

EDITORIAL MR

MAYO

AÑO
2025



ISSN 3045-7629

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz
Gregorio Duro
Emilio Piñeiro
Abraham Santana
Jonatthan Hermida

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

Rosa Fernández
Elena de la Parte

José Ignacio Olmos
Antonio Cozano Fernández
Carlos Serrano
Carlos Miguel Ortiz

@Metrorisk.es

ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

Presidente:

D. Francisco Medina cruz

Vicepresidente Económico:

D. Abraham Santana Herrera

Vicepresidente Relaciones Institucionales:

D. Juan Carlos Galindo

Secretario General:

D. Emilio Piñeiro

Vocal Comunicación:

Dña. Elena González de la Parte

Vocal Temas Legales:

Dña. Rosa Fernández Fernández



MeTroRisk
Seguridad Patrimonial y CPTED

Editado por:

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

ISSN 3045-7629



COLABORADORES



PATROCINADO POR LAS FIRMAS



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

EL VALOR ESTRATÉGICO DEL DIRECTOR DE SEGURIDAD CONSULTOR EXTERNO.

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Fran Medina Cruz Director de MetroRisk

En un contexto global caracterizado por riesgos multidimensionales y amenazas dinámicas, contar con un profesional experto en seguridad, especialmente un director o consultor de seguridad especializado, no solo es una ventaja competitiva, sino una necesidad vital para garantizar la continuidad, tranquilidad y resiliencia tanto en el ámbito profesional como en el personal.



1. Enfoque Personalizado y Evaluación Integral del Riesgo

Uno de los principales beneficios de contratar a un experto en seguridad es la capacidad de adaptar el diagnóstico y las medidas de protección a la realidad específica de cada cliente. Esto implica:

- Evaluación de Riesgo a Medida: Análisis detallado de amenazas físicas, digitales, sociales y reputacionales que afectan a personas, familias, ejecutivos o empresas.
- Informes de Seguridad Personalizados y Discretos: Documentación estratégica elaborada con carácter confidencial, orientada a ofrecer soluciones concretas y viables sin generar alarma innecesaria.
- Consultoría Adaptativa: Servicios ajustados en tiempo real al contexto cambiante del cliente (viajes, mudanzas, eventos, conflictos, exposición pública, etc.).

2. Seguridad Integral: Profesional, Familiar y Patrimonial

El perfil de un director o asesor de seguridad profesional se orienta a una protección 360°, incluyendo:

- Entorno profesional: Gestión de riesgos corporativos, protección de la información, análisis de vulnerabilidades, evaluación de empleados y terceros.
- Entorno familiar y doméstico: Protección perimetral del hogar, hábitos cotidianos seguros, formación básica para todos los miembros de la familia, análisis de entornos escolares y sociales.
- En viajes y desplazamientos: Planificación previa, análisis geoestratégico del destino, rutas seguras, protocolos de emergencia, escoltas auditados o anónimos según el nivel de riesgo.

3. Asesoramiento Continuo y Acompañamiento Directivo

El profesional de seguridad no actúa como un mero prestador de servicios ocasional, sino como un acompañante estratégico y continuo, lo cual aporta:

- Prevención proactiva: Anticipación a incidentes mediante la monitorización discreta de señales de alerta.
- Intervención inmediata: Capacidad de reacción coordinada ante cualquier incidente detectado, gracias a protocolos previamente diseñados.
- Actualización constante: Adaptación a nuevas amenazas (ciberdelitos, stalking, hackeo de redes domésticas, ingeniería social)



4. Vigilancia Auditada y Protocolos Éticos

Una diferencia esencial de un experto verdaderamente profesional radica en que su vigilancia no solo es eficiente, sino auditada y ética, mediante:

- Sistemas de supervisión interna: Seguimiento transparente del desempeño de escoltas, equipos técnicos, o personal auxiliar.
- Cumplimiento legal y normativo: Garantía de que todas las medidas aplicadas cumplen con las normativas locales e internacionales de privacidad, protección de datos y derechos fundamentales.
- Confidencialidad estricta: Manejo seguro y reservado de toda la información sensible del cliente.

5. Imagen, Tranquilidad y Control

Contratar a un consultor o director de seguridad profesional también aporta un beneficio intangible pero fundamental:

- Tranquilidad psicológica: Saber que uno está protegido por un sistema diseñado para su perfil y que evoluciona con él.
- Control situacional: Acceso inmediato a información clave para la toma de decisiones ante amenazas o dudas.
- Refuerzo de la imagen profesional y personal: Discreción y eficacia que transmiten seguridad sin generar sensación de vigilancia excesiva o invasión





Los Estudios de Seguridad implementan matrices que ayudan a mantener la continuidad del negocio de manera estable y saludable. ¡Con ello, las organizaciones se empoderan para cumplir con sus compromisos de evitar riesgos y fortalecer la protección en múltiples ámbitos. ¡Las soluciones que brindamos como profesionales del sector, llevan la marca y el estilo del buen hacer de años de experiencia y de investigación.

Fran Medina Cruz. Consultor



**El futuro del
Director de Seguridad**

MRCONSULTING

¿Contratar a un consultor como Director de Seguridad externo?

Si, para gestionar y auditar los procesos de seguridad de su empresa, la cual posee de un servicio de seguridad ejerciendo la vigilancia de su bien. Implica un mejor control, seguimiento y efectividad en su seguridad. Ya que las partes no entran en conflicto de intereses al no estar relacionada empresa de seguridad y consultor

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

EL DIRECTOR DE SEGURIDAD: PILAR ESTRATÉGICO EN LAS ORGANIZACIONES MODERNAS

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

En un mundo cada vez más complejo, interconectado y expuesto a riesgos de diversa índole, el Director de Seguridad ha dejado de ser un mero gestor de incidentes para convertirse en un agente estratégico indispensable dentro de las organizaciones. La seguridad ya no se concibe únicamente como una función reactiva frente a amenazas tangibles. Hoy, la seguridad integral abarca la protección de las personas, los activos, la información y la reputación, configurándose como un elemento clave para garantizar la continuidad de negocio, el cumplimiento normativo y la sostenibilidad operativa.



En este contexto, el Director de Seguridad ocupa un rol transversal, que conecta áreas como el compliance, la gestión de riesgos, la ciberseguridad, la protección de infraestructuras críticas, la inteligencia corporativa y la resiliencia organizacional.

¿Por qué es fundamental la figura del Director de Seguridad?

- 1. Anticipación y prevención de riesgos: El Director de Seguridad identifica amenazas emergentes y vulnerabilidades internas, permitiendo a la organización adelantarse a escenarios de crisis y adoptar medidas de prevención eficaces.
- 2. Protección del capital humano: Más allá de proteger infraestructuras o activos materiales, su misión primordial es salvaguardar la vida y el bienestar de las personas, garantizando entornos de trabajo seguros y saludables.
- 3. Aseguramiento de la continuidad del negocio: Diseña e implementa planes de contingencia y recuperación ante incidentes, asegurando que la actividad empresarial pueda continuar aun en circunstancias adversas.
- 4. Cumplimiento normativo y reputacional: Ayuda a la organización a cumplir con las normativas locales e internacionales en materia de seguridad y protección de datos, contribuyendo a preservar la reputación corporativa, uno de los activos más valiosos en la actualidad.
- 5. Apoyo a la toma de decisiones estratégicas: Contribuye con información fiable y análisis de riesgos al proceso de toma de decisiones de la alta dirección, reforzando la gobernanza corporativa.

La evolución hacia un liderazgo estratégico

El perfil del Director de Seguridad contemporáneo es el de un profesional altamente cualificado, con visión global, capacidad analítica, habilidades de comunicación y, sobre todo, un profundo sentido ético y de responsabilidad. En **ADISPO** trabajamos cada día para reivindicar y fortalecer esta figura, fomentando su profesionalización, su reconocimiento institucional y su papel como interlocutor imprescindible entre el sector privado, la administración pública y la sociedad.

La seguridad no es un coste: es una inversión estratégica que protege el valor, impulsa la competitividad y refuerza la confianza de clientes, inversores y empleados.

En un entorno donde los riesgos evolucionan a la velocidad de la tecnología y los cambios sociales, el Director de Seguridad seguirá siendo —más que nunca— el guardian estratégico de las organizaciones. Desde **ADISPO**, invitamos a todas las entidades a reconocer y potenciar el papel de sus Directores de Seguridad como socios estratégicos para construir entornos más seguros, resilientes y sostenibles.

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



José Ignacio Olmos Casado
Presidente AEAS

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@auditoressseguridad.es*



CARTA DEL PRESIDENTE

La **Asociación Española de Auditores de Seguridad (AEAS)** viene a llenar un hueco en el ámbito de la seguridad necesario en el momento actual de madurez del sector.

La esencia de **AEAS** es aglutinar en el seno de la Asociación a los profesionales del ámbito de la consultoría de seguridad, para la mejor defensa de sus intereses y dar la relevancia que merece a todo el colectivo, con presencia en los principales foros y eventos del sector.

Al mismo tiempo, en un mercado donde cada vez se tiende más a la externalización de funciones y al trabajo por proyectos queremos que el hecho de pertenecer como asociado a nuestra Asociación sea sinónimo de calidad contrastada tanto a la hora de que las compañías seleccionen profesionales adecuados a sus objetivos como para el prestigio y reputación profesional de los consultores integrados en **AEAS**, por eso los criterios restrictivos de integración en la misma, ya que pretendemos tener socios de absoluta solvencia profesional y no ser masivos en detrimento de esa calidad.

No podemos olvidarnos que hoy día se imponen los modelos tendentes a la normalización, donde el certificarse en normas es garantía de cumplir un estándar; cobra aquí especial importancia en todas las fases del proceso la figura del auditor, por lo que el contar con personal con una formación adecuada y una experiencia contrastada hace necesaria una promoción adecuada de estos profesionales.

Pero no sólo debemos trabajar en el ámbito externo, sino también en el interno, de manera que la Asociación se constituya como un lugar de encuentro, debate y propuestas de futuro para los profesionales de la auditoría y consultoría.

Es por ello por lo que os animo a todos a impulsar la asociación con vuestra colaboración y vuestras ideas.

Asociación Española de Auditores de Seguridad



AEAS

Asociación Española de
Auditores de Seguridad

SECCIÓN ESTUDIOS TÉCNICOS

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Gregorio Duro
Técnico en licitaciones y Proyectos

LA DESIGUALDAD DE LA INCERTIDUMBRE EN EL PROCESO DE ANÁLISIS DE RIESGOS

En el artículo de este mes, me gustaría tratar el concepto de desigualdad de la incertidumbre en el proceso de cálculo realizado para un análisis de riesgos. En este contexto, la desigualdad de la incertidumbre se refiere a las diferencias o disparidades en la forma en que la incertidumbre impacta los resultados o las posibles consecuencias de un evento, dadas las diferentes distribuciones de probabilidad o niveles de variabilidad en los factores estimados.



La desigualdad de la incertidumbre se puede entender como una medida que refleja cómo de dispersos o distribuidos están los resultados de un proceso incierto, dependiendo de las probabilidades asociadas a las variables involucradas. En otras palabras, mide la diferencia en la magnitud de la incertidumbre que se experimenta en diversas situaciones o escenarios dentro de un análisis de riesgos. En el proceso de análisis de riesgos, no todas las incertidumbres afectan a los resultados de manera uniforme. Algunas variables pueden tener un impacto mucho mayor en los resultados que otras, y algunas distribuciones de probabilidad pueden ser más "anchas" o "estrechas", lo que implica una mayor o menor incertidumbre en el resultado.

En un análisis de riesgos, la dispersión de resultados se refiere a la variabilidad de los factores inciertos, donde una mayor dispersión indica mayor incertidumbre sobre los resultados, y una menor dispersión sugiere menor incertidumbre. No todas las fuentes de incertidumbre tienen el mismo impacto en los resultados, ya que algunas variables pueden generar importantes fluctuaciones, mientras que otras tienen un efecto constante y pequeño, lo que implica una distribución desigual de la incertidumbre. Esta desigualdad puede medirse a través de métricas estadísticas como el coeficiente de variación, que relaciona la desviación estándar con la media, la entropía, que mide la incertidumbre en una distribución, o el índice de Gini, que evalúa la desigualdad en los resultados.

El enfoque de la desigualdad de la incertidumbre en el análisis de riesgos parte de la premisa de que no toda la incertidumbre presente en un sistema tiene el mismo peso ni se distribuye de manera equitativa en los diferentes factores que intervienen en el proceso de evaluación del riesgo. En este sentido, algunas fuentes de incertidumbre pueden ser más dominantes o impactantes que otras, generando un efecto desproporcionado sobre los resultados del análisis y, por lo tanto, sobre la toma de decisiones respecto a las medidas de mitigación. En lugar de tratar la incertidumbre como un elemento uniforme o homogéneo, es importante identificar y clasificar aquellas incertidumbres que tienen un mayor potencial de afectar la precisión y fiabilidad en un análisis de riesgos. Para ello, se emplean metodologías como el análisis de sensibilidad, la modelización estocástica y la simulación de escenarios, que permiten determinar cuáles son las variables más críticas dentro del sistema evaluado y qué nivel de incertidumbre presentan. Este enfoque reconoce que, en muchos casos, la reducción de toda la incertidumbre no es factible ni económicamente viable, por lo que se deben priorizar esfuerzos en aquellas áreas donde una disminución de la incertidumbre puede generar el mayor beneficio en términos de precisión en la evaluación de riesgos y mejora en la gestión de estos. Un ejemplo claro de esta desigualdad de la incertidumbre se observa en el ámbito financiero, donde factores como la volatilidad del mercado tienen una incertidumbre mucho más significativa que otros elementos con comportamientos más predecibles, lo que obliga a los analistas a centrar su atención en estos factores de alto impacto.

De manera similar, en el contexto de la gestión de desastres naturales, la incertidumbre sobre la ocurrencia de eventos extremos, como terremotos o huracanes, suele ser mucho mayor que la incertidumbre sobre sus efectos directos en infraestructuras específicas, lo que hace que la planificación y asignación de recursos deba enfocarse en comprender y reducir, en la medida de lo posible, la incertidumbre sobre la probabilidad de ocurrencia de estos eventos. En seguridad industrial, por ejemplo, la identificación de puntos críticos de falla con alta incertidumbre permite diseñar sistemas de control más robustos y eficientes, evitando que pequeñas incertidumbres acumuladas en aspectos clave del sistema deriven en eventos catastróficos.



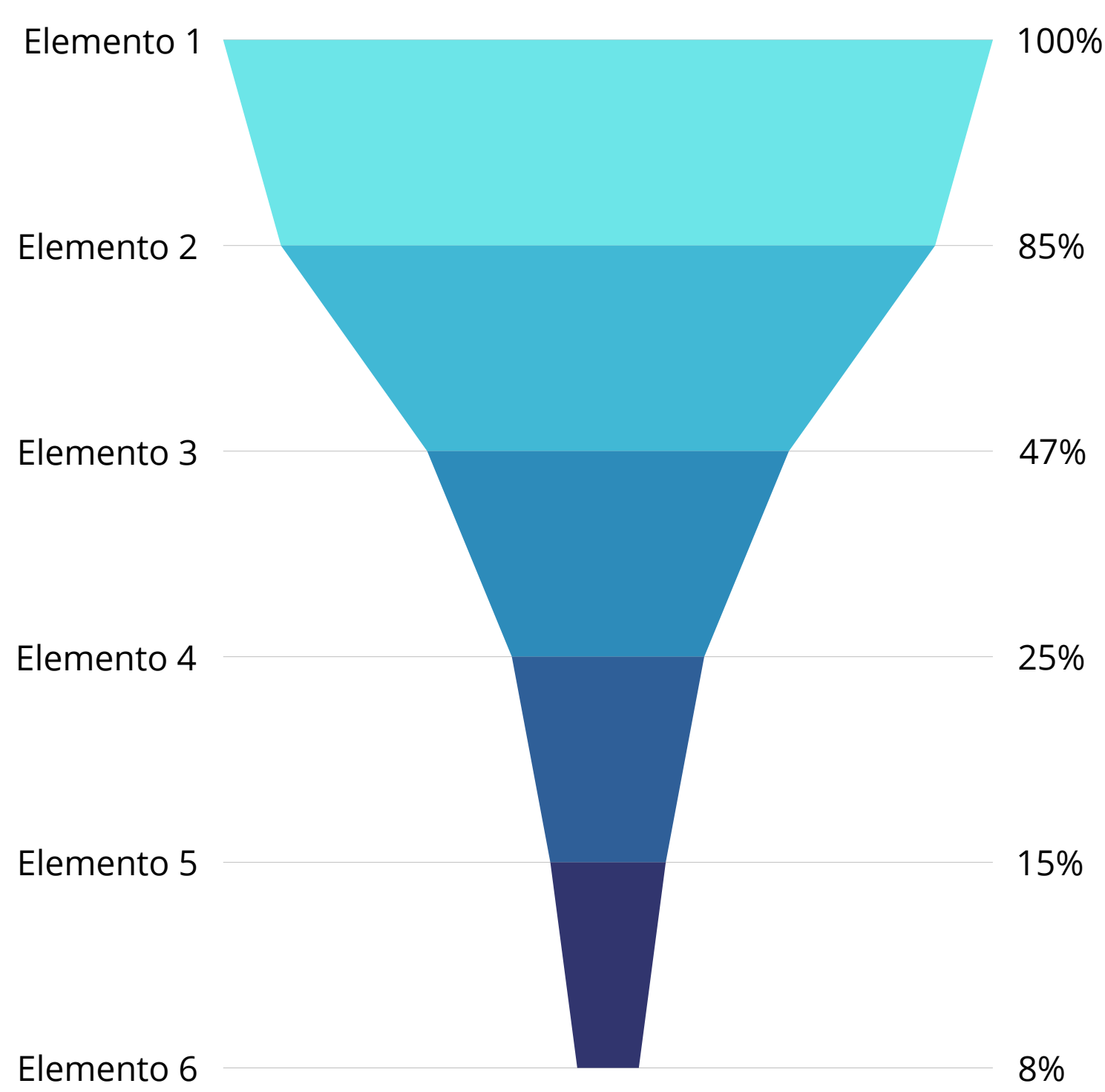


Así, el enfoque de la desigualdad de la incertidumbre en los procesos de análisis de riesgos no solo ayuda a optimizar la asignación de recursos y la efectividad de las estrategias de mitigación, sino que también permite desarrollar una toma de decisiones más rápida y eficiente, basada en la identificación y priorización de aquellas incertidumbres que representan la mayor amenaza para la precisión del análisis y la efectividad de las acciones preventivas. En el entorno de un proceso de análisis de riesgos, comprender la desigualdad de la incertidumbre es fundamental porque permite identificar las variables o factores que generan mayor incertidumbre en el desarrollo del modelo de cálculo, evaluar la resiliencia del sistema ante cambios inciertos, ya que la incertidumbre desigual puede hacer que algunas áreas sean más vulnerables a ciertos riesgos, y tomar decisiones consecuentes, ajustando las estrategias para mitigar los riesgos más significativos o inciertos. De este modo, la desigualdad de la incertidumbre no solo ayuda a entender el comportamiento incierto del sistema, sino que también permite diseñar intervenciones más precisas y eficientes, mejorando la fiabilidad y la efectividad en la gestión del riesgo.

La aplicación del concepto de desigualdad de la incertidumbre en el ámbito de un proceso de análisis de riesgos conlleva múltiples conclusiones fundamentales que influyen en la manera en que se identifican, evalúan y gestionan los riesgos dentro de cualquier sistema, ya sea en el ámbito financiero, industrial, medioambiental o de seguridad. En primer lugar, se confirma que la incertidumbre no es uniforme ni afecta a todas las variables previstas para un proceso de análisis de riesgos de la misma manera, lo que obliga a priorizar aquellas incertidumbres que tienen un impacto desproporcionado en la precisión y fiabilidad de las evaluaciones. Esta conclusión lleva a la necesidad de aplicar técnicas avanzadas de análisis de sensibilidad y modelización probabilística para detectar qué variables críticas presentan la mayor incertidumbre y, por lo tanto, requieren una atención especial en la gestión del riesgo. Como resultado, se optimiza la asignación de recursos, ya que no se desperdicia tiempo ni esfuerzo en tratar de reducir incertidumbres marginales o con escaso impacto, sino que se focalizan los esfuerzos en aquellas que verdaderamente pueden alterar las decisiones estratégicas.

Otro aspecto clave derivado de este enfoque es que, al aceptar la desigualdad de la incertidumbre como una característica intrínseca de los sistemas complejos, se refuerza la importancia de desarrollar estrategias de mitigación que sean dinámicas y adaptativas, permitiendo a los departamentos de seguridad ajustar sus respuestas a medida que se obtiene nueva información y se reducen las incertidumbres más significativas. Finalmente, la desigualdad de la incertidumbre también crea la necesidad de integrar múltiples enfoques en la gestión herramientas del riesgo, cuantitativas combinando con juicios cualitativos basados en la experiencia y en la información contextual, lo que contribuye a un proceso de toma de decisiones más robusto y alineado con las limitaciones del conocimiento disponible. Quiero expresar mi agradecimiento a Metrorisk por compartir mensualmente artículos de carácter técnico que contribuyen al crecimiento y mejora del conocimiento en nuestro sector.

Gregorio Duro Navarro
Técnico de Licitaciones y Proyecto



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

LA CONVERGENCIA ESTRATÉGICA: RESPONSABILIDAD SOCIAL EMPRESARIAL Y PROYECTOS BAJO LAS NORMAS ISO CPTED

En un mundo cada vez más consciente de la interconexión entre el éxito empresarial y el bienestar social, la Responsabilidad Social Empresarial (RSE) ha trascendido de la filantropía para integrarse como un pilar estratégico de las organizaciones. Paralelamente, la Prevención del Delito a Través del Diseño Ambiental (CPTED) ha demostrado su eficacia en la creación de entornos más seguros, sociales, incluyentes y habitables. Las Normas ISO CPTED emergen como un marco valioso para articular la implementación de proyectos utilizando esta Metodología dentro de una estrategia de RSE, generando un impacto positivo tanto para las empresas como para las comunidades.

La RSE impulsa a las empresas a ir más allá de sus obligaciones legales y a considerar el impacto de sus actividades en diversos grupos de interés, incluyendo la comunidad donde operan. La seguridad y el bienestar de esta comunidad son elementos intrínsecos a la RSE. Al adoptar proyectos CPTED, las empresas demuestran un compromiso tangible con la mejora de la calidad de vida, la reducción de la delincuencia y la promoción de entornos seguros, lo que se alinea directamente con los principios de la RSE.

Beneficios de la RSE Impulsando CPTED:

- Legitimidad y Reputación: involucrarse en proyectos CPTED mejora la imagen pública y la reputación de la empresa, fortaleciendo la confianza de los clientes, inversores y la comunidad en general.
- Licencia Social para Operar: al contribuir a la seguridad y el bienestar de la comunidad, las empresas construyen una licencia social más sólida para operar, facilitando sus actividades y minimizando potenciales conflictos.
- Atracción y Retención de Talento: los empleados valoran trabajar para empresas con un fuerte compromiso social. Proyectos CPTED pueden hacer que la empresa sea percibida como un actor positivo en la comunidad, atrayendo y reteniendo talento.
- Reducción de Costos a Largo Plazo: un entorno más seguro puede reducir los costos asociados al vandalismo, el robo y la inseguridad, beneficiando tanto a la empresa como a la comunidad.
- Innovación y Nuevas Oportunidades: la implementación de proyectos CPTED puede estimular la innovación en el diseño urbano, la tecnología de seguridad y la colaboración comunitaria, abriendo nuevas oportunidades de negocio.



Las Normas ISO CPTED proporcionan directrices para establecer, implementar, mantener y mejorar la seguridad y la resiliencia de las ciudades. Si bien no se enfoca exclusivamente en CPTED, sus principios y recomendaciones son altamente relevantes para la implementación de proyectos dentro de una estrategia de RSE. La norma enfatiza la importancia de:

- Comprensión del Contexto: analizar las necesidades y los desafíos específicos de seguridad de la comunidad donde opera la empresa.
- Participación de las Partes Interesadas: involucrar a la comunidad, las autoridades locales y otras partes interesadas en la identificación de problemas de seguridad y el diseño de soluciones CPTED.
- Planificación y Diseño: incorporar los principios de CPTED en la planificación y el diseño de espacios públicos, infraestructuras y entornos construidos.
- Implementación y Operación: ejecutar los proyectos de manera efectiva, asegurando el mantenimiento y la sostenibilidad de las soluciones implementadas.
- Seguimiento y Evaluación: monitorear el impacto de los proyectos en la reducción del delito y la mejora de la seguridad, utilizando indicadores clave de desempeño.
- Mejora Continua: adaptar y mejorar las estrategias en función de los resultados del seguimiento y la retroalimentación de la comunidad.





Las empresas pueden integrar la RSE y los proyectos CPTED bajo el paraguas de las Normas ISO 22341 y 22344 CPTED siguiendo estos pasos:

1. Identificar las Necesidades de Seguridad de la Comunidad: a través de estudios, consultas y la participación de las partes interesadas, la empresa puede identificar las áreas donde los principios de CPTED pueden tener un mayor impacto en la mejora de la seguridad.
2. Seleccionar Proyectos CPTED Estratégicos: elegir proyectos que se alineen con los objetivos de RSE de la empresa y que tengan un potencial significativo para generar un impacto positivo en la comunidad. Esto podría incluir la mejora de la iluminación pública en zonas de alta criminalidad, el diseño de parques más seguros y accesibles, o la implementación de sistemas de vigilancia comunitaria.
3. Colaborar con las Partes Interesadas: trabajar en estrecha colaboración con las autoridades locales, las organizaciones comunitarias y los propios residentes en el diseño e implementación de los proyectos CPTED.
4. Implementar Soluciones CPTED Sostenibles: asegurar que las soluciones implementadas sean duraderas, mantenibles y respetuosas con el medio ambiente, contribuyendo a la sostenibilidad a largo plazo.
5. Comunicar el Impacto de la RSE a través de CPTED: informar de manera transparente a las partes interesadas sobre los proyectos CPTED implementados y su impacto en la mejora de la seguridad y el bienestar de la comunidad, destacando el compromiso de la empresa con la RSE.
6. Evaluar y Mejorar Continuatamente: utilizar los marcos de seguimiento y evaluación del Ciclo Deming para medir la efectividad de los proyectos CPTED y realizar ajustes para maximizar su impacto, tal como lo piden las normas ISO CPTED.



La convergencia entre la Responsabilidad Social Empresarial y los proyectos de Prevención del Delito a Través del Diseño Ambiental, guiada por los principios de las Normas ISO CPTED, representa una oportunidad estratégica para que las empresas generen valor compartido.

Al invertir en la seguridad y el bienestar de las comunidades donde operan las empresas, no solo cumplen con sus responsabilidades sociales, sino que también fortalecen su reputación, construyen relaciones sólidas y contribuyen a la creación de entornos más seguros y resilientes para todos.

La adopción de un enfoque integrado y estratégico, respaldado por un marco normativo adecuado como lo son las Normas ISO 22341 y 22344, puede transformar la manera en que las empresas interactúan con sus comunidades, generando un impacto positivo y sostenible a largo plazo. Una Empresa Socialmente Responsable ve en CPTED la llave para desbloquear comunidades seguras y habitables, construyendo un legado de bienestar que trasciende el presente.

GOBERNANZA PARTICIPATIVA & CPTED



LA SEGURIDAD INTEGRAL EN URBANIZACIONES: UNA NECESIDAD ESTRATÉGICA, NO UNA OPCIÓN

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Antonio Cozano Fernández
CEO Cofer Seguridad.

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

D. Antonio Cozano Fernández



**COFER**
SEGURIDAD

TEL: 952 409 846

¿Y SI LO ÚNICO QUE QUIERES
ES DORMIR TRANQUILO?

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



Active su sistema
de seguridad en
un clic

29,95 € mes+IVA*

En un contexto de creciente complejidad urbana y amenazas cada vez más diversificadas, las urbanizaciones residenciales especialmente de alto valor, se han convertido en objetivos sensibles para la delincuencia organizada, ocupaciones ilegales, actos vandálicos y amenazas a la convivencia. Frente a este escenario, la seguridad no puede dejarse en manos de soluciones improvisadas o parciales. La respuesta debe ser integral, profesional y multidisciplinar. Contar con empresas expertas en seguridad de urbanizaciones se convierte en una necesidad estructural para garantizar la protección efectiva de residentes, bienes y entornos.

¿Por qué una empresa especializada?

Las urbanizaciones presentan un conjunto de particularidades que exigen un enfoque específico:

- Entradas múltiples y control de accesos complejos.
- Convivencia entre privacidad y espacios comunes.
- Necesidad de respuesta rápida y protocolos claros ante incidentes.
- Integración de sistemas humanos y tecnológicos de vigilancia.

Solo una empresa experta puede diseñar e implementar un sistema de seguridad que abarque:

- Seguridad humana profesionalizada, adaptada al entorno residencial.
- Tecnología de última generación: CCTV con análisis inteligente, sensores perimetrales, control de accesos, vigilancia mediante drones o sistemas LPR.
- Protocolos de actuación, planes de emergencia y formación continua a la comunidad.
- Evaluación CPTED (Prevención del delito mediante el diseño ambiental), para mejorar la seguridad desde el urbanismo.

Información general
info@coferseguridad.com
952 409 846



DE DARWIN A LA IA: EVOLUCIÓN, ENTORNOS VUCA-BANI

Metro
Risk

Edición propiedad de @MetroRisk, asociación

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

...y el Nuevo Paradigma del Compliance y Liderazgo

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

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

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

En este mundo BANI, la adaptación reactiva deja de ser suficiente. Las organizaciones necesitan anticiparse, cuestionar modelos de negocio tradicionales y, sobre todo, cultivar la resiliencia para responder con rapidez y criterio a las disrupciones constantes.



La IA como acelerador de la evolución empresarial

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

Un nuevo enfoque de compliance: de norma a ecosistema vivo

El cumplimiento normativo ha pasado de ser una lista de requisitos legales a un ecosistema vivo que conecta regulación, ética, tecnología, estrategia y liderazgo. El viejo enfoque de compliance se limitaba a “evitar multas” o “reducir riesgos legales”. En cambio, el compliance del futuro: □ Se anticipa a los riesgos: La evolución de las normas y la rápida obsolescencia de los modelos obliga a que la supervisión sea continua, no anual. □ Integra la IA: Los algoritmos ayudan a monitorizar procesos con una precisión y alcance imposibles para un equipo humano. Pero siempre con supervisión final de personas. □ Fomenta la cultura de la transparencia: Más que imponer reglas, se trata de construir un contexto donde cada miembro de la organización asuma la integridad como valor esencial. Lejos de ser un “costo”, el compliance se convierte en ventaja competitiva, pues inspira la confianza de inversores, clientes y colaboradores, tan necesaria en un entorno cada vez más volátil y desconfiado.



Emilio Piñeiro
Consultor de cumplimiento normativo,
Compliance Officer, Docente y Divulgador

La ética como eje vertebrador

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



Liderazgo transformacional: más allá del control, hacia la influencia

En el pasado, el liderazgo se asociaba al poder jerárquico y al control centralizado. Sin embargo, en un entorno BANI, la clave está en la influencia, la inspiración y la creación de confianza. Los líderes que triunfarán son aquellos que combinan: 1. Empatía: En un contexto ansioso y frágil, un líder debe saber escuchar, contener y guiar a su equipo. 2. Visión crítica: La IA ofrece datos, pero el líder traza el propósito y define los límites éticos y estratégicos. 3. Adaptabilidad: La capacidad de aprender y desaprender a gran velocidad, asumiendo que lo válido hoy puede no servir mañana. Dejar atrás el liderazgo autoritario implica reconceptualizar el poder. La autoridad no radica en imponer órdenes, sino en inspirar compromisos que motiven a la gente a dar lo mejor de sí misma.

Convergencia total: IA, compliance y liderazgo

El verdadero salto evolutivo sucede cuando la IA, el compliance y el liderazgo ético dejan de verse como “silos” y se convierten en un tejido estratégico único. En esta convergencia: □ Compliance da coherencia, asegurando un ecosistema de transparencia y responsabilidad. □ La IA potencia la capacidad de análisis y la anticipación, pero sin anular el juicio humano. □ El liderazgo actúa como catalizador, orquestando la visión, la confianza y el compromiso ético. Las organizaciones que entiendan esta integración no solo sobrevivirán, sino que definirán las nuevas reglas del juego. En un mercado ansioso por innovación, la diferenciación no se basa únicamente en productos o servicios, sino en la coherencia ética y en la calidad de la toma de decisiones. Ten presente que ... Hoy, más que nunca, no podemos limitarnos a sobrevivir. Frente a las amenazas y oportunidades del entorno BANI, necesitamos transformarnos conscientemente, abrazando la IA con cautela y ambición, y erigiendo un compliance inteligente que sea referente de integridad. La próxima era no se decide en un tablero de ajedrez, sino en la capacidad de construir puentes entre la ética y la innovación. La clave no es resistir el cambio, sino liderarlo con visión y compromiso



C2C Consultoría&Compliance



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



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

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

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

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

LA IMPERATIVA DUAL DE LA CIBERSEGURIDAD EN 2025: RESILIENCIA Y GESTIÓN DE LA SUPERFICIE DE ATAQUE EXTERNA

Metro
Risk

Edición propiedad de @MetroRisk, asociación

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

Las organizaciones se enfrentan a un panorama de amenazas cibernéticas en todo momento, pero hay una verdad ineludible: la prevención absoluta de ataques es una quimera. La sofisticación de los actores de amenazas, impulsada por avances en inteligencia artificial y la creciente interconexión digital, exige un cambio fundamental en la estrategia de ciberseguridad. Ya no basta con erigir muros defensivos; la clave reside en la capacidad de resistir, recuperarse y adaptarse a las inevitables intrusiones. Esta es la esencia de la resiliencia cibernética, un concepto que se ha consolidado como un pilar fundamental en la protección de los activos digitales.

Paralelamente a la necesidad de resiliencia, emerge con fuerza la Gestión de la Superficie de Ataque Externa (EASM) como una disciplina crítica. En un mundo donde las organizaciones extienden su presencia digital a través de múltiples nubes, aplicaciones web, dispositivos IoT y una vasta red de socios y proveedores, la visibilidad completa de los activos expuestos a Internet se ha vuelto primordial. La EASM proporciona esta visión crucial, permitiendo a las organizaciones identificar, analizar y mitigar los riesgos inherentes a su huella digital externa, que a menudo se convierte en el punto de entrada preferido por los atacantes. La resiliencia cibernética abarca un enfoque holístico que va más allá de la mera implementación de controles de seguridad. Implica una comprensión profunda de las posibles amenazas a través de una inteligencia de amenazas avanzada y un modelado de amenazas específico.

La capacidad de resistencia se fortalece mediante arquitecturas de seguridad Zero Trust y controles adaptativos que responden dinámicamente a las condiciones cambiantes. Sin embargo, la verdadera fortaleza radica en la capacidad de recuperación estratégica, con planes de recuperación ante desastres y continuidad del negocio robustos y probados rigurosamente. Finalmente, la adaptación continua, impulsada por el análisis post incidente y la actualización proactiva de políticas, asegura que la organización evolucione y se fortalezca con cada experiencia.

La Gestión de la Superficie de Ataque Externa complementa esta visión de resiliencia al proporcionar la conciencia situacional necesaria sobre los activos digitales expuestos. A través de un descubrimiento continuo y exhaustivo, las organizaciones obtienen un inventario dinámico de su presencia en línea, incluyendo activos no gestionados que a menudo representan vulnerabilidades ocultas. El análisis detallado de estos activos revela configuraciones erróneas, exposiciones de datos y vulnerabilidades conocidas, proporcionando una imagen clara de los posibles puntos de entrada para los atacantes.



La sinergia entre la resiliencia cibernética y la EASM se manifiesta en la capacidad de anticipar mejor las amenazas al comprender las vulnerabilidades expuestas. Una superficie de ataque externa bien gestionada reduce las oportunidades para que los atacantes exploten debilidades, fortaleciendo así la resistencia general de la organización. En el desafortunado caso de un incidente, el conocimiento preciso de los activos externos críticos facilita una recuperación más rápida y eficiente. Más importante aún, el monitoreo continuo de la superficie de ataque y el análisis de las vulnerabilidades descubiertas alimentan el ciclo de adaptación, permitiendo mejoras continuas en las defensas y los procesos de seguridad.

En mayo de 2025, las herramientas de EASM han evolucionado significativamente, integrando inteligencia artificial y aprendizaje automático para automatizar el descubrimiento de activos, la identificación de amenazas emergentes y la priorización de riesgos con una precisión sin precedentes. Estas plataformas se integran cada vez más con otras soluciones de seguridad, como los sistemas de gestión de eventos e información de seguridad (SIEM) y las plataformas de orquestación, automatización y respuesta de seguridad (SOAR), creando un ecosistema de seguridad más cohesivo y eficiente.

La adopción generalizada del trabajo remoto y la proliferación de servicios en la nube han expandido exponencialmente la superficie de ataque externa de las organizaciones, haciendo que la EASM sea una necesidad ineludible. Las organizaciones que no logran obtener una visibilidad clara y actuar sobre los riesgos identificados en su superficie de ataque externa se exponen a un mayor riesgo de sufrir ataques exitosos, con las consiguientes pérdidas financieras, daños a la reputación e interrupciones operativas.

La resiliencia cibernética y la gestión de la superficie de ataque externa ya no son conceptos aislados, sino dos caras de la misma moneda. La capacidad de una organización para resistir y recuperarse de los ciberataques depende intrínsecamente de su comprensión y gestión proactiva de su huella digital externa. Aquellas organizaciones que adopten esta visión dual estarán mejor equipadas para navegar por las turbulentas aguas del ciberespacio y asegurar la continuidad y el éxito en un mundo cada vez más interconectado y amenazado. La inversión estratégica en estas dos áreas no es solo una medida de protección, sino una inversión fundamental en la supervivencia y el crecimiento en la era digital.

TU COMUNIDAD SEGURA Y LEGAL. CUMPLE CON EL RGPD

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Rosa Fernández

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

ASUNTO: RGPD EN COMUNIDADES DE PROPIETARIOS

Seguramente que has tenido la experiencia de ser presidente de la comunidad. Suerte que siempre tenemos la opción de contratar a los administradores de fincas, ya que nos ayudan a resolver muchos problemas en el la gestión de una comunidad de propietarios. No sé si sabes, que la Comunidad de Propietarios per se no es considerada una persona jurídica, pero si que es sujeto de derechos y obligaciones en su dinámica y operativa, de tal suerte que, sí, también tiene que cumplir con el RGPD, puesto que trata datos de comuneros, arrendatarios, proveedores, vehículos, y todo un variado repertorio.

En esta ocasión me voy a detener en la vigilancia que las comunidades de propietarios, leáse garajes, fincas, urbanizaciones con diversos dispositivos para la seguridad. Dicha seguridad en estas comunidades de propietarios ha evolucionado con la tecnología: videovigilancia, videoporteros y mirillas digitales son ahora parte del día a día. Pero su uso no está exento de responsabilidad legal. Para evitar sanciones y conflictos, es fundamental cumplir con el Reglamento General de Protección de Datos (RGPD), la LOPDGDD y las directrices actualizadas de la Agencia Española de Protección de Datos (AEPD), y sobre todo, saber qué tienes que hacer para que no tengas que pagar una derrama por sanciones.

Por ejemplo, cuando decides que tu comunidad va a instalar cámaras de Videovigilancia en Zonas Comunes, esta medida está sujeta a una serie de Obligaciones Legales para la Comunidad de Propietarios. El uso de sistemas de videovigilancia en comunidades de propietarios está sujeto a una estricta regulación por parte de la Agencia Española de Protección de Datos (AEPD). Este tipo de tratamientos, que implican la captación y posible grabación de imágenes de personas físicas identificadas o identificables, debe ajustarse plenamente a la normativa vigente en materia de protección de datos, especialmente al Reglamento General de Protección de Datos (RGPD) y a la Ley Orgánica 3/2018 (LOPDGDD). Uno de los primeros requisitos es la necesidad de contar con una aprobación expresa por mayoría cualificada en Junta de Propietarios, conforme a la Ley de Propiedad Horizontal. La decisión de instalar cámaras debe ser adoptada formalmente, quedando reflejada en el acta correspondiente. Esta medida no puede ser ejecutada de forma unilateral ni por decisión de una minoría de vecinos. Además, las cámaras deben estar orientadas exclusivamente hacia las zonas comunes autorizadas. Está terminantemente prohibida la captación de imágenes de la vía pública, viviendas privadas o espacios ajenos al inmueble, salvo que se cuente con la debida habilitación legal o autorización administrativa. La captación indebida de estos espacios ha motivado sanciones por parte de la AEPD, como en el caso resuelto en julio de 2024, donde una comunidad fue multada con 1.000 euros por grabar parte de la vía pública



Asimismo, es obligatorio colocar cartelería visible que informe del uso del sistema de videovigilancia. Esta señalización debe indicar claramente la identidad del responsable del tratamiento, la finalidad del mismo y los derechos que asisten a las personas cuyas imágenes pudieran ser captadas. La ausencia de esta información constituye una infracción que puede conllevar consecuencias legales. El acceso a las imágenes debe limitarse exclusivamente a las personas autorizadas por la comunidad. No se permite un acceso indiscriminado, ni siquiera por parte de todos los propietarios. Además, las grabaciones no pueden conservarse indefinidamente: el plazo general máximo es de 30 días, salvo que deban conservarse más tiempo por razones justificadas, como una investigación en curso.

Los sistemas de videoportero, aunque muy comunes, también están regulados según sus funcionalidades. Si únicamente permiten la transmisión en tiempo real sin grabación ni acceso remoto, no se consideran un tratamiento de datos personales y por tanto no estarían sujetos al RGPD, aunque se recomienda alguna medida adicional. Sin embargo, si incluyen almacenamiento de imágenes o permiten su visualización en diferido a través de aplicaciones o servicios en la nube, entonces sí se activa toda la normativa de protección de datos.

Las mirillas digitales, que sustituyen a las tradicionales, también han sido objeto de análisis. Cuando estas disponen de sistemas que permiten grabar o almacenar imágenes de zonas comunes (por ejemplo, pasillos o rellanos), se considera que están realizando un tratamiento de datos personales y, por tanto, están sujetas al cumplimiento del RGPD. En este sentido, la AEPD ha sancionado con 300 euros a un particular que grababa con una mirilla digital sin autorización comunitaria.

Aviso a navegantes: es importante tener en cuenta que las comunidades de propietarios pueden incurrir en infracciones no solo por el uso de cámaras, sino también por otras prácticas relacionadas con el tratamiento de datos personales.

TU ELIGES EL NIVEL DE SEGURIDAD

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



Rosa 6.0

Código Experiencia



Diplomada en Derecho, Tecnología e Innovación

Compliance (RGPD, RIA, LOPDgdd, LSICE)

Consultora Sr Calidad (ISO, EFQM, 5S)

Consultora Jurídica

Técnica en Ciberseguridad

Formadora veterana*

Diseñadora de material didáctico

Miembro Comité Técnico Asesor en MetroRisk

Socia de ENATIC, asociación de Abogacía Digital

Competencias técnicas:

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



REINVENTAR LA SEGURIDAD PRIVADA EN ESPAÑA: HACIA UN NUEVO MODELO PROFESIONAL, MODERNO Y EFICIENTE

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Carlos Serrano
Director de Contenidos de Seguridad y Empleo

La seguridad privada en España necesita reinventarse para afrontar los desafíos de una sociedad en constante transformación. No basta con parches ni modificaciones puntuales: es necesario un cambio estructural, que parta de una nueva Ley de Seguridad Privada acompañada de un reglamento moderno, eficaz y realista, diseñado de la mano de los profesionales y no de espaldas a ellos.

El momento es ahora. La seguridad privada ha demostrado ser un pilar esencial en la protección de infraestructuras, bienes y personas. Sin embargo, su marco legal, sus procedimientos y su reconocimiento social están anclados en un modelo que ya no responde a las necesidades actuales. Si queremos un sector fuerte, respetado y eficaz, debemos actuar.

Propuestas para un nuevo modelo de Seguridad Privada

- Endurecer la habilitación de empresas de seguridad.
- Actualizar los requisitos de habilitación del personal e integrar nuevas vías de acceso.
- Digitalizar la cartilla profesional.
- Modernizar el sistema de depósitos de licencias de armas.
- Reformar el sistema de delegación de funciones.
- Adaptar la legislación a las nuevas funciones emergentes.

Endurecer la habilitación de empresas de seguridad: No se puede permitir que cualquier empresa acceda al sector sin demostrar una solvencia económica contrastada, un compromiso real con la calidad del servicio y el respeto a los derechos laborales de sus trabajadores. Propuestas específicas:

- Auditorías periódicas de solvencia y cumplimiento.
- Planes de formación obligatoria para sus empleados.
- Protocolos de calidad certificados externamente.
- Endurecimiento de sanciones ante prácticas laborales abusivas o reiteradas

Actualizar los requisitos de habilitación del personal e integrar nuevas vías de acceso: El profesional de la seguridad debe ser un especialista cualificado, y no alguien con una formación mínima o desactualizada. El sector exige una capacitación continua, adaptada a los nuevos riesgos y realidades sociales. Propuestas específicas:

- Ampliar la formación inicial obligatoria, incluyendo materias como protección de infraestructuras críticas, autoprotección, gestión de emergencias, ciberseguridad básica y derechos fundamentales.
- Introducir especialidades reconocidas, que permitan a los profesionales acreditarse en diferentes áreas según su formación y experiencia (por ejemplo: protección personal, eventos, control de accesos inteligentes, vigilancia aérea con drones, etc.).
- Establecer formación continua obligatoria cada dos años, para mantener actualizados los conocimientos y habilidades del personal habilitado.
- Evaluaciones periódicas de aptitud y actualización de conocimientos, combinando pruebas teóricas, prácticas y psicotécnicas.



www.seguridadyempleo.com



Además, es imprescindible adaptarse a las nuevas formas de habilitación que se están impulsando, permitiendo que los futuros profesionales puedan formarse a través de:

- Certificados de profesionalidad oficiales de Vigilancia, Seguridad Privada y Protección de Explosivos (como ya se exige en muchos casos).
- Formación reglada acreditada en centros homologados por Interior, que garantice estándares de calidad y contenidos actualizados.
- Reconocimiento de competencias profesionales adquiridas a través de la experiencia laboral, mediante procesos de evaluación y acreditación (ACREDITA).
- Programas de formación modular online, para determinadas especialidades, combinados con prácticas presenciales obligatorias en entornos controlados.

Estas nuevas vías de acceso deben coexistir con un control estricto de la calidad, para garantizar que la habilitación se traduzca en profesionales plenamente preparados para asumir su responsabilidad en la seguridad de las personas y bienes.

Digitalizar la cartilla profesional: El actual sistema de cartillas físicas está completamente desfasado. Propuestas específicas:

- Crear una app oficial de la Seguridad Privada.
- Permitir la consulta de habilitación, historial de servicios, prácticas de tiro, cursos realizados y renovaciones necesarias.
- Facilitar la comunicación entre profesionales, empresas y autoridades a través de la app.
- Garantizar la seguridad de los datos mediante tecnología blockchain o similar.



SEGURIDAD Y EMPRESAS

GRUPO SEGURIDAD Y EMPLEO

Modernizar el sistema de depósitos de licencias de armas

Hoy en día, el sistema de gestión de licencias de armas resulta ineficaz y burocrático. Propuestas específicas:

- Eliminación de trámites presenciales innecesarios.
- Digitalización completa del control de licencias y depósitos.
- Recordatorio: la tenencia de una licencia no implica derechos automáticos de uso en servicio sin la correspondiente autorización y vinculación contractual.

Reformar el sistema de delegación de funciones Se deben establecer criterios claros para coordinar y dirigir equipos de seguridad. Propuestas específicas:

- Toda persona que supervise servicios públicos o privados debe estar habilitada como Director o Jefe de Seguridad.
- Eliminar prácticas de “delegación informal” donde vigilantes asumen funciones de coordinación sin la formación ni la habilitación necesarias.
- Profesionalizar el liderazgo dentro del sector, garantizando la eficacia y la responsabilidad

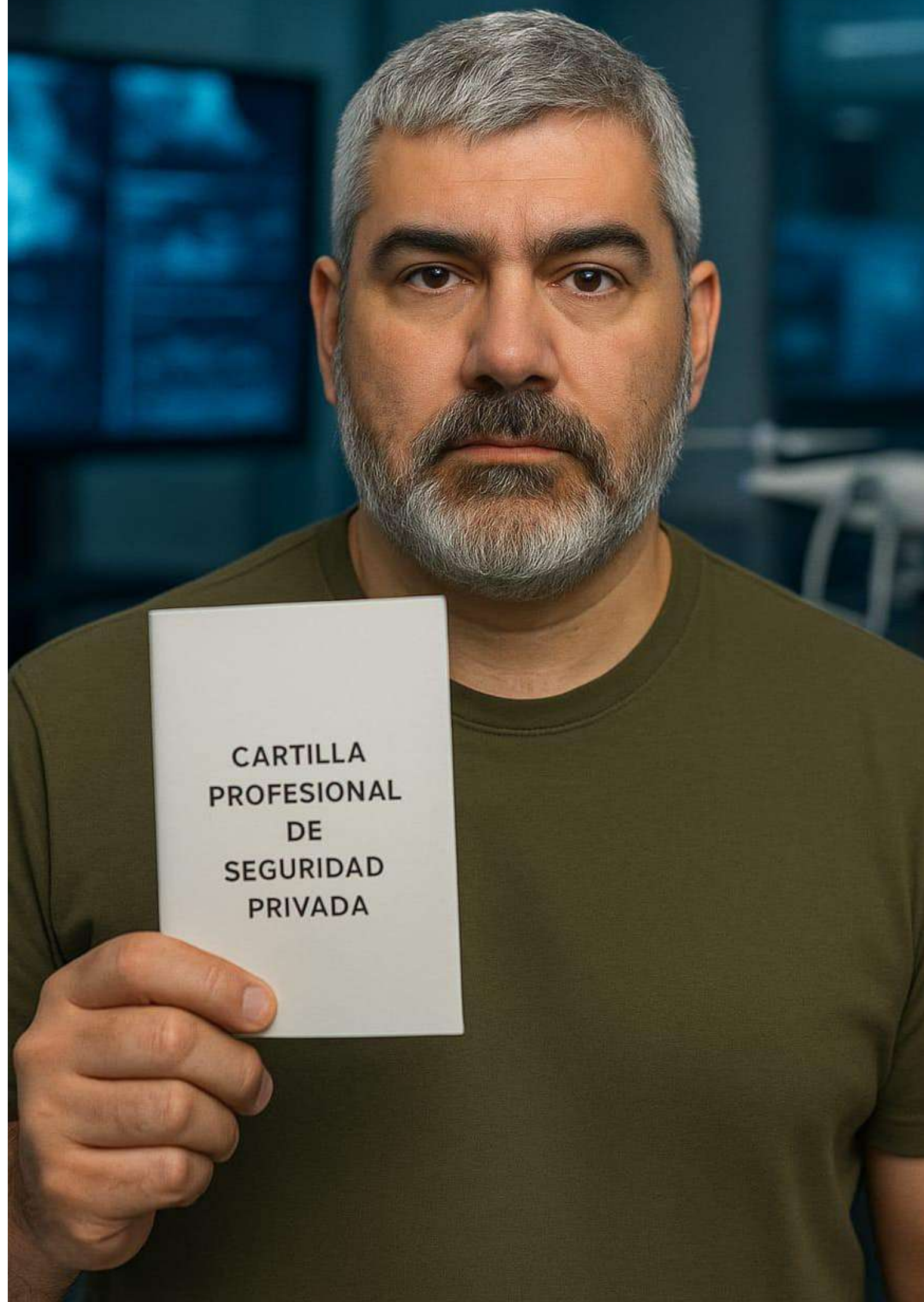
Adaptar la legislación a las nuevas funciones emergentes

La tecnología ha traído nuevos perfiles que deben ser reconocidos oficialmente. Propuestas específicas:

- Crear habilitaciones específicas para pilotos de drones de seguridad privada.
- Definir formación homologada para estos perfiles.
- Regular el uso de tecnologías de videovigilancia aérea, ciberseguridad preventiva, protección de infraestructuras críticas mediante drones y sistemas autónomos



HORA DE MODERNIZA NUESTRO SECTOR



Abraham Santana Herrera
Director de seguridad. Perito

La seguridad corporativa no debe concebirse como un gasto accesorio, sino como un pilar estratégico imprescindible para la continuidad del negocio, la protección del capital humano, el resguardo de activos críticos y la garantía de cumplimiento normativo. Esta premisa cobra aún mayor relevancia en sectores de alta criticidad como el bancario, el financiero, el logístico y el de gestión de valores.

Normalmente siempre se habla sobre la importancia de contar con un departamento de seguridad en cualquier actividad económica, pero es extraño leer algún artículo sobre uno que es real y obligatorio como es el departamento de seguridad bancaria.

Los bancos como todos sabemos, tienen una actividad estratégica en el día a día del Estado, he ahí, que estas entidades, están obligadas a disponer de un departamento de seguridad, donde al frente esté un director de seguridad.

Todos sabemos que el Reglamento de Seguridad Privada, es muy anterior a la Ley de Infraestructuras Críticas, pero aún así, este Reglamento reconoce la importancia de que las entidades bancarias y Cajas de Ahorros, cuenten con un departamento y unas medidas básicas en seguridad privada. Esto lo vemos reflejado dentro del reglamento en el CAPITULO II, Medidas de seguridad específicas, Sección 1.ª Bancos, cajas de ahorro y demás entidades de crédito. Este capítulo cuenta con 7 artículos que van desde el 119 al 126.

Considero que estos artículos forman parte del sentido común para una actividad empresarial de primera necesidad para el país, donde estos artículos hacen referencia a todas las medidas Físicas y Electrónicas mínimas necesarias con dos claras intenciones.

En primer lugar, la de protegerse de los riesgos antrópicos, como pueden ser los atracos y asaltos, junto a la protección de las personas que son utilitarias de los servicios bancarios y a sus empleados.

En segundo lugar, la de retrasar al máximo la acción de los delincuentes para dar tiempo a la actuación de las Fuerzas y Cuerpos de Seguridad del Estado.

Ya hace muchos años que no vemos a vigilantes armados en las entidades bancarias, debido a las excepciones reglamentarias que evitan su presencia en las sucursales, dejando de ser un importante gasto para las empresas del sector.

Pero este Reglamento ha quedado obsoleto, en un aspecto que si incluye la Ley de infraestructuras Críticas; la Ciberseguridad.



En la actualidad, podemos decir que los Sistemas Financieros y Tributarios (entidades bancarias, información, valores e inversiones), forman parte y están incluidos en la Ley de Infraestructuras Críticas.

En la actualidad, no es que los atracos a las sucursales bancarias hayan dejado de ser una preocupación, sino que en una sociedad cada vez más global y globalizada, las relaciones cibernautas son cada vez más importantes y necesarias, aunque esto genera nuevas vulnerabilidades y brechas de seguridad. Por no decir, la cantidad ingente de datos personales que maneja estas entidades, tanto a nivel de personas físicas como jurídicas, las hace especialmente atractivas para los ciberataques.

Una brecha de seguridad en esta materia, pondría en un importante peligro, a las empresas y usuarios de las entidades bancarias ante los extorsionadores de las redes. O peor aún, la pérdida de millones de euros por parte de las entidades bancarias ante una negación de servicio, dejando a la entidad desconectada de sus clientes o las bolsas de valores, entre otros.

Por lo tanto, considero que, en la actualidad este es uno de los retos más importantes con los que se tiene que enfrentar un departamento de seguridad bancario.

No me cabe duda, que la labor del director de seguridad requiere de una entrega total a los retos que se le presenta en el sector bancario.

No es solo el análisis de riesgos, la generación de PSS o los PSO, los Planes de Autoprotección, es la vigilancia constante de que todo el equipo de seguridad esté en máxima alerta ante cualquier riesgo.

Los constantes cursos de formación a los empleados para formarlos ante situaciones de emergencia y de que adquieran y comprendan las rutinas necesarias para evitar los riesgos Físicos, Electrónicos y Cibernéticos.



EL SEGURO DE RESPONSABILIDAD CIVIL PROFESIONAL: GARANTÍA ESENCIAL EN LA EJECUCIÓN DE FUNCIONES DE SEGURIDAD

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Alina Rubio de las Casas Experta en Seguros Generales

En un entorno donde la seguridad corporativa, patrimonial y personal se ha convertido en un factor crítico para la sostenibilidad empresarial, los profesionales que intervienen en su diseño, ejecución y supervisión asumen un alto grado de responsabilidad jurídica, técnica y operativa. Entre ellos se encuentran figuras como el Director de Seguridad, el Consultor o Asesor de Seguridad, el Perito Judicial y el Auditor Técnico.

Para todos ellos, la tenencia de un Seguro de Responsabilidad Civil Profesional (RS-P) no es solo recomendable, sino imprescindible, tanto para la protección personal como para la garantía frente a terceros.



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

¿Qué es el Seguro de Responsabilidad Civil Profesional (RC-P)?

Es una póliza de seguros que cubre los daños materiales, personales y patrimoniales causados a terceros por errores, omisiones o negligencias cometidas en el ejercicio profesional. Abarca tanto reclamaciones civiles derivadas de actos profesionales como posibles consecuencias económicas asociadas.

La figura del profesional de la seguridad: riesgos específicos

Director de Seguridad

Encargado de definir estrategias, protocolos, planes de autoprotección, políticas de accesos, coordinación de medios humanos y tecnológicos, etc. Un error en la evaluación de riesgos o en el diseño de medidas puede generar consecuencias graves, incluso penales, en caso de incidentes.

Consultor / Asesor de Seguridad

Responsable de emitir diagnósticos, informes técnicos, propuestas normativas y recomendaciones de seguridad que serán base para decisiones empresariales o administrativas. Una mala prescripción o una omisión puede provocar daños económicos directos al cliente.

Perito de Seguridad

Actúa en el marco judicial o asegurador, sus informes tienen consecuencias legales. Un error en un informe pericial puede tener un impacto directo sobre sentencias, compensaciones o desestimaciones de siniestros.

Auditor de Seguridad

Evalúa sistemas de seguridad existentes, su idoneidad y conformidad normativa. Sus conclusiones pueden determinar la continuidad operativa de una empresa o la validación de cumplimiento legal.

La necesidad real del seguro: razones técnicas y legales

El trabajo de estos profesionales se basa en el análisis, el juicio experto y la toma de decisiones bajo riesgo. Ningún profesional está exento de cometer errores, y el impacto económico de un fallo puede ser devastador.

Una mala decisión o un informe defectuoso puede dar lugar a:

- Demandas por parte del cliente.
- Responsabilidades solidarias con otras figuras profesionales.
- Reclamaciones por incumplimiento contractual o negligencia.

Contar con profesionales asegurados genera mayor confianza y seguridad jurídica al contratante. Saber que cualquier daño derivado del asesoramiento estará cubierto garantiza la trazabilidad y la solvencia del servicio.

- En licitaciones públicas, muchas Administraciones exigen el seguro como requisito de acceso.
- Entidades financieras y aseguradoras lo solicitan como medida obligatoria de cobertura en contratos de colaboración.
- El Código Civil español, en sus artículos 1902 y siguientes, establece la responsabilidad directa de los actos profesionales, incluso por omisión.

¿Qué debe cubrir un buen seguro de RC profesional en seguridad?

- Reclamaciones por errores de diseño, planificación, evaluación, implementación o supervisión.
- Daños personales, materiales y patrimoniales a terceros.
- Defensa jurídica y fianzas procesales.
- Cobertura retroactiva (actos anteriores no conocidos).
- Cobertura internacional, si se opera fuera del territorio nacional.
- Reclamaciones por incumplimiento de normativa técnica o legal aplicable



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, cibercrimes y delitos económicos.

DETECCIÓN

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

INVESTIGACIÓN

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

SEGURIDAD INTEGRAL

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

GREEN SEGURO: CUANDO EL SWING. SE PROTEGE CON SINERGIAS DE ACERO

Metro
Risk

Edición propiedad de @MetroRisk, asociación

Elena de la Parte

¿Es el golf realmente un deporte exento de riesgos? Aunque muchos lo asocian con tranquilidad exclusiva y naturaleza. La realidad es que, como cualquier evento deportivo, requiere medidas de seguridad rigurosas. detrás de cada torneo detrás de cada green se despliega una coordinación precisa entre las fuerzas y cuerpos de seguridad del Estado FCSE y la seguridad privada. Esta colaboración garantiza que tanto jugadores como asistentes puedan disfrutar del deporte un buen torneo seguro y controlado. La complejidad de los escenarios de seguridad actuales demanda soluciones innovadoras; La integración de la seguridad privada, lejos de ser una opción, se consolida como una necesidad para fortalecer el tejido protector de nuestra sociedad.

Los campos de golf presentan especificidades. A tener muy en cuenta a la hora de elaborar un Plan Integral y personalizado de seguridad. El Plan de Seguridad es elaborado por el Jefe de Seguridad y su contenido es el siguiente:

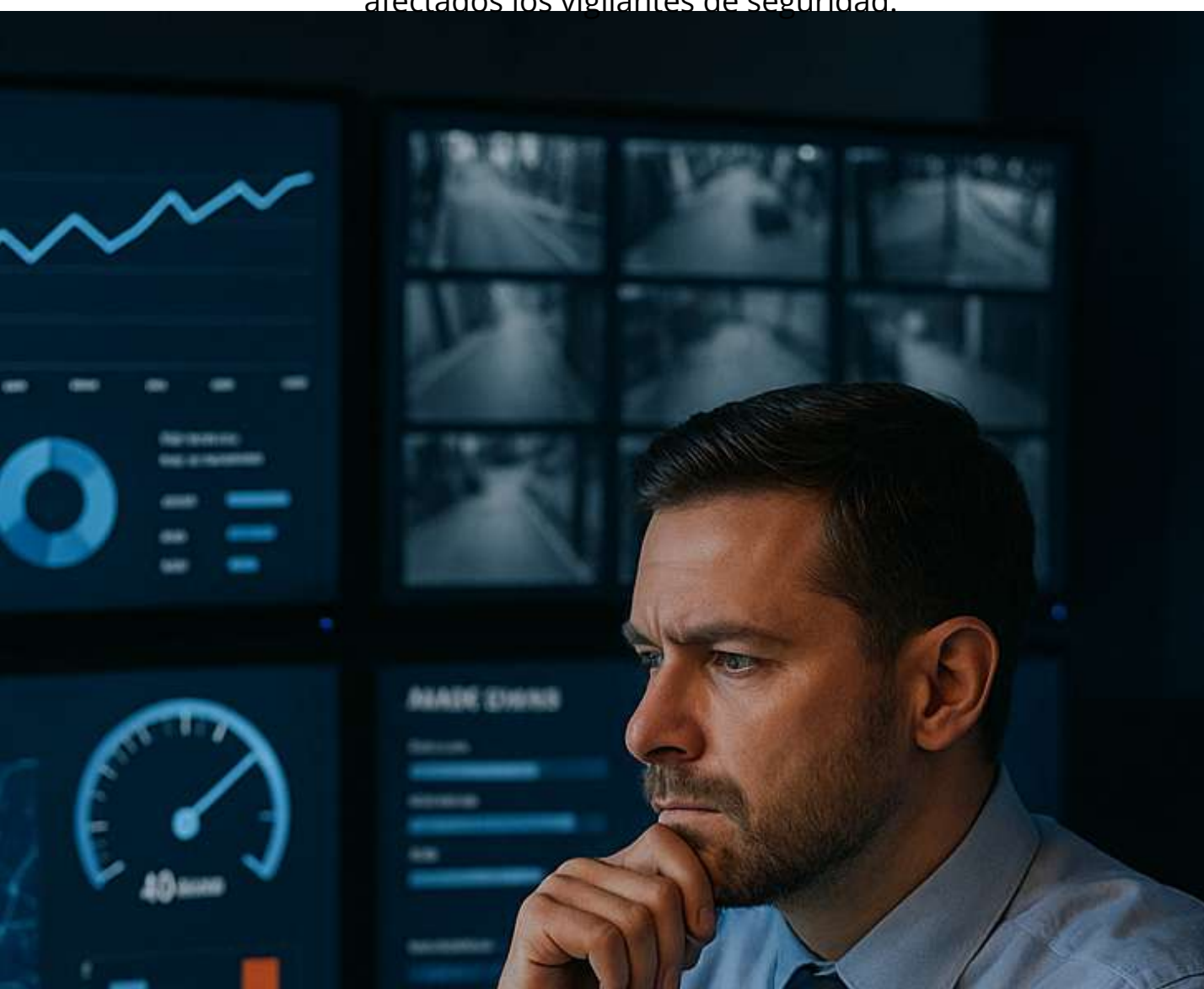
- Analizar los posibles riesgos y cómo afectarían a las instalaciones.
- Describir y ubicar todos los puntos de seguridad de las instalaciones, como son: Puestos de Control, Área de Videovigilancia, Controles de accesos, así como de todos los medios técnicos de seguridad que existan, cámaras, sensores de movimiento, barreras, etc.
- Detallar la ubicación del personal, horarios, rutas e itinerarios de vigilancia, así como la elaboración de partes sobre el mal funcionamiento o deterioro de objetos que se detecten en las instalaciones.
- Listado de los medios materiales y personales que formarán parte del servicio.
- Composición del servicio y estructuración, cuadrante y horario.
- Descripción detallada de las características del servicio.
- Indicar quién es el Jefe de equipo responsable y cómo comunicarle las incidencias.
- Análisis de Riesgos Laborales a los que se puedan ver afectados los vigilantes de seguridad.



El contenido de este Plan es vinculante respecto a la prestación del servicio.

En el sector del ocio y de los grandes eventos es fundamental disponer de sistemas que ayuden a los vigilantes de seguridad a garantizar la integridad de todos los usuarios, debido a la gran afluencia de gente y al amplio horario. Los campos de golf requieren soluciones de seguridad avanzada, eficientes y cómodas, tanto para sus miembros como para el personal. El rol de las fuerzas y cuerpos de seguridad del Estado cohesionado con la seguridad privada en el golf. Las fuerzas y cuerpos de seguridad del Estado desempeñan un rol esencial para garantizar el orden público y la protección de los asistentes en eventos deportivos. Amparadas por la Ley Orgánica 2/1987, de 13 de marzo, de Fuerzas y cuerpos de seguridad, estas instituciones tienen entre sus objetivos las siguientes:

- Control y verificación de accesos; Garantizando que solo el personal acreditado, prensa y público autorizado ingresen a las áreas designadas.
- Vigilancia y protección de bienes, establecimientos, certámenes o convenciones.
- Protección de personas.
- Depósito y custodia de objetos valiosos o peligrosos.
- Vigilancia perimetral y de zonas sensibles; Protegiendo áreas exclusivas como el club, zonas VIP o infraestructuras técnicas esenciales.
- Intervenciones rápidas; Actuando en incidentes menores como hurtos o altercados, agresiones y colaboración en la prevención de disturbios.
- Transporte y distribución de objetos valiosos o peligrosos.
- Prevención de amenazas y terrorismo; Su presencia es fundamental en torneos internacionales o cuando concurren personalidades de alto perfil coordinándose estrechamente con el Ministerio del Interior. En esta ocasión también Se cuenta con escoltas cualificados profesionalmente y acreditados, por el Ministerio del Interior.





- Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad.
- Empresas con domicilio en Ceuta y Melilla.
- Aparte de ello, también hay que considerar que en los campos de golf también pueden producirse incendios, explosiones, paso a zonas restringidas, robos y hurtos en sus distintas estancias (como oficinas o parking).
- Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad
- Gestión de emergencias; Gracias a protocolos de como el establecido en el Real Decreto, 393/2007, Que aprueba la norma Básica de autoprotección. Pueden coordinar eficazmente Respuestas ante situaciones críticas, Desde emergencias médicas, conatos de incendio, hasta evacuaciones.
- Asimismo, la Ley 19/2007, de 11 de julio, Contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte refuerza la necesidad de medidas preventivas en todos los ámbitos deportivos, incluido el golf.

Todas estas razones, hacen que contar con un sistema de videovigilancia en los campos de golf, sea una decisión valorada y de gran importancia.

Toda empresa de seguridad debe estar registrada a través de instancia. Dirigida a la Unidad Orgánica Central de Seguridad privada de la Dirección General de la Policía de la actividad. En este rol que nos compite, los vigilantes de seguridad con su excelente deontología profesional. Se encargarán también de proteger y supervisar todas las instalaciones y espacios del recinto y de controlar el acceso a las mismas, una intervención al que suman los mejores sistemas de seguridad y mecanismos de vigilancia y soluciones para los campos de golf.

El objeto principal de los servicios de seguridad es proteger los edificios públicos y privados, principalmente urbanizaciones proporcionando altos niveles de seguridad para las personas y bienes que se encuentren en su interior. Si las instalaciones no estuviesen equipadas previamente con sistemas de seguridad, y fuesen requeridas por el contratante, se procedería a su instalación y mantenimiento. Los servicios incluyen la realización de un Plan de Vigilancia y Seguridad por personal capacitado al efecto, en el cual se analizan los riesgos y se planifica la implantación y mantenimiento del servicio integral de seguridad

Existen varias razones para contar con cámaras de videovigilancia CCTV, en los campos de golf, ya que nos proporcionan una serie de beneficios en términos de seguridad, gestión y protección de la propiedad y en mejorar la experiencia general en el campo de golf.

- Protección contra robos y vandalismo: Los campos de golf suelen tener áreas extensas y, a menudo, áreas remotas que pueden ser vulnerables a robos o actos de vandalismo. La videovigilancia puede ayudar a disuadir estos comportamientos y proporcionar pruebas en caso de incidentes.
- Seguridad de los jugadores: Asegurarse de que los jugadores estén seguros es fundamental. Las cámaras pueden utilizarse para supervisar áreas de alto tráfico, como estacionamientos y zonas de inicio y finalización, para garantizar que los jugadores estén protegidos.
- Monitoreo de las instalaciones: La videovigilancia puede ser útil para supervisar y así prevenir robos y daños en; las instalaciones del club de golf, las canchas de práctica, las áreas de almacenamiento de equipos y las casetas de mantenimiento deben estar seguras y bien cerradas.
- Prevención de conflictos y problemas: La videovigilancia también puede ser útil para resolver disputas entre jugadores o para verificar el cumplimiento de las reglas del campo de golf.
- Cumplimiento normativo: Las regulaciones requieren que los campos de golf tengan sistemas de videovigilancia para cumplir con las normativas de seguridad y para proteger la propiedad.
- Respaldo legal: En caso de disputas legales, las grabaciones de videovigilancia pueden servir como evidencia crucial

Al implementar un sistema de videovigilancia en un campo de golf, es importante considerar la privacidad de los jugadores y el personal, así como cumplir con las leyes y regulaciones locales relacionadas con la videovigilancia. También es esencial notificar a las personas sobre la presencia de cámaras en el lugar y garantizar que los datos grabados se almacenen y manejen adecuadamente. La seguridad en el campo de golf es responsabilidad tanto de la dirección del campo como de los jugadores. La educación y la comunicación efectiva son clave para mantener un ambiente seguro y agradable en el campo de golf.



El artículo 41 de la Ley de seguridad privada recalca La colaboración y lealtad institucional. Estableciendo que, ante hechos delictivos o situaciones de riesgo, Los vigilantes deben coordinarse con las FCSE. Para optimizar la respuesta. Coordinación estratégica para un golf seguro. El éxito en la seguridad de eventos de golf radical, la estrecha cooperación entre la FCSEY, la seguridad privada. En grandes torneos se establecen centros de coordinación de seguridad, Donde se comparten planes integrales que definen los roles, niveles de alerta y protocolos de comunicación.

El Artículo 38 de la Ley de seguridad privada enfatiza este aspecto, Las empresas de seguridad a colaborar y suministrar información relevante a las autoridades. Esta integración permite:

- La respuesta inmediata ante emergencias.
- La optimización de recursos y personal.
- La implementación de medidas preventivas y correctivas en tiempo real

Nuevos retos y el uso de la tecnología.

El entorno del golf, como parte de la evolución de los eventos deportivos, también enfrenta desafíos asociados a la innovación tecnológica y cambios normativos. Entre estos se destacan:

- Drones no autorizados: Que interfieren en el espacio aéreo del campo. Regulados por él. Real. Decreto 1036/2017, Su uso para la vigilancia o grabación de áreas debe contar con la autorización de la AESA, garantizando al mismo tiempo el respeto a la privacidad.
- Ciberseguridad: La protección de sistemas de gestión, acreditación y vigilancia depende del cumplimiento estricto del. Reglamento General de Protección de Datos (RGPD) y La Ley Orgánica 3/2018, de Protección de Datos personales y garantía de los derechos digitales.
- De conformidad con lo dispuesto en la Norma UNE 19601:2017 sobre Sistemas de Gestión de Compliance, la RFEG y sus sociedades participadas ha habilitado un canal de comunicación, el Canal de Denuncias de la RFEG
- Protocolos sanitarios post COVID: Manteniendo medidas Adaptativas para enfrentar nuevos desafíos sanitarios en eventos internacionales

Los sistemas de seguridad que pueden integrarse, y que son de gran utilidad, en los campos de golf, son los siguientes:

- Sistemas de grabación de vídeo y de análisis. Un equipo que incluye la captura de imágenes, el almacenamiento, el análisis de vídeos en cuestión de minutos, y otras capacidades que aumentan las posibilidades de investigación y de visualización de contenido obtenido. Con él podrás cubrir grandes rangos, funciones sencillas y económicas, pero de gran utilidad. Permite gran número de canales y de usuarios.
- Cámaras de visión térmica de corto y largo alcance: Este tipo de sistemas de videovigilancia están capacitados para obtener imágenes y grabaciones de grandes rangos, detectando incluso en condiciones de baja luminosas, presencia de humo, polvo y niebla. Todas estas condiciones, convierten este sistema en uno de los más usados, debido a que realizarán su función tanto de día como de noche.
- Sistema de centralización e integración de un Centro de Control. Este sistema permite conocer qué ocurre, cómo y en qué lugar de forma exacta, permitiendo una rápida actuación ante cualquier tipo de incidencia. Con él se obtiene una visión global e integral, permitiendo la interacción entre tecnologías, usuarios y respuestas. Podrás controlar accesos, grabaciones de vídeos y de audios, detecciones perimetrales, entre otras muchas

Un compromiso compartido para la excelencia deportiva. El golf es un juego que requiere de una cierta mentalidad. Un juego en el que la precisión encuentra la recompensa. Las Reglas de Golf reflejan esta mentalidad, un conjunto de normas precisas ante las cuales todos los jugadores de Golf,son responsables ante ellos mismos. Un código de honor e integridad, pensado para ser fácilmente accesible de forma que cada jugador pueda ser su propia Autoridad de Reglas. Aun así, todo evento deportivo es esencial la contratación de seguridad privada, para minimizar incidentes de toda índole.

La Ley Orgánica 3/2013, de 20 de junio, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva. La seguridad en el Golf es el resultado de una colaboración meticulosa y coordinada entre las fuerzas y cuerpos de seguridad del Estado y la seguridad privada. Este trabajo conjunto,

“Imagina tu cuerpo como una máquina de precisión: El ejercicio es el combustible que enciende los motores de la felicidad, propulsores que aceleran tu energía interior, pulverizando el estrés y pintando tu estado de ánimo con la fuerza de un Guerrero” En definitiva, detrás del swing perfecto existe un compromiso firme con la seguridad y la excelencia operativa en cada jornada deportiva. “Juega la bola como repose. Juega el campo como lo encuentre. Y si no puede hacer esto, Haga lo que es justo. Pero para hacer lo que es justo, Tiene que conocer las Reglas del deporte del golf.



CONVENIO COLECTIVO Fuente utilizada: el BOE

Compañeros y estimados lectores, recordemos algunas cuestiones de importancia recogidas en el convenio colectivo de seguridad privada. **Por ELENA de la Parte**

Artículo 22. Confidencialidad Profesional. En aplicación de lo previsto en la legislación vigente, el personal de seguridad privada tendrá prohibido comunicar a terceros, salvo a las autoridades judiciales y policiales para el ejercicio de sus respectivas funciones, cualquier información que conozcan en el desarrollo de sus servicios y funciones sobre sus clientes o personas relacionadas con éstos, así como sobre los bienes y efectos de cuya seguridad o investigación estuvieran encargados.

Artículo 39. Anticipos. El trabajador tendrá derecho a percibir anticipos a cuenta, por el trabajo ya realizado, sin que pueda exceder del 90 por ciento del importe de su retribución total mensual de las tablas de retribución del Anexo más la antigüedad y del 90% del importe de las pagas extraordinarias ya devengadas y no abonadas, en un plazo máximo de cuatro días hábiles desde la solicitud.

Artículo 50. Ayudas a hijos y cónyuge discapacitados. Las Empresas abonarán a los trabajadores con hijos discapacitados a su cargo la cantidad de 136,02 euros mensuales en 2023, 141,46 euros mensuales en 2024, 145,70 euros mensuales en 2025 y 150,07 euros mensuales en 2026 por hijo de esta condición como complemento a la prestación que la Seguridad Social le tenga reconocida en concepto de ayuda para discapacitados, entendiéndose como tales los así definidos en la legislación aplicable.

Asimismo, recibirán la cuantía establecida en el anterior párrafo, en aquellos supuestos en los que el cónyuge del trabajador tenga derecho a una prestación pública como consecuencia de una discapacidad del 65% o superior. La cuantía acreditada de la prestación será abonada por la Empresa en la que el trabajador preste sus servicios en proporción al número de días trabajados en el mes



DRONES Y SEGURIDAD: NUESTRA EXPERIENCIA EN SEDEXPO CON RITRAC INTERNATIONAL

Metro
Risk

Edición propiedad de @MetroRisk, asociación

SEDEXPO: Innovación y Tecnología al Servicio de la Seguridad

En un mundo donde la seguridad es una prioridad creciente, la tecnología drones ha pasado de ser un lujo a convertirse en una herramienta esencial. En SEDEXPO, Ritrac International demostró cómo la innovación aérea está transformando la manera en que protegemos a las personas y el entorno.

SEDEXPO se ha consolidado como una de las ferias más importantes en el ámbito de la seguridad, la defensa y las emergencias. Este evento reúne a profesionales de diversos sectores para conocer las últimas innovaciones tecnológicas, establecer sinergias y debatir sobre los desafíos actuales en seguridad pública y privada. En este contexto, Ritrac International tuvo la oportunidad de participar activamente, presentando sus soluciones con drones y su formación especializada.

Ritrac International: Referente en Tecnología Drone y Formación

Ritrac International es una empresa especializada en soluciones con drones para múltiples sectores, incluyendo seguridad, inspección industrial, lucha contra incendios, búsqueda y rescate, y agricultura. Como entidad certificada por AESA, ofrece formación reglada para pilotos y profesionales que buscan implementar esta tecnología en sus operaciones. Nuestra misión es proporcionar herramientas que optimicen procesos y aumenten la seguridad en cada aplicación.

SEDEXPO: Un Espacio de Encuentro y Aprendizaje

Desde el primer momento en SEDEXPO, quedó claro que iba a ser una experiencia intensa y enriquecedora. Empresas de seguridad pública y privada, organismos de inspección industrial y profesionales del sector mostraron un gran interés en cómo los drones pueden mejorar su operativa diaria. Las preguntas giraban en torno a la integración de esta tecnología en sus procedimientos, las certificaciones necesarias y la formación disponible para sus equipos.

El evento no solo sirvió como una vitrina para mostrar nuestras capacidades, sino también como un espacio para escuchar las necesidades del sector y adaptar nuestras soluciones a sus requerimientos específicos. Según estudios recientes, el uso de drones en seguridad ha aumentado en un 35% en los últimos cinco años, lo que refuerza la importancia de nuestra labor en formación y consultoría.



El Apoyo de DJI Barcelona y la Unidad Pegaso de la Guardia Civil de Galicia

Uno de los momentos destacados de SEDEXPO fue la colaboración con DJI Barcelona, quienes nos brindaron la oportunidad de presentar el nuevo DJI Matrice 4T. Este dron, con su capacidad para realizar inspecciones de alta precisión y su versatilidad en diferentes escenarios, generó un gran impacto, especialmente entre el personal de las fuerzas y cuerpos de seguridad del Estado. La posibilidad de probarlo en vivo permitió a los asistentes conocer su potencial operativo y abrir nuevas oportunidades de colaboración.

La Unidad Pegaso de la Guardia Civil de Galicia, representada por Agustín y Omar, también brindó un gran apoyo durante el evento. Su experiencia en la regulación y supervisión del uso de drones en seguridad nos permitió profundizar en la importancia del cumplimiento normativo y en cómo mejorar la integración de estos dispositivos en operativos policiales.

Drones y Seguridad: Ponencias Claves

Durante SEDEXPO, realizamos varias ponencias que captaron la atención del público especializado:

- "Drones y Unidades K9": Analizamos cómo la combinación de tecnología aérea y equipos caninos puede mejorar la detección y respuesta en operaciones de seguridad y rescate.





Metro
Risk

•“Drones: ¿Una Herramienta Clave en la Lucha Antiterrorista?”: En esta presentación, el personal de Aduanas mostró un especial interés en el uso de drones para la vigilancia y detección de actividades ilícitas en fronteras y puertos

La Seguridad Pública como Prioridad

Uno de los temas más recurrentes en nuestras conversaciones fue la seguridad pública. Autoridades y profesionales del sector mostraron un gran interés en cómo los drones pueden ser utilizados en prevención del delito, vigilancia de grandes eventos, control fronterizo y respuesta ante emergencias.

La Policía Municipal de Sabadell asistió con su unidad canina, donde la estrella fue Kala, una pastor malinois entrenada para la detección de estupefacientes. La combinación de drones con unidades caninas y otros recursos tecnológicos representa un avance significativo en la seguridad ciudadana. Según informes recientes, el uso de drones en vigilancia y detección de amenazas ha reducido los tiempos de respuesta en un 40% en algunas unidades especializadas.

También destacamos el interés de los profesionales de la lucha contra incendios, quienes nos consultaron sobre cómo detectar puntos críticos en la fase de prevención de incendios. Explicamos cómo el uso combinado de drones con sensores térmicos y software especializado permite identificar zonas de riesgo con antelación, lo que podría prevenir desastres y optimizar la respuesta en caso de incendios activos.

Además, Protección Civil de varias regiones nos consultó sobre las mejores estrategias para la búsqueda de desaparecidos mediante drones. Compartimos metodologías y herramientas avanzadas que permiten mejorar la eficiencia en este tipo de operaciones.

Colaboraciones Estratégicas en SEDEXPO

SEDEXPO también nos permitió conectar con otros actores clave en el ámbito de la seguridad y el desarrollo humano. Un ejemplo destacado fue nuestra interacción con ASADESA - Cooperadores Españoles para el Desarrollo y Desminado en el Sahara, quienes expusieron sobre el desminado humanitario en esa región de África. La posibilidad de colaborar en este tipo de iniciativas reafirma el papel fundamental que los drones pueden desempeñar en misiones de alto impacto social.

Carlos Miguel Ortiz

Delegado Regional

Comunidad Autónoma de Madrid

Piloto remoto UAS certificado EASA

Instructor-examinador UAS certificado RITRAC

Ritrac International UAS professional services worldwide RUPSW



Correo electrónico: cmiguel@ritrac.eu

Móvil/Whatsapp: +34 685040875

Sitio web: <https://ritrac.eu>

Plataforma formación: <https://remotepilot.online>

Reuniones telemáticas: <http://webex.ritrac.eu>

Conclusiones y Agradecimientos

Lo más gratificante de SEDEXPO fue ver cómo las conversaciones evolucionaban desde la simple curiosidad hasta el planteamiento serio de colaboración. Nos encontramos con responsables de empresas y entidades que buscan integrar drones en su operativa, y pudimos ofrecerles soluciones reales y adaptadas a sus necesidades.

Además, fue evidente cómo la percepción sobre los drones ha cambiado. Ya no se ven solo como herramientas para tomas aéreas, sino como elementos clave para mejorar la seguridad pública, reducir riesgos y optimizar la eficiencia en múltiples sectores.

Quiero aprovechar este espacio para agradecer a mi compañero Cristóbal Granados por brindarme la oportunidad de asistir a este evento y representar a Ritrac International. Su apoyo ha sido clave en nuestra participación y en la difusión de nuestra labor.

El futuro de la seguridad está en el aire. SEDEXPO nos ha permitido demostrar que la tecnología drone no solo es el presente, sino que marcará el camino en la protección y prevención de riesgos. Desde Ritrac International, seguiremos trabajando para que más profesionales accedan a esta herramienta clave en la seguridad del mañana



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

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

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

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

Colaboramos con MR-CONSULTING.



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

En el Ámbito de la:

Seguridad Privada, Balística Forense.

Ciberseguridad, Inteligencia y
Geopolítica.

Seguros de Embarcaciones Recreo.

Grafología, Documentoscopia,
Grafopsicopatología Criminal y
Forense.

Due Diligence (Debida Diligencia).

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

"RESCATE CIVIL Y SEGURIDAD CORPORATIVA: EL VOLUNTARIADO QUE REGENERA EL TEJIDO SOCIAL DESDE LAS EMPRESAS"

Metro
Risk

Edición propiedad de @MetroRisk, asociación



Jonatthan Hermida Sosa
SAPPC, SFPC, DAS, CPO, CSI, GER,
CRESA. SEO Hermida Seguridad S.A.S.
Licenciado en Seguridad Pública y
Criminología.

Hacia una seguridad con rostro humano: La era de la seguridad blindada y desconectada de su entorno ha terminado. La nueva seguridad corporativa es participativa, resiliente, incluyente y comunitaria. En este nuevo esquema, los grupos como Rescate Culiacán no son actores periféricos, sino piezas clave de un engranaje que protege, educa y transforma. Porque al final del día, una empresa que protege vidas no solo sobrevive.

Se convierte en ejemplo. Culiacán, Sinaloa. En un entorno marcado históricamente por desafíos complejos en materia de seguridad, surge un nuevo paradigma que promete transformar tanto la protección civil como la seguridad corporativa: los grupos de rescate voluntarios y servicios prehospitarios comunitarios como pilares estratégicos en la estructura preventiva de las empresas. El ejemplo más reciente y prometedor: Rescate Culiacán. En una ciudad que ha sido durante años identificada por su lucha contra la narco cultura, se abre paso una revolución silenciosa, tejida no con armas ni discursos políticos, sino con camillas, botiquines y una férrea voluntad de servir. Rescate Culiacán, formado por jóvenes comprometidos, técnicos en urgencias médicas y ciudadanos con vocación, representa no solo un movimiento comunitario sino una herramienta vital para integrar a las nuevas generaciones a un entorno de servicio, responsabilidad civil y profesionalismo.

Más allá del auxilio, una nueva dimensión de la seguridad: Históricamente, la seguridad corporativa se ha centrado en los pilares de la vigilancia, la tecnología y los planes de contingencia reactiva. Sin embargo, el mundo actual demanda una evolución del concepto hacia una visión holística que incluya la prevención comunitaria, la respuesta inmediata y la colaboración interinstitucional. En este contexto, los grupos de rescate y paramédicos voluntarios se han convertido en activos críticos que permiten una sinergia entre el entorno social y el ecosistema empresarial. Las empresas en Latinoamérica, especialmente en regiones con alta vulnerabilidad social, enfrentan no solo riesgos físicos y operativos, sino también desafíos de impacto comunitario y reputacional. Integrar a estos grupos a sus sistemas de gestión del riesgo no solo fortalece su capacidad de respuesta ante emergencias médicas, incendios o fenómenos naturales, sino que inserta un componente de responsabilidad social activa que resuena positivamente con la ciudadanía, autoridades y grupos de interés.

Hacia un nuevo contrato social empresarial Integrar a los grupos voluntarios de rescate en los planes de seguridad corporativa no es un acto de caridad. Es una decisión estratégica. Su inclusión puede significar la diferencia entre una evacuación caótica y una intervención organizada; entre una crisis reputacional y una respuesta humanitaria efectiva. Las empresas que logren vincularse con estos grupos, ya sea mediante convenios de colaboración, programas de voluntariado empresarial, patrocinios o certificaciones compartidas, estarán fortaleciendo no solo sus líneas de defensa operativa, sino su legitimidad social



Rescate Culiacán: Modelo de resiliencia y contención cultural/ La creación de Rescate Culiacán representa una bocanada de esperanza. Este grupo no es solo un escuadrón de atención prehospitalaria; es una trinchera de transformación social. Jóvenes, muchos de ellos expuestos a entornos de riesgo o tentados por caminos violentos, encuentran aquí una alternativa digna, profesional y profundamente humana. El grupo ha establecido su base de operaciones en el fraccionamiento Prados del Sur, desde donde despliegan capacitaciones, simulacros, brigadas comunitarias y asistencia médica básica. Además, han comenzado a establecer vínculos con empresas locales, instituciones educativas y autoridades de protección civil, promoviendo la cultura de prevención y la corresponsabilidad ciudadana. Este enfoque se alinea con una tendencia internacional que impulsa la integración de la comunidad civil organizada a los sistemas de seguridad y emergencia de alto nivel, como se observa en países como Japón, Israel o Alemania. Pero en Culiacán, este movimiento tiene un componente adicional: la contención cultural del narcotráfico a través del servicio civil organizado.

La juventud como capital humano para la seguridad futura: Uno de los grandes valores agregados de iniciativas como Rescate Culiacán es su rol como incubadora de talentos para las profesiones de la seguridad pública. Muchos de sus integrantes aspiran a convertirse en bomberos, paramédicos, policías o profesionales de protección civil. Su paso por el voluntariado no solo les otorga experiencia técnica, sino que los conecta con valores fundamentales como el servicio, la disciplina, la empatía y el liderazgo. Este modelo ha despertado el interés de empresas de seguridad privada, unidades de protección civil empresarial y organizaciones internacionales, quienes ven en estos jóvenes una cantera de futuros colaboradores bien entrenados, con visión ciudadana y habilidades prácticas.

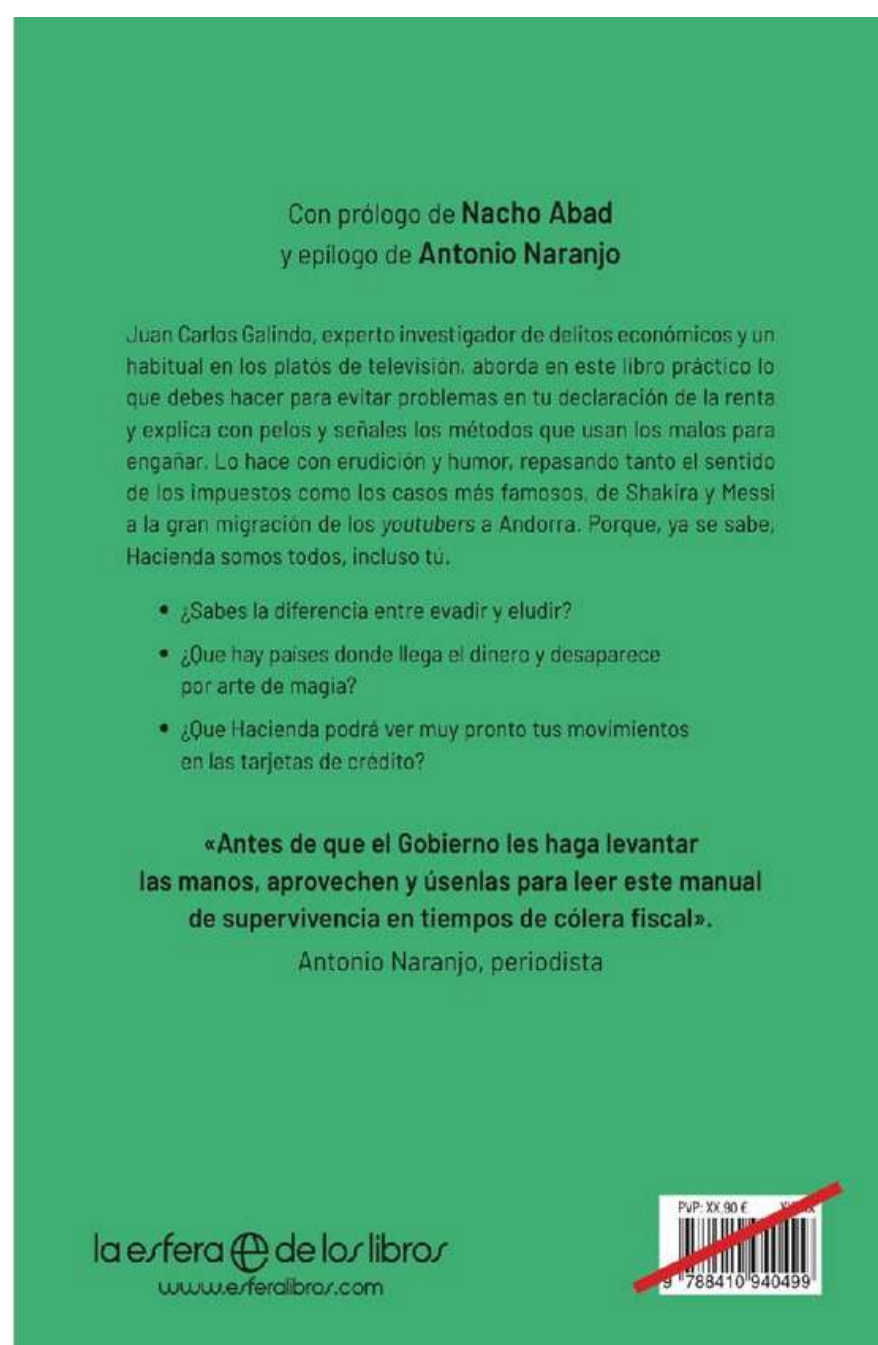
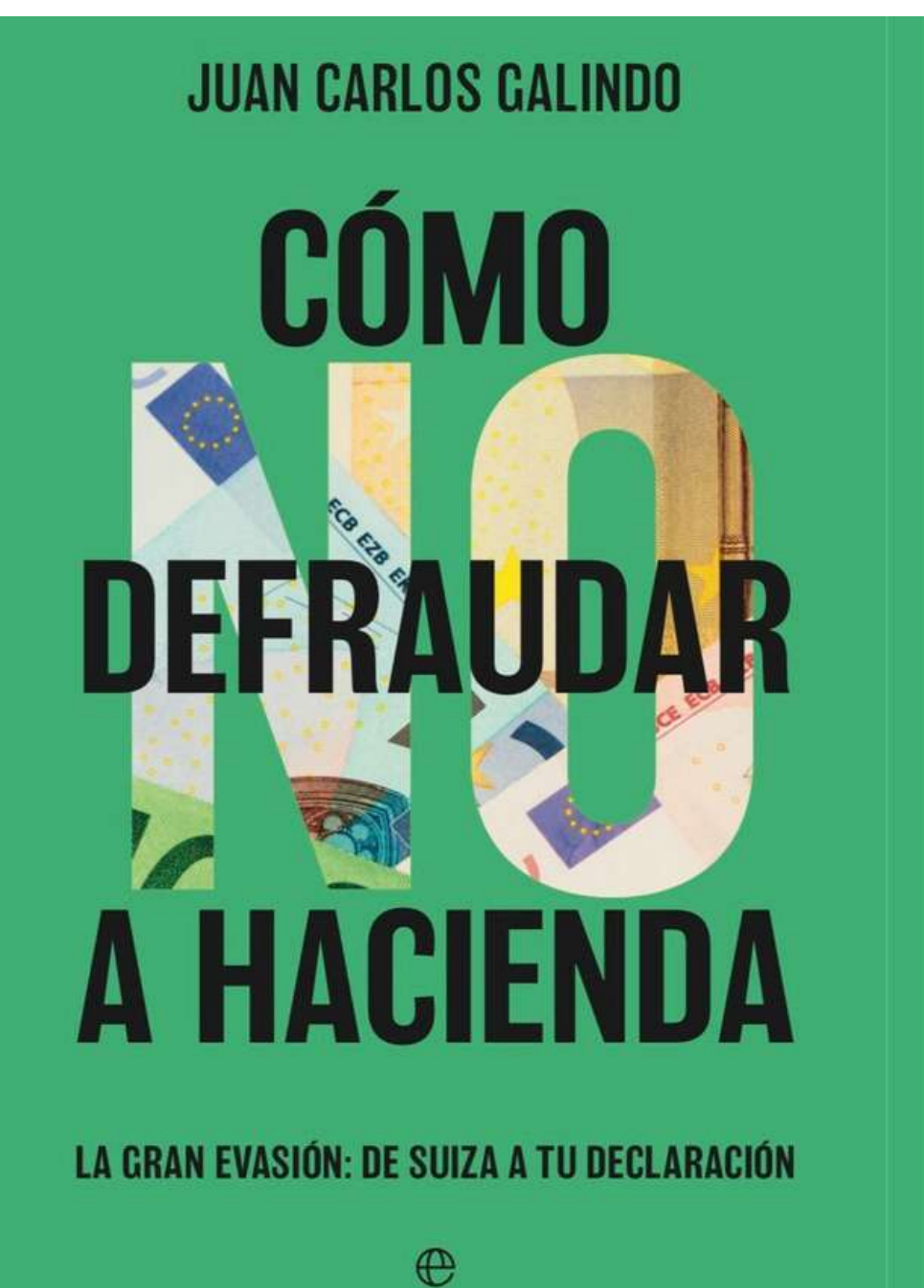
AGENDA

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.



Organizan:



SEGURITECNIA

Patrocinan:

casmar



EL CANAL DEL CORONEL



LOS CONSEJOS DE CIBERSEGURIDAD DE ADOLFO GELDER.

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

WWW.ALBERTORAY.COM

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





Metrorisk Proyecto Asociativo

www.metrorisk.es