.

Los eventos públicos, por su escala y complejidad, requieren una planificación impecable y una ejecución profesional. Cuando algo falla, la figura del perito judicial se convierte en pieza clave para esclarecer los hechos y depurar responsabilidades.

Promotores, administraciones y cuerpos de seguridad deben entender que la prevención no solo se materializa antes del evento, sino también en la transparencia y rigurosidad del análisis posterior, donde el perito aporta una mirada técnica y objetiva que protege tanto al ciudadano como al sistema judicial.

Por, Francisco Javier González Fuentes
Presidente de ADISPO
(Asociación de Directores de Seguridad)



LA IMPORTANCIA DE LAS AUDITORÍAS DE SEGURIDAD EN EVENTOS PÚBLICOS: RIGOR Y PREVENCIÓN EN ACCIÓN

Metro
Risk

Edición propiedad de @MetroRisk, asociación

José Ignacio Olmos Casado
Presidente AEAS

La organización de eventos públicos, ya sean conciertos, festivales, celebraciones institucionales o manifestaciones populares, conlleva un alto nivel de responsabilidad. En estos entornos dinámicos, donde confluyen grandes aglomeraciones humanas, infraestructuras temporales, personal externo y un amplio abanico de riesgos, las auditorías de seguridad se convierten en una herramienta esencial para garantizar un desarrollo seguro, ordenado y eficaz del evento.

¿Qué es una auditoría de seguridad en el contexto de eventos?

Una auditoría de seguridad es un proceso técnico y riguroso que evalúa de forma objetiva si las medidas de seguridad previstas y ejecutadas en un evento cumplen con la normativa, las buenas prácticas y los estándares profesionales. No se trata de un simple trámite, sino de una revisión integral del sistema de protección previsto, desde la planificación hasta la ejecución operativa.

Incluye aspectos como:

- Evaluación de riesgos y amenazas realistas.
- Comprobación de medios humanos y técnicos.
- Revisión de planes de emergencia y evacuación.
- Análisis de accesos, salidas, controles y zonas sensibles.
- Verificación de habilitaciones, licencias y contrataciones.
- Coordinación entre seguridad privada y fuerzas públicas.
- Protocolos de actuación ante incidentes, agresiones o crisis.

Rigor técnico frente a la improvisación

En tiempos de eventos públicos, donde los niveles de exposición y vulnerabilidad se multiplican, no se puede improvisar la seguridad. La auditoría garantiza que las medidas adoptadas no se limitan a una apariencia de control, sino que responden a criterios funcionales, legales y estratégicos.

Este proceso actúa como un filtro profesional que identifica debilidades, omisiones o errores antes de que estos se traduzcan en incidentes. Su carácter objetivo permite mejorar en tiempo real los planes de seguridad y reforzar los dispositivos antes del inicio del evento.



Efectividad contrastada y valor añadido

Las auditorías no solo previenen fallos operativos; también generan documentación técnica sólida, trazabilidad de decisiones, y una percepción de control que transmite seguridad a todas las partes: organizadores, autoridades, patrocinadores, cuerpos de emergencia y ciudadanía.

En caso de incidentes, la existencia de una auditoría profesional permite demostrar diligencia y previsión, algo crucial a nivel jurídico y reputacional. Asimismo, su implementación es cada vez más demandada por aseguradoras, administraciones públicas y grandes promotores.

Cuando el evento es masivo, la auditoría es obligatoria de facto

En eventos con alta concentración de personas, múltiples accesos, zonas VIP, infraestructura crítica o riesgo de alteración del orden público, la auditoría no debería ser una opción, sino un estándar mínimo exigible. Su ausencia supone un vacío técnico que puede traducirse en descoordinación, reacciones tardías o una respuesta ineficaz ante emergencias. El mensaje debe ser claro: la seguridad no se delega, se gestiona, se supervisa y se audita. Y esto solo puede hacerse desde la figura de un consultor o Director de Seguridad con la formación y experiencia adecuadas para asumir esta responsabilidad.

En el actual contexto de transformación social, donde los eventos públicos se han convertido en escaparates de imagen, cultura y marca ciudad, la auditoría de seguridad debe consolidarse como una herramienta estratégica de prevención, control y excelencia operativa. Invertir en una auditoría no solo protege a las personas y los bienes: protege también la credibilidad del evento y el prestigio de quienes lo organizan.

SECCIÓN ESTUDIOS TÉCNICOS

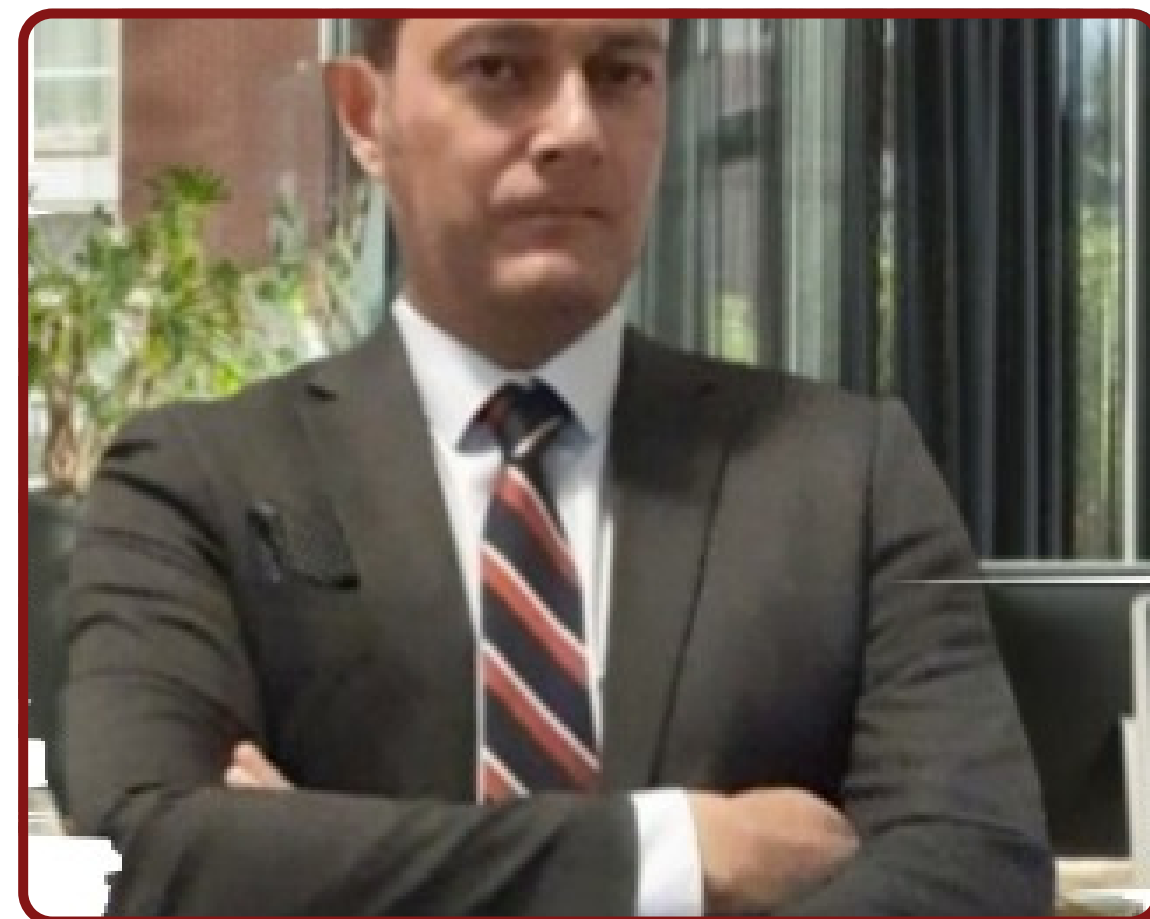
Metro
Risk

Edición propiedad de @MetroRisk, asociación

Gregorio Duro
Tecnico en licitaciones y Proyectos

PRINCIPIO DE OPTIMALIDAD DE BELLMAN EN PROCESOS DE ESTIMACIÓN DE RIESGOS

En el artículo de este mes, quiero realizar una aplicación del principio de optimalidad de Bellman en el ámbito de la estimación de riesgos. El principio de optimalidad de Bellman, formulado por Richard Bellman en el contexto de la programación dinámica, constituye un fundamento esencial en la toma de decisiones secuenciales bajo incertidumbre y ha sido ampliamente adoptado en disciplinas como la teoría de control, la economía, la inteligencia artificial y el análisis de riesgos.

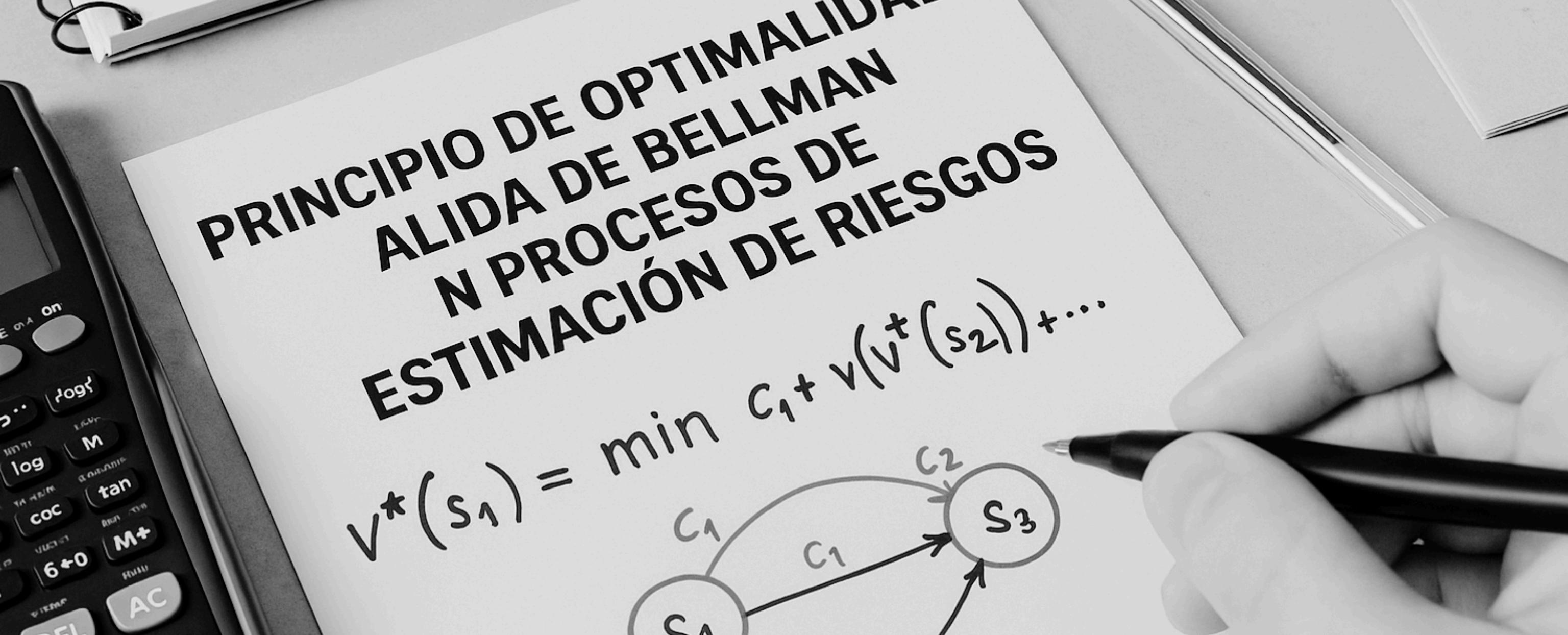


La programación dinámica, propuesta por Richard Bellman en la década de 1950, es una técnica de optimización matemática diseñada para resolver problemas complejos al descomponerlos en una serie de subproblemas más simples. Su fundamento principal es el principio de optimalidad de Bellman, que establece que la solución óptima de un problema de múltiples etapas puede obtenerse resolviendo de forma óptima cada uno de sus subproblemas, y utilizando estas soluciones parciales para construir la solución completa. Esta propiedad de "optimalidad anidada" resulta particularmente útil en entornos dinámicos donde el sistema evoluciona a lo largo del tiempo, y donde las decisiones deben adaptarse a nuevas condiciones o información emergente. En el análisis de riesgos, el principio de optimalidad ofrece un marco riguroso para seleccionar estrategias que minimicen la exposición o el impacto acumulado del riesgo, permitiendo construir soluciones adaptativas que se ajusten a distintos escenarios futuros mediante la evaluación continua de las mejores decisiones disponibles en cada etapa del proceso. En esencia, este principio afirma que, para que una política o estrategia sea considerada óptima, las decisiones tomadas en cada etapa del proceso deben ser óptimas dadas las condiciones presentes, independientemente de las decisiones previas.

El principio de optimalidad de Bellman encuentra una aplicación particularmente valiosa en los procesos de estimación de riesgos que involucran múltiples etapas de decisión, incertidumbre y dinámicas evolutivas. Este principio permite estructurar modelos en los que el riesgo no se estima de forma estática, sino como una variable que cambia en función de las decisiones tomadas a lo largo del tiempo, posibilitando así una evaluación secuencial y adaptativa. En la gestión de riesgos financieros, por ejemplo, se aplica para determinar estrategias óptimas de cobertura ante fluctuaciones del mercado, minimizando la exposición acumulada a eventos adversos mediante políticas de inversión dinámicas. En el ámbito de la ingeniería y los proyectos de infraestructura, se utiliza para planificar medidas de mitigación progresivas, considerando cómo las decisiones de hoy afectan la vulnerabilidad del sistema en etapas futuras. En ciberseguridad, el principio permite modelar la evolución de amenazas y defensas en función del comportamiento del atacante y las respuestas del sistema, facilitando la asignación óptima de recursos de protección. Asimismo, en logística y cadenas de suministro, ayuda a evaluar riesgos operacionales como interrupciones o retrasos, proponiendo rutas o decisiones de inventario que minimicen el impacto total. Incluso en políticas públicas y gestión de emergencias, este enfoque permite simular escenarios futuros de riesgo (como pandemias, desastres naturales o crisis energéticas) y diseñar respuestas estratégicas basadas en la minimización del riesgo esperado. En todos estos casos, la clave está en aprovechar la estructura recurrente del cálculo de Bellman para construir modelos que, al dividir el proceso en subproblemas interrelacionados, permiten obtener soluciones óptimas globales mediante decisiones localmente óptimas en cada etapa.

Un ejemplo práctico de la aplicación del principio de optimalidad de Bellman en un proceso de estimación de riesgos puede encontrarse en la gestión del riesgo operacional en un proyecto de infraestructura crítica, como la construcción de una planta hidroeléctrica en una zona geológicamente inestable.

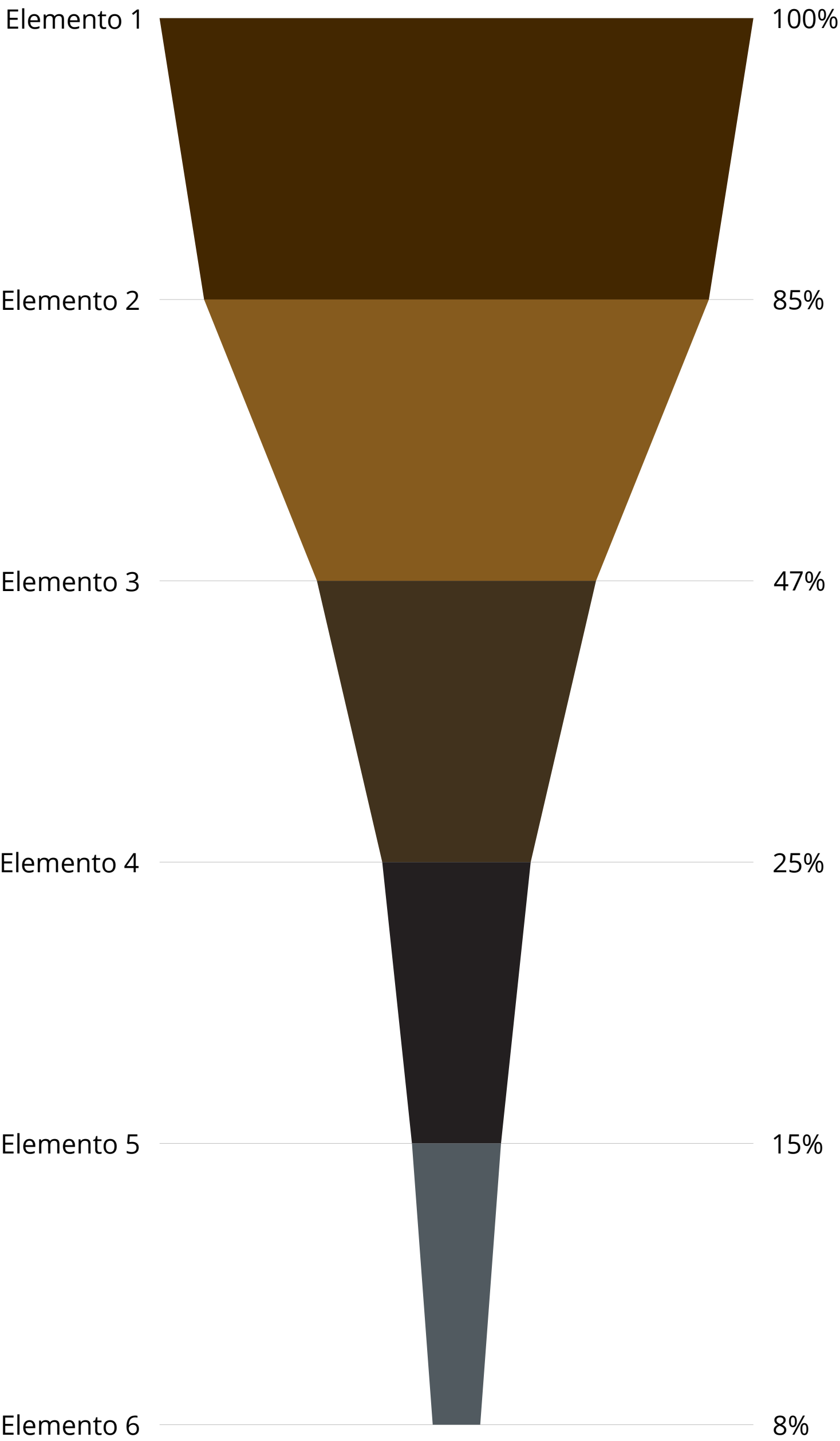
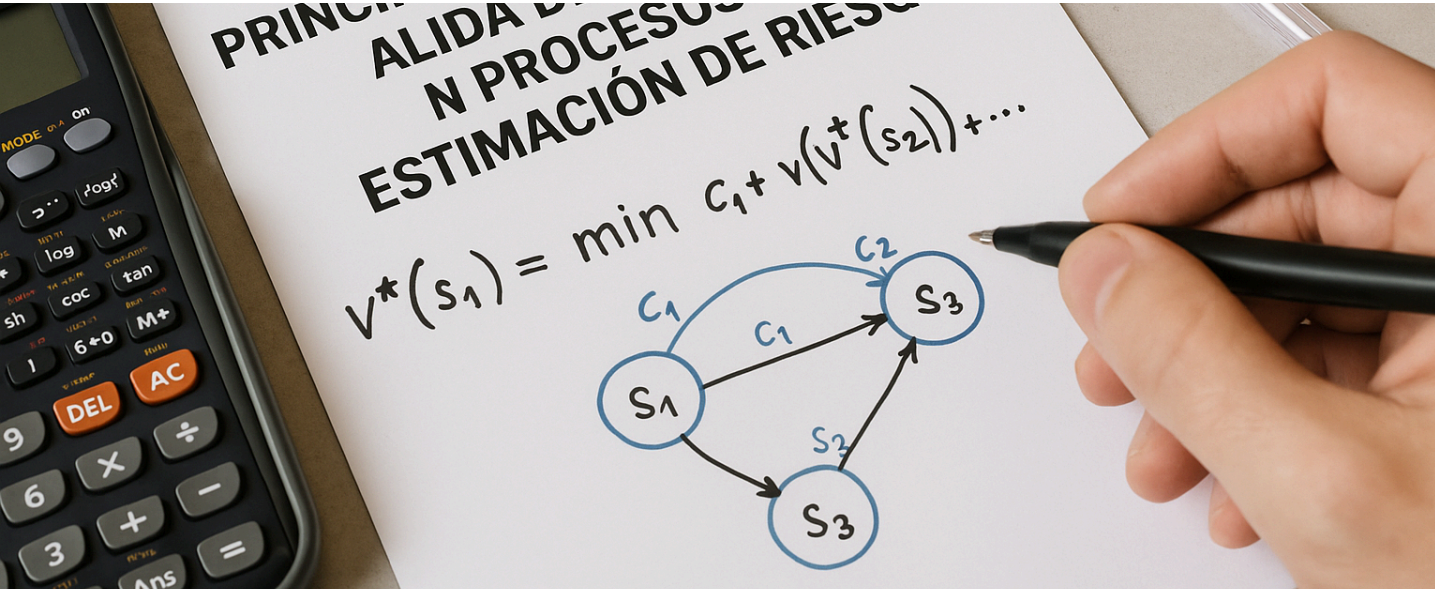




Durante la planificación del proyecto, los ingenieros y gestores deben tomar una serie de decisiones secuenciales a lo largo de diferentes fases —estudio de suelos, diseño estructural, ejecución de obras y operación futura— cada una con implicaciones significativas para el perfil de riesgo del sistema. En este contexto, el principio de optimalidad permite modelar el proceso de toma de decisiones como una cadena de etapas en la que cada elección — por ejemplo, invertir en estudios geotécnicos más detallados, reforzar estructuras con mayores costes o aplicar tecnologías de detección temprana— no solo afecta el riesgo inmediato, sino también las condiciones y decisiones óptimas en etapas futuras. Así, al aplicar programación dinámica basada en el principio de Bellman, se parte del final del proyecto (la etapa de operación) y se retrocede hasta el presente, evaluando en cada estado posible del sistema cuál es la decisión que minimiza la pérdida esperada acumulada, considerando tanto el coste de la acción como la probabilidad de eventos adversos (como deslizamientos, fallas estructurales o interrupciones operativas). Por ejemplo, aunque en la etapa inicial pueda parecer costoso la instalación de sensores sísmicos en la estructura, el modelo puede revelar que esa inversión reduce significativamente la incertidumbre futura y evita decisiones de emergencia costosas en etapas posteriores, lo que la convierte en parte de la política óptima. Esta metodología permite incorporar escenarios inciertos, costos futuros esperados y retroalimentación del entorno en un modelo coherente de estimación de riesgo, donde cada decisión tomada forma parte de una estrategia global óptima, validando así el enfoque adaptativo propuesto por Bellman.

Quiero expresar mi agradecimiento a Metrorisk por compartir mensualmente este tipo de artículos de contenido técnico que contribuyen a la difusión y mejora del conocimiento en nuestro sector.

Gregorio Duro Navarro Técnico de Licitaciones y Proyecto



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

LA IMPORTANCIA DE LOS PROCESOS DE COMUNICACIÓN EN LA GESTIÓN DE RIESGOS

La gestión de riesgos es un componente crítico para la estabilidad y el desarrollo de cualquier sociedad, organización o proyecto. En este contexto, la comunicación no es un mero acto informativo, sino un proceso estratégico fundamental que permea todas las fases de la gestión de riesgos, desde la identificación hasta la mitigación y la recuperación.

La gestión de riesgos implica la identificación, análisis, evaluación, tratamiento y monitoreo de las incertidumbres que podrían afectar el logro de los objetivos. Para que este ciclo sea efectivo, la comunicación es indispensable para las siguientes fases:

- Identificación y Análisis: facilita la recolección de información de diversas fuentes, incluyendo la percepción de riesgo de las comunidades y expertos. Un diálogo abierto permite identificar riesgos que de otra manera podrían pasar desapercibidos.
- Evaluación y Priorización: manejar transparencia de datos sobre la magnitud y probabilidad de los riesgos ayuda a las partes interesadas a comprender su impacto y a priorizar las acciones.
- Tratamiento y Mitigación: la implementación de medidas de mitigación requiere una comunicación clara de roles, responsabilidades y procedimientos.
- Monitoreo y Revisión: la comunicación constante sobre el estado de los riesgos y la efectividad de las medidas y contramedidas permite ajustes oportunos fomentando la mejora continua.

La norma ISO 22341:2021, "Seguridad y resiliencia - Seguridad protectora Directrices para la Prevención del Delito mediante el Diseño Ambiental (CPTED)", enfatiza la importancia de integrar la prevención del delito en el diseño y la gestión de los entornos construidos. En este marco, la comunicación es vital porque incluye:

- La participación de las partes interesadas: la ISO 22341, al igual que otras normas de gestión de riesgos (como la ISO 31000), subraya la necesidad de involucrar a todos los stakeholders (usuarios, residentes, autoridades, diseñadores, fuerzas de seguridad, entre otras). La comunicación bidireccional garantiza que las percepciones de inseguridad, las experiencias de victimización y las ideas de solución sean incorporadas en el diseño.



- La sensibilización sobre el diseño seguro: comunicar cómo elementos de diseño específicos como: la iluminación, visibilidad, territorialidad, mantenimiento y, principalmente, la conectividad y cohesión social mediante la participación de la comunidad, lo cual contribuye a la seguridad y reducción del miedo al delito. Esto educa a la comunidad y fomenta su apropiación y cuidado de los espacios.
- La transparencia en la evaluación de riesgos: la norma ISO 22341 requiere la comprensión del riesgo delictivo y saber comunicar los resultados de las evaluaciones de manera clara y comprensible para poder justificar las intervenciones desde el diseño y obtener el apoyo necesario para la implementación.
- La gestión de expectativas: comunicar lo que CPTED puede y no puede lograr ayuda a gestionar y no fomentar expectativas erróneas hacia la comunidad. Con ello, evitamos percepciones negativas y cuidamos el riesgo reputacional.



LA IMPORTANCIA DE LOS PROCESOS DE COMUNICACIÓN EN LA GESTIÓN DE RIESGOS

CPTED

La comunicación es el hilo conductor que une la gestión de riesgos en sus diversas dimensiones –desde el diseño ambiental con CPTED y la ISO 22341, hasta la seguridad ciudadana y la seguridad humana. No se trata solo de transmitir información, sino de construir entendimiento mutuo, generar confianza, empoderar a los individuos y movilizar a la sociedad hacia la construcción de entornos más seguros, resilientes y justos. Una estrategia de comunicación robusta y bien integrada es, por tanto, un activo invaluable en cualquier esfuerzo por gestionar los riesgos y promover la paz y el bienestar colectivo.

Desde la perspectiva de la Seguridad Ciudadana se enfoca en la protección de las personas frente a la violencia y el delito en el espacio público. Aquí, la comunicación en la gestión de riesgos es esencial para:

La construcción de confianza: las instituciones de seguridad (policía, fiscalías) deben comunicar de manera transparente sus acciones, resultados y desafíos. Esto es fundamental para reconstruir la confianza ciudadana, a menudo erosionada por la percepción de ineficacia o corrupción.

- El fomento de la denuncia y la colaboración: una comunicación efectiva sobre cómo y por qué denunciar, y sobre los mecanismos de protección para denunciantes, es vital para aumentar la participación ciudadana en la reducción del delito.
- La gestión de percepciones de miedo: el miedo al delito puede ser tan debilitante como el delito mismo. La comunicación estratégica debe equilibrar la información sobre riesgos con mensajes que promuevan la resiliencia comunitaria y muestren los esfuerzos y éxitos en la prevención.
- La promoción de la cultura de la legalidad y la justicia cívica: comunicar los principios de la justicia cívica y los mecanismos alternativos de resolución de conflictos ayuda a desescalar tensiones y a promover la convivencia pacífica en todas las comunidades.

Desde la Seguridad Humana, con su enfoque en la protección integral de la vida y la dignidad de las personas frente a una amplia gama de amenazas (no solo el delito), requiere que la comunicación sea:

- Inclusiva y adaptada: reconoce la diversidad de vulnerabilidades. La comunicación debe adaptarse a las necesidades de grupos específicos como: mujeres, niños, adultos mayores, personas con discapacidad, minorías; culturalmente sensibles. utilizando formatos y lenguajes
- Preventiva y de alerta temprana: para amenazas como desastres naturales, pandemias o crisis económicas, la comunicación oportuna y clara sobre riesgos, medidas preventivas y protocolos de emergencia es vital para salvar vidas y minimizar el impacto.
- Empoderadora: la comunicación debe proporcionar a las personas y comunidades la información y las herramientas para tomar decisiones informadas sobre su propia seguridad y bienestar, fortaleciendo su capacidad de resiliencia.
- Generadora de cohesión social: en tiempos de crisis o riesgo, la comunicación puede unir a las comunidades, fomentar la solidaridad y coordinar esfuerzos de respuesta y recuperación

Con todo anterior, estamos planteando un modelo de Comunicación para la Paz verdaderamente efectivo que integra las visiones mencionadas. Reconoce que no puede haber seguridad ciudadana sostenible sin abordar las dimensiones de la seguridad humana, y viceversa. La comunicación se convierte en un puente que conecta las necesidades individuales y comunitarias con las respuestas institucionales, promoviendo un ciclo virtuoso de confianza, participación y bienestar. Esto implica:

Narrativas coherentes: desarrollar mensajes que conecten la protección individual con la acción colectiva y la responsabilidad institucional.

- Plataformas integradas: utilizar canales que permitan tanto la expresión de necesidades humanas como la interacción con las fuerzas de seguridad.
- Capacitación cruzada: formar a comunicadores, líderes comunitarios y agentes de seguridad en ambos enfoques para que puedan facilitar el diálogo y la acción conjunta.

La Comunicación para la Paz es el hilo conductor que teje la visión de seguridad con visión preventiva que es el ADN de CPTED. Una estrategia de comunicación bien planificada y ejecutada no solo facilita la comprensión de los principios, sino que también fomenta la participación social, construye confianza, gestiona expectativas y, en última instancia, contribuye a la creación de entornos más seguros, resilientes y habitables, convirtiéndose en un Territorio de Paz.

GOBERNANZA PARTICIPATIVA & CPTED



¿POR QUÉ ES VITAL ELEGIR BIEN TU SISTEMA DE ALARMAS?

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Antonio Cozano Fernández
CEO Cofer Seguridad.

Si algo he aprendido es que es un trabajo duro, poco reconocido y lleno de grandes profesionales que cada día dan lo mejor de sí para que el resto pueda vivir más tranquilo, estos grandes profesionales llamados vigilantes de seguridad, escoltas y resto de especialidades complementan día a día a nuestras fuerzas y cuerpos de seguridad sin dar ruido sin ser protagonistas sin reconocimiento y entregados día a día a una sociedad que aún no reconoce su gran labor al ciudadano, cada día en esta profesión me da nuevas experiencias y a veces grandes satisfacciones, de vez en cuando alguien te da las gracias cuando tú equipo, tus trabajadores le han ayudado en situaciones a veces muy complicadas y con casi cero medios y son estos momentos los que te hacen sentir que estás haciendo algo bueno por los demás..... vigilantes de seguridad los grandes desconocidos de una sociedad que cada vez es menos generosa y ofrece menos reconocimiento a los que velan con todo su afán por el bienestar y descanso del resto de ciudadanos

D. Antonio Cozano Fernández



**COFER**
SEGURIDAD

TEL: 952 409 846

¿Y SI LO ÚNICO QUE QUIERES
ES DORMIR TRANQUILO?

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

Active su sistema
de seguridad en
un clic



29,95 € mes+ IVA*

Seleccionar un sistema de alarmas adecuado no es una simple decisión técnica: es una inversión directa en seguridad, tranquilidad y prevención. Muchas personas adquieren alarmas genéricas sin considerar si realmente responden a las necesidades específicas de su vivienda, negocio o estilo de vida. Esta decisión, mal orientada, puede derivar en una falsa sensación de protección y en una exposición real al riesgo.

Un buen sistema de alarmas debe cumplir tres funciones esenciales: disuadir a posibles intrusos, detectar de forma anticipada cualquier intento de acceso no autorizado, y permitir una respuesta rápida y eficaz. Para ello, es imprescindible que esté bien dimensionado, correctamente instalado y adaptado al entorno físico y al perfil de riesgo del usuario.

Además, debe integrarse con otros elementos de seguridad, como sensores perimetrales, videovigilancia, control de accesos o iluminación disuasoria. Y no menos importante: debe contar con soporte técnico y servicio de mantenimiento que asegure su funcionamiento continuo.

Elegir mal un sistema de alarmas no solo compromete la seguridad: también puede afectar a pólizas de seguro, generar pérdidas económicas y, lo que es más importante, poner en riesgo a quienes habitan o trabajan en el espacio.

Por eso, la clave está en dejarse asesorar por profesionales cualificados, que analicen los puntos vulnerables y diseñen un sistema eficaz, discreto y fiable.

Información general
info@coferseguridad.com
952 409 846



HOY QUIERO HABLARTE DE ERRORES...

SI, UNO QUE CAMBIÓN EL MUNDO Y LA SALUD

Metro
Risk

Edición propiedad de @MetroRisk, asociación

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

..te invito a reflexionar:

Alexander Fleming no buscaba descubrir la penicilina.

Volvió de vacaciones y encontró una placa olvidada,
contaminada con moho, si, es así como se dice que fué...

- Un error.
- Un descuido.
- Una "alucinación" para el método científico clásico.

Sin embargo,
Fleming observó lo que muchos otros habrían tirado a la
basura.

💡 Vio que alrededor del moho no crecían bacterias.

Y se preguntó por qué!?

Así comenzó una revolución que salvó millones de vidas.

Casi 100 años después,
una nueva clase de "errores"
llama nuestra atención cada día:
Estas son "las alucinaciones algorítmicas."

Sí, voy por ahí...ya lo sabes....
esos deslices de la IA que tantos temen y con razón.

Pero,
- ¿y si algunas fueran como aquella placa contaminada?
- ¿Y si, bajo ciertas condiciones, pudieran ser fértiles para
avanzar?
- ¿Y si también merecieran ser observadas, comprendidas
y encauzadas?

El Dr. Horacio Granero lo expuso en el reciente
Congreso de IA en la Justicia Argentina:

"¿Puede la IA alucinar con sentido?"

Y la respuesta, como en el caso de Fleming...

...siempre desde mi punto de vista,
no depende (solo) de "la máquina", sino de...
quién la observa, con qué propósito y en qué contexto.

En ciencia, diseño, políticas públicas o diagnóstico
institucional,
la IA puede no solo responder, sino también "imaginar".

El riesgo no está en que fabule,
sino en no tener un marco ético y estratégico
para canalizar su potencia desde el pensamiento crítico



¿Estamos tirando nuestras
"placas contaminadas" a la
basura sin mirar?

La frontera no es entre verdad y
mentira, sino entre uso crítico y
uso ingenuo.

¿Y tú?

¿Has visto alguna "alucinación útil"
últimamente?

Aprovecho para enviaros un fuerte
abrazo



C2C Consultoría&Compliance



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



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

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

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

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

LA CIBERSEGURIDAD NO ES SOLO PROTEGER, ES TAMBIÉN CUMPLIR LA LEY

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Adolfo M. Gelder
S&S Consultores Corporativos C.A.

¡Saludos, lectores! ¿Listos para enterarse de lo que sucede en el mundo de la ciberseguridad este mes de junio de 2025? Olvídense de los términos complicados y los rollos técnicos. Hoy vamos a conversar, de tú a tú, sobre esas cosas que, aunque no lo creas, pueden afectar tu vida digital (¡y hasta tu cartera!) si no les pones un poquito de atención.

Porque, seamos honestos, hoy en día casi todo lo hacemos por internet: desde pagar la energía eléctrica hasta echar chismecito con las panas. Y así como nos cuidamos al salir a la calle, también hay que echarle un ojo a la seguridad de nuestra información en el mundo digital.

Las reglas del juego digital están cambiando: más ojo con la seguridad informática

Primero, hablemos de las reglas. Hay un montón de normativas nuevas que están haciendo que las empresas (y nosotros) tengamos que ponernos las pilas con la ciberseguridad. Piensa en MiCA, DORA y NIS2 si estás en Europa; estas no son solo letras, son marcos que obligan a las organizaciones a cuidar mejor tus datos y su propia seguridad digital. Pero no solo eso.

Otros estándares importantes como PCI DSS 4.0 han subido el nivel de protección cuando pagas con tarjeta por internet, exigiendo medidas como:

- Autenticación multifactor obligatoria: Ya no basta con tu contraseña; te pedirán un código extra o algo más para acceder a tus datos de pago.
- Más flexibilidad: Ahora, las empresas pueden adaptarse mejor a cómo manejan sus pagos, sin dejar la seguridad de lado.
- Cifrado más fuerte: Tus datos bancarios estarán más protegidos con mejores candados digitales.
- Más supervisión: Se harán más pruebas y auditorías para garantizar que todo esté en orden.

Y si hablamos de tu privacidad, la norma ISO/IEC 27701 se ha convertido en un súper aliado. Este estándar ayuda a las empresas a manejar tus datos personales con más cuidado y a cumplir con leyes de privacidad como el RGPD europeo. Es como tener un guardaespaldas para tu información, asegurando que se use de forma transparente y solo para lo que se debe. ¡Cuidado! La inteligencia artificial está cambiando el juego para los ciberdelincuentes.

La ciberseguridad en junio de 2025 es un tema que no podemos ignorar. Con nuevas regulaciones, amenazas más sofisticadas debido a la inteligencia artificial y programas que impulsan la inclusión, estamos en un momento emocionante (y desafiante) para el mundo digital

@adogel
Adolfo M. Gelde



Ahora, lo que nos compete: las amenazas. La inteligencia artificial generativa (sí, esa que crea textos e imágenes increíbles) se ha convertido en la nueva arma favorita de los ciberdelincuentes. Esto significa que están desarrollando:

- Phishing automatizado: Correos electrónicos falsos tan bien redactados que te harán dudar. Ya no son esos mensajes mal escritos de antes; ahora son personalizados y súper convincentes.
- Deepfakes avanzados: Videos y audios falsos tan perfectos que no sabrás si son reales o no. Imagina que alguien use tu voz o la de un famoso para estafar. ¡Qué locura, ¿no?!
- Malware evolucionado: Virus informáticos que se adaptan y evaden las defensas de tu computadora. Es como un bicho que aprende a esconderse.

No es de extrañar que casi el 70 % de las empresas estén preocupadas por esto. Por eso, muchas ya están invirtiendo en herramientas de seguridad que usan inteligencia artificial para combatir la inteligencia artificial de los ciberdelincuentes. Es una batalla de "IA contra IA" para proteger nuestros datos. Un futuro más inclusivo en ciberseguridad: ¡Mujeres al poder! Finalmente, una buena noticia y un punto clave para el futuro: la inclusión en ciberseguridad. Programas como IT For Girls 2025 están abriendo puertas y rompiendo barreras para las mujeres en el mundo tech. ¿De qué trata? Es una iniciativa gratuita de formación y mentoría para mujeres mayores de 18 años que quieren entrarle o crecer en tecnología.

El programa es una joya porque incluye:

- Charlas en vivo con expertas.
- Un examen para ganar becas de estudio.
- Cursos en la academia Udemy (que valga la cuña) sobre ciberseguridad básica, seguridad en sistemas de control y hasta inglés.
- 900 certificaciones de Claroty (otro spoiler más).
- Mentorías con mujeres que ya trabajan en el sector.
- Acceso a una comunidad para seguir aprendiendo.

EL NUEVO CAMPO DE BATALLA: INNOVACIÓN, DATOS Y LEY

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Rosa Fernández

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

ASUNTO: SEGURIDAD, TECNOLOGÍA Y DERECHOS

Este artículo es para ti, si, ya sé. Es muy especializado porque no todo el mundo es Director de Seguridad, pero por eso quiero que salgas ahí y hagas tu trabajo con la máxima protección legal. Así que lee con atención. Como directores de seguridad, la responsabilidad de integrar tecnología avanzada en los sistemas de vigilancia sin vulnerar el derecho fundamental a la privacidad exige una planificación meticulosa y un compromiso con la transparencia, la formación y la mejora continua. Cumplir con el RGPD no solo es un requisito legal, sino también una oportunidad para fortalecer la confianza de clientes y ciudadanos, garantizando que la seguridad y la innovación vayan de la mano en un entorno ético y legalmente sólido.

Y para eso ¿Qué puedes hacer? A continuación te doy unas cuantas claves para que las apliques, para que las valores y para que, cuando tengas que tomar acción, pienses en que el dato es un activo más a proteger.

Principios al principio. Principio de Legalidad y Proporcionalidad Toda actividad de vigilancia debe estar sustentada en una base jurídica que justifique el tratamiento de datos personales. Es imprescindible: Definir objetivos claros: Establecer y documentar la finalidad de cada acción de vigilancia, asegurando que sea legítima y necesaria para la protección de bienes o personas. Evaluar la proporcionalidad: Garantizar que la captación y el tratamiento de datos sean adecuados y limitados al objetivo perseguido, evitando la recogida masiva o innecesaria de información.

Evalúa impactos La incorporación de tecnologías disruptivas, como los drones, requiere la realización de una Evaluación de Impacto en la Protección de Datos (EIPD) Identificación y análisis de riesgos: Determinar las posibles vulnerabilidades en el tratamiento de imágenes y otros datos sensibles recogidos durante la vigilancia. Medidas de mitigación: Diseñar y aplicar estrategias que reduzcan los riesgos, tales como la anonimización de datos y la implementación de protocolos de seguridad robustos.

Sus datos son sus derechos Así que Transparencia, y no pierdas de vista los Derechos de las Personas Vigiladas El respeto a la privacidad implica informar de manera clara y accesible a las personas sobre el uso de sistemas de vigilancia: Información previa: Colocar avisos visibles en las zonas vigiladas, indicando la presencia de tecnologías de monitorización y los fines para los que se utilizan los datos. Ejercicio de derechos: Facilitar el acceso, rectificación, supresión y oposición en relación con los datos captados, garantizando un procedimiento ágil y efectivo.



Procesa datos con seguridad Gestión Segura de las Imágenes y Datos Recogidos La seguridad de la información es un pilar fundamental: Almacenamiento seguro: Implementar medidas técnicas como el cifrado y controles de acceso estrictos para evitar accesos no autorizados. Plazos de conservación: Establecer políticas de retención de datos que aseguren la eliminación o anonimización de la información una vez cumplida la finalidad para la que se recabó.

La seguridad empieza en tu empresa Medidas Técnicas y Organizativas La integración de dispositivos innovadores debe estar acompañada de medidas robustas: Control de acceso y autenticación: Solo personal autorizado y debidamente formado deberá tener acceso a los sistemas de vigilancia y a los datos. Auditorías y revisiones periódicas: Realizar controles internos y auditorías de cumplimiento para detectar posibles incidencias y adoptar medidas correctivas de forma oportuna

Sin formación, no hay protección Formación y Concienciación del Personal El factor humano es clave en la gestión de la seguridad y la protección de datos: Capacitación continua: Asegurar que todo el personal involucrado en las actividades de vigilancia esté actualizado en cuanto a la normativa RGPD y en las mejores prácticas de protección de datos. Cultura de privacidad: Fomentar una cultura organizacional basada en el respeto a la privacidad y la protección de datos, garantizando que los operativos de vigilancia se realicen con la debida ética y profesionalidad.

Siempre alerta Actualización y Adaptación a la Innovación Tecnológica El dinamismo del sector tecnológico exige una constante revisión de las medidas implementadas: Vigilancia normativa: Mantenerse al día con las actualizaciones y modificaciones del RGPD y otras normativas complementarias a nivel nacional e internacional. Innovación responsable: Evaluar periódicamente el impacto de nuevas tecnologías en el tratamiento de datos y ajustar las políticas y procedimientos internos para asegurar la conformidad legal.

TU ELIGES EL NIVEL DE SEGURIDAD

Consultoría Jurídica
Implantación RGPD RIA
Formación con IA
Mantenimiento RGPD
Guías especializadas



Rosa 6.0

Código Experiencia



Diplomada en Derecho, Tecnología e Innovación

Compliance (RGPD, RIA, LOPDgdd, LSICE)

Consultora Sr Calidad (ISO, EFQM, 5S)

Consultora Jurídica

Técnica en Ciberseguridad

Formadora veterana*

Diseñadora de material didáctico

Miembro Comité Técnico Asesor en MetroRisk

Socia de ENATIC, asociación de Abogacía Digital

Competencias técnicas:

WORDPRESS, PRESTASHOP, POWTOON, DOODLY,
ADOBE AUDITION, MOODLE, OBS, VIMEO, IA.



LA SEGURIDAD FERROVIARIA EN LA LEY DE SEGURIDAD PRIVADA: INFRAESTRUCTURAS CRÍTICAS Y RETOS OPERATIVOS

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Carlos Serrano
Director de Contenidos de Seguridad y Empleo

El transporte ferroviario, gestionado por operadores como Renfe, ADIF, Metro de Madrid o FGV, constituye una red esencial para la movilidad nacional. Su protección es una prioridad estratégica recogida en la Ley 5/2014, de Seguridad Privada, que reconoce y regula la participación del sector privado en la vigilancia de servicios considerados esenciales, incluyendo muchas de las infraestructuras ferroviarias designadas como infraestructuras críticas conforme a la Ley 8/2011.

El refuerzo de la seguridad ferroviaria pasa actualmente por una mayor presencia de personal de seguridad privada en estaciones, trenes y centros logísticos, con dispositivos ampliados que permiten una cobertura operativa más eficiente, disuasoria y adaptada a la realidad delictiva creciente en entornos de alta concurrencia. Se ha consolidado además la ampliación de los servicios armados en ubicaciones estratégicas, especialmente en estaciones de gran afluencia, terminales de larga distancia, centros de control o instalaciones técnicas consideradas de alto valor.

Estos servicios incluyen protección estática, patrullas móviles y dispositivos preventivos ante situaciones de riesgo elevado o niveles de alerta antiterrorista. Asimismo, las operaciones de recaudación y recarga de máquinas de autoventa y billetes, consideradas de especial sensibilidad, requieren una vigilancia específica, con vigilantes armados y binomios coordinados para garantizar la integridad de los fondos y la seguridad de los equipos técnicos y del personal de intervención. La separación de estos binomios o su debilitamiento operativo se ha señalado en diversas ocasiones como una medida contraproducente en términos de seguridad.

En el ámbito del control y supervisión, se refuerza la operatividad del CECOM (Centro de Control de Seguridad), que actúa como punto neurálgico para la recepción de incidencias, coordinación con las Fuerzas y Cuerpos de Seguridad del Estado y activación de protocolos de emergencia. La mejora de su capacidad de respuesta y de sus herramientas tecnológicas, incluyendo videovigilancia, geolocalización de efectivos y monitorización en tiempo real, constituye una prioridad dentro de los planes de modernización del sistema ferroviario.



www.seguridadyempleo.com



Los retos operativos siguen siendo múltiples. Entre ellos, destacan:

La creciente conflictividad social en determinadas líneas o franjas horarias, que exige reforzar la vigilancia presencial, especialmente en servicios nocturnos, trenes regionales o estaciones intermodales.

- La necesidad de protocolos de intervención actualizados frente a actos vandálicos, sabotajes, agresiones al personal, tentativas de intrusión y situaciones de pánico colectivo.
- La implementación de formación específica para los vigilantes de seguridad destinados al ámbito ferroviario, con módulos obligatorios sobre riesgos ferroviarios, primeros auxilios, autoprotección, procedimientos de evacuación y coordinación en emergencias.
- La integración de medidas de ciberseguridad ferroviaria frente a posibles ataques a sistemas críticos (SCADA, ticketing digital, señalización automatizada, etc.), con colaboración activa entre los departamentos de seguridad física y digital.
- La consolidación de planes de resiliencia y continuidad operativa, ante situaciones como fenómenos climáticos extremos, alteraciones del orden público o interrupciones del servicio por causas técnicas o humanas.

La seguridad ferroviaria se encuentra, por tanto, en una fase de refuerzo estructural, donde la seguridad privada desempeña un papel esencial en la prevención, respuesta operativa y garantía de la continuidad del servicio, en colaboración permanente con la seguridad pública y los órganos de gestión de cada operador ferroviario

Carlos Serrano
Director de la Web, Seguridad y Empleo

HORA DE MODERNIZAR NUESTRO SECTOR

CARTILLA
PROFESIONAL
DE
SEGURIDAD
PRIVADA

Digitalización, formación y dignidad profesional.

¡PROMOCIÓN METRORISK 35 €

(Precio habitual: 50 €)

OFERTA EXCLUSIVA PARA SOCIOS O
SIMPATIZANTES DE METRORISK

Elaboración del mapa de riesgos

Promoción válida hasta el 15/06/2025

Antes 50 h



50 horas



1 mes



2 créditos ECTS



Online



Certificado por:

**Universidad Vitoria-Gasteiz
- EUNEIZ**

La Universidad EUNEIZ.(Vitoria-Gasteiz), a través de su
Departamento de Titulos Propios, lo que garantiza
su calidad y reconocimiento como diploma
de universidad



25/05/2025 – 24/06/2025

SEGURIDAD EN EVENTOS: CONFIANZA, LEGALIDAD Y RESPONSABILIDAD

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Abraham Santana Herrera
Director de seguridad. Perito

Organizar un evento implica mucho más que logística, imagen o entretenimiento: implica garantizar la seguridad de todos los asistentes, trabajadores y bienes implicados. Y para ello, la contratación del servicio de seguridad debe realizarse con absoluta seriedad, respeto a la legalidad y criterios técnicos profesionales.

Lamentablemente, en muchos eventos aún se observan prácticas irregulares: personal sin habilitación legal, ausencia de directores de seguridad, empresas sin licencia o con medios inadecuados. Este tipo de actuaciones no solo incumplen la normativa vigente, sino que ponen en riesgo real la integridad de las personas, y desprotegen al organizador ante cualquier incidente.

La seguridad no puede improvisarse ni abaratarse. Un evento profesional exige una respuesta contundente ante cualquier abuso o ilegalidad en este ámbito. La contratación debe incluir empresas acreditadas, personal cualificado, un plan de seguridad específico, y una supervisión continua antes, durante y después del acto.

Pero más allá del cumplimiento legal, está lo más importante: la percepción del público y los clientes. Saber que están protegidos por profesionales bien formados, visibles y eficaces, genera confianza, mejora la reputación del evento y refuerza su prestigio.

Quien organiza un evento debe entender que, al igual que invierte en sonido, iluminación o comunicación, también debe invertir en lo más valioso: la tranquilidad de estar en buenas manos.



Contrataciones irregulares: una amenaza oculta

En los últimos años se ha hecho común observar prácticas que bordean, cuando no infringen directamente, la legalidad. Se contrata personal sin habilitación oficial, se prescinde de la figura del Director de Seguridad incluso en eventos de alto riesgo, o se recurre a empresas no inscritas en el registro de seguridad privada. En ocasiones, incluso se opta por meros auxiliares sin formación específica, a los que se les exige actuar ante situaciones críticas para las que no están preparados.

Estas decisiones no solo suponen un fraude normativo, sino que comprometen la eficacia del servicio de seguridad y la integridad física de los asistentes y trabajadores. Las leyes que regulan la seguridad privada no son un formalismo burocrático: son la garantía de que el personal está cualificado, que la empresa responde legalmente, y que existe un plan específico de actuación.

La necesidad de una respuesta contundente

Frente a estos abusos, es imprescindible actuar con determinación. Como consultores de seguridad, debemos denunciar, rechazar y combatir cualquier intento de precarizar o falsear el servicio. Un evento seguro empieza con una contratación responsable. No se trata solo de cumplir con la ley, sino de proteger a las personas.

Los organizadores deben ser plenamente conscientes de que delegar la seguridad en manos no profesionales puede derivar en incidentes graves, responsabilidades penales y un deterioro irreversible de su imagen pública. Las autoridades también deben vigilar y sancionar las malas prácticas, y fomentar una cultura preventiva en el sector.

El valor estratégico de la confianza

Más allá de la normativa, hay un valor intangible que se construye en cada evento bien gestionado: la confianza del público y del cliente. Un sistema de seguridad profesional, visible pero no invasivo, bien coordinado y respaldado por un plan de acción sólido, genera tranquilidad. Las personas perciben que están en un entorno controlado, en el que si ocurre algo, habrá respuesta inmediata y eficaz.



SEGUROS Y SEGURIDAD PRIVADA EN EVENTOS: DOS PILARES DE UNA GESTIÓN RESPONSABLE

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Alina Rubio de las Casas Experta en Seguros Generales

La organización de eventos conlleva una serie de responsabilidades legales, operativas y reputacionales que no deben ser subestimadas. Uno de los aspectos más sensibles, y a menudo mal entendidos, es la gestión del riesgo. Aquí es donde el binomio seguros + seguridad privada se convierte en una herramienta estratégica imprescindible.

Agente exclusivo, Generali Seguros
Planes diseñados a medida de tus necesidades,
con atención directa y profesional
alinarubiodecasas@gmail.com

El seguro como respaldo financiero ante el riesgo

Toda actividad pública genera riesgos: desde caídas y lesiones, hasta daños a instalaciones, problemas de aforo, evacuaciones o incluso incidentes de orden público. El seguro, en este contexto, no es un simple requisito legal o administrativo, sino una protección financiera ante eventualidades que pueden comprometer gravemente la viabilidad del evento o la continuidad del organizador.

Las pólizas más comunes en eventos incluyen:

- Responsabilidad civil general y profesional
- Daños a terceros y a instalaciones
- Coberturas por cancelación o suspensión
- Seguro de accidentes para asistentes o personal
- Robo o daño de equipamiento técnico

Sin embargo, la póliza es solo efectiva si va acompañada de una gestión activa de la seguridad, que minimice la probabilidad de siniestros y demuestre diligencia profesional ante cualquier reclamación.

Seguridad privada: prevención, control y actuación

Aquí entra en juego la seguridad privada profesional, que no debe confundirse con la mera presencia física de vigilantes. La seguridad efectiva en un evento parte de un plan de seguridad redactado por un Director de Seguridad o consultor cualificado, con análisis de riesgos, planes de contingencia, control de accesos, coordinación con servicios públicos, y protocolos específicos según el tipo y escala del evento.

Una seguridad mal diseñada o ejecutada no solo incrementa el riesgo real, sino que puede invalidar la cobertura del seguro si se demuestra negligencia, personal no habilitado, o incumplimiento de las medidas de control establecidas en el propio contrato de seguros.



Complementariedad estratégica: seguro + seguridad

El enfoque profesional debe ser integrador: el seguro no reemplaza a la seguridad, y la seguridad no elimina la necesidad del seguro. Ambos elementos son complementarios. La seguridad privada reduce la probabilidad del siniestro; el seguro, en caso de que este se produzca, responde económicamente.

Un organizador que contrata ambos servicios con criterios técnicos, y los alinea en un único plan de prevención, está construyendo un evento sólido, responsable y resiliente, capaz de afrontar no solo los desafíos logísticos del día a día, sino también cualquier imprevisto con respaldo legal y financiero.

Ventajas operativas y reputacionales

Contar con un dispositivo de seguridad profesional y una cobertura aseguradora bien definida no solo es una obligación moral y legal: es una ventaja comercial. Refuerza la imagen del organizador, transmite confianza a patrocinadores y participantes, y facilita la autorización administrativa del evento.

Además, cada vez más aseguradoras solicitan informes de seguridad, presencia de personal habilitado y memoria de riesgos como condición previa para ofrecer o mantener la póliza. De ahí que trabajar con consultores especializados en seguridad de eventos sea una inversión estratégica, no un gasto accesorio.

SEGUROS Y SEGURIDAD PRIVADA EN EVENTOS: DOS PILARES DE UNA GESTIÓN RESPONSABLE

La organización de eventos exige minimizar riesgos, tanto con una cobertura adecuada de seguros como con medidas eficaces de seguridad privada

SECURITY



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, cibercrimen y delitos económicos.

DETECCIÓN

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

INVESTIGACIÓN

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

SEGURIDAD INTEGRAL

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

BLINDANDO LA CIUDAD INTELIGENTE SMART CITIES: UNA ESTRATEGIA DE CIBERSEGURIDAD HOLÍSTICA PARA EL ALUMBRADO PÚBLICO.

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Elena de la Parte

El zumbido, casi imperceptible de los datos, fluyendo a través de las redes, se ha convertido en la banda sonora silenciosa de nuestra era. El pulso constante de los datos viajando a la velocidad de la luz ha transformado radicalmente la textura de nuestras vidas. Las tecnologías de la información y la comunicación (TIC), invisibles pero omnipresentes, han redibujado el mapa de nuestras relaciones, dejando una huella digital indeleble en cada interacción, desde el fugaz intercambio de un mensaje hasta la construcción de comunidades virtuales enteras.

Piense por un momento en la paradoja de esta editorial: Imaginemos este precioso instante:

Tú leyendo estas palabras desde tu ciudad y yo, hilvanando estas palabras desde este rincón asturiano y tejiendo esta reflexión, un entorno digital que, aunque intangible.

Es tan real como la brisa que recorre las calles de Gijón, naciendo bajo el sol que ilumina Málaga, ese astro andaluz que irradia su calidez, no solo a la Costa del Sol, sino que también alcanzan con sus rayos virtuales otras urbes o el bullicio cosmopolita de Madrid tomando forma mientras el sol Mediterráneo baña Valencia, y siendo leído, quizás bajo el cielo castellano y otros asoman a esa misma reflexión desde la vibrante Barcelona o la histórica Sevilla.

Incluso se percibe en todos los continentes de mapa del mundo. "Sin embargo, en este universo donde los "me gusta" y los "compartir" proliferan con la rapidez con la que los helados se derriten bajo el sol de junio, a menudo dejando tras de sí solo un recuerdo fugaz del dulzura...."

¿Estamos realmente cultivando la profundidad de nuestros vínculos o nos estamos conformando con la fugacidad de la interacción digital?

La conectividad nos une, pero también nos expone. La seguridad de nuestros sistemas ya no es una preocupación periférica, sino una urgencia central en la evolución de nuestras sociedades tecnológicamente avanzadas.

Las (TIC) han trascendido su función original como herramienta de progreso para convertirse en el entramado invisible que sostiene una existencia digital. En la era de la hiper conectividad urbana, donde cada farola puede ser un sensor y cada puesto un nodo de información, la promesa de las ciudades inteligentes se entrelaza inevitablemente con la creciente superficie del ataque digital. Tal como las tecnologías de la información y la comunicación (TIC), han permeado, cada aspecto de nuestras vidas, transformando desde la colaboración remota hasta la aparición de algunas formas de criminalidad, la infraestructura inteligente de nuestras ciudades no es una excepción. El alumbrado público, columna vertebral de la vida nocturna y creciente fuente de datos urbanos, emerge como un punto crítico que demanda una atención prioritaria en materia de ciberseguridad.



La visión de un alumbrado público inteligente capaz de optimizar el consumo energético, recopilar datos ambientales o incluso facilitar la movilidad urbana, se materializa a través de una intrincada red de luminarias, sensores y sistemas de gestión centralizados. Sin embargo, esta misma interconexión que potencia la eficacia y la innovación, (I+D+i), abre una ventana de oportunidad para los ciberdelincuentes. Si bien los datos de intensidad lumínica pueden aparecer inocuos, las credenciales de acceso a estos sistemas representan un botín mucho más valioso. Una vez comprometidos los puntos de control del alumbrado, los atacantes pueden moverse literalmente hacia otras redes internas de la ciudad inteligente con consecuencias potencialmente devastadoras.

Las amenazas tradicionales, desde el sigiloso spyware hasta el paralizante ransomware y los disruptivos virus informáticos, encuentran un nuevo caldo de cultivo en estos entornos de control y supervisión. Ataques de Sniffing acechan en los flujos de datos entre luminarias y sistemas de gestión buscando vulnerabilidades, la vasta cantidad de puntos de red convierte al alumbrado público en un objetivo atractivo para ataques de denegación de servicio distribuido (D DOS), capaces de asumir barrios enteros en la oscuridad y paralizar servicios esenciales. Más allá de la interrupción inmediata, los costes asociados a la reparación de sistemas comprometidos y la implementación de defensas robustas contra futuros ataques puede ascender a cifras significativas. Ante este programa, la estrategia de seguridad perimetral tradicional se revela como una defensa incompleta. Proteger únicamente la entrada a la red es análogo a fortificar la puerta principal de una casa con ventanas y muros desprotegidos. La complejidad y la distribución de las infraestructuras inteligentes exigen un enfoque más; granular resistente, resiliente a una estrategia de defensa en profundidad. Esta filosofía de ciberseguridad de extremo a extremo implica reconstruir la arquitectura de la ciudad conectada con la seguridad como principio fundamental, analizando cada capa de las redes industriales hasta llegar al último sensor del alumbrado público.



La ciberseguridad urbana debe cimentarse en la protección activa de cada subconjunto del sistema, implementando una serie de medidas interconectadas y redundantes, como las citadas a continuación:

- **-Segmentación de la red:** *Dividir la red en zonas aisladas, lógicamente impide que un ataque a un componente del alumbrado se propague sin control a otros sistemas críticos de la ciudad.*
- **-Control de flujos:** *Implementar políticas estrictas sobre el tráfico de datos entre los diferentes segmentos de la red, limitando la comunicación solo a lo estrictamente necesario.* **-Cifrado de los canales de comunicación:** *Proteger la confidencialidad e integridad de los datos transmitidos entre los dispositivos del alumbrado y los sistemas de gestión, mediante protocolos de cifrado robustos de extremo a extremo (E2EE).*
- **-Aplicación multi factor (MFA):** *Exigir múltiples formas de verificación de identidad para acceder a los sistemas críticos, añadiendo una capa adicional de seguridad contra el robo de credenciales.*
- **-Cortafuegos avanzados:** *Desplegar cortafuegos con funcionalidades de segmentación de red, sistemas de prevención de intrusiones (IPS) y capacidades de bypass para garantizar la continuidad y disponibilidad del servicio ante posibles fallos o ataques. Además, asegurar los accesos remotos para el tele -mantenimiento a través de redes privadas virtuales (VPN).*
- **-Formación y concienciación de los empleados:** *Capacitar al personal encargado de la gestión y mantenimiento del alumbrado sobre las mejores prácticas en higiene digital, los riesgos de ingeniería social y la identificación de comportamientos sospechosos*
- **-Políticas de gestión de parches:** *Implementar un proceso riguroso para la aplicación oportuna de actualizaciones y parches de seguridad en todos los sistemas y dispositivos conectados.*
- **-Administración de derechos y autorizaciones:** *Adoptar una política de mínimos privilegios, otorgando a los usuarios solo los permisos necesarios para realizar sus tareas.*
- **-Capacitación de los equipos de seguridad:** *Dotar a los equipos de seguridad de las habilidades y herramientas necesarias para detectar, analizar y responder eficazmente a incidentes de seguridad*

La promesa de las ciudades inteligentes Smart cities se sostiene sobre la robustez de su ciberseguridad. Proteger La infraestructura del alumbrado público no es solo una cuestión de evitar interrupciones del servicio; se trata de salvaguardar la integridad de los datos urbanos, la seguridad de otros sistemas interconectados y en última instancia, la confianza de los ciudadanos.

Adoptar una estrategia de defensa en profundidad, centrada en la protección de cada subsistema y respaldada por una cultura de seguridad proactiva, es el camino para iluminar el futuro de nuestras ciudades de manera segura y resiliente.

“En un mundo hiper conectado, donde quizás ahora mismo estas palabras se encuentran en tus ojos, la seguridad digital no es solo una precaución, sino el pilar fundamental de nuestra protección en la era digital”



ENTRENAMIENTO RECURSIVO CON DRONES: HACIA UNA SEGURIDAD PRIVADA MÁS DINÁMICA, PROFESIONAL Y TECNOLÓGICA

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Introducción: drones, vigilancia y evolución del rol del profesional de seguridad

La seguridad privada está experimentando una transformación en la que la tecnología juega un papel protagonista. La incorporación de sistemas aéreos no tripulados (UAS o drones) está permitiendo nuevas formas de vigilancia, patrullaje, control perimetral y respuesta ante emergencias. Lo que hasta hace poco era exclusivo del ámbito militar o de cuerpos policiales especializados, hoy comienza a consolidarse como una herramienta accesible para los profesionales de la seguridad privada. Pero esta integración tecnológica no se puede abordar de manera superficial. No basta con disponer del equipo: es necesario saber operarlo con responsabilidad, criterio y conocimiento, en entornos reales y bajo presión. En este contexto, la formación cobra un papel clave, y dentro de ella, el llamado entrenamiento recursivo se presenta como una metodología especialmente valiosa.

Operar un dron en seguridad privada: más que pilotar El operador de drones en seguridad no es simplemente un piloto. Su función implica tareas complejas: supervisar zonas amplias desde el aire, detectar movimientos o elementos sospechosos, dar apoyo visual en tiempo real a equipos en tierra, o incluso colaborar en la verificación de alarmas y en operaciones de evacuación. Este profesional debe combinar habilidades técnicas de vuelo con competencias propias del ámbito de la seguridad, como la gestión de riesgos, la observación estratégica o la toma de decisiones rápidas. Además, debe conocer las normativas aéreas, las limitaciones operativas según cada tipo de entorno, y los requisitos legales que rigen el uso profesional de drones. Por tanto, formar a estos operadores no consiste en un simple curso de iniciación. Se trata de un proceso continuo y exigente, que requiere práctica realista, actualización constante y capacidad de análisis. Aquí es donde entra el entrenamiento recursivo.

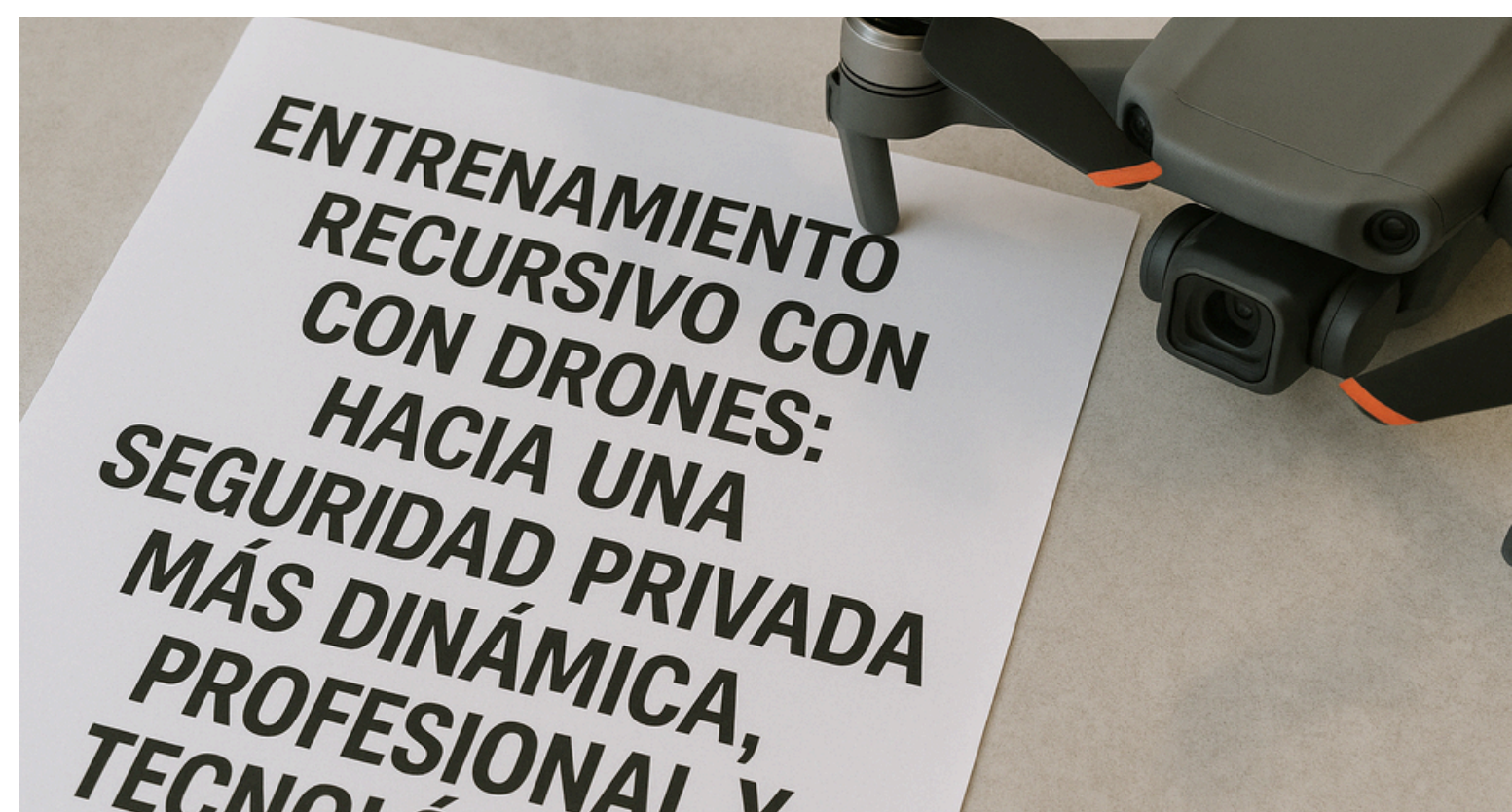
Entrenamiento recursivo: aprender desde la práctica estructurada El entrenamiento recursivo es un modelo basado en la repetición deliberada y el análisis reflexivo. Cada práctica no se considera un fin en sí mismo, sino una base sobre la cual se construye el siguiente ejercicio. Se parte de la experiencia, se evalúa, se corrige y se vuelve a ejecutar con mejoras. Este ciclo continuo permite que el operador desarrolle:

- Adaptación progresiva a diferentes escenarios (urbanos, rurales, industriales, nocturnos).
- Mejora en la toma de decisiones tácticas, al identificar patrones operativos.
- Disminución de errores, mediante la anticipación a fallos comunes.
- Confianza operativa, resultado del dominio adquirido con la práctica crítica.

Este tipo de entrenamiento se aleja de los modelos formativos estáticos o puramente teóricos, proponiendo un camino más dinámico y ajustado a las necesidades reales del terreno.



La formación certificada: un pilar para operar con legitimidad En paralelo al desarrollo técnico y táctico, todo operador profesional de drones debe cumplir con una serie de requisitos legales y certificaciones oficiales, establecidos por la Agencia Estatal de Seguridad Aérea (AESA) y regulados a nivel europeo por la EASA. Esto incluye: - Formación teórica y práctica adecuada a la categoría de operación. - Conocimiento de las zonas de vuelo restringidas y gestión del espacio aéreo. - Capacitación en seguridad operacional, mantenimiento del equipo y respuesta ante incidentes. - Capacidad para planificar, documentar y justificar cada vuelo profesional. Estas exigencias no solo responden a razones legales. Cumplirlas es una garantía de que el operador entiende los límites, responsabilidades y riesgos asociados al uso de drones. Y en un sector como el de la seguridad privada, donde los errores pueden tener consecuencias importantes, la profesionalización y la cualificación son fundamentales.



ENTRENAMIENTO RECURSIVO CON DRONES: HACIA UNA SEGURIDAD PRIVADA MÁS DI

Un ejemplo práctico: formación especializada desde la experiencia En los últimos años, distintas entidades han comenzado a desarrollar programas de entrenamiento enfocados en las necesidades específicas del sector de la seguridad.

Un ejemplo de ello es Ritrac International, organización especializada en formación con drones, que trabaja con pilotos, instructores y examinadores repartidos por todo el territorio nacional. Ritrac International ha diseñado entrenamientos que aplican el enfoque recursivo en contextos reales de seguridad privada, incluyendo simulaciones de vigilancia perimetral, control de accesos en eventos, búsqueda de intrusos en zonas boscosas o apoyo aéreo a patrullas. Esta experiencia acumulada permite no solo enseñar a volar, sino formar a operadores que entienden el contexto en el que van a intervenir y que pueden desenvolverse en situaciones complejas con criterio propio.

El aporte de entidades como Ritrac también ha sido relevante a la hora de acompañar a profesionales del sector en su proceso de obtención de certificados oficiales, promoviendo una visión de la formación como un proceso integral y continuado.

Beneficios para el profesional y la empresa Para el profesional de la seguridad privada, contar con formación certificada y entrenamiento recursivo supone:

- - Acceder a un perfil profesional con alta demanda.
- - Mejorar su autonomía y nivel de responsabilidad dentro del equipo.
- - Aumentar su capacidad de análisis y toma de decisiones en situaciones de riesgo.
- - Estar en condiciones de adaptarse a nuevas herramientas tecnológicas.

Para la empresa de seguridad, incorporar operadores de drones bien formados significa:

- - Elevar la calidad y efectividad del servicio ofrecido.
- - Ganar independencia tecnológica y capacidad de respuesta.
- - Cumplir con los estándares normativos sin necesidad de terceros.
- - Reforzar su imagen como empresa innovadora y preparada.

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>

Conclusión:

hacia una nueva cultura operativa en seguridad privada La introducción de drones en seguridad privada representa un cambio de paradigma. Ya no se trata solo de tener más medios, sino de repensar cómo se forman y evolucionan los profesionales encargados de proteger infraestructuras, personas y bienes.

El entrenamiento recursivo, como metodología formativa basada en la práctica constante, la evaluación crítica y la mejora continua, se presenta como una herramienta clave para afrontar este cambio. Y cuando esta formación se desarrolla de la mano de entidades con experiencia real en el sector, como Ritrac International, se convierte en un camino viable hacia la profesionalización sostenible.

En un mundo en constante cambio, la seguridad privada no puede quedarse quieta. Necesita adaptarse, y para ello, formar operadores con herramientas tecnológicas avanzadas, criterio táctico y capacidad de aprendizaje continuo es una necesidad más que una opción.



**Servicios de Peritaje y Consultoría en Andalucía y Ceuta,
España.**

**Due Diligence - Debida Diligencia, a Nivel Nacional como
Internacional.**

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

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

Colaboramos con MR-CONSULTING.



**Asesoramiento Técnico
Especializado, para Situaciones
legales y Técnicas:**

En el Ámbito de la:

Seguridad Privada, Balística Forense.

Ciberseguridad, Inteligencia y
Geopolítica.

Seguros de Embarcaciones Recreo.

Grafología, Documentoscopia,
Grafopsicopatología Criminal y
Forense.

Due Diligence (Debida Diligencia).

**[https://www.oterotrillogabinetepericial-
andaluciaceuta.es/](https://www.oterotrillogabinetepericial-andaluciaceuta.es/)**

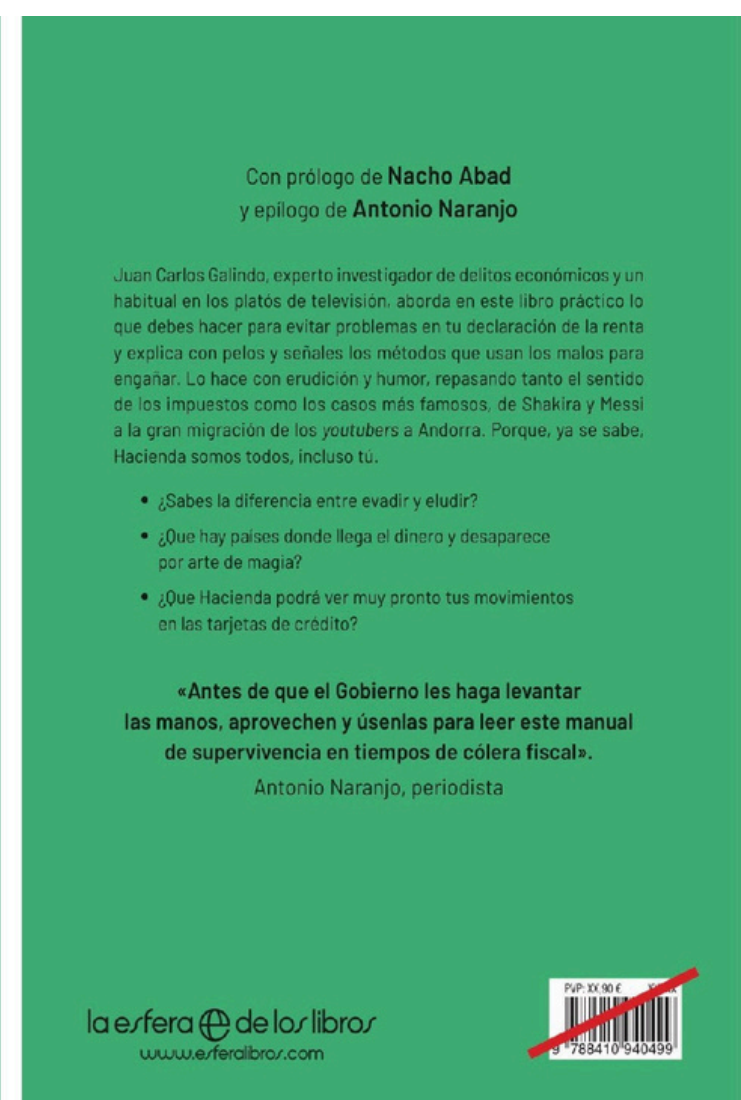
AGENDA

Metro
Risk

Edición propiedad de @MetroRisk, asociación

RADIO

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



EL CANAL DEL CORONEL



LOS CONSEJOS DE CIBERSEGURIDAD DE ADOLFO GELDER.

en: www.linkedin.com/in/adolfo-gelder-b2327bb4/

WWW.ALBERTORAY.COM

El blog de Alberto Ray, donde encontrarás todo lo relacionado con: #amenazas, #gerencia, #seguridad y #complejidad





Metrorisk

Proyecto Asociativo

www.metrorisk.es