EDITORIAL MR

ISSN 3045-7629

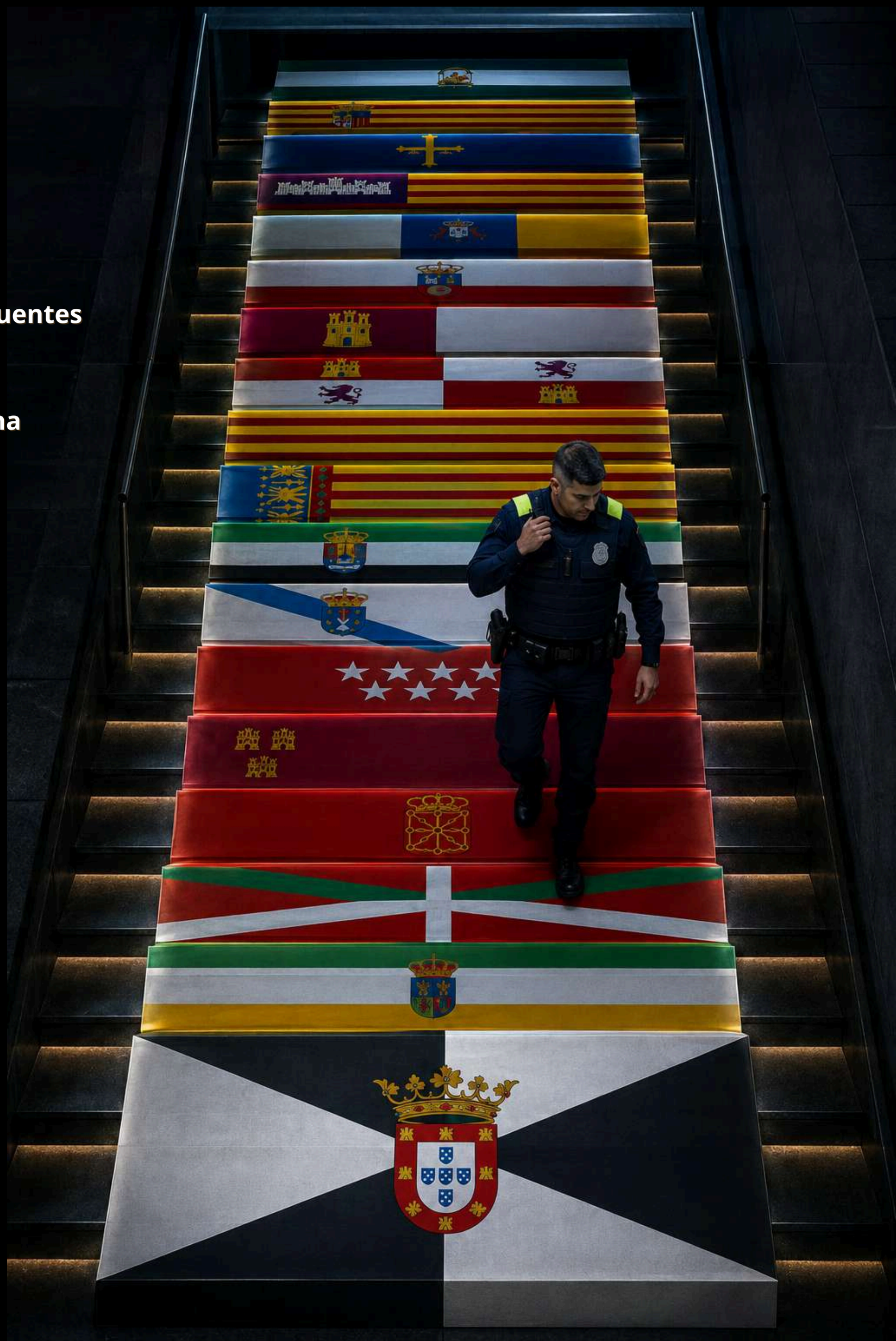
ESPECIAL OTOÑO

AÑO 2026

Edición propiedad de @MetroRisk, asociación

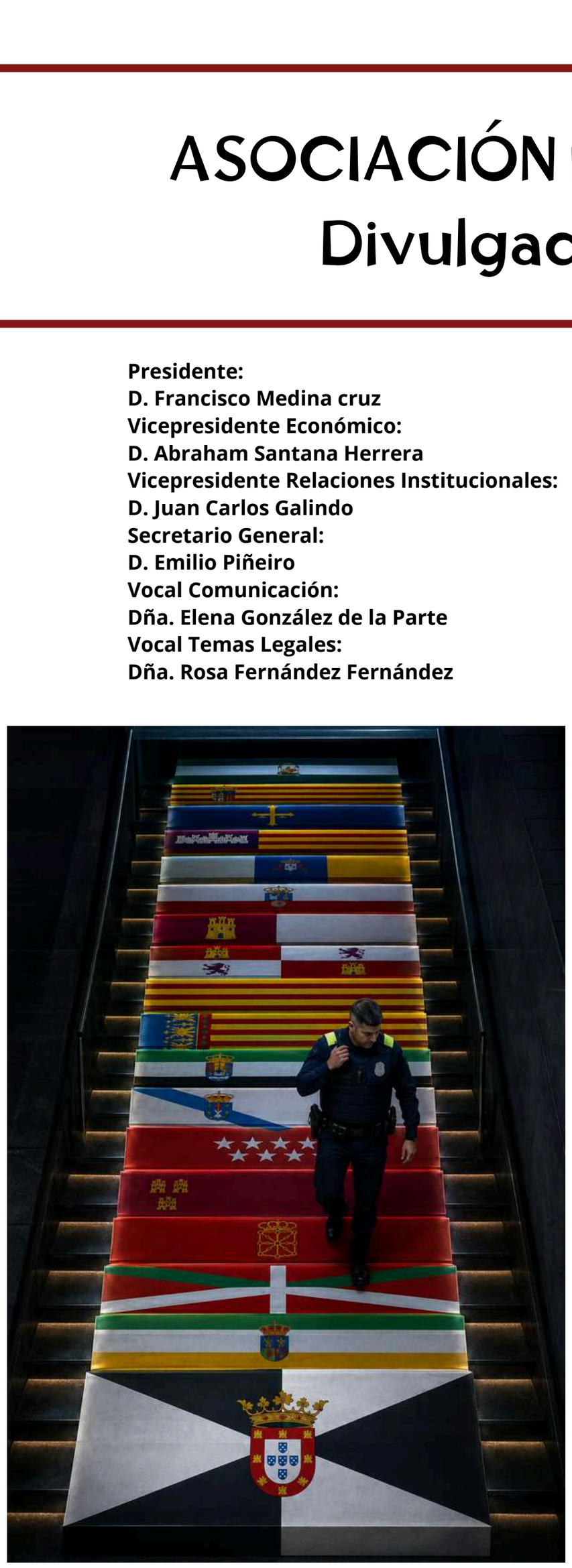
Fran Medina Cruz
Francisco Javier Gonzales Fuentes
Carlos G. Barrett
Gregorio Duro
Mercedes Escudero Carmona
Iván Cantalapiedra
Emilio Piñeiro
Joaquín Sampedro
Rosa Fernández
Carlos Serrano
Abraham Santana
Alina Rubio
Elena de la Parte
Esther Domínguez
Antonio Pérez Cala
Jonatthan Hermida Sosa
Carlos E. Pérez Barrios
Eduardo Reyes
Edison Cadena Ayala

@Metrorisk.es



ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

Editado por:
Fran Medina Cruz y Elena González de la Parte,
en Málaga, España
ISSN 3045-7629



COLABORADORES

PATROCINADO POR LAS FIRMAS

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

LA SEGURIDAD PRIVADA NO ADMITE ATAJOS

Metro Risk

Fran Medina Cruz
Director de MetroRisk

Profesionalización, control y tolerancia cero ante el incumplimiento.

La seguridad privada protege empresas, infraestructuras, centros sanitarios, espacios públicos y, sobre todo, a millones de personas. Su importancia social exige que deje de ser tratada como una actividad auxiliar y avance hacia un modelo basado en la profesionalidad, el control y la ejemplaridad.

No basta con obtener una autorización administrativa o superar inspecciones ocasionales. Las empresas de seguridad deben someterse periódicamente a auditorías especializadas, independientes y exhaustivas, supervisadas por las autoridades competentes. Estas revisiones deben comprobar su solvencia, organización, formación, cumplimiento laboral, medios técnicos, protocolos operativos y capacidad real para prestar los servicios contratados.

Una empresa que consigue una adjudicación mediante una oferta económicamente inviable y después reduce plantillas, incumple jornadas o escatima recursos no está compitiendo: está degradando el sector y poniendo en peligro a trabajadores, clientes y ciudadanos.

Cumplir todas las normas, sin excepciones

En seguridad privada no existen incumplimientos insignificantes cuando está en juego la protección de las personas. Cada protocolo omitido abre una brecha y cada profesional insuficientemente preparado aumenta el riesgo.

Las obligaciones legales, laborales y operativas no pueden considerarse obstáculos que deben sortearse para reducir costes. La profesionalidad comienza por cumplir rigurosamente todas y cada una de las normas aplicables.

Las administraciones y los clientes también deben asumir su responsabilidad. No se puede exigir excelencia mientras los contratos se adjudican casi exclusivamente por precio. Deben valorarse la calidad, la formación, la estabilidad de las plantillas, los recursos disponibles y el historial de cumplimiento de cada empresa.

Contratar la seguridad más barata no siempre supone ahorrar. Con demasiada frecuencia significa trasladar el coste del riesgo a los vigilantes, a los usuarios y a la sociedad.
Quien incumpla gravemente debe quedar fuera

Las sanciones económicas resultan insuficientes cuando pueden asumirse como un coste más de la actividad. Si incumplir continúa siendo rentable, la sanción pierde su función. Las infracciones graves o reiteradas deben producir consecuencias proporcionales: suspensión de autorizaciones, exclusión de contratos públicos, pérdida de acreditaciones y, en los casos extremos, retirada definitiva del derecho a operar. No se trata de perseguir errores administrativos involuntarios, sino de expulsar del mercado a quienes demuestren un desprecio sistemático por la legalidad, los derechos laborales o la seguridad de las personas.

Además, debe impedirse que las empresas sancionadas reaparezcan mediante sociedades instrumentales o simples cambios de denominación. La supervisión debe alcanzar a sus administradores, responsables efectivos y grupos empresariales vinculados.

Un nuevo enfoque para el siglo XXI

La seguridad privada ya no puede limitarse a la vigilancia estática. El siglo XXI exige profesionales capaces de trabajar en entornos tecnológicos, conectados y globalizados.

La ciberseguridad, la inteligencia aplicada, los sistemas remotos, los drones, la inteligencia artificial y la protección de infraestructuras críticas forman parte de esta nueva realidad. La tecnología, sin embargo, debe estar al servicio de profesionales mejor preparados, no utilizarse para sustituirlos indiscriminadamente o reducir garantías. Los vigilantes tampoco pueden seguir siendo considerados simples presencias uniformadas. Previenen incidentes, gestionan conflictos y toman decisiones de enorme responsabilidad. Necesitan formación continua, estabilidad laboral, reconocimiento social, protección jurídica y remuneraciones acordes con sus funciones.

Recursos, autoridad y ejemplaridad

La profesionalización no se consigue únicamente imponiendo nuevas obligaciones. Es necesario proporcionar recursos económicos, técnicos, formativos y legales suficientes. Las empresas responsables necesitan invertir en equipamiento e innovación. Los profesionales requieren herramientas eficaces y protocolos claros. Las autoridades deben disponer de unidades inspectoras especializadas, mientras que los clientes deben asumir que la seguridad de calidad tiene un coste real.

Fran Medina

La seguridad se contempla desde la fase de diseño.

MRConsulting

LA MEDIDA DEL RIESGO
SELLO DE GARANTIA
AÑO 2026
MR CONSULTING
SEGURIDAD · RIESGO · RESILIENCIA

ARQUITECTURA & DISEÑO
LUXURY LIVING

LA MEDIDA DEL RIESGO
SELLO DE GARANTIA
AÑO 2026
MR CONSULTING
SEGURIDAD · RIESGO · RESILIENCIA

LA MEDIDA DEL RIESGO

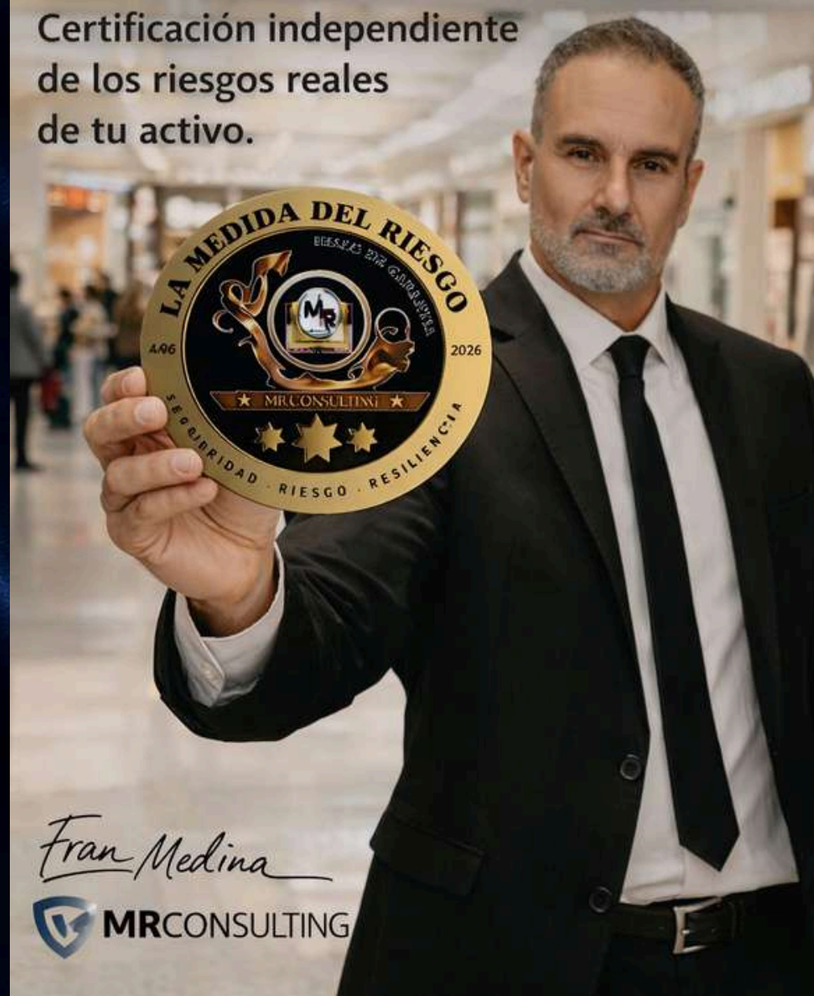
SELLO DE GARANTIA

MRCONSULTING

La seguridad no es contratar lo que te venden.

Es medir què seguridad necesitas en realiciad.

Certificación independiente de los riesgos reales de tu activo.



Fran Medina

MRCONSULTING

DEL DIRECTOR DE SEGURIDAD HABILITADO AL PROFESIONAL UNIVERSITARIO: UNA OPORTUNIDAD HISTÓRICA PARA DIGNIFICAR LA PROFESIÓN

Metro Risk

Edición propiedad de @MetroRisk, asociación

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

Universidad, habilitación profesional y experiencia deben dejar de caminar por vías paralelas. El futuro de la Dirección de Seguridad exige un marco académico común capaz de reconocer lo aprendido, valorar la trayectoria profesional y facilitar la progresión hacia el Grado.

La Dirección de Seguridad ha cambiado profundamente en las últimas décadas. También lo han hecho las organizaciones, los riesgos y las responsabilidades que recaen sobre quienes tienen encomendada la protección de personas, patrimonio, información, infraestructuras y procesos críticos.

El Director de Seguridad de hoy ya no puede ser entendido únicamente como el responsable de la vigilancia física de una instalación. Participa en la estrategia de las organizaciones, analiza riesgos, gestiona crisis, integra tecnologías, coordina recursos humanos y económicos, interviene en planes de continuidad, protección de la información, ciberseguridad, emergencias, cumplimiento normativo y relaciones con las Fuerzas y Cuerpos de Seguridad.

Sin embargo, la evolución académica de la profesión no siempre ha avanzado con la misma velocidad que sus responsabilidades.
Y quizá haya llegado el momento de abordar este debate con una perspectiva diferente.

No se trata de cuestionar lo construido. Se trata de construir sobre ello.

Dos realidades distintas que deben aprender a convivir
Uno de los primeros elementos que debemos aclarar es la diferencia entre titulación académica y habilitación profesional.
En España, el ejercicio de determinadas funciones de seguridad privada requiere la correspondiente habilitación del Ministerio del Interior, expedida a través de la Dirección General de la Policía. La Ley 5/2014, de Seguridad Privada, establece además que la formación previa para jefes y directores de seguridad puede obtenerse mediante un título universitario oficial de grado en el ámbito de la seguridad que reúna las competencias correspondientes o mediante el título del curso de Dirección de Seguridad reconocido por el Ministerio del Interior.

La Orden INT/318/2011 desarrolla esta segunda vía y establece que los cursos de Dirección de Seguridad deben estar programados e impartidos por centros universitarios reconocidos oficialmente, incluir determinadas materias y alcanzar, como mínimo, las 400 horas de formación.

Entre sus contenidos figuran la normativa de seguridad privada, seguridad física y electrónica, protección de personas, seguridad lógica, protección contra incendios, protección civil, protección de datos, dirección de equipos, planificación, análisis de riesgos, gestión de recursos y colaboración con la seguridad pública, entre otros.

Por tanto, existe ya desde hace años una conexión entre Universidad, Ministerio del Interior y formación profesional del Director de Seguridad.

Pero debemos dar un paso más.
Porque superar un curso universitario reconocido para obtener una habilitación profesional y obtener un Grado universitario oficial de 240 ECTS son realidades académicas diferentes. Una habilitación acredita legalmente la capacidad para ejercer unas funciones profesionales reguladas; un grado acredita además un determinado nivel académico dentro del Espacio Europeo de Educación Superior y permite continuar posteriormente hacia másteres oficiales, doctorado y otros itinerarios académicos.

No debemos enfrentar ambas realidades. Debemos conectarlas. No partimos de cero.

España cuenta ya con grados oficiales relacionados directamente con las Ciencias de la Seguridad, algunos de cuyos programas permiten igualmente acceder a las habilitaciones de Director y Jefe de Seguridad.

Existen, además, modelos con orientaciones diferentes: seguridad corporativa, seguridad pública, criminología y seguridad, gestión de riesgos, inteligencia o seguridad internacional. El Grado en Seguridad del Instituto de Seguridad Pública de Cataluña, centro adscrito a la Universidad de Barcelona, cuenta por ejemplo con 240 ECTS y menciones en Seguridad Corporativa y Seguridad Internacional y contempla las habilitaciones de Director y Jefe de Seguridad. También existen grados en Ciencias de la Seguridad en otras universidades españolas. Como por ejemplo en la Universidad Internacional de la Rioja UNIR.

Esta diversidad demuestra algo importante: la Seguridad ya dispone de entidad suficiente para constituir un verdadero campo universitario de conocimiento y desarrollo profesional.

Pero también plantea una cuestión.
¿Estamos aprovechando suficientemente el conocimiento acumulado por miles de profesionales que llevan diez, quince, veinte o treinta años trabajando en seguridad?
Probablemente no.

El profesional experimentado no debería tener que empezar desde cero. Este es, a nuestro juicio, uno de los grandes debates pendientes.

Pensemos en un Director de Seguridad habilitado por el Ministerio del Interior que dispone de su formación universitaria específica, veinte años de experiencia, formación continua, responsabilidades directivas, participación en grandes proyectos de seguridad, conocimientos tecnológicos, certificaciones profesionales y experiencia real gestionando crisis y riesgos.
Si ese profesional decide hoy elevar su cualificación académica y obtener un Grado en Ciencias de la Seguridad, el sistema universitario debería ser capaz de analizar todo ese patrimonio formativo y profesional y determinar qué competencias ya tiene acreditadas.

Eso no significa regalar títulos.
Significa exactamente lo contrario: evaluar rigurosamente las competencias que una persona ya posee para exigirle después aquellas que todavía debe adquirir.

La normativa universitaria española permite avanzar en esta dirección. El Real Decreto 822/2021 contempla el reconocimiento académico tanto de determinados estudios previos como de la experiencia profesional y laboral cuando esté estrechamente relacionada con las competencias del título. También establece los límites y garantías que deben respetar las universidades en esos procedimientos.

Por tanto, jurídicamente no podemos sostener que una habilitación o veinte años de experiencia equivalgan automáticamente a un Grado. Pero tampoco debemos aceptar que veinte años de ejercicio profesional cualificado equivalgan académicamente a cero. Entre ambos extremos existe un enorme espacio para trabajar.

Hacia verdaderos itinerarios de adaptación al Grado
Desde ADISPO consideramos que las asociaciones profesionales pueden desempeñar aquí un papel fundamental trabajando junto a las universidades.
.

El objetivo debería ser diseñar itinerarios académicos específicos para profesionales de la seguridad, transparentes, rigurosos y homologables entre instituciones.

Un Director de Seguridad habilitado podría presentar un verdadero expediente profesional de competencias: formación de Dirección de Seguridad realizada, titulaciones universitarias previas, formación permanente, cursos especializados, certificaciones profesionales nacionales e internacionales, años de experiencia, responsabilidades desempeñadas y proyectos acreditables.

La universidad evaluaría posteriormente qué conocimientos y competencias del correspondiente grado pueden reconocerse conforme a la legislación universitaria y a su propio plan de estudios.

A partir de ahí podría establecerse un itinerario o curso de adaptación personalizado, compuesto exclusivamente por las materias necesarias para completar las competencias universitarias restantes y, necesariamente, por aquellos elementos académicos que la normativa no permita reconocer.

No todos los profesionales partirían del mismo punto. Y eso sería precisamente lo razonable. Un profesional que ya posee una licenciatura o un grado universitario, la habilitación de Director de Seguridad, formación complementaria y quince años de ejercicio profesional no debería tener el mismo itinerario que quien accede por primera vez a la Universidad.

El reconocimiento tendría que realizarse de acuerdo con criterios académicos objetivos, no corporativos. Pero esos criterios podrían ser comunes, públicos y previsibles. El papel de las asociaciones profesionales Aquí aparece una magnífica oportunidad para las asociaciones representativas del sector.
Las universidades poseen la capacidad académica. La Administración determina las condiciones de habilitación profesional. Pero las asociaciones conocen de primera mano qué está sucediendo realmente en la profesión. Conocemos las funciones que desempeñan los directores de seguridad, las nuevas responsabilidades que están asumiendo, las competencias demandadas por las empresas, las carencias formativas existentes y la velocidad con la que aparecen nuevas amenazas.

Por eso sería especialmente útil constituir una mesa estable de trabajo entre universidades, asociaciones profesionales, administración y representantes empresariales. Una mesa que pudiera desarrollar un mapa común de competencias del profesional de la seguridad del siglo XXI.

La propuesta de ADISPO

Desde ADISPO entendemos que ha llegado el momento de impulsar una alianza académica y profesional con varias líneas de actuación.

En primer lugar, trabajar con universidades interesadas en las Ciencias de la Seguridad para definir un mapa actualizado de competencias profesionales.

En segundo lugar, estudiar sistemas objetivos de reconocimiento de formación y experiencia para Directores de Seguridad y otros profesionales que deseen continuar hacia titulaciones oficiales.

En tercer lugar, promover itinerarios de adaptación compatibles con la legislación universitaria, diferenciados según la formación y experiencia previa de cada candidato.

En cuarto lugar, acercar al ámbito universitario las certificaciones y estándares internacionales más relevantes para la función de seguridad.

Y, finalmente, promover una cultura de formación continua en la que obtener una habilitación no represente el final del proceso formativo, sino el inicio de una carrera de actualización permanente.

ADISPO quiere contribuir a ese diálogo.
Desde la defensa de una formación de calidad, alejada de soluciones puramente comerciales. Desde la apuesta por la certificación objetiva de conocimientos y competencias. Desde la incorporación de estándares y certificaciones internacionales. Y, sobre todo, desde el compromiso con la dignificación de quienes han elegido la Seguridad como profesión.

Elevar estándares, no levantar barreras. Dignificar una profesión no consiste simplemente en exigir más títulos. Consiste en conseguir que sus conocimientos sean reconocidos, que la formación tenga calidad, que la experiencia tenga valor y que existan verdaderas posibilidades de progresión profesional y académica. España dispone hoy de Directores de Seguridad extraordinariamente cualificados que, sin embargo, han seguido itinerarios académicos y profesionales muy diferentes.

- **Tenemos universidades.**
- **Tenemos grados en Seguridad.**
- **Tenemos una habilitación profesional consolidada.**
- **Tenemos asociaciones profesionales.**
- **Tenemos miles de profesionales con experiencia.**

Lo que todavía necesitamos es conectar todas esas piezas. El objetivo de los próximos años debería ser conseguir que un joven que comienza sus estudios y un Director de Seguridad con veinte años de experiencia puedan visualizar una misma carrera profesional, aunque entren en ella por caminos distintos.

Una carrera en la que sea posible avanzar desde la formación profesional hacia la especialización, desde la experiencia hacia el reconocimiento académico, desde el Grado hacia el posgrado y desde la realidad española hacia estándares internacionales.
Ese es el verdadero salto que necesita la profesión.

Porque la dignificación no consiste en elevar barreras de acceso, sino en elevar los estándares de conocimiento, competencia y reconocimiento profesional. Y en ese camino las asociaciones profesionales y las universidades tienen mucho que construir juntas.

CEUTA, LA FRONTERA QUE ESPAÑA NO PUEDE SEGUIR DEJANDO EN MANOS AJENAS

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos G. Barrett
Gerente general en Spy Investigación & Barrett

Investigador Privado, Experto en Criminalista, especialista en investigación privada y periodística.
Con experiencia en casos a nivel particular o de interés público con repercusión mediática.
Ejerciendo labores de investigación para empresas y particulares.
Experto en investigación con licencia como Investigador Privado / Director de Seguridad en la sección de inteligencia de la policía nacional española.
Perito Judicial en ASPEJURE.
Asesor en Criminalistica.

Seguridad, soberanía y humanidad ante una crisis sin precedentes

Ceuta no ha vivido una simple presión migratoria. Los días 30 y 31 de julio de 2026, más de 70.000 personas cruzaron desde Marruecos hacia una ciudad de apenas 85.000 habitantes. La frontera quedó desbordada y el Centro de Estancia Temporal de Inmigrantes, con unas 500 o 600 plazas, resultó claramente insuficiente.

Conviene llamar a las cosas por su nombre: cuando decenas de miles de personas atraviesan una frontera internacional sin identificación ni control previo, se produce un descontrol fronterizo. Reconocerlo no significa criminalizar la inmigración. Significa admitir un fracaso operativo con consecuencias para la seguridad, la convivencia y los derechos humanos.

El Gobierno asegura que entre el 90 % y el 95 % de quienes entraron regresó a Marruecos durante las primeras 48 horas. La reacción evitó que la emergencia alcanzara dimensiones mayores, pero no responde a la pregunta fundamental: ¿cómo fue posible que una frontera exterior de España y de la Unión Europea quedara desbordada en cuestión de horas?

Una peligrosa dependencia de Marruecos
España necesita cooperar con Marruecos, pero cooperación no puede significar dependencia. El 15 de agosto, las autoridades marroquíes consiguieron impedir un nuevo intento colectivo anunciado en redes sociales. Su capacidad de contención contrastó con lo ocurrido dos semanas antes.

Un informe policial apuntó posteriormente a un posible “guiado activo” de personas hacia determinados lugares de paso durante la crisis de julio. Son indicios que deben investigarse, no una responsabilidad estatal demostrada. Sin embargo, resultan suficientemente graves para exigir explicaciones y transparencia.

La seguridad de Ceuta no puede depender de la temperatura diplomática del momento. España necesita medios propios, vigilancia marítima, inteligencia preventiva, capacidad de reacción y un respaldo europeo permanente.

Improvisación jurídica y operativa
La sentencia del Tribunal Supremo del 8 de julio limitó el rechazo en frontera para quienes accedieran a nado mientras no existieran elementos físicos que delimitaran ese espacio. Tras la crisis, Interior instaló una barrera neumática y boyas en el espigón del Tarajal. Las resoluciones judiciales deben cumplirse. Lo inadmisible es que las autoridades no anticiparan suficientemente las consecuencias de la nueva situación. Una frontera no puede funcionar a golpe de sentencia, rumor digital e improvisación. Todo cambio jurídico con efectos previsibles debe acompañarse de un plan operativo inmediato y coordinado.
Los menores, rostro del fracaso

CARLOS G. BARRETT
Investigador Privado
Experto en Criminalística

El Gobierno había identificado el 1 de septiembre a 1.129 menores llegados durante la crisis. Las organizaciones sociales denunciaron que numerosos niños y adolescentes permanecieron fuera de los recursos de protección. Un menor durmiendo en la calle es una derrota del Estado. La falta de identificación, alojamiento y tutela lo expone a la explotación, la trata y la violencia. Controlar la frontera y proteger a la infancia no son objetivos incompatibles. El Estado debe impedir las entradas irregulares y ejecutar las devoluciones legalmente procedentes, pero también tramitar individualmente las solicitudes de asilo y garantizar el interés superior del menor.

CEAR ha advertido de que las devoluciones sin evaluación individual pueden vulnerar el derecho de asilo. CEAR La firmeza sin garantías puede convertirse en abuso; las garantías sin capacidad de control desembocan en impotencia.

Recuperar el control sin perder la humanidad
El Gobierno ha anunciado 309 millones de euros para reforzar la seguridad, la acogida, los servicios públicos y la economía ceutí. También ha habilitado miles de plazas y enviado refuerzos policiales, judiciales y administrativos. Son medidas necesarias, pero llegaron después del colapso. La Moncloa lo ocurrido en Ceuta perjudicó a todos: a sus habitantes, a las fuerzas de seguridad y a los propios migrantes, convertidos en instrumentos de traficantes, campañas digitales o intereses geopolíticos.

La respuesta no debe ser el miedo ni el odio. Debe ser el Estado: un Estado que controle su territorio, anticipe las crisis, cumpla la ley y no delegue su soberanía en Marruecos. Una frontera desbordada no es una política migratoria. Es la ausencia de ella.

Gregorio Duro
Tecnico en licitaciones y Proyectos

PRINCIPIO DE OPTIMALIDAD DE BELLMAN EN PROCESOS DE ESTIMACIÓN DE RIESGOS (II)

El verano ha llegado a su fin y, con él, retomamos la actividad habitual y la creación de contenidos técnicos en Metrorisk. En la primera parte de este artículo presentamos el principio de optimalidad de Bellman y su aplicación conceptual al análisis de riesgos en distintos ámbitos. En esta segunda parte formalizamos el principio de forma sencilla y lo aplicamos a un ejemplo propio del ámbito de la seguridad física, con el fin de mostrar cómo se traduce en la práctica el razonamiento expuesto anteriormente.

Formalización

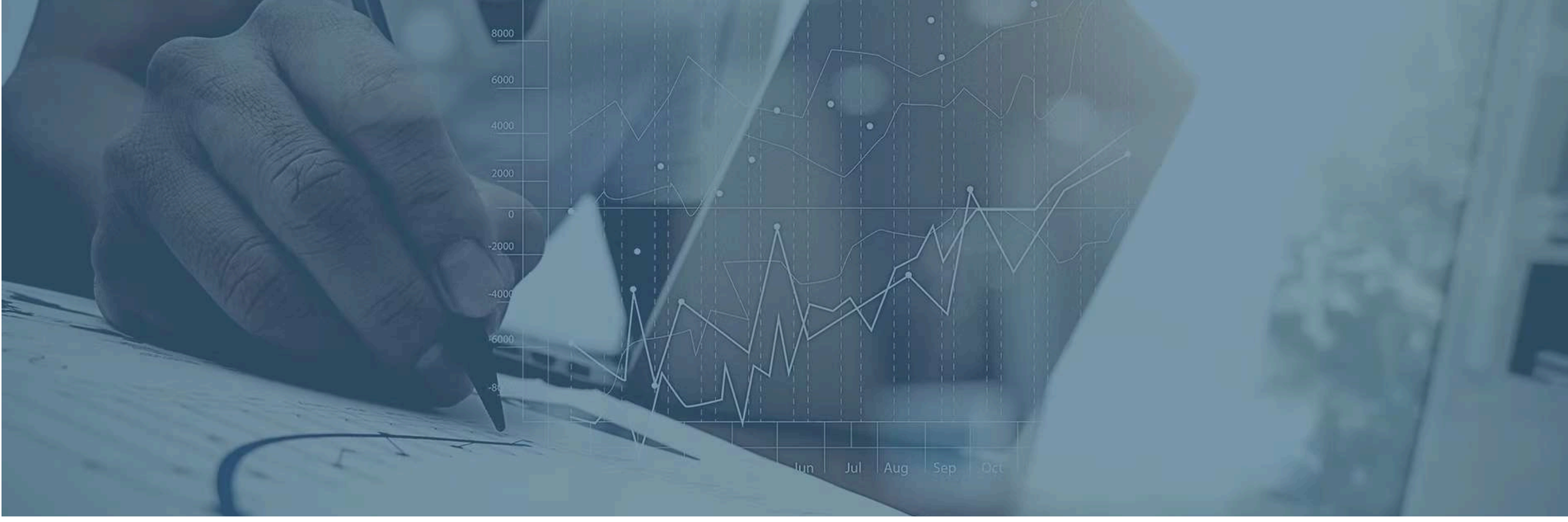
El principio de optimalidad de Bellman puede expresarse, de forma simplificada, como la suma entre el coste de la decisión tomada en el momento actual y el coste esperado que esa decisión deja para el futuro: Valor óptimo = Coste de la decisión + (Probabilidad de riesgo alto × Coste si el riesgo es alto) + (Probabilidad de riesgo bajo × Coste si el riesgo es bajo) Esta fórmula conserva la lógica esencial del principio: la mejor decisión no es la más barata en el momento, sino la que minimiza la suma del coste inmediato y el coste esperado que arrastra hacia el futuro, ponderado por la probabilidad de cada escenario posible. El cálculo se resuelve mediante inducción hacia atrás (backward induction): se parte de la última etapa del proceso, normalmente la fase de operación ordinaria del inmueble, y se retrocede etapa a etapa hasta llegar al presente, determinando en cada punto cuál es la decisión que minimiza el coste total esperado. Conviene detenerse un momento en por qué esta forma de calcular resulta tan distinta de la manera habitual en que se valoran las inversiones en seguridad. Lo natural, cuando se presenta un presupuesto, es comparar directamente el coste de una opción frente a otra: la planificación básica cuesta menos que la detallada, luego parece la elección razonable si el objetivo es contener el gasto. El principio de Bellman rompe precisamente con ese razonamiento lineal, porque obliga a preguntarse no solo cuánto cuesta decidir hoy, sino qué puerta abre o cierra esa decisión para las etapas siguientes. Una decisión barata en el presente puede resultar, vista así, la más cara del proceso completo si empuja al sistema hacia estados futuros de mayor coste o mayor probabilidad de fallo.

Ejemplo aplicado a un proceso de análisis de riesgos físicos

Consideremos el caso de un edificio de uso público que requiere una evaluación de riesgos previa a la contratación de un servicio de vigilancia y seguridad, con tres etapas de decisión: valoración inicial de vulnerabilidades, refuerzo de sistemas de protección y operación del servicio. En la etapa de valoración inicial, el responsable de seguridad debe decidir entre dos acciones: realizar una planificación técnica básica de los sistemas existentes, con un coste de 3.000 € y una probabilidad del 45 % de que el inmueble quede clasificado en un estado de vulnerabilidad alta; o realizar una planificación detallada, incluyendo pruebas de intrusión y verificación in situ de cada sistema (CCTV, detección de incendios, control de accesos), con un coste de 9.000 € y una probabilidad de solo el 15 % de alcanzar ese mismo estado de vulnerabilidad alta. Si el inmueble llega a la etapa de refuerzo en estado de vulnerabilidad alta, el coste esperado de gestionar ese estado, incluyendo la implantación urgente de medidas correctoras y el riesgo residual de incidentes durante el periodo sin protección adecuada, se estima en 60.000 €. Si llega en estado de vulnerabilidad baja, ese coste esperado se reduce a 12.000 €. Aplicando la fórmula a cada opción disponible en la etapa inicial.

- **Planificación básica: 3.000 + (0,45 × 60.000 + 0,55 × 12.000) = 3.000 + 33.600 = 36.600 €**
- **Planificación detallada: 9.000 + (0,15 × 60.000 + 0,85 × 12.000) = 9.000 + 19.200 = 28.200 €**

El resultado es concluyente: pese a su mayor coste inicial, la planificación detallada resulta la decisión óptima, al reducir de forma sustancial la probabilidad de alcanzar el estado de vulnerabilidad alta y, con ello, el coste total esperado del proceso. Este resultado muestra el núcleo del principio de optimalidad: la decisión correcta en la primera etapa no se valora por su coste aislado, sino por su efecto sobre el coste esperado de las etapas posteriores.

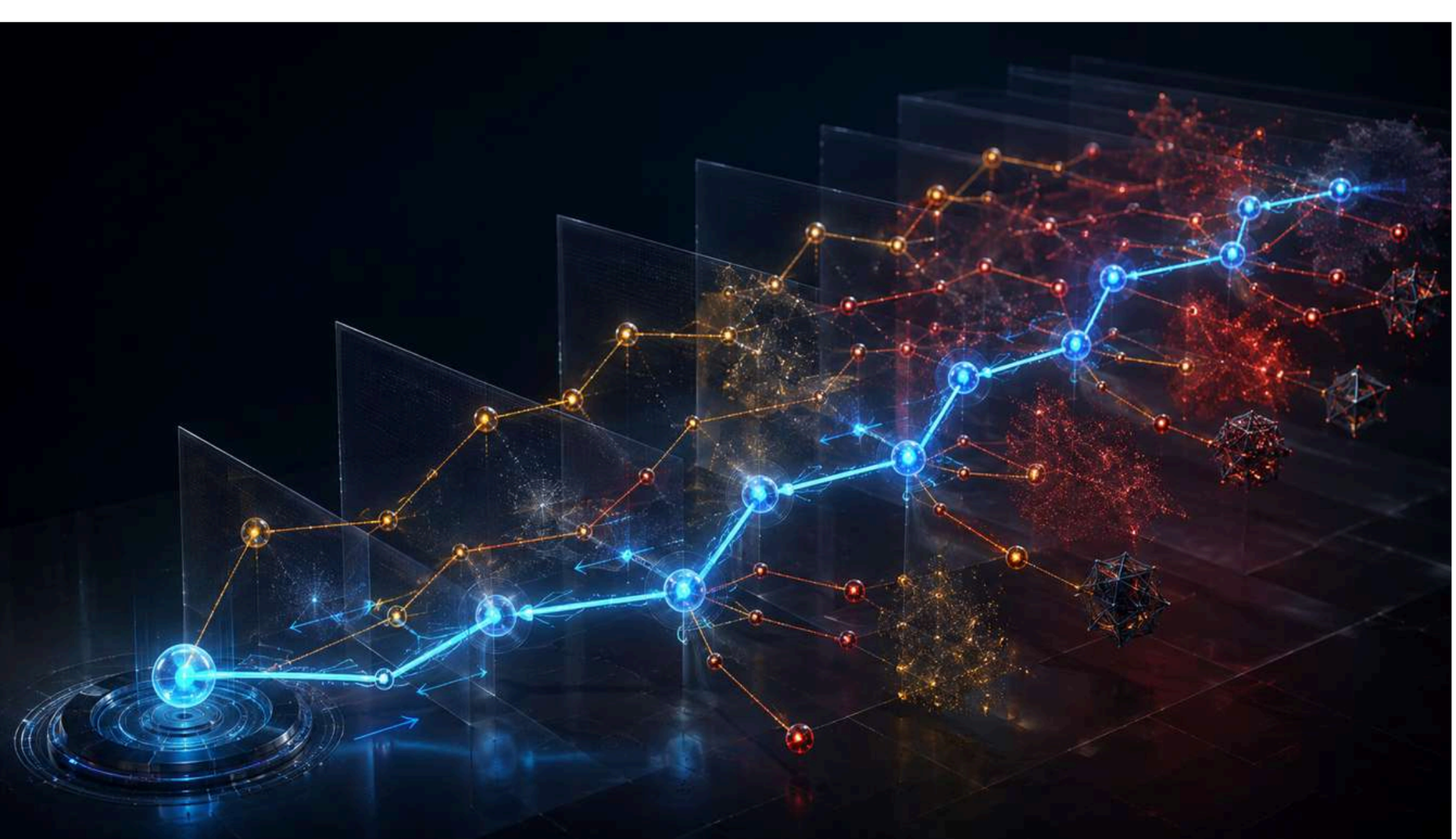


Es interesante poner de manifiesto que el resultado podría invertirse fácilmente si cambiaran las condiciones del escenario. Si el coste de gestionar un estado de vulnerabilidad alta fuera menor, por ejemplo, porque el edificio cuenta ya con un plan de seguridad sólido que reduce el impacto de un incidente, o si la diferencia de coste entre ambas planificaciones fuera mayor, la planificación básica podría volver a ser la opción más racional. Esto es precisamente lo que aporta el principio de Bellman frente a una regla fija de decisión: no ofrece una respuesta universal del tipo de "siempre invertir más en la fase inicial", sino un método para recalcular la decisión óptima cada vez que cambian los costes, las probabilidades o el número de etapas del proceso.

El resultado es concluyente: pese a su mayor coste inicial, la planificación detallada resulta la decisión óptima, al reducir de forma sustancial la probabilidad de alcanzar el estado de vulnerabilidad alta y, con ello, el coste total esperado del proceso. Este resultado muestra el núcleo del principio de optimalidad: la decisión correcta en la primera etapa no se valora por su coste aislado, sino por su efecto sobre el coste esperado de las etapas posteriores. Dicho de otro modo, comparar únicamente los 3.000 € frente a los 9.000 € de la etapa inicial, como haría un análisis presupuestario convencional, llevaría a la conclusión errónea de que la opción básica es la más eficiente, cuando en realidad es la que arrastra un mayor coste acumulado a lo largo de todo el proceso

Es interesante poner de manifiesto que el resultado podría invertirse fácilmente si cambiaran las condiciones del escenario. Si el coste de gestionar un estado de vulnerabilidad alta fuera menor, por ejemplo, porque el edificio cuenta ya con un plan de seguridad sólido que reduce el impacto de un incidente, o porque dispone de una póliza que absorbe parte del coste de un siniestro, o si la diferencia de coste entre ambas planificaciones fuera mayor, la planificación básica podría volver a ser la opción más racional. Del mismo modo, si la probabilidad de alcanzar un estado de vulnerabilidad alta tras la planificación básica fuera solo ligeramente superior a la de la planificación detallada, el ahorro inicial podría no compensarse con un riesgo apenas mayor, invirtiendo de nuevo cuál es la decisión óptima. Esto es precisamente lo que aporta el principio de Bellman frente a una regla fija de decisión: no ofrece una respuesta universal del tipo de "siempre invertir más en la fase inicial", sino un método para recalcular la decisión óptima cada vez que cambian los costes, las probabilidades o el número de etapas del proceso. Su utilidad no está en la cifra concreta que arroja un ejemplo puntual, sino en la disciplina de razonamiento que impone: obliga a hacer explícitos los costes y probabilidades futuros que, de otro modo, quedarían implícitos, o directamente ignorados, en una comparación presupuestaria convencional.

No quiero cerrar este artículo sin reconocer el trabajo de Metrorisk, cuya publicación de contenidos técnicos supone una aportación constante al avance del conocimiento compartido en el sector.



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

LA ESCUELA COMO UNIDAD DE GESTIÓN DEL RIESGO SOCIO-URBANO

CPTED EN EL ENTORNO ESCOLAR: DEL PROYECTO AISLADO AL SISTEMA DE GESTIÓN

I. El punto de partida: la escuela no es un edificio que hay que blindar: En América Latina llevamos tres décadas respondiendo a la violencia escolar con la misma gramática: más barda, más alambre de púas, más cámaras, más filtros de acceso, a veces detectores de metales. Es una respuesta comprensible —es visible, es rápida, es fácil de presupuestar— y es, en la mayoría de los casos, la respuesta equivocada, o al menos la última que deberíamos aplicar y no la primera.

La evidencia que recogió el ICA es incómoda para esa costumbre. Cuando se preguntó a estudiantes, docentes y familias qué elementos del entorno físico escolar los hacían sentirse seguros y en bienestar, la escala del edificio, la visibilidad entre espacios, las oportunidades de socialización y una paleta cálida de materiales quedaron muy por encima de los dispositivos técnicos convencionales de seguridad. Es decir: lo que produce sensación de seguridad y lo que compramos cuando compramos seguridad no son la misma cosa. Mi tesis es sencilla de enunciar y exigente de aplicar: la escuela debe dejar de tratarse como un activo que se protege y empezar a tratarse como una unidad de gestión del riesgo socio-urbano, con gobernanza, ciclo de mejora continua, indicadores y rendición de cuentas. No un proyecto. Un sistema.

Y hay una razón para empezar precisamente por la escuela. La escuela es un microcosmos donde se manifiestan todos los comportamientos humanos: es donde se aprende a convivir, pero también donde la agresión se organiza como acoso y como vandalismo. La violencia es una conducta aprendida, construida sobre múltiples fuentes de información e insumos sociales; y si se aprende, se puede desaprender. Quien aprende a resolver sin violencia a los diez años sostiene una cultura de paz a los cuarenta. Ninguna otra infraestructura urbana ofrece ese apalancamiento.

II. Por qué “socio-urbano” y no simplemente “escolar”: El riesgo escolar no se detiene en la barda perimetral. Se produce, en buena medida, fuera de ella y entra con los estudiantes cada mañana: la ruta escolar mal iluminada, el paradero sin vigilancia natural, el lote baldío, el comercio informal que se apropia de la banqueta, el control territorial de un grupo criminal que marca la fachada de la escuela para demostrar quién manda.

Ese último ejemplo no es hipotético. En el caso documentado por el ICA en Tegucigalpa —una escuela de 250 estudiantes, presupuesto mínimo, asociación de padres inactiva, entorno con narcomenudeo y presencia de maras— la principal amenaza externa se expresaba en una marca de pandilla sobre la fachada. La respuesta no fue una reja más alta. Fue recuperar la identidad del lugar: un mural expresivo, macetas colgantes, retiro del alambre de púas, aplicación deliberada de los conceptos de territorialidad e imagen que Oscar Newman formuló hace medio siglo. Una intervención de bajo costo que disputa simbólicamente el territorio, que es exactamente donde se estaba perdiendo. Al mismo tiempo, la escuela es un productor de seguridad urbana, no solo un consumidor.

En Nueva Zelanda, estudiantes que habían aprendido a hacer auditorías CPTED en su propio plantel fueron convocados por el municipio para auditar un paradero de autobús desde la mirada juvenil. Recorrieron el sitio con personal del cabildo, formularon recomendaciones sobre vigilancia natural, control de accesos, territorialidad y calidad del entorno, encuestaron a sesenta vecinos y trabajaron con la comunidad en la obra artística resultante. Seis años después no había vandalismo sobre esas piezas. Ese es el sentido pleno de “socio-urbano”: la escuela como nodo que gestiona su riesgo interno y como plataforma de gobernanza que produce ciudadanía y mejora el barrio. Cualquier hoja de ruta que se detenga en la puerta del plantel está incompleta.

III. El marco: ISO 22341 convierte el CPTED en un sistema: Lo que faltaba al CPTED latinoamericano no era doctrina —tenemos manuales, tenemos casos, tenemos formación—, sino estructura de gestión. La ISO 22341:2021 la aporta, y por eso insisto tanto en ella con las autoridades educativas. La norma parte de una definición operativa del riesgo con tres componentes: activos, amenazas y vulnerabilidades. Los activos pueden ser el estado del entorno construido y bienes de valor financiero, pero también intangibles de valor blando —en una escuela: el clima de aula, la reputación del plantel, la confianza de las familias, la trayectoria educativa de un adolescente—. Las amenazas son los posibles ofensores o peligros, que conviene caracterizar por escenarios: quién, dónde, con qué medios. Las vulnerabilidades son las oportunidades de daño y la falta de madurez de las contramedidas existentes. El riesgo crece cuando un ofensor motivado y un objetivo adecuado coinciden en tiempo y lugar sin contramedidas apropiadas. Sobre esa base, la norma organiza el CPTED como un proceso de gestión de riesgo con tres piezas institucionales y cinco pasos

Las tres piezas institucionales

1. Un órgano rector (oversight body): la autoridad que declara la política, asume el compromiso, define las áreas sujetas al procedimiento, garantiza soporte técnico y asegura la disponibilidad de recursos. En materia escolar, típicamente la autoridad educativa estatal o municipal en corresponsabilidad con la dirección del plantel.
2. Una declaración de objetivos de desempeño (performance target statement): objetivos de la situación futura de seguridad, composición del equipo, fases que requieren evaluación, plazos, requisitos documentales, recursos y marco legal aplicable.
3. Un equipo de proyecto multidisciplinario, con representación de las partes interesadas, que ejecuta esa declaración.

Antes de arrancar, la norma exige responder cuatro preguntas preliminares: dónde (identificación exacta del área), qué (los problemas delictivos que ocurren o pueden ocurrir), quién (las partes interesadas) y cómo (el tratamiento eficaz y eficiente del riesgo).

Paso	Contenido	Traducción escolar
1. Comunicación y consulta	Las partes interesadas juzgan el riesgo según su percepción; hay que identificarla, registrarla e incorporarla a la decisión	Consultar CON estudiantes, no decidir SOBRE ellos
2. Alcance, contexto y criterios	Definir el alcance, el contexto interno y externo, y los criterios de riesgo y de tolerancia	Delimitar el polígono escolar ampliado y qué es inaceptable
3. Valoración del riesgo	Identificación, análisis y evaluación: activos / amenazas / vulnerabilidades, probabilidad y consecuencias	Auditoría CPTED en los tres ambientes más datos duros
4. Tratamiento del riesgo	Selección de contramedidas comparando la pérdida evitable con el valor de la inversión	Cartera priorizada, no lista de deseos
5. Seguimiento, revisión, registro y reporte	Verificar eficacia, detectar cambios de contexto y riesgos emergentes, documentar	Tablero de indicadores y evaluación anual

Tabla 1. Los cinco pasos del proceso CPTED de la ISO 22341:2021 aplicados al entorno escolar.

La norma señala además que las consecuencias del delito incluyen pérdidas tangibles (gasto, daño patrimonial, gasto en seguridad privada) e intangibles (daño reputacional, impacto en valores y conductas sociales, miedo, dolor, pérdida de calidad de vida). En la escuela, las intangibles son casi siempre las mayores, y son las que ningún presupuesto de seguridad contabiliza. Finalmente, los principios generales del proceso —enfoque conceptual equilibrado, costo-eficacia, sostenibilidad y resiliencia, enfoque ecológico, aplicación adaptativa y base en evidencia— son el antídoto contra la tentación del blindaje. La norma es explícita en que el CPTED físico y el social deben interactuar tanto como sea posible en lugar de operar por separado.

IV. Proporcionalidad: la contramedida se gradúa según el riesgo: Este es, a mi juicio, el aporte más subestimado de la ISO 22341 para el debate escolar. La norma escala las contramedidas por nivel de riesgo, y en todos los niveles la estrategia natural está presente; lo que varía es cuánto se agrega de mecánico y de organizado:

Nivel de riesgo	Respuesta esperada	Composición de la estrategia CPTED
Muy alto / intolerable	Acciones correctivas prioritarias; involucrar niveles altos de dirección	Fuerte componente organizado + fuerte componente mecánico + natural
Alto / intolerable	Acción correctiva y controles adicionales	Componente organizado y mecánico moderado-alto + natural
Medio / tolerable	Acción correctiva y controles adicionales	Mínimo organizado + mecánico moderado + natural
Bajo / tolerable	Monitorear y gestionar	Sin componente organizado + mecánico limitado + predominantemente natural
Muy bajo / aceptable	Monitorear y gestionar	Solo estrategia natural

Tabla 2. Graduación de contramedidas por nivel de riesgo, adaptada de la ISO 22341:2021.

Léase al revés: si una escuela llegó a necesitar torniquetes y guardias, es que el diagnóstico se hizo tarde. La discusión pública sobre seguridad escolar suele saltar directo al renglón mecánico sin haber evaluado el riesgo, con lo cual se paga caro por una respuesta desproporcionada que además comunica a los estudiantes que su escuela es un lugar peligroso —y esa comunicación tiene efectos.

V. Los tres ambientes: el enfoque integral: El CPTED de la ICA trabaja simultáneamente sobre tres ambientes que se refuerzan entre sí en un ciclo de retroalimentación continua. No hay orden correcto de entrada; lo que no es negociable es que los tres avancen en paralelo. Ambiente físico (1.ª generación). Las seis estrategias que reconoce la ISO 22341: vigilancia natural, control natural de accesos, refuerzo territorial, imagen y mantenimiento, apoyo a la actividad, y endurecimiento del objetivo. En clave escolar: pasillos supervisables en lugar de callejones ciegos entre muros; ventanas entre aula y circulación que aportan luz y visibilidad al mismo tiempo; exhibición permanente y actualizada del trabajo estudiantil para generar identidad y propiedad; espacios de socialización de distintas escalas a lo largo de accesos y circulaciones; áreas exteriores visibles, supervisables y atractivas; luz natural y vistas a la naturaleza. El propio guidebook documenta cómo un patio que parece patio de prisión produce conductas de reclusos indisciplinados en lugar de estudiantes que cuidan.

Ambiente social (2.ª generación). Las cuatro estrategias que recoge la norma: cohesión social, conectividad, cultura comunitaria y capacidad umbral. En la escuela se traducen en: asociación de familias activa, mentoría entre pares, convenios con organizaciones del barrio y con el municipio, y conocimiento del estado real de la convivencia. Vale la pena recordar que la 2.ª generación fue codesarrollada por Gerard Cleveland, exdirector de escuela, precisamente porque su experiencia en prevención de la violencia le mostró que las condiciones sociales pesaban tanto como las físicas. Y su formulación del rol docente sigue siendo la correcta: el docente como facilitador, mientras los propios estudiantes evalúan riesgos y desarrollan sus estrategias.

Ambiente psico-emocional (3.ª generación). Formulado por Mateja Mihinjac y Gregory Saville en 2019 sobre la jerarquía de necesidades de Maslow, atiende el entorno interno del comportamiento: regulación emocional, inteligencia emocional, atención plena, expresión artística, autorrealización. Es el ambiente más difícil de medir —se llega a él por conversación con docentes y estudiantes, que revela apatía, mala comunicación, consumo, peleas, racismo, sexismo o xenofobia— y el que más advertencias éticas exige: los instrumentos de evaluación no deben ser prescriptivos ni derivar en estigmatización de ningún estudiante; sirven para diseñar programas, no para etiquetar personas. Sobre esta base el ICA propone cinco categorías de amenaza en el entorno escolar —externas, internas, autolesión, a la propiedad y ambientales—, y esa taxonomía es la que recomiendo adoptar como estructura de la matriz de riesgo, porque obliga a mirar lo que las auditorías de seguridad tradicionales no miran. La categoría de autolesión, en particular, exige el acompañamiento de personal profesional de salud mental y protocolos de derivación: el CPTED aporta condiciones ambientales que favorecen el sentido de pertenencia, logro y valor propio, pero no sustituye la atención clínica.

VI. Hoja de ruta para implementar CPTED escolar como sistema de gestión: La siguiente ruta está construida sobre el proceso de la ISO 22341 y el enfoque integral del ICA, con la escala y los tiempos de un plantel de educación básica o media en contexto urbano latinoamericano. El horizonte de un primer ciclo completo es de un ciclo escolar; la mejora continua no tiene fin.

Fase 0 — Decisión y gobernanza (mes 0–1)

Elemento	Contenido
Acciones	Constituir el órgano rector (autoridad educativa + dirección del plantel + gobierno municipal). Designar a una persona responsable con autoridad para asegurar que los pasos se establezcan, implementen y mantengan, y para reportar al órgano rector. Emitir la declaración de objetivos de desempeño. Integrar el equipo de proyecto.
Quiénes	Autoridad educativa, dirección escolar, municipio (obras públicas y seguridad ciudadana), docentes, estudiantes, familias, policía de proximidad, salud / psicología, especialista CPTED certificado.
Productos	Acta de instalación · política de seguridad y convivencia escolar · declaración de objetivos de desempeño con plazos, recursos y requisitos documentales.
Criterio de cierre	Las cuatro preguntas preliminares (dónde, qué, quién, cómo) están respondidas por escrito.

Tabla 3. Fase 0 de la hoja de ruta.

> **Advertencia de fase.** Sin esta fase, todo lo demás es voluntarismo. La mayoría de las intervenciones CPTED escolares que he visto fracasar no fallaron en el diagnóstico: fallaron porque nadie tenía mandato ni presupuesto para sostenerlas al año siguiente.

Fase 1 — Comunicación y consulta:

- Mapa de partes interesadas y plan de comunicación desarrollado desde el inicio, no al final.
- Consulta a estudiantes por generación escolar, con metodologías apropiadas a la edad.
- Regla operativa: **las percepciones de riesgo se registran y se incorporan a la decisión**, aunque no coincidan con los datos duros. La percepción de inseguridad es un daño en sí misma.
- Producto: informe de percepciones y plan de comunicación permanente.

Fase 2 — Alcance, contexto y criterios:

- Delimitar el **polígono escolar ampliado**: predio + entorno inmediato + rutas escolares principales + paraderos y puntos de transferencia.
- Inventario de activos, tangibles e intangibles.
- Establecer los criterios de riesgo y la tolerancia: qué nivel es inaceptable para esta comunidad y con estos recursos, revisables durante el proceso.
- Producto: documento de alcance, contexto interno / externo y criterios de riesgo.

Fase 3 — Valoración del riesgo en los tres ambientes:

Ambiente	Instrumentos
Físico	Auditoría CPTED con participación estudiantil; marchas exploratorias diurnas y nocturnas; levantamiento de iluminación, visibilidad, accesos y mantenimiento; herramientas de análisis espacial.
Social	Encuestas de clima escolar; grupos focales; mapeo de activos y déficits comunitarios; diagnóstico de la asociación de familias y de vínculos con organizaciones externas.
Psico-emocional	Conversaciones estructuradas con docentes y estudiantes; instrumentos de convivencia; instrumentos especializados SOLO con personal profesional, consentimiento y resguardo de no estigmatización.
Datos duros	Incidencias policiales y llamadas de emergencia en el polígono; reportes escolares; ausentismo; reincidencia de vandalismo y grafiti; datos sociodemográficos del área.

Tabla 4. Instrumentos de valoración del riesgo por ambiente.

- Analizar probabilidad y consecuencia; escalar los niveles de riesgo con el sistema de ponderación que mejor se ajuste a prioridades y recursos disponibles.
- **Producto clave: matriz de riesgo por las cinco categorías de amenaza, con mapa de calor sobre el polígono.**
- El resultado se comunica a las partes interesadas como insumo de decisión y se discute con el órgano rector. Sin devolución, no hay legitimidad.

Fase 4 — Tratamiento del riesgo:

La cartera se ordena por nivel de riesgo, siguiendo la lógica de proporcionalidad de la sección IV, y se decide comparando el valor monetario de la inversión con el valor de la reducción del riesgo.

Bloque A — Acciones inmediatas de bajo costo (0–90 días). Aplanado y pintura de muros; mural de identidad escolar que sustituya marcas ajenas; retiro de alambre de púas; poda para recuperar visibilidad; reparación de luminarias; señalética clara; macetas y vegetación a cargo de los estudiantes; contenedores de residuos diferenciados; reparación de bancas; celebración de los accesos a las aulas; áreas fijas para exhibir el trabajo estudiantil.

Bloque B — Intervención física de mediano plazo. Ventanas entre aulas y circulaciones; rediseño del patio con programación deliberada de usos; espacios de socialización de distintas escalas; canalización de visitantes a un punto único de registro; accesibilidad universal, barandales y superficies seguras; captación pluvial y huerto como infraestructura pedagógica.

Bloque C — Ambiente social. Comité estudiantil CPTED permanente; sistema de mentoría entre pares con espacios localizados cerca del aula; reactivación de la asociación de familias; convenios con el municipio y con organizaciones del barrio; **integración curricular**: las auditorías, encuestas y propuestas como proyecto de aprendizaje que cumple objetivos formativos y desarrolla competencias de investigación, colaboración y resolución de problemas.

Bloque D — Ambiente psico-emocional. Momento de silencio mental o respiración al inicio de la jornada; programas de expresión artística y musical; actividad física y práctica atencional previa al deporte; formación docente en las mismas técnicas —la evidencia disponible sugiere que el clima de aula media entre la práctica de relajación-atención plena y el desempeño académico, y recomienda que el propio profesorado las practique—; huerto escolar como práctica de atención en la naturaleza.

Bloque E — Componente socio-urbano. Convenio con el municipio para rutas escolares seguras, alumbrado, mobiliario y paraderos; auditoría estudiantil de un espacio público del barrio con presentación formal de resultados a la autoridad; coordinación con policía de proximidad en horarios de entrada y salida; recuperación de un espacio público colindante con participación vecinal.

> **Regla de composición.** Ninguna cartera se aprueba si no contiene acciones simultáneas de los tres ambientes. Un plan que solo tenga bloques A y B es una obra, no un sistema de gestión de riesgo.

Fase 5 — Seguimiento, revisión, registro y reporte (permanente)

Responsabilidades de monitoreo claramente definidas y un tablero mínimo:

Dimensión	Indicadores sugeridos
Físico	Reincidencia de grafiti y vandalismo; luminarias operativas; porcentaje de superficie con vigilancia natural efectiva; tiempo medio de reparación.
Social	Reportes de acoso (se espera que SUBAN al inicio: mide confianza, no deterioro); participación en la asociación de familias; número de convenios activos; uso de espacios en recreo.
Psico-emocional	Clima de aula; ausentismo; derivaciones atendidas; participación en programas artísticos.
Percepción	Encuesta semestral de sensación de seguridad, desagregada por género y grado.
Entorno	Incidencias en el polígono ampliado en horarios de entrada y salida.

Tabla 5. Tablero mínimo de indicadores para el seguimiento.

El proceso y sus resultados se documentan y reportan. Cuando el problema persista por encima de niveles aceptables, corresponde al órgano rector decidir **acciones correctivas** para eliminar la causa de la no conformidad, no simplemente repetir la intervención. Evaluación formal anual, con objetividad e imparcialidad en la selección de quien evalúa.

Fase 6 — Escalamiento (ciclo 2 en adelante)

- De plantel piloto a **red de escuelas** por zona escolar, con acompañamiento entre pares y aprendizaje cruzado.
- Formación y certificación de personal técnico de la autoridad educativa y del municipio.
- Incorporación del procedimiento a la normativa de obra educativa: que ninguna escuela nueva se proyecte ni se rehabilite sin valoración de riesgo CPTED previa, que es donde la etapa de planeación y diseño rinde más que cualquier corrección posterior.
- Documentación pública de casos y lecciones aprendidas, para que el enfoque siga siendo un documento vivo.

VII. Siete errores que conviene no repetir:

4. Empezar por lo mecánico. La cámara antes del diagnóstico es gasto, no prevención.
5. Diagnosticar sin devolver. Un estudio que no se discute con la comunidad destruye la confianza que el CPTED necesita.
6. Excluir a los estudiantes. Son la fuente primaria de información sobre el riesgo y el principal activo de sostenibilidad. Sin ellos, cada mural se vuelve a rayar.
7. Confundir mantenimiento con proyecto. Pintar es una acción; sostener la imagen del plantel es una función permanente que requiere responsable y presupuesto.
8. Trabajar un solo ambiente. La obra sin trabajo social se degrada; el trabajo social sin obra se agota.
9. Usar instrumentos psicológicos sin salvaguardas. Cualquier evaluación del ambiente psicoemocional que derive en etiquetar estudiantes es un daño, no una prevención.
10. No presupuestar el segundo año. El sistema de gestión vive en la Fase 5. Si no hay recursos para monitorear, no había sistema: había un evento.

VIII. Cierre:

Lo que propongo no requiere tecnología nueva ni presupuestos extraordinarios. Requiere algo más difícil: aceptar que la seguridad escolar es una función de gestión permanente con gobernanza, ciclo y evidencia, y no una compra. La ISO 22341 nos dio la estructura; el enfoque integral del ICA nos dio el contenido de los tres ambientes; los casos de Honduras y Nueva Zelanda nos mostraron que funciona tanto con presupuesto mínimo como con institucionalidad municipal robusta. La ICA lo formula sin rodeos y vale la pena repetirlo cada vez que alguien plantea esperar al siguiente ciclo presupuestal: la falta de fondos, de poder político o cualquier otro obstáculo no debería posponer la acción, y el mejor momento para empezar es siempre hoy.

Fuentes

- International CPTED Association (2022). CPTED in Schools: A Comprehensive Approach. ICA Guidebook, edición 2022 en inglés. Comité de CPTED en Escuelas presidido por Carlos Gutiérrez Vera; editores Gregory Saville y Gerard Cleveland.
- ISO 22341:2021, Security and resilience — Protective security — Guidelines for crime prevention through environmental design.
- 22341-2:2025. Security and resilience — Protective security — Guidelines for crime prevention through environmental design.
- Mihinjac, M. y Saville, G. (2019), sobre CPTED de tercera generación, referidos en el guidebook del ICA.
- Newman, O., teoría del espacio defendible, referida en el guidebook del ICA.

Asociación Española de Auditores de Seguridad

Verificando el cumplimiento de normativas en Seguridad Privada

NUESTRAS VENTAJAS

El ser asociado nuestro tiene una serie de beneficios prácticos que marcarán la diferencia en el mercado para los profesionales de esta área

CÓMO ASOCIARSE

PROCEDIMIENTO

Para poder asociarse a nuestra organización, existen 2 alternativas

- Al matricularse en el curso Experto Auditor de Seguridad impartido por INISEG, automáticamente el alumno entra como socio invitado en AEAS y desde ese momento puede obtener todos los beneficios que corresponden como socio.
- El interesado puede asociarse de forma directa en AEAS cumpliendo los siguientes requisitos:
  - Tener estudios relacionados con la seguridad privada
  - Solicitar su ingreso enviando el CV a info@auditoresseguridad.es

AEAS
Asociación Española de Auditores de Seguridad

NUESTROS SERVICIOS

Conoce todos nuestros servicios que ofrecemos a nuestros asociados y de manera particular. Podrás solicitar información directa a los profesionales encargados haciendo clic en más información para enviar un mail directo.

El concepto y sus funciones

Las auditorías tienen por objeto la comprobación de que los sujetos auditados mantienen los requisitos generales y específicos que dieron lugar a su autorización y el cumplimiento de la normativa de aplicación en el ámbito de la seguridad privada, como requisito adicional de garantía de calidad en la prestación de los servicios, entendida como confiabilidad y profesionalidad Áreas de trabajo del auditor de seguridad. El reglamento de seguridad privada implementa la obligatoriedad de prestación de servicios en los sectores estratégicos en la realización de auditoria externa obligatoria realizada por una empresa de seguridad que cuente con la certificación emitida por una entidad certificadora acreditada.

Por otro la posibilidad de realización de auditorías voluntarias para verificar el cumplimiento de la normativa de seguridad privada:

1.- inspecciones a empresas de seguridad para comprobar que cumplen los requisitos de inspección a empresas de seguridad
2.- inspección de despachos de detectives
3.- inspección servicios de seguridad
Inspección de otro sujetos de seguridad , sujetos obligados a cumplimiento de medidas de seguridad y otros usuarios de seguridad privada:
4.- inspección a centros de seguridad privada
5,. Inspección a departamentos de seguridad privada
6. inspección y verificación a centros universitarios donde que impartan cursos de seguridad privada
7. centrales receptoras de alarmas de uso propio
8.- empresas de seguridad informática

VIGILANCIA DISCONTINUA: CUANDO PROTEGER NO SIGNIFICA ESTAR SIEMPRE ALLÍ

Metro Risk

Edición propiedad de @MetroRisk, asociación

Iván Cantalapiedra.Director de Seguridad. CEO IONIQ Seguridad

Durante muchos años hemos entendido la vigilancia de una forma muy sencilla: existe una instalación que proteger y colocamos en ella a un vigilante durante 8, 12 o 24 horas. Este modelo sigue siendo imprescindible en multitud de servicios. Pero debemos hacernos una pregunta: ¿realmente todas las instalaciones necesitan presencia permanente? Una nave industrial durante la noche, un centro educativo fuera de su horario, unas oficinas durante el fin de semana o una comunidad de propietarios pueden necesitar presencia física de seguridad sin requerir un vigilante durante 8 horas consecutivas. Ahí aparece una modalidad con un enorme potencial: la vigilancia discontinua.

NO SE TRATA DE VENDER HORAS, SINO SEGURIDAD La normativa reguladora de Seguridad Privada, contempla los servicios de ronda o vigilancia discontinua, basados en visitas intermitentes y programadas a los lugares objeto de protección. Esto permite que un vigilante se desplace entre diferentes instalaciones realizando rondas, comprobación de accesos y perímetros, control de puntos vulnerables o comunicación de incidencias. La clave está en cambiar la pregunta.

En lugar de preguntarnos ¿cuántas horas de vigilante necesita una instalación?, deberíamos preguntarnos qué riesgos necesitamos cubrir y en qué momentos se producen. Entre una instalación protegida únicamente mediante sistemas electrónicos y otra con vigilancia permanente existe un espacio intermedio. La tecnología puede detectar, registrar y transmitir información; el vigilante aporta presencia física, observación y capacidad de actuación.

IONIQ PROXIME: UN VIGILANTE, VARIOS CENTROS

Partiendo de esta filosofía, en IONIQ Seguridad hemos desarrollado IONIQ PROXIME, nuestro servicio de vigilancia discontinua.

El concepto es sencillo: «Un vigilante, varios centros». Nuestros vigilantes se desplazan en vehículos de IONIQ Seguridad entre diferentes instalaciones a proteger, realizando visitas programadas durante las 24 horas del día.

Cada servicio se configura según las necesidades del cliente. Una instalación puede necesitar una visita diaria; otra, varias comprobaciones durante la noche; y otra concentrarlas durante fines de semana o periodos sin actividad. Además, cada instalación dispone de un procedimiento que determina qué debe comprobarse, qué puntos requieren especial atención y cómo actuar ante una incidencia. Así, cada visita se convierte en una actuación de seguridad planificada y genera, además, un importante efecto disuasorio.

APERTURAS Y CIERRES Dentro de este modelo hemos desarrollado también PROXIME OPENCLOSE, dirigido a momentos especialmente sensibles como la apertura y el cierre de las instalaciones. En determinados centros, la necesidad puede concentrarse cuando el primer trabajador llega por la mañana o cuando el último abandona las instalaciones por la noche. La vigilancia discontinua permite dirigir los recursos hacia esos momentos concretos.

UNA ALTERNATIVA PARA MUCHAS INSTALACIONES Este modelo resulta especialmente interesante para naves industriales, centros logísticos, oficinas, centros educativos, comunidades de propietarios o aparcamientos que quieren incorporar presencia física de vigilantes sin asumir necesariamente un servicio permanente. Esto no significa que la vigilancia discontinua pueda sustituir cualquier servicio. Hay instalaciones y niveles de riesgo que requieren presencia continua.

Pretender sustituirla exclusivamente para reducir costes sería diseñar la seguridad desde el presupuesto y no desde el riesgo. Pero también existen muchos espacios donde la vigilancia permanente puede resultar innecesaria y depender exclusivamente de medios electrónicos puede ser insuficiente. Ahí es donde la vigilancia discontinua encuentra su espacio.

Con IONIQ PROXIME queremos combinar profesionales habilitados, vehículos, tecnología, procedimientos y planificación para acercar la vigilancia privada a un mayor número de instalaciones.

Quizá debamos cambiar una de las preguntas tradicionales de nuestro sector. En lugar de:

- ¿Cuántas horas de vigilante necesita? preguntemos:
- ¿Qué necesita proteger? Porque la seguridad no debería medirse únicamente en horas de presencia, sino en nuestra capacidad para reducir riesgos.

IONIQ PROXIME
VIGILANCIA DISCONTINUA

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

Taxonomía de Bloom: de memorizar contenidos a construir aprendizaje

Evaluar bien empieza mucho antes del examen. Empieza cuando decidimos qué queremos que una persona sea capaz de recordar, comprender, aplicar, analizar, valorar o crear al finalizar un proceso de aprendizaje. La Taxonomía de Bloom sigue siendo, décadas después de su formulación, una de las herramientas más útiles para convertir esa intención educativa en objetivos observables, actividades coherentes y evidencias evaluables.

1. Una brújula para diseñar el aprendizaje. En educación y formación es relativamente fácil caer en una trampa: confundir haber explicado un contenido con haber generado aprendizaje. Que una materia haya sido presentada no significa que haya sido comprendida; y comprenderla tampoco implica saber utilizarla ante una situación real. Ahí reside buena parte del valor de la Taxonomía de Bloom. Su función no consiste simplemente en ordenar verbos o construir una pirámide atractiva. Nos obliga a preguntarnos qué operación cognitiva esperamos del alumnado y qué evidencia nos permitirá comprobar que realmente la ha alcanzado. Benjamin Bloom y su equipo publicaron en 1956 una clasificación de objetivos educativos que distinguía tres grandes dominios: cognitivo, afectivo y psicomotor. El dominio cognitivo —el más difundido— organizaba las capacidades desde operaciones relativamente elementales, como recordar información, hasta procesos de mayor complejidad intelectual.

2. Tres dimensiones del aprendizaje. La propuesta de Bloom recuerda algo especialmente relevante: aprender no es únicamente acumular conocimiento. La formación puede afectar a lo que sabemos, a cómo valoramos y respondemos ante determinadas situaciones y a lo que somos capaces de ejecutar.

Dimensión	Qué aborda
Cognitiva	Procesamiento de información, comprensión, resolución de problemas, juicio y creación.
Afectiva	Actitudes, valores, emociones, intereses y progresiva interiorización de criterios.
Psicomotora	Habilidades físicas, coordinación, precisión, automatización y dominio de procedimientos.

En la práctica docente y en la formación profesional, el dominio cognitivo es el que con mayor frecuencia utilizamos para formular objetivos y construir instrumentos de evaluación.

3. De Bloom a Anderson y Krathwohl: una taxonomía viva La formulación original empleaba las categorías Conocimiento, Comprensión, Aplicación, Análisis, Síntesis y Evaluación. En 2001, Lorin Anderson y David R. Krathwohl, junto con otros especialistas, revisaron el modelo. La modificación fue más que terminológica: las categorías pasaron a expresarse mediante verbos —acciones— y «crear» se situó como el proceso cognitivo de mayor complejidad. La secuencia revisada que hoy suele emplearse es: Recordar, Comprender, Aplicar, Analizar, Evaluar y Crear.

Posteriormente, propuestas como la de Andrew Churches trasladaron esta lógica al entorno digital, incorporando acciones vinculadas a buscar, publicar, programar, colaborar o producir contenidos digitales. La tecnología amplía las posibilidades, pero no altera la pregunta esencial: ¿qué proceso cognitivo está realizando realmente la persona?

4. Los seis niveles cognitivos

1. Recordar Recuperar información relevante de la memoria: conceptos, hechos, términos, procedimientos o datos. Verbos orientativos: identificar, reconocer, nombrar, listar, definir, recordar, describir.
2. Comprender Construir significado, interpretar una idea y ser capaz de explicarla o representarla con palabras propias. Verbos orientativos: explicar, resumir, interpretar, comparar, clasificar, ejemplificar.
3. Aplicar Utilizar un conocimiento, regla o procedimiento en una situación concreta, incluida una situación diferente de aquella en la que se aprendió. Verbos orientativos: aplicar, usar, resolver, ejecutar, organizar, emplear.
4. Analizar Descomponer una realidad en elementos, distinguirlos y determinar las relaciones existentes entre ellos. Verbos orientativos: analizar, diferenciar, comparar, categorizar, atribuir, relacionar.
5. Evaluar Emitir un juicio fundamentado utilizando criterios, evidencias o estándares explícitos. Verbos orientativos: evaluar, justificar, argumentar, valorar, criticar, comprobar, revisar.
6. Crear Integrar conocimientos y habilidades para producir una estructura, propuesta, solución o producto nuevo y coherente. Verbos orientativos: diseñar, crear, formular, construir, planificar, desarrollar, mejorar.

9. Bloom en la era de la inteligencia artificial La expansión de la inteligencia artificial generativa hace todavía más relevante esta cuestión. Cuando una herramienta puede resumir un texto, proponer una estructura o generar una primera respuesta en segundos, la evaluación educativa no puede limitarse a comprobar la reproducción de información. Será cada vez más importante evaluar la capacidad para formular problemas, verificar información, contrastar fuentes, detectar errores, argumentar decisiones, aplicar criterios éticos y profesionales y construir soluciones propias con ayuda —o frente a las limitaciones— de la tecnología. La Taxonomía de Bloom ofrece un lenguaje sencillo para rediseñar esas experiencias: podemos preguntarnos qué parte del trabajo corresponde a recordar, cuál a analizar, qué debe evaluarse críticamente y dónde debe aparecer una creación genuina y responsable.

10. Una herramienta, no una receta La principal fortaleza de Bloom no está en memorizar sus seis niveles, sino en utilizarla para mantener alineados cuatro elementos: objetivos, contenidos, actividades y evaluación. Cuando esos cuatro componentes apuntan en la misma dirección, el diseño formativo gana coherencia y la evaluación deja de ser un trámite final para convertirse en evidencia del aprendizaje. Emilio Piñeiro · Taxonomía de Bloom La metodología, por sí sola, no garantiza una buena experiencia educativa. Tampoco lo hace la tecnología. La pregunta profesional sigue siendo qué queremos que una persona sea capaz de hacer después de aprender algo y qué evidencia aceptaremos para demostrarlo. Quizá por eso, casi setenta años después, la Taxonomía de Bloom conserva su vigencia: porque obliga a transformar la intención de enseñar en una arquitectura consciente del aprendizaje.

11. Referencias orientativas para edición Bloom, B. S. (ed.) et al. (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. Anderson, L. W. y Krathwohl, D. R. (eds.) (2001). A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. Churches, A. Bloom's Digital Taxonomy. Propuesta de adaptación de la taxonomía revisada a actividades y competencias del entorno digital. Material divulgativo y ejemplos de aplicación docente revisados durante la preparación del artículo: recursos sobre Taxonomía de Bloom, objetivos de aprendizaje y diseño de actividades educativas.

Nota para edición

Texto preparado como original editable para revista. La cabecera, subtítulo, entradilla, destacados y tablas pueden adaptarse a la línea gráfica de la publicación. Se recomienda mantener la distinción entre la formulación original de 1956 y la revisión de Anderson y Krathwohl de 2001.

TERRITORIO
COMPLIANCE
Cumple, Crece, Lidera

EL ACCESO COMO PERMISO
ARQUITECTURA, RIESGO Y CONTINUIDAD DURANTE LA VIDA DEL EDIFICIO

Metro Risk

SegurIA SOLUTIONS
Protegiendo el presente.
Anticipando el futuro.

Joaquín Sampedro
Prescriptor independiente en Arquitectura de Accesos

Cuando miro un edificio en construcción, pienso en el día en que se retiren las vallas. En quién llegará con las maletas, quién entrará a reparar una avería y quién tendrá que resolver un problema un domingo por la tarde. Ahí es donde, para mí, un proyecto empieza a demostrar si sus accesos están bien pensados. Vengo de la mecánica. Trabajar durante años con llaves y amaestramientos me enseñó algo que sigue vigente: una llave daba paso a determinados lugares y dejaba otros fuera de su alcance. Detrás había personas y responsabilidades. El permiso ya estaba allí, aunque lo lleváramos en el bolsillo y tuviera forma de metal.

Hoy se construye. Mañana se vive

Hoy podemos llevar una credencial en el teléfono y gestionar el acceso de otras maneras. Valoro la libertad que esa evolución puede ofrecer a las personas y la capacidad de gestión que aporta. Ahora bien, cambiar el medio con el que abrimos exige seguir prestando atención a la autorización que hay detrás. ¿Qué tiene permitido hacer quien lleva esa credencial? Esa es la pregunta que me importa. Abrir una puerta es el gesto visible de una decisión que tiene un motivo, un alcance y, en muchos casos, un final. Por eso hablo del acceso como permiso. La tecnología que elegimos debe responder a lo que el edificio necesita. Conviene abordar estas decisiones pronto. Quienes proyectan y quienes van a gestionar el inmueble necesitan entenderse antes de que todo esté decidido. La seguridad tiene mucho que aportar en ese momento. Esperar a que el edificio esté terminado reduce las posibilidades de resolver bien una parte importante de su uso futuro.

ARQUITECTURA DE ACCESOS Basta pensar en un edificio de alojamiento flexible. Una persona vive en él durante unos meses; otra entra a realizar un mantenimiento; una tercera llega de visita. Comparten una entrada, pero su relación con el lugar es distinta. Al hablar de seguridad, importa esa diferencia: qué necesita cada una para desenvolverse y qué espacios deben seguir protegidos. Imaginemos que la empresa de mantenimiento termina su contrato con el edificio. La puerta sigue cerrando y el lector sigue funcionando, pero una credencial de esa empresa continúa autorizada. Si alguien la utiliza, el sistema puede permitirle entrar aunque ya no tenga motivo para acceder. Un permiso puede durar más que el motivo que lo justificó.

La instalación puede funcionar tal como está configurada y, aun así, permitir un acceso que ya no corresponde. En una situación así, me interesa saber quién debía comunicar el fin del servicio y quién tenía la responsabilidad de retirar aquella autorización. Si cada parte supone que lo hará otra, el permiso puede seguir vigente por simple inercia. Ahí hay una decisión de seguridad que necesita un responsable. También debe estar claro a quién acudir cuando surge una excepción: quien gestiona el edificio necesita poder resolverla sin improvisar quién tiene autoridad para hacerlo. El enfoque CPTED —prevención del delito mediante el diseño ambiental— aporta una mirada útil: el entorno y su gestión también influyen en la prevención y en la vida de la comunidad.

En un acceso, esto se aprecia en cómo se entiende una entrada, qué recorrido invita a seguir y cómo se reconoce el paso de una zona compartida a otra privada. La mecánica me hace volver siempre a la puerta. Podemos hablar de software durante horas, pero esa puerta tiene que cerrar bien. Una solución debe soportar el uso cotidiano. Lo que funciona durante una demostración tiene que seguir funcionando con prisas, con visitas y con el desgaste de los años.

En ese uso cotidiano hay personas con edades, capacidades y hábitos distintos. No doy por hecho que todas quieran o puedan resolver su acceso con un teléfono. Alguien debe poder llegar a su casa, recibir una visita o pedir ayuda sin sentirse perdido. Cuando un gesto se repite cada día, cualquier dificultad acaba pesando.

Pienso también en quien se queda fuera. Esa persona espera una respuesta que pueda entender y una solución que llegue a tiempo. Desde su lado de la puerta, poco importa que el problema sea de conexión, de alimentación o de gestión. Lo que necesita es poder continuar con su día. Ahí cobra sentido la continuidad. Los edificios pasan por incidencias y por cambios de residentes, equipos y responsables. Me cuesta valorar una solución solo por el momento en que se estrena. Una propiedad que va a conservar su activo durante muchos años necesita mirar más lejos. El software tendrá su propia evolución. El inmueble seguirá necesitando accesos que puedan mantenerse y adaptarse. Por eso conviene preguntarse qué significará lo que hoy elegimos cuando el edificio tenga otros usos o esté en otras manos. Hay decisiones cuyo alcance solo se aprecia con el tiempo. Mi aportación está ahí: ayudar a que las decisiones tengan sentido para el edificio y para las personas que lo utilizan. Hay conocimiento técnico detrás, pero el resultado debe poder explicarse con claridad. Un residente necesita desenvolverse con confianza; quien gestiona necesita saber qué puede decidir y cómo obtener ayuda cuando la necesita. Por eso insisto en llevar estas preguntas al proyecto, mientras todavía hay margen para decidir. Cuando se retiren las vallas y lleguen las primeras personas, muchas de esas decisiones pasarán inadvertidas si están bien resueltas. Se notarán en algo tan cotidiano como entrar en casa con tranquilidad, recibir una visita o encontrar ayuda cuando hace falta. Esa es la experiencia que me interesa diseñar.

Joaquín Sampedro
Seguridad inteligente para vivir con confianza

DE APAGAR FUEGOS A PREVENIRLOS: LA IA QUE YA AUMENTA EL VALOR DE LA SEGURIDAD PRIVADA

Metro Risk

Rosa Fernandéz

ASUNTO: IA, ANÁLISIS DE RIESGOS Y ANTICIPACIÓN EN SEGURIDAD PRIVADA

La Inteligencia Artificial ya está entrando en la operativa diaria de la seguridad privada. Está presente en sistemas de videovigilancia, análisis de imágenes, control de accesos, lectura de matrículas, gestión de alarmas, planificación de recursos y tratamiento de información. Su valor no está en sustituir al profesional, sino en ayudarle a trabajar con más criterio, más rapidez y mejor información. Durante años, el sector ha incorporado cámaras, sensores, controles de acceso y sistemas de alarma capaces de generar cada vez más datos. Eso ha mejorado la capacidad de vigilancia, pero también ha creado un problema evidente: no toda la información tiene la misma importancia. Cuando un operador recibe cientos de señales, imágenes o avisos, el reto no es ver más. Es saber qué merece atención. Y precisamente ahí empieza a mostrar su verdadero valor operativo.

- Filtrar el ruido operativo. Uno de los usos más consolidados está en la analítica inteligente de vídeo. Estos sistemas permiten identificar determinados objetos, movimientos o comportamientos previamente definidos y reducir el número de eventos que requieren revisión manual. El movimiento de la vegetación, los cambios de iluminación, la presencia de animales o determinadas alteraciones ambientales pueden separarse de otras situaciones potencialmente relevantes.

No hablamos de sistemas infalibles. La tecnología puede equivocarse y necesita supervisión. Su utilidad está en reducir el volumen de información que llega al profesional y permitirle concentrarse en aquellos eventos que requieren valoración. Eso modifica la función del operador: menos tiempo pendiente de estímulos irrelevantes y más tiempo dedicado a comprobar, analizar y decidir.

- Cuando el vídeo se convierte en información útil. La videovigilancia también está cambiando. Hasta hace pocos años, localizar una persona, un vehículo o una secuencia determinada podía obligar a revisar manualmente horas de grabación. Hoy existen sistemas que permiten acotar búsquedas por zonas, franjas horarias, características visibles o determinados parámetros previamente definidos.

La consecuencia es clara: una incidencia puede reconstruirse con mayor rapidez, una secuencia relevante puede localizarse antes y la información puede facilitarse, cuando proceda, a las Fuerzas y Cuerpos de Seguridad de una forma mucho más ágil. El vídeo deja así de ser únicamente una grabación almacenada y empieza a convertirse en una fuente de información operativa.

- Mucho más que cámaras. La IA aplicada a la seguridad privada no se limita al vídeo. Los controles de acceso, las matrículas, las alarmas, los sensores, los partes de incidencias, los servicios de acuda y los registros de actividad operativa generan información de manera constante

La tecnología permite ordenar mejor la información y ponerla al servicio de la operativa. Pero interpretar lo que esa información significa sigue siendo una función profesional. Planificar un servicio, valorar una amenaza o decidir cómo responder exige conocer el contexto, ponderar el riesgo y asumir la responsabilidad de la actuación. La IA puede ayudar a señalar dónde mirar; corresponde al profesional decidir qué está viendo y qué debe hacer a continuación.

- De reaccionar a anticipar. La seguridad privada ha trabajado durante años sobre una secuencia bien conocida: detectar, verificar y responder. Ese modelo seguirá siendo imprescindible, pero la IA permite añadir una capacidad distinta: reconocer patrones antes de que una incidencia termine convirtiéndose en un problema mayor.

Una entrada fuera de horario, una presencia repetida en una zona concreta o una incidencia menor pueden no tener relevancia por sí solas. La situación cambia cuando esos hechos se repiten, coinciden o se apartan de lo que normalmente ocurre en una instalación. Ahí es donde la información empieza a ofrecer una lectura más útil del riesgo. Anticipar no significa predecir delitos ni entrar en escenarios propios de Minority Report. Significa detectar antes aquellas señales que, vistas por separado, podrían pasar inadvertidas y que, relacionadas entre sí, permiten al profesional decidir si conviene prestar más atención, reforzar una medida o revisar un procedimiento.

Rosa Fernández

- De prestar seguridad a aportar conocimiento. La seguridad privada empieza a competir también por la calidad de la información que es capaz de generar y de interpretar. El cliente seguirá necesitando vigilancia, cámaras, alarmas, controles de acceso y capacidad de respuesta, pero cada vez será más importante saber qué está ocurriendo realmente en su entorno: dónde se concentran las incidencias, qué horarios presentan mayor exposición, qué patrones se repiten y qué medidas están funcionando o conviene revisar.

Ese conocimiento permite ajustar procedimientos, reforzar medidas y adaptar el servicio a la evolución real del riesgo. La empresa de seguridad deja así de limitarse a proporcionar medios y pasa a aportar una lectura más completa del entorno que protege. Ahí puede estar una parte importante de la diferenciación del sector en los próximos años. Porque cuando varias compañías puedan ofrecer tecnologías similares, la ventaja no estará únicamente en disponer de más cámaras o sensores más avanzados, sino en saber convertir toda esa información en decisiones útiles para el cliente.

- La tecnología cambia; el criterio profesional gana peso. La automatización de determinadas tareas no reduce la importancia del profesional cualificado; cambia el lugar en el que aporta más valor. Revisar grandes volúmenes de imágenes, filtrar avisos repetitivos o localizar determinadas secuencias son procesos que la tecnología puede resolver cada vez con mayor rapidez. Pero comprender el contexto, valorar una amenaza, decidir cómo responder y asumir la responsabilidad de una actuación siguen dependiendo del criterio profesional.

Ese cambio también obligará a evolucionar las competencias dentro del sector. Vigilantes, operadores y directores de seguridad tendrán que conocer mejor cómo funcionan estos sistemas, qué tipo de alertas generan, cuáles son sus límites y cómo integrar esa información en la toma de decisiones. La cuestión, por tanto, no es competir con la máquina en aquello que hace más rápido, sino saber utilizarla para reforzar aquello que sigue marcando la diferencia en seguridad: interpretar correctamente una situación, decidir con criterio y actuar con responsabilidad..

- De ver más a entender mejor. La Inteligencia Artificial no cambia la finalidad de la seguridad privada. Prevenir riesgos, proteger personas y bienes y responder con eficacia cuando se produce una incidencia seguirá siendo el centro de la actividad. Lo que sí cambia es la capacidad para hacerlo con más información, mejor analizada y disponible en el momento adecuado.

Filtrar avisos, localizar secuencias con rapidez, relacionar datos, detectar patrones o priorizar recursos son avances importantes. Pero el cambio más relevante no está en acumular más tecnología, sino en utilizarla para comprender mejor lo que está ocurriendo. Durante décadas, buena parte del valor de la seguridad privada ha estado en reaccionar bien y reaccionar a tiempo. La IA permite añadir ahora algo más: reconocer antes aquello que puede convertirse en un riesgo. El cambio de fondo no está en reemplazar la experiencia del profesional, sino en ampliar su capacidad para identificar antes lo relevante, interpretar mejor una situación y decidir con más elementos de juicio.

La seguridad del futuro no será la que más datos genere ni la que más tecnología acumule. Será la que sepa convertir información en criterio, criterio en decisión y decisión en prevención. Y eso, siempre dependerá de profesionales que sepan mirar, analizar, antes de que el riesgo obligue a reaccionar.

EL RIESGO NO SUELE APARECER DE REPENTE: CASI SIEMPRE AVISA

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Serrano
Coordinador de Servicios Grupo Sureste

www.seguridadyempleo.com

Una visión práctica sobre el análisis y la gestión de riesgos desde la experiencia diaria en seguridad privada

Llevo muchos años trabajando en seguridad privada y, si algo he aprendido durante todo este tiempo, es que los problemas importantes casi nunca aparecen de un momento para otro. Antes de que ocurra una incidencia suele haber señales. El problema es que no siempre les prestamos la atención necesaria.

Puede ser una puerta que habitualmente se queda abierta, una cámara que no cubre bien una zona, un trabajador que no tiene claras sus funciones o una incidencia pequeña que nadie comunica porque aparentemente no ha pasado nada. Son situaciones que terminan formando parte de la rutina. Nos acostumbramos a ellas y pensamos que, como hasta ahora no ha sucedido nada grave, tampoco sucederá en el futuro.

En mi opinión, este es uno de los mayores errores que podemos cometer cuando hablamos de seguridad.

Analizar un riesgo no consiste solamente en preparar un documento, marcar unas casillas y guardarlo hasta la próxima revisión. Eso puede servir para cumplir un requisito, pero no necesariamente para mejorar la seguridad de un servicio. El análisis debe ser útil y estar relacionado con lo que sucede realmente en el puesto de trabajo.

Para hacerlo bien, lo primero es conocer qué tenemos delante. No se puede evaluar igual un centro comercial, una instalación militar, una estación ferroviaria, una fábrica o un edificio de oficinas. Cada servicio tiene sus horarios, sus trabajadores, sus usuarios y sus propias situaciones conflictivas.

Incluso dentro de una misma instalación los riesgos cambian a lo largo del día. No es lo mismo la apertura que el cierre. Tampoco es igual una hora de poca actividad que un momento de máxima afluencia. Hay zonas que durante el día están continuamente ocupadas y que, al llegar la noche, quedan completamente aisladas.

Por eso considero fundamental visitar los servicios y hablar con las personas que están diariamente en ellos. Quien trabaja ocho o doce horas en una instalación conoce detalles que difícilmente aparecen en un informe. Sabe qué puerta suele quedarse mal cerrada, cuándo se acumula más público, qué zona tiene poca visibilidad o en qué momentos falta personal.

Muchas veces ese conocimiento existe, pero no llega a quien tiene capacidad para tomar decisiones.

También debemos diferenciar entre aquello que queremos proteger y aquello que puede dañarlo. Cuando hablamos de proteger una instalación, no nos referimos solamente al edificio o a la mercancía. Estamos protegiendo a los trabajadores, a los clientes, la información, los equipos y la propia continuidad de la actividad.

Una avería puede detener un servicio. Un acceso no autorizado puede poner en peligro información sensible. Una agresión puede causar un daño que va mucho más allá de la pérdida económica. Cada situación es diferente y, por tanto, no todas las medidas sirven para todos los casos.

A veces se piensa que aumentar la seguridad consiste en colocar más cámaras, instalar más alarmas o incorporar más personal. No siempre es así. Tener muchos medios no garantiza que estén bien utilizados.

Una cámara mal orientada puede dejar fuera precisamente la zona que necesitamos controlar. Una alarma pierde su utilidad si no existe una respuesta clara cuando se activa. Un vigilante de seguridad tampoco puede trabajar correctamente si recibe instrucciones contradictorias o no dispone de los medios necesarios.
La seguridad funciona cuando las personas, los procedimientos y la tecnología están coordinados. Si falla cualquiera de estas partes, el resto pierde eficacia.
En ocasiones se puede reducir un riesgo con una actuación bastante sencilla. Mejorar la iluminación, cambiar la ubicación de una cámara, limitar el acceso a una zona o dejar por escrito quién debe comunicar una incidencia puede ser más eficaz que realizar una gran inversión.
Para tomar estas decisiones hay que establecer prioridades. No podemos tratar todos los riesgos como si tuvieran la misma importancia.

Debemos valorar la posibilidad de que ocurra un hecho, pero también las consecuencias que tendría. Existen situaciones poco frecuentes que requieren una atención especial porque, si llegan a producirse, pueden causar un daño muy grave. También hay pequeñas incidencias que parecen poco importantes, pero se repiten todos los días. Esa repetición aumenta el riesgo y termina mostrando que algo no está funcionando correctamente. Pongo un ejemplo sencillo. Una puerta que queda abierta durante unos minutos puede no causar ningún problema. Pero si ocurre todos los días, en una zona restringida y sin vigilancia directa, llegará un momento en que alguien pueda acceder sin autorización. Lo importante no es solamente que todavía no haya ocurrido nada, sino comprobar que existe una posibilidad real de que ocurra.

Otro aspecto importante es la forma en la que tratamos los errores. Si cada vez que un trabajador comunica un fallo buscamos inmediatamente un responsable, llegará un momento en que las incidencias dejarán de comunicarse. No porque hayan desaparecido, sino porque nadie querrá trasladarlas.

Creo que esto sucede más veces de las que queremos reconocer.
El trabajador que se encuentra diariamente en el servicio puede ser el primero en detectar un cambio de comportamiento, una persona merodeando o un objeto fuera de lugar. Esa información tiene mucho valor. Para aprovecharla, debe existir una relación de confianza y un canal de comunicación que sea rápido y sencillo. Comunicar una anomalía no debería verse como una molestia. Tampoco quiere decir que estemos ante una emergencia. Significa que alguien ha observado algo diferente y considera que debe ponerse en conocimiento de la persona responsable. Después será necesario comprobar la información, valorar el riesgo y decidir si hay que actuar.

No podemos olvidar que los servicios cambian. Se modifica el personal, aparecen nuevos horarios, se reorganizan las instalaciones y se incorporan nuevos sistemas. Una evaluación realizada hace dos años puede no servir para la situación actual. También debemos revisar lo sucedido después de cada incidencia. No basta con decir que el trabajador actuó bien o mal. Hay que comprobar si tenía instrucciones, si conocía el procedimiento, si pudo comunicarse y si los medios funcionaron correctamente. En muchas ocasiones se exige una buena respuesta, pero no se analiza si previamente se habían facilitado las condiciones necesarias para ofrecerla.

Desde mi experiencia, gestionar los riesgos es estar pendiente de esos pequeños detalles que otras personas pueden pasar por alto. Es visitar los servicios, escuchar al personal, revisar lo que está fallando y no esperar a que se produzca una situación grave para intervenir. Nunca podremos eliminar todos los riesgos. Eso no sería realista. Lo que sí podemos hacer es conocerlos, reducirlos y estar preparados para actuar.

Al final, la seguridad no consiste en decir que todo está controlado. Consiste en saber qué puede ocurrir, qué medios tenemos y cómo vamos a responder si llega el momento. Y eso no se consigue únicamente desde un despacho. Se consigue estando en los servicios, hablando con las personas y conociendo la realidad diaria del trabajo.

Carlos Serrano Lozano
Profesional de la seguridad privada y coordinador de servicios

SEGURIDAD RENTABLE: LA NUEVA CULTURA EMPRESARIAL QUE ESTÁ TRANSFORMANDO LA GESTIÓN DEL RIESGO

Metro Risk

Edición propiedad de @MetroRisk, asociación

Abraham Santana Herrera
Director de seguridad. Perito

Durante décadas, la seguridad ha sido percibida por muchas empresas como un gasto inevitable, un requisito legal o un simple conjunto de medidas técnicas destinadas a "cumplir". Sin embargo, el contexto actual —marcado por la incertidumbre, la presión económica y la creciente complejidad operativa— ha demostrado que esta visión es insuficiente y, en muchos casos, peligrosa. La seguridad moderna ya no se entiende como un coste, sino como una inversión estratégica que protege la continuidad del negocio.

El punto de partida es claro: toda empresa convive con riesgos, y muchos de ellos no dependen de la voluntad del empresario. Robos, incendios, fallos eléctricos, errores humanos, inundaciones o actos vandálicos pueden paralizar una actividad en cuestión de minutos. La diferencia entre sobrevivir o desaparecer no está en la suerte, sino en la preparación. Como afirma el documento: "sin un análisis de riesgos previo, no existe una diagnosis real del estado de la seguridad" . Y sin diagnosis, no hay tratamiento eficaz.

La seguridad rentable parte de un principio sencillo: proteger lo que sostiene el negocio. No se trata de acumular tecnología, sino de invertir con coherencia. Una buena puerta, una alarma conectada a CRA, un extintor revisado o un protocolo de cierre pueden evitar pérdidas de miles de euros. La seguridad no se mide por lo que cuesta, sino por lo que evita perder: robos, incendios, interrupciones operativas, discusiones con aseguradoras o subidas de prima.

El libro del que nace este artículo desmonta varios mitos profundamente arraigados. Uno de ellos es la idea de que "mientras la merma sea inferior al coste de la seguridad, no merece la pena invertir". Esta lógica, aparentemente económica, es en realidad el origen de la pérdida desconocida, de las brechas operativas y de la falsa sensación de seguridad. La experiencia demuestra que la inversión previa siempre es más barata que la reparación posterior.

Otro mito habitual es "el seguro paga". El texto lo explica con claridad: el seguro paga solo si el riesgo está controlado, documentado y gestionado. La mayoría de denegaciones no se deben a mala fe de la aseguradora, sino a errores del asegurado: falta de mantenimiento, medidas obligatorias inexistentes, declaraciones inexactas o ausencia de procedimientos. La seguridad, por tanto, no solo protege el negocio: protege la póliza.

El libro también pone en valor la figura del Director de Seguridad, un profesional habilitado cuya misión no es "poner cámaras", sino dirigir la gestión integral del riesgo, coordinar departamentos, garantizar el cumplimiento normativo y actuar como enlace con las Fuerzas y Cuerpos de Seguridad. Su trabajo no solo reduce incidentes: aumenta la eficiencia, mejora la imagen corporativa y fortalece la capacidad de continuidad.

La conclusión es contundente: la seguridad rentable no salva objetos; salva empresas. Es una mentalidad, una cultura y una forma de dirigir. La seguridad reduce la probabilidad; el seguro reduce el impacto; la continuidad depende de ambos. Y el empresario que entiende esto deja de reaccionar tarde y empieza a dirigir con visión

LO MÁS CARO ES PAGAR POR ALGO QUE NO TE SIRVE DE NADA.

Metro Risk

Edición propiedad de @MetroRisk, asociación

Alina Rubio de las Casas
Experta en Seguros Generales

Centralizar tus seguros no solo simplifica su gestión; también mejora tu capacidad de negociación, optimiza las coberturas y proporciona una protección más eficiente para tu patrimonio.

Vale para la suscripción del gimnasio a la que no vas, para la freidora de aire que tienes cogiendo polvo y, sobre todo, para tus seguros.

En la oficina lo veo a menudo.
Por ahorrarse lo que cuestan un par de cañas y una de bravas al mes, hay quien empieza a recortar sus papeles hasta que los deja en el chasis.

El coche: "Quítame la grúa desde el kilómetro cero, que mi coche es nuevo y no se rompe". (Hasta que se rompe en la puerta del garaje un lunes a las 8:00).

La casa: "No me pongas lo de las tuberías, que las mías son de las buenas". (Hasta que el vecino de abajo tiene una gotera justo el día que te vas de vacaciones).

Decesos: "¡Huy, de esto no me pongas nada, que no me voy a morir todavía! Jajajaja".

Oye, y ojalá que no. Que brindemos con mucho vino antes de eso. Pero el problema de ir quitando piezas al seguro para que el recibo pese poco es que, el día que lo necesitas, el seguro tampoco "pesa".

No se trata de tenerlo todo contratado, se trata de que lo que tengas, funcione y se adapte a tu realidad.

¿Hace cuánto no miras si tus papeles de hoy te sirven para tus problemas de mañana?

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.

LA ARQUITECTURA DEL ENTORNO: ES DISEÑAR ESPACIOS FÍSICOS TICS E INCLUYENTES PARA EL COMPORTAMIENTO SEGURO

Metro Risk

Edición propiedad de @MetroRisk, asociación

Elena de la Parte

EN MEMORIA "A quien me dio la vida y me enseñó que proteger a los demás es el acto más noble de amor y resistencia.A ti, que siempre seràs mi faro en medio de la tormenta. A cada lector que busque en estas lìneas una guìa, una luz y una herramienta para salvar su propia vida y la de quienes le rodean"

El instante crujiente entre el peligro y la salvación.

Un segundo; Eso es todo lo que requiere el caos para fracturar un siniestro. Imagina que estás en tu puesto de trabajo, en esa sala de reuniones del quinto piso, el aire huele al café de la mañana y al murmullo habitual de tecleos y conversaciones cruzadas. De pronto la luz vacila un chasquido seco relumba en las tripas del edificio y el suministro principal colapsa el humo denso agrio y negro no pide permiso se cuela por los conductos de ventilación devorando el oxígeno y cubriendo los ventanales el sonido del pánico es ensordecedor, pero no para todos en ese mismo habitáculo una compañera sorda mira el techo las sirenas acústicas, son para esta un eco inexistente al fondo del pasillo. Un profesional en silla de ruedas descubre que las puertas de emergencia han quedado bloqueadas por la caída de tensión, a pocos metros un compañero en el espectro autista TEA, se paraliza desbordado por el parpadeo errático de las luces de socorro y el griterío que se propaga como una ola de choque en ese instante suspendido en el tiempo. La brecha entre la vida y la tragedia no la decide el azar la decide la arquitectura del espacio y la inteligencia con la que fue diseñado Ahora respira ,siente como el aire vuelva a llenar tus pulmones .La calma regresa porque este escenario, no fue su final ,es la llamada de atención que nos exige transformar la seguridad .La verdadera protección no consiste en levantar muros ni instalar equipos agresivos que nos atrapen cuando el edificio arde. La salvación reside en la arquitectura invisible e incluyente. Un entorno extendido que piensa siente y guía de forma intrínseca a cada ser humano hacia un refugio seguro independiente de sus capacidades.

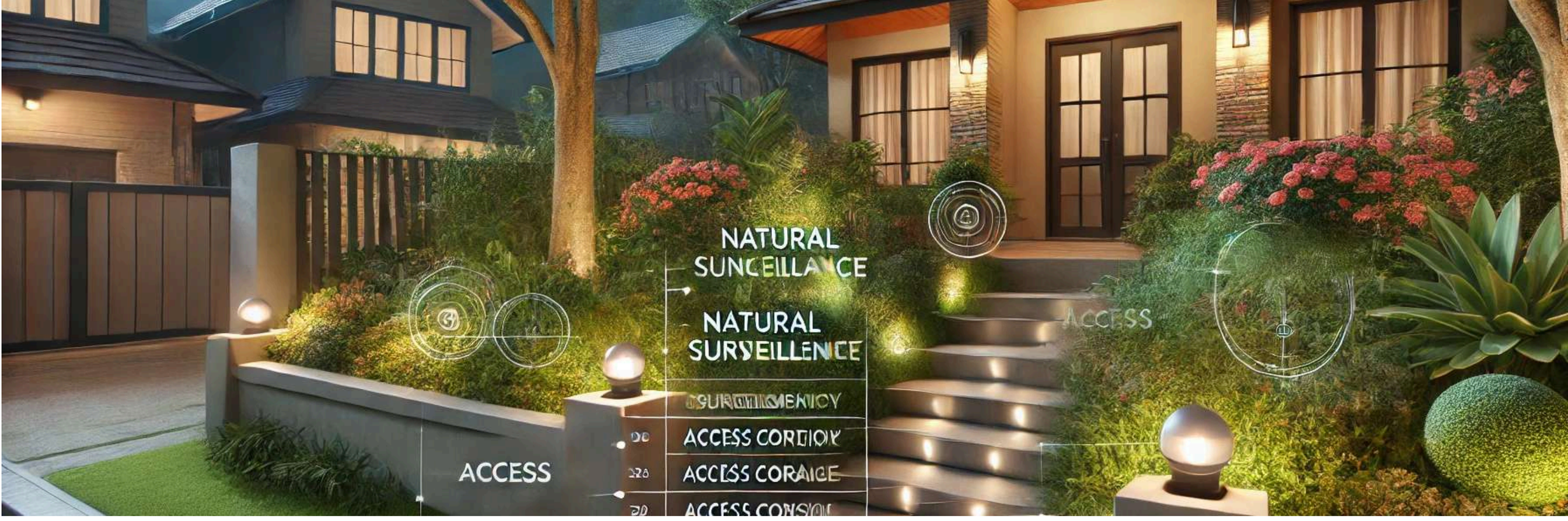
La seguridad invisible y el comportamiento seguro. En la gestión estratégica de riesgos persiste una inercia conceptual que confunde la solidez de la seguridad con la densidad de sus barreras históricamente. La protección de las organizaciones se ha abordado desde la imposición. Normativas punitivas, controles rígidos y vigilancia invasiva, sin embargo la evidencia operativa demuestra que una arquitectura basada en la restricción genera una elevadísima fricción operativa fatiga en el usuario y provoca por ende el diseño de atajos de seguridad. Frente a este modelo reactivo, emerge la seguridad por diseño ,CPTED,la protección más eficaz no sirve músculo disuasorio de forma agresiva; es fluida transparente y profundamente empática la seguridad que salvavidas es aquella que canaliza el comportamiento humano de forma natural logrando que la opción más segura sea intuitivamente la opción más fácil de ejecutar para cualquiera. Esta esta aproximación cobra una urgencia crítica en el escenario actual por dos razones fundamentales:

1. **La difuminación del perímetro corporativo: el espacio de trabajo ya no es una coordenada fija. El trabajo híbrido, la movilidad y el acceso remoto trasladan el riesgo al entorno personal y de tránsito del profesional exigiendo marcos de seguridad física y lógica.**
2. **El Imperativo de la accesibilidad y la inclusión universal: una estrategia de protección que no contempla la diversidad funcional de la plantilla adolece de una falta de madurez operativa básica.Los protocolos de evacuación y los sistemas de alerta deben ser comprensibles y ejecutables por el 100% para las personas.**

El entorno físico corporativo: prevención CPTED cohesionado con LSE y hacer civilidad en emergencias. El diseño del entorno no solo previene el delito ,constituye la infraestructura crítica que determina la supervivencia durante un siniestro o una crisis.Por ende, la madurez de una entidad se miden en la solidez inclusiva de sus protocolos de autoprotección.

A. Prevención ambiental CPTED e inclusión en la evacuación La aplicación de los principios CPTED debe conjugarse con la eliminación radical de barreras:(" sí sí he escrito barreras" has leído bien…

- Rutas de evacuación sin desniveles: los flujos de circulación diseñados para la visibilidad natural deben ser amplios y totalmente accesibles garantizando el desplazamiento autónomo de personas con movilidad reducida.
- Zona de refugio e interfonía adaptada: en edificaciones multinivel, los puntos de espera de rescate deben contar con comunicación bidireccional accesible: pulsadores de emergencia en altura ,normativa (CTE DB-SUA).Bucles magnéticos con prótesis auditivas conectadas y confirmación visual de recepción de la señal de auxilio.



B.Alerta multisensorial y videointerpretación en LSE: protección para personas sordas. Una sirena acústica es inútil en un espacio insonorizado o ante la presencia de personas con discapacidad auditiva severa .Por ende es imprescindible articular un canal multisensorial respaldado por tecnología accesible:

- Secuencias luminosas en habitáculos:la activación de la emergencia desencadena una respuesta visual inmediata, las luminarias del habitáculo salas aseos y demàs dependencias, destellan mediante estrobos cromáticos estandarizados alternando códigos luminosos que señalan dinámicamente la vía de evacuación segura.
- Integraciòn con SVisual y Video-Interpretaciòn en LSE: En España se reconoce de manera oficial la lengua de signos española, recogida tal y como se observa en la ley 27/2007 del 23 de octubre por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas con discapacidad auditivas y sordociegas.Tambièn la lengua de signos catalana en la Ley 17/2010, de 3 de junio, aunque se pueden encontrar muchas más variantes geográficas asociadas a las regiones incluso dentro de una misma región se encuentran signos que varían del entorno rural al entorno urbano de unos grupos sociales a otros etcétera.
- Notificaciones Ópticas asociadas: envió de alertas por liberación diferenciada a través de Wearables o dispositivos corporativos, garantizando que el aviso llegue de forma directa y a tiempo real e inequívoca independientemente de la ubicación de los usuarios.

C.Protocolos de evacuación adaptados al Tea y neuro divergencias. Durante una emergencia la sobreestimulación sensorial,pueden desencadenar un colapso sensorial o bloqueo en personas (con autismo) con TEA.Comprometiendo gravemente su capacidad de reacción y su supervivencia.

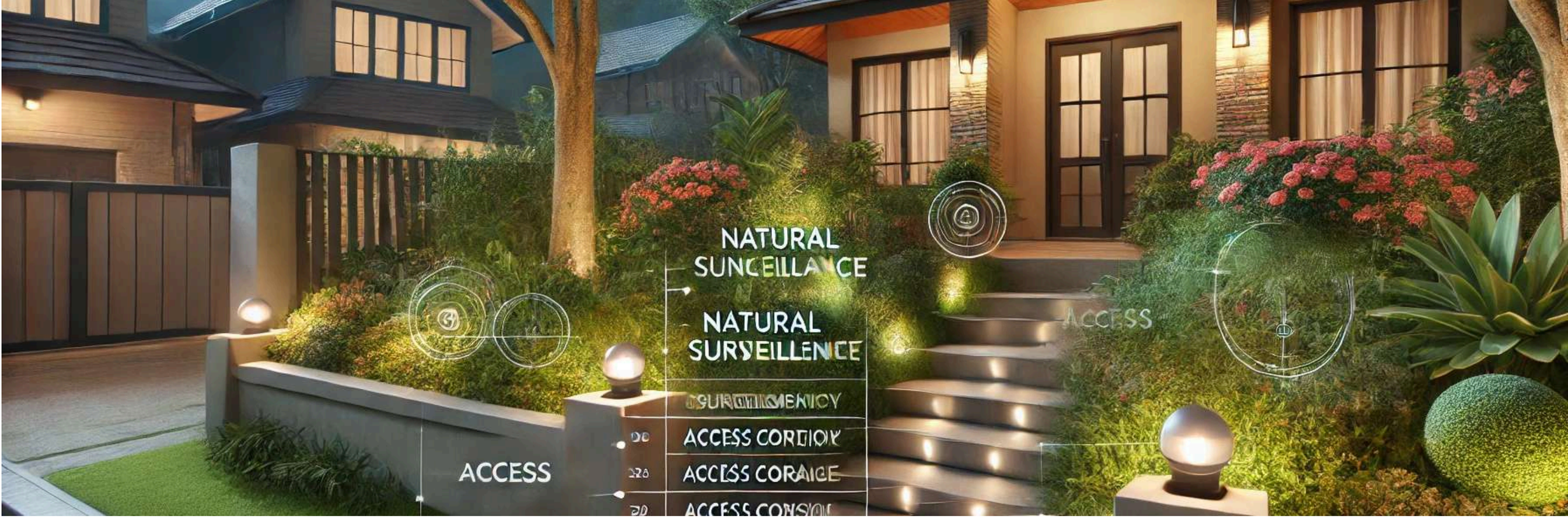
- Señalética de fácil lectura y apoyo pictográfico: planos de evacuación con pictogramas claros y secuencias visuales predecibles. Por ende la estructuración visual del recorrido reduce de forma drástica la sobrecarga cognitiva y la ansiedad y el caos. Minimizando lesiones y pérdidas humanas.
- Ajuste de frecuencias y luminotecnia cuidada: programación de estorbos de emergencia a frecuencias bajas no fotosensibles para prevenir desorientación o crisis epilépticas, combinando la señal acústica con tonos de frecuencia modulada menos agresivos.
- Kits De autorregulación y acompañamiento: protocolos donde los equipos de primera intervención cuentan con pautas pedagógicas específicas para guiar a la persona neuro divergente, mediante instrucciones concisas facilitando elementos de amortiguación sensorial en los puntos de reunión.

La seguridad física de la persona no termina en las puertas de cristal de la sede central. Cuando el profesional trabaja desde su domicilio en tránsito a un espacio público la arquitectura física desaparece, pero la necesidad de un entorno seguro permanece intacta.

- El entorno personal como nuevo Perímetro: se debe dotar al empleado u usuario, de criterios prácticos para evaluar la seguridad física y la accesibilidad de su propio entorno de trabajo: campos de visión en medios de transporte acústica de confidencialidad y riesgos de escucha pasiva .
- Protección del activo movilidad: políticas operativas sobre la custodia de dispositivos, uso de filtros de privacidad de pantalla, gestores de contraseñas de hardware y protocolos de comunicación rápida ante situaciones de extravío o amenaza física inmediata.

La formación corporativa debe abandonar el tono sancionador para transformarse en una herramienta de liderazgo pedagógica y continua. Capacitar a la plantilla significa enseñar a cada individuo a configurar su propio espacio seguro, a reconocer los riesgos de su entorno y a saber cómo actuar con serenidad y empatía ante la vulnerabilidad de un compañero. Decálogo Ejecutivo: la hoja de ruta de la resiliencia humana

1. Garantizar la accesibilidad universal por diseño: ningún plan de autoprotección es válido si deja atrás a una sola persona por motivos de movilidad, capacidad auditiva o neuro divergencia.
2. Implementar avisos multisensoriales en habitáculos:integrar estorbos luminosos y notificaciones ópticas en todas las estancias aisladas de la organización.
3. Integrar plataformas de LSE (LSVisual): facilitar la comunicación bidireccional inmediata en lengua de signos entre las personas sordas y los centros de control de emergencias.
4. Diseñar rutas de evacuación sin barreras cognitivas: incorporar la lectura fácil rápida la señalética mediante pictogramas estandarizados en todos los recorridos de evacuación.
5. Capacitar y formar de forma actualizada los equipos de emergencia en neurodiversidad. Dotar al personal de intervención de pautas pedagógicas y Kiss de regulación sensorial para acompañar a personas con TEA en momentos de crisis
6. Aplicar La prevención ambiental CPTED: diseñar espacios abiertos con visibilidad natural y sin puntos ciegos, reduciendo la fricción operativa y eliminando la sensación de vigilancia invasiva.



7.Extender la seguridad pública en el entorno híbrido: crear protocolos y guías de autoprotección para el profesional en movilidad y en teletrabajo asegurando su bienestar integral en cualquiera coordinación.
8. Auditar la convergencia físico barra digital: evaluar de forma conjunta los controles de accesos a los edificios y los sistemas de autenticación establecidos por protocolos para evitar brechas cruzadas y sesgos.
9.Sustituir la cultura de la culpa por la transformación del apoyo humano: para citar y motivar a la plantilla para que informe de incidentes o vulnerabilidades sin temor a represalias.
10. Ejecutar la seguridad como un acto de humanidad con excelencia deontología óptima y excelente: recordar que detrás de cada protocolo de cada sensor y de cada norma el único objetivo real e irrenunciable es proteger la vida de las personas.

La paz de la tarea cumplida. Cuando la arquitectura se diseña con alma el peligro pierde su capacidad de sembrar el caos,el humo se disipa, las luces guían con precisión y cada persona ,"sin importar sus capacidades ni su ubicación" encuentra el camino de regreso a su casa. Proteger la vida de los demás es el legado más perdurable que podemos construir. Que estas páginas sirvan como; un escudo, una enseñanza viva y con la certeza de que cuando unimos la ciencia técnica con el amor profundo por la condición humana la seguridad deja de ser un trámite para convertirse en nuestro mayor acto de amor de libertad y de paz.

Elena Parte© 2026

Esther Domínguez
Especialista en comercialización de obra nueva, estrategia y posicionamiento inmobiliario

COMPRAR SOBRE PLANO: CUANDO LA INCERTIDUMBRE FORMA PARTE DEL PRODUCTO

La obra nueva obliga a tomar una decisión importante antes de poder ver, tocar o habitar aquello que se compra. Por eso, la verdadera tarea comercial no es eliminar la incertidumbre con promesas, sino convertirla en información comprensible. Comprar una vivienda terminada y comprar una vivienda sobre plano se parecen mucho menos de lo que parece. En una vivienda existente, el comprador puede entrar, recorrer los espacios, mirar por las ventanas, comprobar la luz, escuchar el entorno y decidir con una parte importante de la realidad delante. En obra nueva, en cambio, la decisión se toma sobre planos, memorias de calidades, infografías, documentación técnica, una ubicación y una fecha futura. Eso cambia por completo la naturaleza de la compra. El cliente no está valorando únicamente una vivienda: está intentando anticipar cómo será vivir en algo que todavía no existe. Y ahí aparece un elemento que en el sector inmobiliario se gestiona cada día, aunque rara vez se nombre como tal: la incertidumbre.

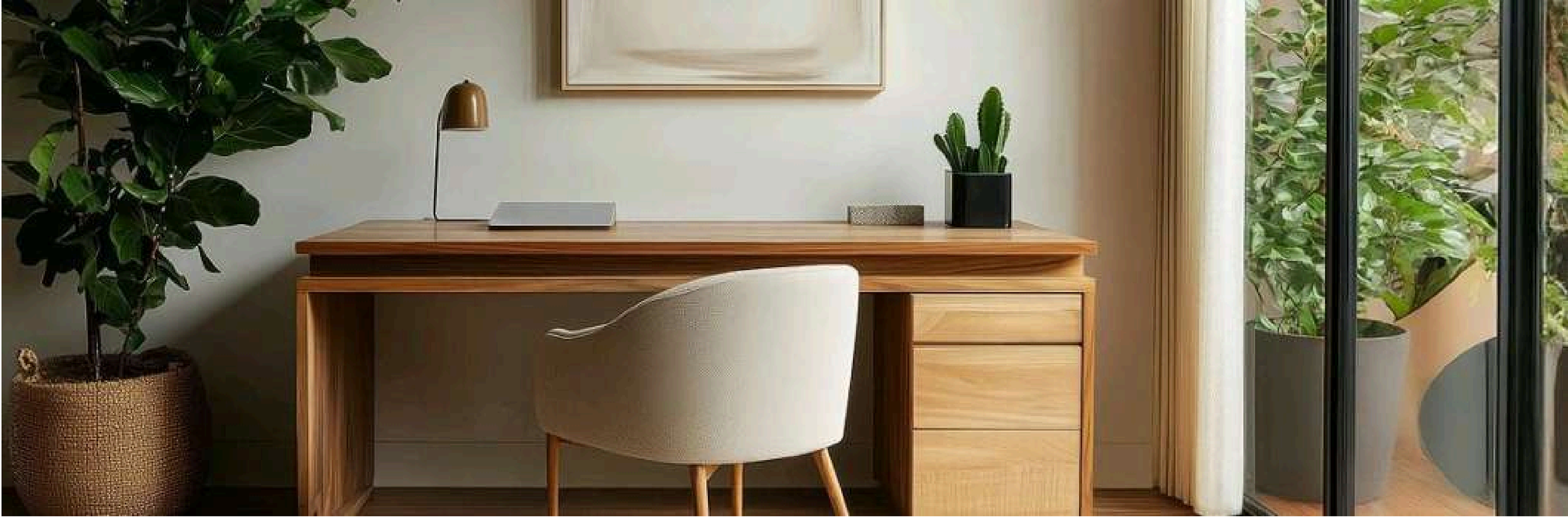
LA DIFERENCIA ENTRE INFORMAR Y TRANQUILIZAR Ante esa incertidumbre existe una tentación comercial evidente: tranquilizar demasiado. Dar por seguro lo que todavía depende de la evolución de una obra, presentar una imagen orientativa como si fuera una fotografía del resultado final o responder con rotundidad a cuestiones que deberían confirmarse técnicamente. Puede parecer una forma de facilitar la venta, pero en realidad aumenta el riesgo. En obra nueva, una buena comercialización no consiste en eliminar todas las dudas a base de certezas aparentes. Consiste en separar con mucha claridad tres cosas: lo que se sabe, lo que está previsto y lo que todavía debe confirmarse. Esa diferencia es fundamental. El comprador no necesita que le prometan que todo será exactamente como lo imagina. Necesita entender qué está comprando y sobre qué elementos puede tomar una decisión sólida.

EL PLANO NO HABLA SOLO Un plano contiene una enorme cantidad de información, pero no todo el mundo sabe interpretarla de la misma manera. Dos metros sobre el papel pueden ser la diferencia entre una terraza que realmente se utiliza y otra que apenas admite el mobiliario que el comprador imaginaba. La orientación, los recorridos, la relación entre cocina y zona de día, la posición de una columna, el tamaño real de una habitación o la distribución de un baño pueden condicionar mucho más la experiencia diaria que determinados acabados. Por eso enseñar un plano no es suficiente. Hay que traducirlo. Una parte importante del trabajo inmobiliario en obra nueva consiste precisamente en convertir documentos técnicos en decisiones de vida cotidiana.

¿Cabe una mesa para seis? ¿Dónde quedaría el sofá? ¿La salida a la terraza está donde el cliente cree? ¿Ese dormitorio permite el uso que tiene pensado? ¿Qué diferencia real hay entre un bajo con jardín y un ático con terraza? No se trata de decidir por el comprador, sino de ayudarle a visualizar con rigor. Cuanto mejor comprende el espacio antes de comprar, menor es la distancia entre la vivienda imaginada y la vivienda que finalmente recibirá.

EL TIEMPO TAMBIÉN FORMA PARTE DE LA OPERACIÓN. Hay otra particularidad que distingue la obra nueva: entre la decisión de compra y la entrega pueden transcurrir muchos meses. Durante ese tiempo cambian cosas. Cambia la obra, avanza la construcción, se concretan determinados aspectos y, a veces, también cambia la vida del comprador. Por eso la relación comercial no debería terminar cuando se firma una reserva. En cierto modo, empieza ahí. La información durante el proceso, la trazabilidad de los cambios, la claridad ante los plazos y la capacidad de explicar qué puede modificarse y qué no forman parte de la calidad percibida de la operación. Cuando durante meses existe silencio, respuestas ambiguas o mensajes contradictorios, la incertidumbre crece. Cuando existe información coherente, incluso una noticia que no sea la esperada puede gestionarse mejor. La confianza no depende de que nunca haya cambios. Depende de cómo se comunican.

Esther Domínguez
especialista de obra nueva, estrategia visualización y marketing inmobiliario
+34 644 561 115



EL RIESGO DE VENDER UNA IMAGEN EN LUGAR DE UNA VIVIENDA. Las herramientas comerciales actuales permiten representar proyectos con un nivel de realismo extraordinario. Infografías, recorridos virtuales, vídeos y renders ayudan muchísimo a comprender una promoción antes de que exista. Pero cuanto más realista es una representación, más importante resulta explicar correctamente qué representa. Una imagen puede ayudar a visualizar un espacio; no debería sustituir la lectura del proyecto. El problema aparece cuando el comprador termina recordando mejor una escena comercial que la documentación que define realmente su vivienda. Ahí nace uno de los riesgos más evitables de la obra nueva: la diferencia entre expectativa y realidad.

Reducir esa distancia exige algo muy poco espectacular, pero muy valioso: precisión. Explicar medidas, distinguir elementos orientativos de elementos definidos, no improvisar respuestas técnicas y dejar constancia de aquello que realmente forma parte de la operación.

VENDER OBRA NUEVA ES GESTIONAR UNA DECISIÓN FUTURA. Durante años se ha asociado la excelencia comercial con la capacidad de convencer. En obra nueva, creo que es más útil asociarla con la capacidad de hacer comprensible una decisión compleja. El buen profesional no sustituye al arquitecto, al promotor, al técnico ni al abogado.

Tampoco debería intentarlo. Su valor está en otro lugar: ordenar la información, detectar qué preocupa realmente al comprador, formular las preguntas adecuadas y conseguir que la persona que tiene delante pueda decidir con más criterio que cuando llegó. Eso también implica saber decir “esto hay que consultarlo”, “esto es orientativo” o “esto no se puede asegurar todavía”. Lejos de debilitar una venta, esas frases pueden reforzarla porque sitúan la relación en un terreno mucho más sólido. Comprar sobre plano siempre contendrá una parte de incertidumbre.

Es inevitable: se está tomando hoy una decisión sobre una realidad que terminará de materializarse mañana. El objetivo profesional no debería ser disfrazar esa incertidumbre, sino hacerla manejable. Porque la seguridad de una compra inmobiliaria no nace de creer que nada puede cambiar. Nace de saber exactamente qué se conoce, qué se ha acordado y qué preguntas todavía necesitan respuesta. Y quizá esa sea una de las diferencias más importantes entre vender metros cuadrados y acompañar de verdad una decisión inmobiliaria.

Esther Domínguez
Especialista en comercialización de obra nueva, estrategia y posicionamiento inmobiliario

LAS CUATRO PUERTAS DE LA HABILITACIÓN

Metro Risk

Edición propiedad de @MetroRisk, asociación

Antonio Pérez Cala
Director de Seguridad
Vocal Presidente de ADISPO Andalucía

Un mismo destino, distintos niveles de exigencia

Cuando alguien me pregunta cómo se puede llegar hoy a ser Vigilante de Seguridad en España, ya no me basta con explicar el examen de toda la vida. Existen cuatro caminos reconocidos, todos amparados en el artículo 29.1.a de la Ley 5/2014, y todos terminan en la misma Tarjeta de Identidad Profesional (TIP). Pero no todos piden lo mismo para llegar hasta ahí, y eso es algo que en el sector sabemos y casi nunca decimos en voz alta.

La vía tradicional, el examen convocado por la Policía Nacional, sigue siendo la más exigente porque es la única evaluada por un tribunal externo e independiente al centro que forma al candidato. Precisamente por eso, cada convocatoria supone una carga logística considerable para la Administración, y cada vez se presenta menos gente. No es casualidad, cuantas más alternativas existen, menos sentido tiene, desde el punto de vista del candidato, asumir el riesgo de un examen que no controla quien le ha formado.

El certificado de profesionalidad (SEAD0112, SEAD0212), impartido por academias privadas, ha crecido precisamente por eso. Aquí es la propia academia quien evalúa a su alumnado, y el incentivo económico es evidente, un alumno que suspende es un cliente insatisfecho, y ninguna academia vive de eso. No digo que se regale el aprobado, pero sí que el diseño del sistema no deja demasiado margen para que el evaluador y el interesado en aprobar sean personas distintas.

La acreditación de competencias por experiencia laboral, gestionada por las comunidades autónomas al amparo del RD 1224/2009, cambia el actor, pero no necesariamente el problema. Aquí quien evalúa es un equipo público, no una academia, así que desaparece el incentivo económico directo. Pero aparece otro, la propia Administración necesita mostrar resultados de sus programas de acreditación, y eso también empuja, aunque de forma más sutil, hacia el aprobado.

Y ahora se suma una cuarta vía, la más nueva: el título de FP de Grado Medio en Seguridad (RD 570/2023), con 2.000 horas lectivas. Aquí la exigencia formal es la mayor de las cuatro, pero conviene no perder de vista que ya hay centros privados autorizados para impartirlo, además de los públicos, y en esos centros privados el mismo incentivo comercial que en las academias de certificado de profesionalidad vuelve a estar presente.

No escribo esto para señalar a nadie en particular. Trabajo con casi todos estos actores, y sé que la inmensa mayoría hace bien su trabajo. Pero seamos honestos de una vez, cuando el que evalúa depende económica o políticamente de que el evaluado apruebe, la exigencia real se resiente, la ponga quien la ponga, y disfrazarlo de calidad no cambia el fondo. Llevamos años hablando de dignificar el sector mientras miramos hacia otro lado con esto, y ese doble discurso empieza a cansar tanto como al propio vigilante que sí se ha dejado la piel en un examen de verdad.

La pregunta no es qué vía elige cada candidato, sino si todas garantizan el mismo nivel al final del camino, y si alguien se siente aludido al leerlo, puede que sea porque algo de razón hay. Y ya puestos a hablar claro, tampoco está de más preguntarse por qué la patronal se ha volcado tanto en asesorar a las comunidades autónomas en el diseño de este Grado Medio, asumiendo buena parte de los convenios de prácticas de sus alumnos, seguramente.

¿Vocación formativa, o necesidad de mano de obra?
Ahí lo dejo

EL GUARDIÁN DEL ÚLTIMO BASTIÓN: CUANDO EL ADMINISTRADOR DE FINANZAS SE CONVIERTE EN EL ARQUITECTO DE LA SEGURIDAD CORPORATIVA.

Metro Risk

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

El administrador de finanzas en América Latina ha experimentado una transformación radical en su rol tradicional. Ya no es únicamente el contralor numérico que vela por la integridad de los estados financieros; hoy se erige como el arquitecto de la seguridad corporativa integral, asumiendo responsabilidades que se extienden desde la ciberseguridad hasta el cumplimiento normativo, pasando por la prevención de delitos económicos y la protección del capital intangible de la organización. Este artículo analiza las nuevas responsabilidades y obligaciones del administrador financiero en el contexto latinoamericano, caracterizado por una acelerada transformación digital, un endurecimiento regulatorio sin precedentes y una amenaza cibernética que crece a un ritmo alarmante. A través del examen de marcos normativos en Brasil, Chile, Colombia y México, así como el estudio de casos emblemáticos como FEMSA, se evidencia que la seguridad corporativa ha dejado de ser un asunto periférico para convertirse en el eje estratégico de la gestión financiera moderna. El artículo concluye con recomendaciones concretas para que los administradores financieros, los consejos de administración y los reguladores enfrenten este nuevo paradigma con la urgencia y la profundidad que la realidad exige.

El Fin del Contralor y el Nacimiento del Arquitecto. Durante décadas, la figura del administrador de finanzas se asoció casi exclusivamente con la custodia de los recursos económicos, la elaboración de estados financieros y el cumplimiento de obligaciones tributarias. Era, en esencia, un guardián de números, un contralor que velaba porque cada partida cuadrara y cada informe reflejara con precisión la realidad económica de la organización.

Ese administrador ya no existe. La transformación digital, la hiperconectividad, la sofisticación de las amenazas cibernéticas y la explosión regulatoria han redefinido por completo el perímetro de responsabilidades del líder financiero. Hoy, el administrador de finanzas debe ser, simultáneamente, un estratega de seguridad, un gestor de riesgos no financieros, un experto en cumplimiento normativo y un agente de cambio cultural. El riesgo cibernético se discute hoy en el mismo lenguaje que el capital, la liquidez y la resiliencia operacional.

América Latina enfrenta este nuevo escenario con una combinación peligrosa de factores: alta exposición digital con baja madurez en seguridad, presupuestos limitados, escasez crónica de profesionales especializados y fallas en la gestión de vulnerabilidades. A esto se suman tasas de informalidad que alcanzan el 47% de los ocupados en la región y un entorno de crimen organizado cuyos costos directos representan el 7% de las ventas anuales de las empresas.

La pregunta que guía este artículo es tan pertinente como urgente: ¿Está el administrador de finanzas latinoamericano preparado para asumir este rol expandido? La respuesta, como se verá a lo largo de estas páginas, es compleja y matizada: hay luces de liderazgo y casos ejemplares, pero también profundas brechas estructurales que amenazan con dejar a muchas organizaciones expuestas en un entorno de riesgos crecientes.

La Nueva Arquitectura de Responsabilidades del Administrador de Finanzas en Seguridad Corporativa.

El administrador financiero contemporáneo no puede limitarse a mirar los estados financieros. Su mirada debe abarcar un espectro mucho más amplio de responsabilidades, todas ellas interconectadas y todas ellas críticas para la supervivencia de la organización.

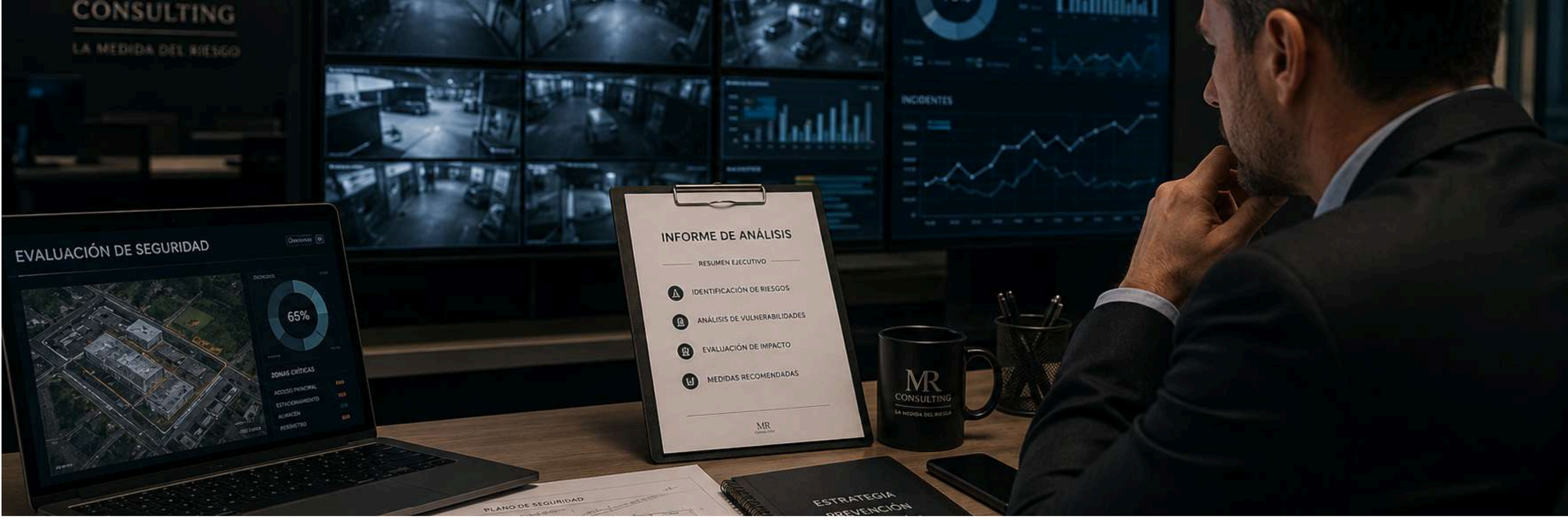
a) Guardianía de activos físicos y digitales.

La custodia tradicional de los activos financieros se ha expandido para incluir la supervisión de infraestructura crítica, sistemas de información y datos sensibles. El administrador de finanzas debe garantizar no solo que los recursos económicos estén seguros, sino que toda la cadena de valor digital que los respalda cuente con controles robustos. Esto implica la implementación de auditorías regulares, la supervisión de controles internos y la salvaguarda de activos intangibles cuya pérdida puede ser tan devastadora como la de los tangibles.

b) Ciberseguridad como extensión natural del control financiero.

El área de finanzas es, paradójicamente, una de las más vulnerables ante ataques malintencionados. Concentra información sensible, maneja transferencias de fondos y opera con sistemas que, si son comprometidos, pueden generar pérdidas millonarias en cuestión de minutos. Por ello, la dirección financiera debe involucrarse activamente en la ciberseguridad, familiarizándose con asuntos de seguridad de TI en el marco de los diversos sistemas legales existentes. El rol del CFO ha evolucionado del cumplimiento interno hacia la protección externa, convirtiéndose en un escudo contra amenazas que trascienden las fronteras de la organización.

En 2025, las organizaciones de América Latina enfrentaron cerca de 3.100 ataques cibernéticos por semana, un volumen que representa más del doble de lo registrado en Estados Unidos. El sector financiero latinoamericano ocupa la sexta posición entre las industrias más atacadas, mientras que en Estados Unidos ni siquiera figura entre las diez primeras. Esta asimetría evidencia la vulnerabilidad estructural de la región y la urgencia de una respuesta coordinada desde la función financiera.



c) Gestión de riesgos financieros y delitos económicos.

La gestión de riesgos financieros sigue siendo responsabilidad central del CFO, pero su alcance se ha ampliado drásticamente. Ya no se trata únicamente de riesgos de mercado, crédito o liquidez; ahora incluye la identificación y mitigación de delitos económicos que pueden manifestarse a través de canales digitales, operaciones con terceros o vulnerabilidades en la cadena de suministro.

La Encuesta Global de Delitos Económicos 2024 reveló que cuatro de cada diez empresas a nivel mundial experimentaron algún tipo de crimen económico o financiero en los últimos dos años. En México, el fraude en el proceso de compras fue señalado como uno de los más disruptivos. El 56% de las empresas mexicanas encuestadas indicó que analiza las transacciones potenciales después de concluirlas, no en tiempo real, lo que evidencia una brecha crítica en la capacidad de detección temprana.

d) Cumplimiento normativo y gobierno corporativo.

El administrador financiero es hoy el principal responsable de asegurar el cumplimiento regulatorio en materia financiera, laboral, ambiental y comercial. Esto incluye el monitoreo e implementación de controles de compliance (LAFT/PTEE), la garantía de adherencia a políticas contables corporativas y normas regulatorias, y la gestión de relaciones con supervisores y entidades de control.

El cambio regulatorio y el cumplimiento normativo se posicionan como el tercer riesgo más importante para las organizaciones latinoamericanas, con un 62.2% de los encuestados identificándolo como una prioridad. Las modificaciones en las leyes y legislaciones, así como el aumento de regulaciones complejas, representan un desafío crucial que recae directamente sobre la función financiera.

e) Liderazgo estratégico y rol de socio del negocio.

Finalmente, el administrador financiero debe ser un socio estratégico del negocio, participando activamente en la estrategia de crecimiento, sostenibilidad y nuevos negocios. Esto implica facilitar la comunicación con casa matriz, aportar análisis y visión financiera para la toma de decisiones, y contribuir a la construcción de una cultura organizacional que integre la seguridad como valor fundamental.

El Administrador de Finanzas como Agente de Cambio Cultural.

La seguridad corporativa no se logra únicamente con tecnología o procedimientos; requiere un cambio cultural profundo que el administrador financiero está llamado a liderar. La literatura especializada ha identificado cuatro roles que el líder financiero debe encarnar para cumplir con esta misión:

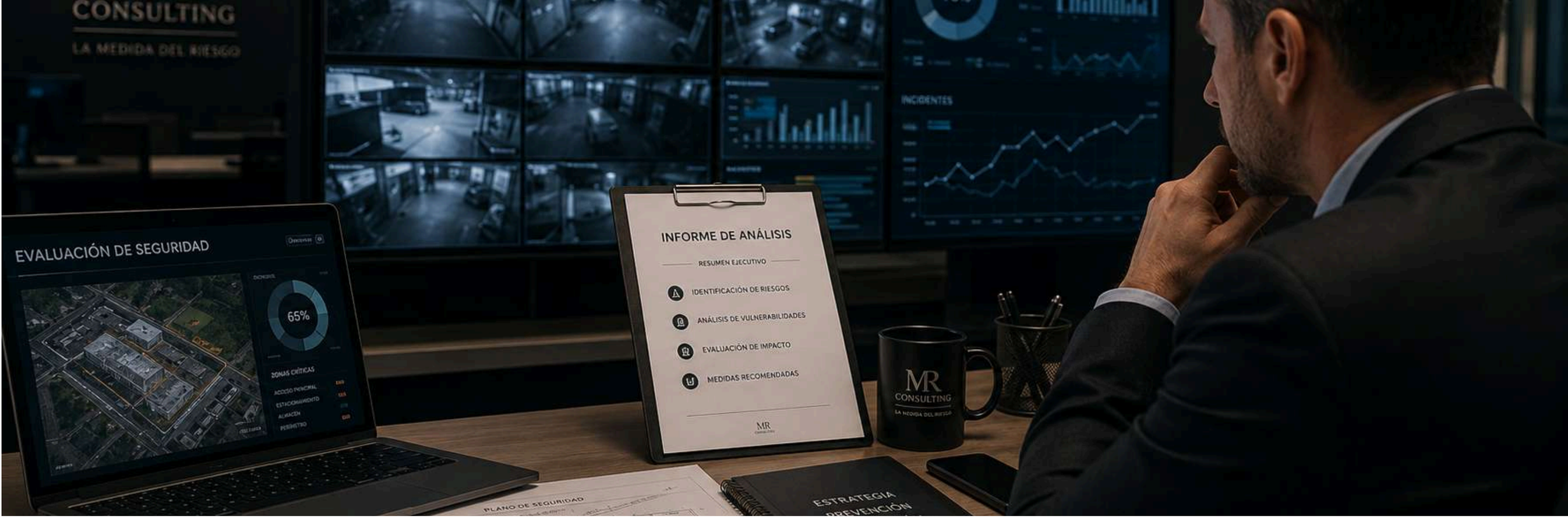
- El Científico: Debe priorizar las necesidades de protección, comprender en profundidad cómo se gestionan los datos y filtrar información sensible y confidencial. Esto exige un conocimiento técnico que tradicionalmente no formaba parte del perfil financiero.
- El Ingeniero: Debe garantizar el cumplimiento de los procedimientos, pues el principal riesgo no es el sistema de TI en sí, sino el uso que los empleados dan a los sistemas. La ingeniería de procesos y la estandarización de prácticas son herramientas fundamentales.
- El Coach: Debe formar al personal sobre los riesgos asociados a los ataques cibernéticos y las medidas para prevenirlos. La capacitación continua y la concientización sobre amenazas como el phishing son líneas de defensa indispensables.
- El Piloto: Debe encontrar el equilibrio entre respetar la privacidad y ejercer el control absoluto. Esta tensión, quizás la más compleja de todas, requiere de un liderazgo que combine firmeza con sensibilidad.

El error humano sigue siendo una de las principales vulnerabilidades en seguridad, lo que subraya la importancia del rol de Coach. La seguridad no es un destino, sino un proceso continuo de aprendizaje y adaptación.

La Realidad Latinoamericana: Un Ecosistema de Riesgos y Oportunidades. América Latina no es un mercado homogéneo, pero comparte desafíos estructurales que configuran un ecosistema de riesgos particularmente complejo para el administrador financiero.

a) Panorama de riesgos específicos de la región.

La ciberseguridad y la protección de datos se mantienen como el riesgo más importante por tercer año consecutivo, con el 67.5% de los encuestados señalándolo como el principal riesgo. El fraude y los delitos financieros ocupan el segundo lugar, con el 48.8% de los encuestados considerándolo un riesgo de alta prioridad.



El panorama de riesgos cibernéticos para el sector financiero de América Latina en 2025 reveló que el 79% de las instituciones financieras de la región han sido objeto de ataques de ransomware, un índice considerablemente superior al promedio mundial del 53%. Esta disparidad evidencia que la región no solo está más expuesta, sino que también está menos preparada para responder.

b) Transformación regulatoria acelerada.
La regulación financiera en América Latina experimenta una transformación acelerada hacia el fortalecimiento de la capacidad de respuesta institucional ante riesgos emergentes del ecosistema digital. Los supervisores financieros elevan los estándares de conducta de mercado, transparencia y continuidad del servicio, introduciendo requisitos operativos más estrictos para la gestión de incidentes, particularmente los relacionados con ciberseguridad y seguridad de la información.

c) Marcos normativos clave por país.
Brasil: La LGPD (Ley General de Protección de Datos) exige reportar incidentes y contar con políticas de privacidad robustas. La Autoridad Nacional de Protección de Datos (ANPD) ha intensificado sus acciones en 2025, aplicando multas de hasta el 2% de los ingresos brutos (con un máximo de R$ 50 millones por infracción) y sanciones no pecuniarias como la suspensión de actividades. Adicionalmente, el Banco Central de Brasil ha emitido resoluciones como la Nº 538/2025 y la CMN 5.274/2025, que exigen comprobación estricta de controles, monitoreo continuo y gobernanza madura, obligando a los bancos a implementar 14 controles obligatorios que van desde autenticación robusta hasta gestión de riesgos en proveedores tercerizados.

Chile: La Ley Nº 21.663, Marco de Ciberseguridad, pionera en Latinoamérica, entró en vigencia el 1 de enero de 2025. El 1 de marzo de 2025 entraron en vigencia las obligaciones para prestadores de servicios esenciales y operadores de importancia vital (OIV), incluyendo el deber de reporte de incidentes de impacto significativo. En septiembre de 2025, se publicó una nómina de casi 1.400 instituciones que podrían ser calificadas como OIV, abarcando sectores como banca, servicios financieros, telecomunicaciones e infraestructura digital. La Agencia Nacional de Ciberseguridad ha establecido lineamientos que incluyen la obligación de designar un encargado de ciberseguridad para el reporte de incidentes.

Colombia: El SARLAFT (Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo) ha sido extendido a nuevos sectores. La Resolución 2328 de 2025 de la Superintendencia de Transporte establece la implementación obligatoria del SARLAFT para todas las empresas del sector transporte. La Superintendencia Financiera ha emitido conceptos clarificando la tercerización de procesos en el marco del SARLAFT.

México: El 53% de las empresas ha enfrentado algún delito económico en los últimos años. El fraude en compras, la corrupción y la extorsión son amenazas recurrentes que exigen una gestión de riesgos robusta desde la función financiera.
Mercosur: Se analiza la aprobación de una Directiva Marco de Ciberseguridad y Protección de Datos del Mercosur, con sanciones económicas proporcionales a la facturación global, lo que podría armonizar los estándares en la región**.**

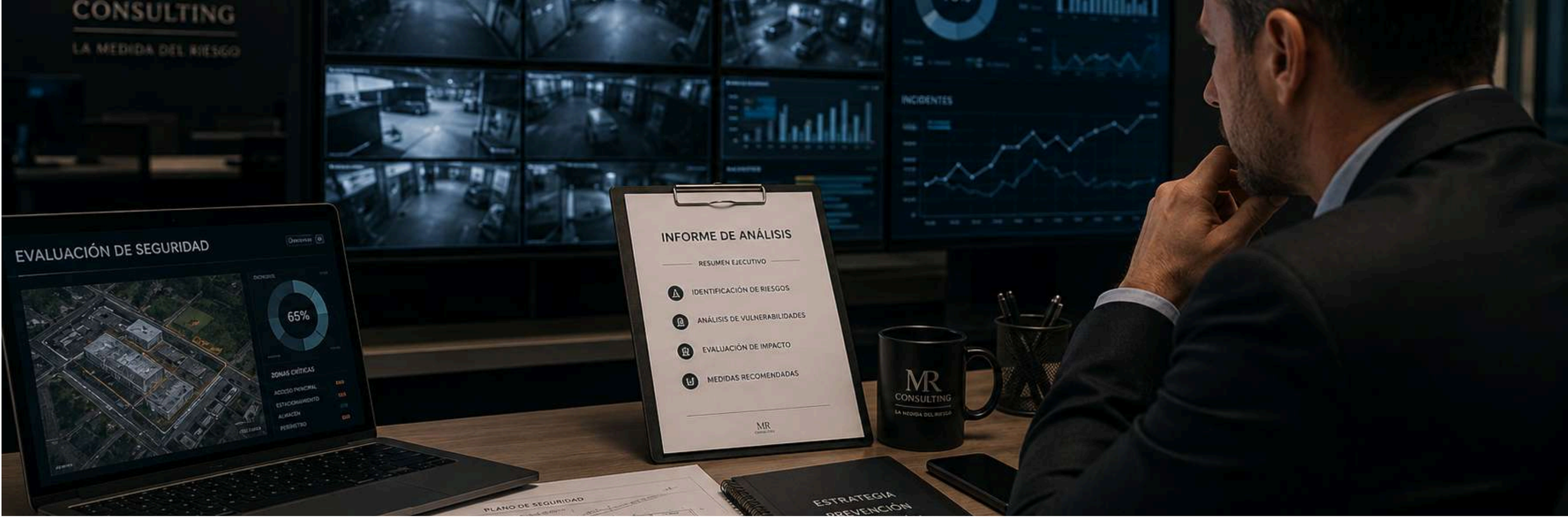
d) Brechas y desafíos estructurales.
A pesar de los avances regulatorios, persisten brechas significativas. La protección de datos financieros en la contabilidad digital se aborda mediante regulaciones en desarrollo, inversiones en ciberseguridad y alfabetización digital, buscando alinearse con normativas globales como el RGPD. Sin embargo, el 56% de los encuestados usa análisis de datos solo después de concluir una transacción, no en tiempo real, lo que limita la capacidad de detección temprana de fraudes.

La evaluación y gestión de riesgos relacionados con terceros es una oportunidad clave que aún no ha sido plenamente aprovechada. Solo el 29% de las organizaciones mexicanas asignan puntajes de riesgo a sus terceros, dejando un vacío significativo en la gestión de la cadena de suministro.

Casos de Estudio y Buenas Prácticas en la Región. Caso FEMSA (México): El tesorero José Manuel Olguín señala que el rol del CFO ha dado un "giro de 180 grados", pasando de manejar cumplimiento e impuestos a ser un asesor estratégico en seguridad. FEMSA ha adoptado políticas y procedimientos integrales relacionados con sus controles de seguridad y privacidad de la información. La compañía mantiene un programa de seguridad de la información que se presenta ante el Comité de Auditoría y el Consejo de Administración, con el Chief Information Security Officer actuando como consultor interno.

Las prácticas implementadas por FEMSA incluyen:
Gobernanza con reglas, controles y procedimientos en todas las áreas.
Revisión de accesos a tokens y comunicación con bancos.
Canales únicos de comunicación con entidades financieras.
Contratación de hackers éticos para pruebas de penetración.
Centralización del departamento financiero para reducir puntos de contacto.
Estandarización de comunicaciones bancarias mediante formatos MT940 de SWIFT.

Lección aprendida: La seguridad no es un gasto, es una inversión estratégica que protege la reputación y la continuidad del negocio. FEMSA ha demostrado que la integración de la seguridad en la función financiera no solo reduce riesgos, sino que también genera eficiencias operativas.



Dimensiones Críticas y Áreas de Tensión. El administrador financiero debe navegar por un conjunto de tensiones que definen los límites de su actuación:

La tensión entre control y agilidad: La rigidez de los controles necesarios para garantizar la seguridad puede entrar en conflicto con la necesidad de agilidad operativa en entornos volátiles. Encontrar el punto de equilibrio es uno de los desafíos más complejos de la gestión financiera contemporánea.

La tensión entre privacidad y vigilancia: El desafío de encontrar el equilibrio entre respetar la privacidad de los empleados y mantener un control absoluto sobre los datos y sistemas es cada vez más acuciante, especialmente con la entrada en vigor de leyes de protección de datos en toda la región.

La tensión entre cumplimiento y competitividad: El costo del cumplimiento normativo - que en Brasil puede alcanzar multas de hasta R$ 50 millones por infracción - debe equilibrarse con la necesidad de mantener competitividad en mercados emergentes.

La tensión entre centralización y descentralización: La centralización financiera reduce riesgos de seguridad pero puede limitar la capacidad de respuesta local. FEMSA optó por la centralización como estrategia de reducción de riesgos, pero esta decisión no es universalmente aplicable.

Recomendaciones Estratégicas.

- Primera: El administrador de finanzas en América Latina debe asumir un rol protagónico en la seguridad corporativa que trasciende lo meramente financiero. La evidencia empírica muestra que las organizaciones que integran la seguridad en la función financiera tienen mayor resiliencia y mejor capacidad de respuesta ante crisis.
- Segunda: La región enfrenta desafíos regulatorios y de riesgo específicos que requieren respuestas adaptadas al contexto local. La heterogeneidad normativa entre países - desde la Ley Marco de Ciberseguridad en Chile hasta la LGPD en Brasil - exige que los administradores financieros desarrollen una visión panorámica y la capacidad de operar en entornos regulatorios diversos.
- Tercera: La transformación digital y la ciberseguridad son inseparables de la gestión financiera moderna. El 79% de las instituciones financieras de la región han sido objeto de ataques de ransomware, y la velocidad de los ataques - 3.100 por semana en la región - exige una respuesta igualmente ágil y sofisticada.
- Cuarta: La brecha entre las capacidades actuales y las requeridas es significativa y requiere acción inmediata. La falta de cultura de riesgos, la escasez de profesionales especializados y la limitada inversión en tecnología de seguridad son obstáculos que deben ser superados con urgencia.

Recomendaciones Estratégicas

<u>Para administradores financieros:</u>

- Desarrollar competencias en ciberseguridad, gobierno de datos y gestión de riesgos no financieros. La formación continua no es opcional; es una condición de supervivencia.
- Establecer alianzas estratégicas con los responsables de TI y seguridad. La seguridad no es un asunto de un área; es una responsabilidad compartida que requiere colaboración transversal.
- Implementar sistemas de monitoreo en tiempo real que permitan detectar anomalías antes de que se materialicen en pérdidas.
- Para consejos de administración:
- Incluir la seguridad corporativa como parte integral de la agenda financiera y de gobierno corporativo.
- Exigir reportes periódicos sobre riesgos de seguridad y su impacto financiero, tratando el riesgo cibernético con la misma seriedad que el riesgo financiero.
- Asegurar que la organización cuente con lineamientos en materia de ciberseguridad y promueva una cultura de ciberseguridad en todos los niveles.

<u>Para reguladores:</u>

- Avanzar hacia la armonización regulatoria en la región, facilitando el cumplimiento para empresas multinacionales sin sacrificar la robustez de los controles.
- Establecer estándares mínimos de ciberseguridad para el sector financiero que sean exigibles y verificables.
- Promover la colaboración público-privada para el intercambio de inteligencia sobre amenazas y buenas prácticas.
- Para el sector académico:
- Incorporar la seguridad corporativa y la ciberseguridad en los currículos de formación de administradores financieros.
- Desarrollar programas de investigación que aborden las particularidades del contexto latinoamericano en materia de riesgos y seguridad.
- Fomentar la formación interdisciplinaria que combine finanzas, tecnología y derecho

<u>Para las organizaciones:</u>

- Invertir en capacitación continua, herramientas de monitoreo avanzado y cultura de seguridad que permee toda la organización.
- Asignar presupuestos adecuados para ciberseguridad, reconociendo que es una inversión y no un gasto.
- Implementar programas de concienciación que involucren a todos los empleados, desde la alta dirección hasta los niveles operativos.

LOS PIONEROS DE LA SEGURIDAD PRIVADA

Metro Risk

Edición propiedad de @MetroRisk, asociación

Carlos Enrique Perez Barrios
Director General de GLOBAL SECURITY ACADEMY USA

Cuando no existían manuales, universidades ni tecnología para enseñarles el camino.
Por Carlos Enrique Pérez Barrios Magíster en Seguridad y Defensa Nacional

Hablar hoy de seguridad privada significa hacerlo dentro de una actividad que dispone de herramientas que hace apenas unas décadas parecían inimaginables. Existen programas académicos, diplomados, certificaciones, libros especializados, revistas, artículos técnicos, asociaciones profesionales, congresos internacionales y una enorme cantidad de información disponible de manera inmediata. A todo ello se suma una revolución tecnológica que ha colocado al alcance del profesional sistemas de videovigilancia inteligente, controles de acceso, biometría, GPS, drones, plataformas de monitoreo, análisis de datos e inteligencia artificial, recursos que han transformado profundamente la manera de prevenir riesgos y proteger personas, bienes, información y operaciones. Precisamente por vivir rodeados de esas posibilidades corremos el riesgo de olvidar algo fundamental: la seguridad privada no nació así. Hubo una generación que comenzó a desarrollar esta actividad cuando prácticamente ninguna de esas herramientas estaba disponible y cuando todavía no existía una estructura académica y profesional capaz de decirle cómo debía hacerlo. Fueron hombres y mujeres que tuvieron que proteger instalaciones, empresas, industrias, bancos, comercios y patrimonios mientras, al mismo

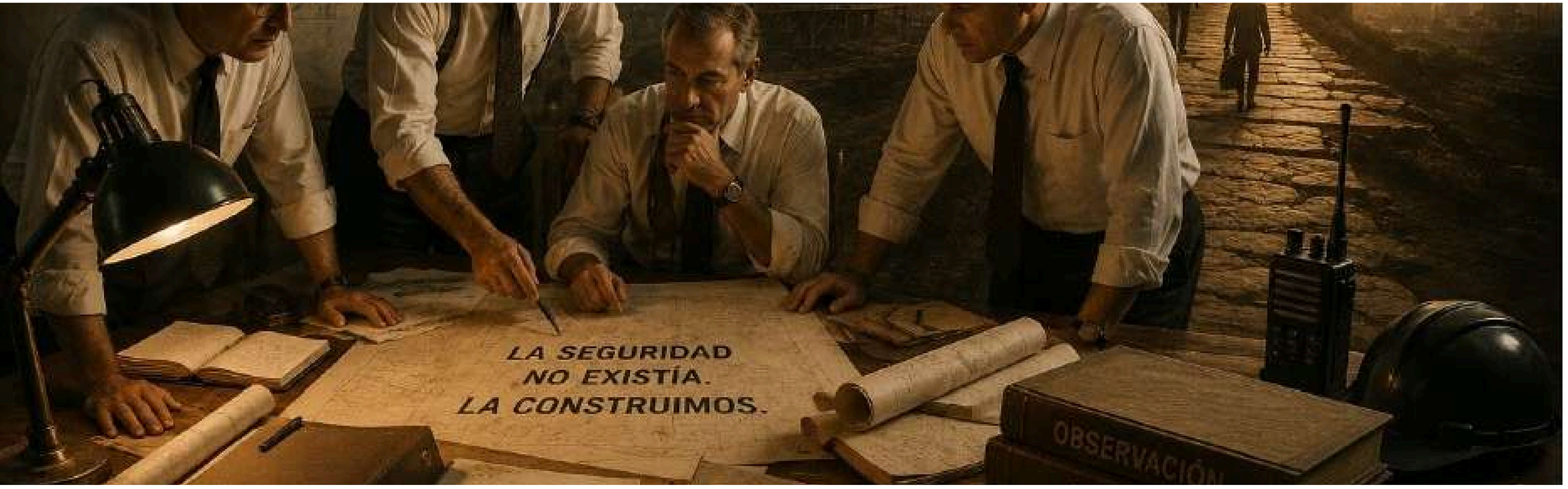
Los pioneros comenzaron a construir una actividad profesional cuando muchas de las herramientas actuales aún no existían.

Hablar hoy de seguridad privada significa hacerlo dentro de una actividad que dispone de herramientas que hace apenas unas décadas parecían inimaginables. Existen programas académicos, diplomados, certificaciones, libros especializados, revistas, artículos técnicos, asociaciones profesionales, congresos internacionales y una enorme cantidad de información disponible de manera inmediata. A todo ello se suma una revolución tecnológica que ha colocado al alcance del profesional sistemas de videovigilancia inteligente, controles de acceso, biometría, GPS, drones, plataformas de monitoreo, análisis de datos e inteligencia artificial, recursos que han transformado profundamente la manera de prevenir riesgos y proteger personas, bienes, información y operaciones. Precisamente por vivir rodeados de esas posibilidades corremos el riesgo de olvidar algo fundamental: la seguridad privada no nació así. Hubo una generación que comenzó a desarrollar esta actividad cuando prácticamente ninguna de esas herramientas estaba disponible y cuando todavía no existía una estructura académica y profesional capaz de decirle cómo debía hacerlo. Fueron hombres y mujeres que tuvieron que proteger instalaciones, empresas, industrias, bancos, comercios y patrimonios mientras, al mismo tiempo, aprendían cómo organizar una actividad que apenas comenzaba a adquirir identidad propia. No recibieron un camino terminado. Tuvieron que construirlo mientras avanzaban.

No recibieron un camino terminado: lo fueron construyendo mientras avanzaban.

Los pioneros de la seguridad privada construyeron una profesión cuando todavía había pocas herramientas, escasa tecnología y casi ningún camino trazado.

https://youtu.be/OrnCl79j9Ec?si=tbisjMQtkGwoAnOJ



CUANDO LA SEGURIDAD PRIVADA TODAVÍA BUSCABA SU CAMINO Muchos de aquellos pioneros llegaron a la seguridad privada procedentes de otras actividades y trajeron consigo conocimientos adquiridos en las Fuerzas Armadas, los cuerpos policiales, la banca, la industria, los seguros, la administración, la investigación o el mundo empresarial. Cada uno incorporó lo que sabía y trató de adaptarlo a una realidad diferente, porque una cosa era haber dirigido personal, investigado delitos, administrado organizaciones o protegido instalaciones desde el Estado, y otra muy distinta convertir esas experiencias en un servicio privado capaz de responder a las necesidades específicas de un cliente. Esa transición obligó a aprender haciendo. Había que determinar cómo seleccionar adecuadamente al personal, cómo capacitarlo, establecer consignas, organizar puestos de servicio, diseñar recorridos, supervisar operaciones, responder ante emergencias, elaborar informes y mantener relaciones con clientes y autoridades. Lo que actualmente puede encontrarse explicado en manuales, libros, programas académicos o procedimientos corporativos, entonces debía descubrirse muchas veces mediante la observación, la experiencia y, por supuesto, también mediante el error. Aquí aparece una primera deuda de reconocimiento: resulta muy fácil juzgar el pasado utilizando las herramientas del presente, pero sería profundamente injusto hacerlo sin considerar las condiciones en las cuales aquellos profesionales tuvieron que trabajar.

APRENDER HACIENDO, CORREGIR APRENDIENDO Naturalmente, aquellos primeros modelos no fueron perfectos. Hubo procedimientos que posteriormente debieron modificarse, conceptos que evolucionaron y prácticas que hoy resultan insuficientes; sin embargo, su verdadero mérito no radica en haber acertado siempre, sino en haber tenido que encontrar respuestas cuando muchas veces no existía dónde buscarlas. Cuando aparecía un problema nuevo no podían consultar inmediatamente decenas de documentos, observar experiencias internacionales mediante Internet o comunicarse en segundos con especialistas ubicados en otros países. El conocimiento viajaba lentamente y, por ello, había que observar, preguntar, experimentar, equivocarse, corregir y volver a intentar. De esa dinámica fue naciendo una experiencia que comenzó a transformarse en procedimientos y que posteriormente pasó de empresarios a gerentes, de gerentes a supervisores y de supervisores a nuevas generaciones de trabajadores. De alguna manera, la propia operación se convirtió en una escuela, porque cada incidente dejaba una enseñanza y cada problema obligaba a buscar una solución que, con el tiempo, podía convertirse en una práctica profesional.

CUANDO EL CONOCIMIENTO TAMBIÉN ERA UN RECURSO ESCASO A la falta de formación especializada se agregaba otra dificultad que hoy cuesta dimensionar: acceder al conocimiento era complicado. Los libros técnicos especializados eran escasos, las revistas profesionales circulaban con dificultad, los cursos eran limitados y los congresos representaban oportunidades excepcionales para conocer lo que otros estaban haciendo. Una conversación entre colegas podía aportar una experiencia que, de otra manera, habría tardado años en llegar. Por esa razón, quienes impulsaron cámaras empresariales, asociaciones profesionales, encuentros, cursos, conferencias y publicaciones también contribuyeron decisivamente a la construcción de la seguridad privada. Aquellos espacios permitieron comenzar a compartir experiencias que hasta entonces permanecían aisladas dentro de cada empresa y, poco a poco, el conocimiento individual comenzó a transformarse en conocimiento colectivo. Allí encontramos otra de las grandes contribuciones de los pioneros: no solamente construyeron empresas; ayudaron a construir una actividad profesional.

CUANDO LA PRINCIPAL TECNOLOGÍA ERA EL HOMBRE Si existe un terreno donde la distancia entre aquellas generaciones y las actuales resulta extraordinaria es precisamente el tecnológico. Hoy hablamos con absoluta normalidad de cámaras digitales de alta resolución, centros de monitoreo, controles biométricos, geolocalización, reconocimiento de placas, drones, sensores, plataformas integradas y sistemas capaces de procesar enormes cantidades de información; sin embargo, durante buena parte de aquellos primeros años, la comunicación podía depender de un teléfono fijo o de un equipo de radio, los registros se realizaban manualmente, los informes se escribían sobre papel y la supervisión exigía presencia física. En esas condiciones, el principal componente tecnológico del sistema terminaba siendo inevitablemente el ser humano, porque de su capacidad para observar, interpretar, informar y reaccionar dependía buena parte de la protección. Aquella limitación obligó a desarrollar algo que continúa siendo indispensable incluso en medio de la revolución tecnológica actual: criterio profesional, porque ninguna cámara, algoritmo o sistema de inteligencia artificial elimina la necesidad de contar con personas capaces de comprender qué está ocurriendo y tomar decisiones responsables.

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

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

DEL OFICIO A LA PROFESIÓN Mientras aquellos empresarios resolvían problemas cotidianos también estaban respondiendo, quizás sin proponérselo, una pregunta mucho mayor: ¿qué debía ser la seguridad privada? Había que convencer al mercado de la necesidad del servicio, organizar estructuras administrativas, establecer tarifas, seleccionar y capacitar trabajadores, crear sistemas de supervisión, desarrollar procedimientos y, paralelamente, participar en la construcción de regulaciones, organizaciones gremiales y criterios profesionales. Con el paso de los años, aquella experiencia comenzó a organizarse y la actividad fue evolucionando. Surgieron programas de formación, publicaciones especializadas, congresos, asociaciones, certificaciones y metodologías; al mismo tiempo, la seguridad empezó a relacionarse cada vez más con la administración, el análisis de riesgos, la criminología, la tecnología, los recursos humanos, la continuidad de negocios, la inteligencia, la investigación y la planificación estratégica. Así comenzó a producirse una transformación trascendental: la seguridad privada fue dejando de ser solamente un oficio para convertirse progresivamente en una profesión.

RECONOCER EL PASADO SIN QUEDARNOS EN ÉL Ahora bien, reconocer a los pioneros no significa convertir sus métodos en modelos eternos ni utilizar su historia para justificar prácticas que el conocimiento actual ya superó. Ellos tuvieron que improvisar muchas veces porque no existían alternativas; nosotros vivimos una realidad completamente diferente y, precisamente por ello, tenemos una responsabilidad mucho mayor. Hoy existen universidades, diplomados, certificaciones, libros, revistas, congresos, asociaciones profesionales, plataformas digitales y acceso prácticamente ilimitado a experiencias internacionales. La experiencia continúa siendo extraordinariamente valiosa, pero ya no puede caminar sola; debe encontrarse acompañada por conocimiento, metodología, tecnología y actualización permanente. Y aquí surge inevitablemente una pregunta que debería incomodar a quienes todavía consideran suficiente administrar la seguridad únicamente sobre la base de los años de servicio: si aquellos pioneros fueron capaces de construir tanto disponiendo de tan poco, ¿cómo podemos justificar que algunos profesionales actuales hagan tan poco disponiendo de tanto?

LA RESPONSABILIDAD DE LAS NUEVAS GENERACIONES Cada generación recibió una responsabilidad diferente. A los pioneros les correspondió abrir el camino; a quienes vinieron después, organizarlo y profesionalizarlo; mientras que a las generaciones actuales les corresponde transformarlo y llevarlo hacia niveles que aquellos primeros empresarios difícilmente pudieron imaginar. Por eso el mejor homenaje no consiste solamente en recordar nombres, empresas o anécdotas, sino también en recuperar documentos, fotografías, testimonios y experiencias de quienes participaron en aquellos primeros años, especialmente porque muchos todavía pueden contarnos cómo comenzó todo y cuáles fueron los obstáculos que debieron superar. Una profesión que desconoce su historia corre el riesgo de creer que todo comenzó con ella y, peor todavía, de repetir errores que generaciones anteriores ya habían aprendido a superar.

LEGADO Los pioneros de la seguridad privada nos dejaron mucho más que empresas, procedimientos y organizaciones gremiales. Nos demostraron que una profesión puede comenzar incluso antes de que existan universidades que la enseñen, libros que la expliquen o tecnologías que faciliten su desarrollo, porque ellos construyeron mientras aprendían y aprendieron mientras construían. Ahora corresponde a las nuevas generaciones convertir aquella experiencia acumulada en conocimiento, ese conocimiento en profesionalismo y ese profesionalismo en una seguridad privada capaz de responder a los riesgos del futuro. Respetar a los pioneros, por tanto, no significa hacer las cosas exactamente como ellos las hicieron, sino comprender por qué tuvieron que hacerlas de aquella manera y asumir que nosotros, contando con muchísimo más, estamos obligados a hacerlo mejor.

FRASE DOCTRINARIA

“Los pioneros de la seguridad privada no encontraron un camino profesional que seguir; tuvieron que abrirlo. La responsabilidad de las nuevas generaciones no es caminar como ellos, sino llevarlo mucho más lejos.”

GESTIÓN DEL CAMBIO DE SEGURIDAD DE LA AVIACIÓN CIVIL (AVSEC) EN LOS AEROPUERTOS.

Metro Risk

Eduardo Reyes
Gerente de Aseguramiento de Calidad, Seguridad Ocupacional

Los aeropuertos están catalogados como infraestructuras críticas e inclusive en algunos casos, de seguridad nacional. Son entes vivos con capacidad de adaptarse a contextos externos e internos diversos, esta flexibilidad en cierta medida, los vuelve vulnerables desde el punto de vista de seguridad. Por ejemplo, la construcción de una nueva terminal de pasajeros, implica riesgos asociados tanto desde el punto de vista de Seguridad Operacional (Safety) como de Seguridad de la Aviación Civil (AVSEC).

Uno de los procesos más importantes incluido en uno de los 4 Componentes del Safety Management System (SMS) es la Gestión del Cambio, sin embargo, dicha gestión también se aplica a temas de AVSEC (Aviation Security) y es base para definir acciones que minimicen el impacto que puedan generar dichos cambios, desde un cambio regulatorio, personal directivo o gerencial, una nueva ruta, pista o terminal de pasajeros entre muchos otros. El avance tecnológico en materia de seguridad es cada vez más rápido, nuevos equipos de inspección de equipajes, de carga, de pasajeros, nuevos sistemas de cámaras con IA capaces de identificar conductas sospechosas, el uso de pases de abordar biométricos a través de geometría del rostro y características oculares, cercados perimetrales inteligentes basados en geocercas y sistemas de alertamiento temprano, entre muchos otros, requieren una evaluación previa a fin de determinar cómo influirán dichos sistemas en los procesos actuales de seguridad del aeropuerto, aerolíneas, prestadores de servicio y demás partes involucradas incluyendo evidentemente a los pasajeros. Recuerdo que con la implementación de e-gates en varios aeropuertos de México, el cambio cultural fue una de las principales barreras.

Este sistema permite a través del código QR del pase de abordar, ingresar a los Puntos de Inspección de Pasajeros y Equipaje de Mano (PIPEM). Su implementación no fue fácil, innovar en un sistema que era totalmente desconocido en todos los aeropuertos de México, implicó desde convencer a las autoridades aeronáuticas acerca de su confiabilidad hasta educar al pasajero, previo a que el sistema ya estuviera en operación. Los tiempos de procesamiento se redujeron de manera sustancial, pero sobre todo, los errores, pues anteriormente la verificación positiva del pase de abordar se llevaba a cabo de manera “manual” a través del personal de seguridad, con alto porcentaje de dependencia del factor humano. Otro ejemplo aplicado a los operadores de aeronaves, es la apertura de una nueva ruta. Independientemente del cumplimiento regulatorio del país del nuevo destino, evaluar el nivel de riesgo de la ruta (que no sobrevuele espacio aéreo en conflicto por ejemplo), la existencia de grupos terroristas o de la delincuencia organizada en el lugar o en países o localidades vecinas, fenómenos migratorios que en décadas anteriores era muy común el apoderamiento ilícito de aeronaves por parte de emigrantes, que en busca de mejores oportunidades de vida, secuestraban aeronaves para salir de su país.

La Gestión del Cambio en términos de AVSEC, implica mayor cantidad de variables a evaluar que para Seguridad Operacional, la diferencia estriba en que, para AVSEC el factor humano siempre juega un papel fundamental, a diferencia de entornos de Seguridad Operacional, en donde variables como el clima, van más allá del control del factor humano. Gestionar el cambio AVSEC no solamente es identificar amenazas, medir impactos o establecer niveles de riesgo, su alcance va mucho más allá, es educar al personal, prepararlo para lo que viene, motivarlo para que siga el proceso del cambio de tal manera que este convencido de los beneficios del mismo. Los seres humanos estamos biológicamente predispuestos a resistir el cambio, nuestro cerebro está diseñado para formar hábitos y conservar la energía cognitiva, así como la preferencia natural del ser humano por mantener el estatus quo, representan los principales desafíos a vencer en el proceso de Gestión del Cambio. Introducir cambios desencadena en el ser humano una respuesta de luchar o huir, exactamente lo mismo sucede con las organizaciones. La mejor estrategia para hacer frente a una Gestión del Cambio en términos de AVSEC, es preparar, apoyar y guiar a las personas a través del cambio e influir en su comportamiento, permitir a las organizaciones aprovechar los beneficios de una transición o transformación organizacional y ayudar a minimizar la interrupción de las actividades habituales y el riesgo de consecuencias inesperadas.

El enfoque ADKAR de Prosci aplicado en AVSEC Prosci considera un enfoque centrado en las personas que guía a los individuos a través del cambio utilizando cinco bloques de construcción: Conciencia, Deseo, Conocimiento, Habilidad y Refuerzo.

La Gestión del Cambio comienza con el Enfoque de Preparación a través de una estrategia que incluye cambiar la visión del personal involucrado, mapear las partes interesadas, evaluar el impacto y elaborar un plan de recursos para el cambio. El proceso involucra la elaboración de una Hoja de Ruta, establecer una estrategia de comunicación y participación de las partes interesadas y adoptar un enfoque de capacitación y concientización del conocimiento. Posterior al cambio, el proceso de gestión continúa a través de reforzamiento, que consiste en establecer métricas de éxito y la comunicación de historias de éxito a las partes interesadas.

La gran dependencia del factor humano en AVSEC, obliga a trabajar previamente con el personal involucrado, de otra manera la Gestión del Cambio será muy complicada, Nuestro proceso de gestión debe estar principalmente enfocado en la concientización, capacitación y desarrollo de competencias del personal, para lo cual, el liderazgo juega un papel fundamental. El mejor ejemplo lo tenemos con los atentados del 11 de Septiembre de 2001, posterior a estos eventos, se crea la Transportation Security Administration (TSA) de los Estados Unidos y con ella vinieron cambios disruptivos en materia de Seguridad de la Aviación Civil, que llevaron años en su implementación (por ejemplo, la inspección del 100% de carga hacia ese país tomó a la industria 10 años) y mucho pero mucho dinero en inversión, pero sobre todo, un gran cambio cultural que no estaba previsto o al menos, no a tan corto plazo y que simple y sencillamente las aerolíneas que quisieran operar o los pasajeros que quisieran o necesitaran viajar a ese país, tendrían que adaptarse a esa nuevas reglas del juego, la curva de aprendizaje fue dolorosa, el costo no únicamente en inversiones de equipos e infraestructuras, sino también en tiempo invertido en pruebas de ensayo y error, instrucción, capacitación y definición de nuevos perfiles de personal de seguridad fue muy alto.

Por el contrario, uno de los proyectos que me tocó liderar, fue la implementación de una Enmienda de Emergencia de la TSA, en donde se exigió la entrevista previa el check-in a todos los pasajeros con destino a los Estados Unidos, un proceso que impactaría los flujos y tiempo de procesamiento de pasajeros. En aquella ocasión, desde 4 meses de antelación sostuvimos reuniones frecuentes con las diversas áreas involucradas, entre ellas, servicio al cliente, legal, operaciones, comunicación corporativa, aeropuertos y evidentemente autoridades diversas. El proyecto se llevó a cabo casi al 100% como fue planeado, las afectaciones a la operación y a los pasajeros fueron mínimas (menores al 0.05%), se efectuaron pruebas piloto antes del arranque y el resultado fue tal que, nuestro proceso sirvió de modelo para otras líneas aéreas e inclusive para que la TSA modificara algunos puntos de la Enmienda derivados de nuestras pruebas piloto. Nada de lo anterior hubiera sido posible sin el factor humano, el haber trabajado previamente con cada una de las personas involucradas en todos los niveles, fue clave del éxito, y se evitó un derroche de recursos, afectaciones operativas, sanciones por incumplimiento y lo más importante…quejas y molestia de pasajeros inconformes por tales medidas, lo que si sucedió con otras aerolíneas, lo anterior gracias a una adecuada Gestión del Cambio.

Expertos estiman que, con una excelente Gestión del Cambio, se tiene seis veces más probabilidad de alcanzar los objetivos, luego entonces, la Gestión del Cambio es la disciplina que aborda el lado humano del cambio, permitiendo que las personas se involucren, adopten y usen la solución. En conclusión… la Gestión del Cambio en AVSEC, siempre debe iniciar con el factor humano y es éste, quien hace que la transición de un estado presente a un estado futuro deseado, se lleve de manera exitosa. Me despido con mi máxima de siempre… En Seguridad de la Aviación Civil, el primer error es el último.

Alineamiento estratégico y de liderazgo Asegurar que los líderes y las partes interesadas clave, estén alineados en cuanto a visión, prioridades y roles durante toda la transformación.	**Gestión de riesgos e impactos para el personal** Identificar y mitigar los riesgos para las personas, la moral y la productividad durante la transformación	**Involucramiento y comunicación con las partes interesadas** Entregar mensajes claros, consistentes y oportunos para generar comprensión, confianza y aceptación	**Aprendizaje y desarrollo de capacidades** Dotar a los empleados de las habilidades, conocimientos y herramientas necesarios para tener éxito en el nuevo entorno
Cambios culturales y conductuales Definir y reforzar las mentalidades, los valores y los comportamientos necesarios para sostener el cambio	**Diseño y gobernanza de la organización** Estructuración de equipos, roles y procesos de toma de decisiones para apoyar el nuevo modelo operativo	**Transición de la fuerza laboral** Gestionar los cambios de rol, las reasignaciones y la preparación de los empleados a través de planes de transición estructurados	**Estrategia de talento y programas de recursos humanos** Alinear los programas de adquisición, desempeño, recompensas y desarrollo de talento con las metas de transformación

CUANDO CUMPLIR NO SIGNIFICA PROTEGER Y LA SEGURIDAD NECESITA DEMOSTRAR SU EFECTIVIDAD

Metro Risk

Edición propiedad de @MetroRisk, asociación

Edison Cadena Ayala
Presidente AIMCSE Ecuador

“No se puede gestionar lo que no se puede medir.” — Peter Drucker (frase ampliamente atribuida al autor, aunque no existe evidencia concluyente de que la formulara literalmente en estos términos).

Durante años uno de nuestros objetivos ha sido el demostrar que la seguridad existe. Mostramos cámaras instaladas, procedimientos aprobados, controles de acceso funcionando, personal capacitado, auditorías cumplidas e indicadores que, siendo nuestra meta que estos aparezcan y más que ello que permanezcan en verde, dando esta apariencia que llegue a confirmar que todo marcha correctamente. Sin embargo, pocas veces nos detenemos frente a una pregunta mucho más incómoda: ¿qué evidencia tenemos de que todo aquello realmente está produciendo protección?

La diferencia no es menor. Una cámara operativa demuestra disponibilidad tecnológica, pero no necesariamente capacidad de detección. Una persona que asistió a una capacitación demuestra cumplimiento de un programa, pero no necesariamente competencia para actuar correctamente bajo presión. Una barrera construida conforme a especificaciones puede cumplir técnicamente su diseño y, sin embargo, no generar la demora suficiente para que detección y respuesta impidan que un adversario alcance el activo.

Cumplir importa. Sería un error minimizar el valor de la conformidad, los procedimientos o los indicadores. El problema comienza cuando confundimos cumplimiento con efectividad. La gestión del riesgo planteada por ISO 31000 no termina con la implementación de un tratamiento; incorpora seguimiento, revisión y mejora como elementos necesarios del proceso (International Organization for Standardization [ISO], 2018). Desde otra perspectiva, el enfoque Enterprise Security Risk Management propone vincular las decisiones de seguridad con los activos, objetivos organizacionales, tolerancia al riesgo y evaluación de las medidas adoptadas (ASIS International, 2019). NIST profundiza esta lógica al diferenciar la implementación de un control de la evaluación de su efectividad y establecer procedimientos destinados precisamente a obtener evidencia sobre su funcionamiento (National Institute of Standards and Technology [NIST], 2022).

Figura 1. Cadena de efectividad de la seguridad

La seguridad madura demuestra qué capacidad de protección producen sus controles y cómo contribuyen al tratamiento del riesgo.

Nota: Esta figura integra principios de gestión del riesgo y evaluación de controles de ISO 31000, ESRM (ASIS International) y NIST SP 800-53A Rev. 5. Elaboración propia.

Esto obliga a cambiar nuestra manera de mirar la seguridad. No basta preguntar qué controles tenemos. Necesitamos determinar qué capacidad deben producir, en qué condiciones deben hacerlo y qué evidencia permite comprobarlo. Allí aparece una secuencia que considero útil para evaluar la madurez de nuestros sistemas de protección: riesgo, control, capacidad, criterio de desempeño, evidencia, efectividad y riesgo residual. No pretende constituirse en un nuevo estándar, sino ordenar una pregunta que con frecuencia dejamos pendiente después de implementar un control: ¿funcionó realmente para aquello que fue diseñado? Pensemos nuevamente en una barrera perimetral. Saber que existe, que cumple especificaciones y que se encuentra en buenas condiciones es importante. Pero si su propósito es retrasar una intrusión, necesitamos conocer si la demora generada permite detectar, evaluar y responder antes de que el adversario alcance su objetivo.

En ese momento dejamos de medir solamente presencia y comenzamos a evaluar capacidad. Lo mismo ocurre con la tecnología, las personas y los procedimientos. Esta mirada también modifica el sentido de nuestros indicadores. El número de rondas efectuadas, cámaras disponibles, capacitaciones realizadas o procedimientos actualizados continúa aportando información necesaria; pero principalmente describe actividad, disponibilidad o cumplimiento. Una organización madura necesita avanzar hacia indicadores capaces de aportar evidencia sobre desempeño y efectividad. Quizá uno de los mayores desafíos de la seguridad contemporánea sea precisamente este: dejar de sentirnos protegidos porque podemos demostrar todo lo que tenemos y comenzar a preguntarnos cuánto de aquello que tenemos realmente funciona cuando lo necesitamos. Porque, al final, la seguridad no adquiere valor por la cantidad de controles que podemos mostrar, sino por la capacidad de protección que somos capaces de demostrar.

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

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

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

Colaboramos con MR-CONSULTING.

Asesoramiento Técnico Especializado, para Situaciones legales y Técnicas:
En el Ámbito de la:

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

www.oterotrillogabinetepericial-andaluciaceuta.es/

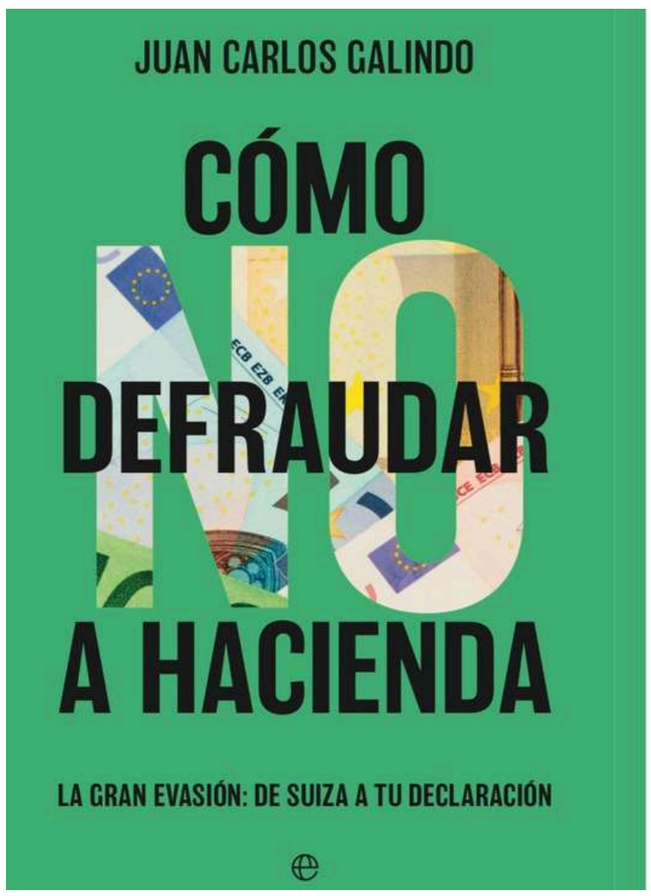
AGENDA

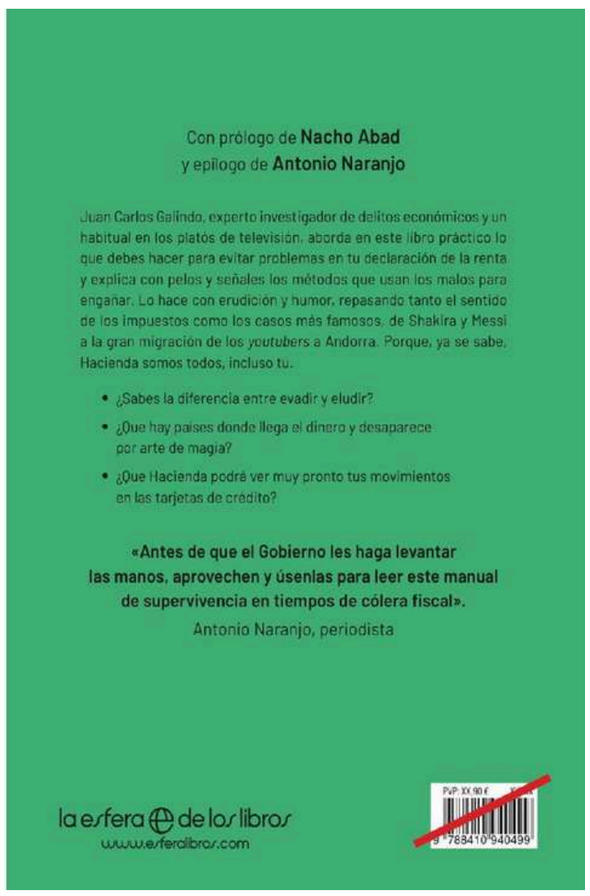
Metro Risk

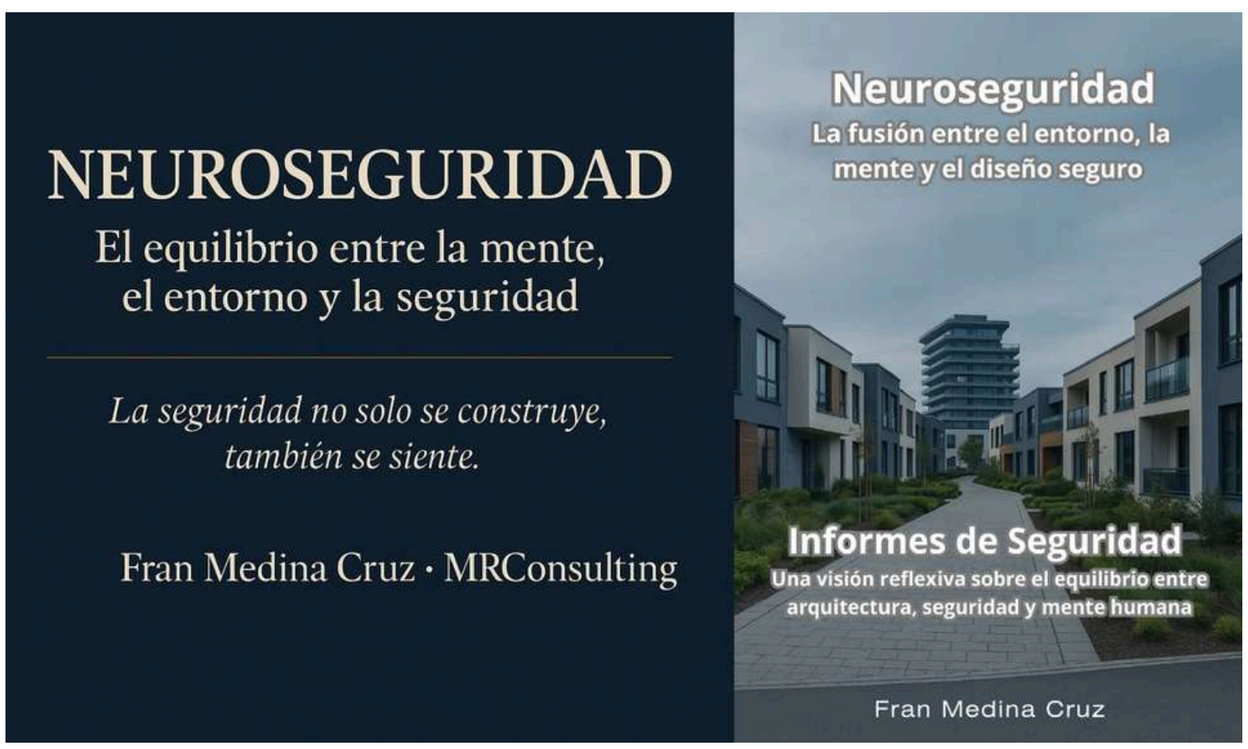
Edición propiedad de @MetroRisk, asociación

RADIO

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







Metrorisk

Proyecto Asociativo

www.metrorisk.es