EDITORIAL MR

ISSN 3045-7629

ABRIL

AÑO 2025

Fran Medina Cruz
Francisco Javier Gonzales Fuentes
José Ignacio Olmos
Gregorio Duro
Mercedes Escudero Carmona
Antonio Cozano Fernández
Emilio Piñeiro
Adolfo M. Gelder
Rosa Fernández
Carlos Serrano
Abraham Santana
Alina Rubio
Elena de la Parte
Carlos Miguel Ortiz
Jonatthan Hermida
Carlos Tejada Morán

@Metrorisk.es

ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

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

COLABORADORES

PATROCINADO POR LAS FIRMAS

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

EL FUTURO DE LA SEGURIDAD PRIVADA: UN CAMBIO NECESARIO

Metro Risk

Fran Medina Cruz
Director de MetroRisk

El mundo enfrenta un panorama de seguridad cada vez más hostil, marcado por el aumento de la violencia indiscriminada, la pérdida de temor hacia la intervención policial y la ineficacia de los marcos legales para disuadir el crimen. Factores como la pobreza, la desinformación y los choques culturales han convertido la seguridad en un campo de batalla donde los actores tradicionales han quedado obsoletos frente a las nuevas amenazas. Ante este escenario, la seguridad privada no solo debe adaptarse, sino que tiene la obligación de evolucionar. La transformación del sector es inminente y debe incluir reformas estructurales que garanticen su eficacia en un contexto donde los recursos estatales son insuficientes para combatir la creciente ola de inseguridad.

Ámbitos Clave de Evolución

Modernización Tecnológica

- Implementación de inteligencia artificial y analítica predictiva en la vigilancia.
- Uso de drones y robots de patrullaje para la cobertura de grandes superficies.
- Desarrollo de sistemas biométricos avanzados para el control de accesos.
- Integración de herramientas de ciberseguridad para mitigar amenazas digitales.

Formación y Capacitación Profesional

- Creación de estándares educativos más rigurosos y especializados.
- Entrenamiento en resolución de conflictos y técnicas de negociación.
- Formación en el manejo de situaciones de crisis con énfasis en derechos humanos.
- Instrucción en el uso de nuevas tecnologías de vigilancia y protección.

Revisión y Ampliación de la Regulación

- Modificación de los marcos legales para otorgar mayor cobertura y respaldo a los agentes de seguridad privada.
- Implementación de normativas internacionales para homologar procedimientos y competencias.
- Definición clara de los límites y facultades de acción de la seguridad privada en colaboración con las fuerzas públicas.

Desarrollo de un Marco de Innovación y I+D

- Incentivar la inversión en investigación y desarrollo dentro del sector.
- Fomentar la creación de startups de tecnología aplicada a la seguridad.
- Implementar programas de colaboración entre empresas privadas y organismos estatales.

Uniformidad y Profesionalización del Sector

- Creación de una uniformidad única y estandarizada que refuerce la identidad y el reconocimiento del sector.
- Implementación de un código de ética profesional obligatorio.
- Formación de un colegio profesional de seguridad privada que garantice la calidad del servicio y la dignificación del oficio.

El futuro de la seguridad privada no solo dependerá de su capacidad de adaptación, sino de su transformación integral. Un sector que adopte la tecnología, refuerce su marco legal, profesionalice su recurso humano y se dote de una identidad homogénea tendrá el potencial de convertirse en un pilar fundamental de la seguridad moderna. La evolución de la seguridad privada es una necesidad impostergable en un mundo donde las amenazas evolucionan más rápido que las respuestas convencionales.

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

Agente Consultor

El ser agente significa que trabajas en nombre de una empresa (Como un asociado a ella, comercializando todos sus productos)

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

LA MEDIACIÓN EN SEGURIDAD: UNA NUEVA HERRAMIENTA PROFESIONAL PARA LOS DIRECTORES DE SEGURIDAD

Metro Risk

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

En un contexto cada vez más complejo, donde los conflictos vinculados a la seguridad se presentan tanto en entornos públicos como privados, la mediación se consolida como un instrumento eficaz para la resolución pacífica de controversias. En España, esta figura ha ganado peso jurídico con la entrada en vigor de diversas normativas que la legitiman, y hoy se presenta como una salida profesional innovadora y con gran proyección para los Directores de Seguridad.

Mediación y su base normativa

La Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles, establece el marco legal para esta actividad en España. Aunque centrada inicialmente en ámbitos civiles, su espíritu se ha ido extendiendo hacia sectores como el sanitario, el educativo, y más recientemente, el de la seguridad privada, donde los conflictos laborales, contractuales, vecinales o incluso entre empresas de servicios de seguridad, encuentran en la mediación un cauce menos costoso, más ágil y menos hostil que la vía judicial. Asimismo, el Real Decreto 980/2013, que desarrolla dicha ley, establece los requisitos formativos y de inscripción en los registros de mediadores, consolidando un marco profesional para quienes deseen ejercer

El rol del Director de Seguridad como mediador Los Directores de Seguridad son profesionales con formación técnica, experiencia en gestión de crisis y una visión estratégica de la prevención y resolución de conflictos. Estas capacidades los sitúan en una posición privilegiada para actuar como mediadores especializados en seguridad, capaces de intervenir en conflictos como:

- Disputas entre contratistas y empresas de seguridad.
- Problemas entre comunidades de propietarios y servicios de vigilancia.
- Conflictos laborales dentro de empresas del sector.
- Desacuerdos entre clientes y proveedores de tecnología de seguridad.

El conocimiento del marco normativo específico (Ley 5/2014 de Seguridad Privada, normativa sobre protección de datos, prevención de riesgos laborales, etc.) permite a estos profesionales intervenir con rigor y eficacia, ofreciendo soluciones con alto grado de aceptación por las partes implicadas.

La Ley Orgánica 1/2025, de 2 de enero, de medidas en materia de eficiencia del Servicio Público de Justicia. Es una oportunidad tal como la figura de Perito Judicial conforme la LEC y LECRIM , pueda tener profesionales especializados al servicio de la justicia como mediadores en Seguridad. Dentro de la Mediación Civil , familiar y Mercantil , en definitiva en la resolución de conflictos.

Una salida profesional desde ADISPO: Turno de Peritos Judiciales Desde la Asociación de Directores de Seguridad Privada —ADISPO— se ha impulsado la creación de una plataforma de visibilización, formación y acreditación para los profesionales interesados en esta vía: el Turno de Peritos Judiciales disponible en www.peritajes.adispo.es. Este turno no solo contempla la actuación como perito judicial en el ámbito de la seguridad, sino que también abre la puerta al ejercicio como mediador especializado, integrando conocimientos técnicos y jurídicos con habilidades de negociación y gestión del conflicto.

El acceso a este turno se convierte así en una salida profesional complementaria para muchos directores de seguridad que desean ampliar su campo de actuación más allá de los tradicionales entornos operativos o de consultoría.

Conclusión: una profesión en evolución La mediación aplicada a la seguridad no solo es una realidad jurídica reconocida, sino una oportunidad creciente para quienes entienden la prevención y resolución de conflictos como parte esencial de su misión profesional. Desde ADISPO, apostamos por seguir generando espacios de formación, especialización y acreditación que contribuyan a consolidar esta figura en el ecosistema de la seguridad integral y corporativa en España. Porque el futuro de la seguridad también pasa por el diálogo, la profesionalización y la justicia alternativa

Mtro. Francisco Javier González Fuentes

PROFESIONES Y PERSONAL MÁS ALLÁ Y EN LA NORMATIVA DE SEGURIDAD PRIVADA

Metro Risk

José Ignacio Olmos Casado
Presidente AEAS

Para los profesionales, y en general para todos los ciudadanos, la seguridad, además de ser un valor esencial en cualquier aspecto de la vida en sociedad, se plasma a su vez en el ordenamiento jurídico en el artículo 17 de la Constitución, el cual alude también al derecho a la libertad. No es casualidad que aparezcan juntos ambos derechos, y es manida la expresión "no hay libertad sin seguridad y no hay seguridad sin libertad"; seguramente es verdad.

Esa seguridad, pública o privada, apellidos de un mismo sustantivo esencial, se presta bien por Fuerzas y Cuerpos de Seguridad y sus agentes en un caso, bien a través de empresas de seguridad (prestando servicios) y de su personal (además del caso de los detectives privados y, en ocasiones, los guardas rurales). Pero más allá de esto, existen figuras, además de en la propia normativa de seguridad privada, en otros contextos, públicos o privados.

Operadores de Centrales Receptoras de alarma Este personal, que presta su servicio en las centrales receptoras de alarma (CRA), tanto de empresas de seguridad como de uso propio, no se encuentra entre las profesiones de seguridad privada. En la actual Ley 5/2014 aparecen en el artículo 19.1 c) (también en el Convenio colectivo de empresas de seguridad) de igual manera que los ingenieros y los técnicos de las empresas de seguridad, como personal acreditado, que no habilitado. Es decir, este personal deberá obtener algún tipo de acreditación, que previsiblemente deberá ser regulada en normativa de desarrollo tanto en su forma como contenidos formativos, carga lectiva, etc.

Particularmente nos centramos en los operadores por ser una figura que venía desempeñando sus cometidos en el ámbito de la seguridad privada. Este personal, no es personal de seguridad privada, tiene únicamente la formación para sus cometidos que su empresa contratante haya querido darles (se lo exige la Orden INT 316/2011) y pueden, por ejemplo, desconectar nuestros sistemas de alarma o tener acceso a nuestras contraseñas, todo ello sin certificado de penales alguno. No parece lo ideal…

Como consecuencia de ello en el anteproyecto de la actual Ley de Seguridad Privada aparecía un artículo especificando que las funciones de recepción, verificación no personal y transmisión a las Fuerzas y Cuerpos de Seguridad de las alarmas se prestarían exclusivamente por vigilantes de seguridad. Eso sí parecía lo ideal, pero finalmente no pudo llevarse a término por algunas dificultades: -

- Gran parte de los operadores son personal discapacitado (algunas CRA son incluso centro especial de empleo) y no podrían habilitarse como vigilantes, debiendo ser despedidos.
- El coste de esos despidos en las plantillas, además de suponer desempleo para personas pertenecientes a colectivo de difícil inserción profesional, supondría pérdidas importantes a los empresarios, haciendo peligrar empresas.

Finalmente en el último párrafo del artículo 32 de la actual ley 5/2014 se establece la posibilidad de que los vigilantes de seguridad puedan realizar las funciones de los operadores. Problema por tanto aún no terminado de resolver…

Figuras de seguridad fuera de la normativa de seguridad privada Al margen, al menos de momento, de la normativa que regula la seguridad privada en España, existen diversas figuras cuyo común denominador es realizar funciones de seguridad en el ámbito normativo del Ministerio de Fomento.

Sin ánimo de extendernos en demasía, pues disponemos aquí de un espacio limitado, mencionaremos en el ámbito de la seguridad de la aviación civil las figuras del "Responsable de seguridad aérea AVSEC-RA" (Agente acreditado) y "Responsable de seguridad aérea AVSEC-KC" (Expedidor conocido), cuya principal responsabilidad es la aplicación del programa de seguridad en cada ubicación, analizando riesgos, gestionando al equipo de vigilancia, supervisando formación y otros similares; es decir, siendo personas fuera de la seguridad pública, pues pertenecen a entidades tales como compañías logísticas por ejemplo, realizan las funciones establecidas en la Ley de seguridad privada para los directores de seguridad fundamentalmente (artículo 36). Sería, por tanto, exigible a este personal dicha habilitación de seguridad privada, de la cual carece en la práctica un porcentaje muy significativo y, sobre las cuales, no cabría ni siquiera la delegación de funciones del director de seguridad por carecer de ninguna experiencia en seguridad pública o privada, como establece la normativa al respecto.

AEAS
Asociación Española de Auditores de Seguridad

En base a esto ya se interpeló a la Unidad Central de Seguridad Privada, que en su informe 2013/094 trató de justificar esta situación, no sabemos muy bien debido a qué motivos, con una respuesta que oscila entre el error al pensar que tiene que ver con el Departamento de Seguridad de AENA (último párrafo) cuando la figura ejerce en compañías privadas, y la ineptitud, pues no hay manera de dar la vuelta por mucho que nos empeñemos al artículo 58.1 a) de la Ley, que califica como infracción muy grave "El ejercicio de funciones de seguridad privada para terceros careciendo de la habilitación o acreditación necesaria" y de la misma manera el 59.1 h) "La contratación o utilización a sabiendas de personas carentes de la habilitación o acreditación necesarias para la prestación de servicios de seguridad".

En el ámbito portuario existen aún más figuras similares con funciones diversas: Oficial de protección del puerto, oficial de protección de la compañía, oficial de protección del buque, oficial de protección de la instalación portuaria, cuyos nombres nos dan ya la idea de las funciones que realizan. Más de lo mismo. Viendo esto, como profesional de la seguridad privada y como jurista, tengo que acordarme del hincapié que hace la propia Unidad Central de Seguridad Privada en la colaboración y de que dentro de Red Azul exista un programa operativo para controlar el intrusismo profesional. No hacen falta más comentarios.

Personal de seguridad en el ámbito público? Como cierre de estas breves reflexiones me vienen a la cabeza también figuras que se han ido estableciendo recientemente en algunas ciudades, dependiendo fundamentalmente de los ayuntamientos, como puedan ser los agentes cívicos y los serenos (en otro contexto podría hablarse del personal de orden y control para la admisión a recintos). Estas figuras, aunque parecen tener bien definido su estatus fuera de la seguridad ya que velan por el civismo, atienden emergencias y no tienen poder coercitivo, se mueven en un ámbito muy próximo y no están exentas de polémica.

El sereno, como figura tradicional vigilaba las calles entre otras funciones y disponía de su famoso chuzo como elemento defensivo. Las figuras actuales, aunque carecen de elementos defensivos, van conectados con radios o teléfonos móviles a la policía local. Y yo me pregunto, ¿por qué un trabajador de una empresa contratada por un ayuntamiento patrulla una calle y avisa a la policía local y un auxiliar de servicios en turno de noche en una nave de un polígono industrial que, si ve un delito avisa a las fuerzas de seguridad, es sancionado por las Unidades territoriales de seguridad privada entendiendo que realiza funciones de vigilancia careciendo de la habilitación correspondiente?

La Ley Orgánica 2/86 de Fuerzas y Cuerpos de Seguridad reza en su artículo 1.4 "El mantenimiento de la seguridad pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad"; ya sabemos todos por lo que expresa el artículo siguiente de esa misma Ley cuáles son esos cuerpos, y no se citan estas figuras que estamos tratando. Por poner un ejemplo reciente leo en la edición digital de La Vanguardia del pasado 17 de enero en una noticia cuyo titular es "Santa Coloma de Gramenet y Premià de Dalt rescatan la figura del sereno" y en la que aparece un párrafo entrecomillado de la alcaldesa de Santa Coloma, Nuria Parlón, que dice: "La seguridad no sólo está vinculada a la policía y a la prevención del delito, sino que se trata de generar entornos amables".; es decir, la alcaldesa vincula esta figura a la seguridad, figura por cierto que hará por la noche las funciones que por el día hacen los agentes cívicos.

En Premiá de Dalt por el contrario, este servicio sí lo prestan vigilantes de seguridad privada; dos soluciones para una misma prestación. Añado en este punto que echo de menos a las asociaciones de la Guardia Civil y sindicatos policiales manifestando su opinión contraria al respecto, como sí hicieron al aprobarse la Ley 5/2014 de seguridad privada respecto a algunos servicios a realizarse por ésta como en los centros penitenciarios y servicios en vía pública; quizás su silencio radica en que los cuerpos más afectados sean los de las policías locales.

En el artículo de La Vanguardia que citaba más arriba leo también que entre las funciones de los serenos de Santa Coloma están asistir a personas que tienen miedo a bajar la basura o, según aparece respecto de la misma noticia en la web de Antena 3, comprobar que los comercios están bien cerrados o acompañar a personas que vayan a retirar dinero de cajeros automáticos. No sé si comprobar instalaciones podríamos encuadrarlo en un servicio de vigilancia discontinua de los que se mencionan en el artículo 41.1 e) de la actual Ley de seguridad privada, pero pocas dudas me quedan, ni a mí, ni a nadie, de que el acompañamiento, defensa y protección de una persona al cajero o bajar la basura es la función atribuida a los escoltas privados en el artículo 33.1 de la misma Ley, y por tanto, como ya hemos visto anteriormente, el sereno realiza conducta tipificada como infracción muy grave, lo mismo que el ayuntamiento. La pregunta sería ¿por qué siendo estos hechos públicos y notorios no actúa de oficio la Unidad Central de Seguridad Privada? Yo pensaba que una de sus funciones era ejercer como unidad de control… En definitiva, como es habitual en nuestros artículos, pretendemos más que exponer una lección magistral que siente cátedra, incitar al debate y la reflexión para la mejora, por lo que esperamos se susciten muchos y provechosos comentarios y, por qué no, se muevan conciencias

José Ignacio Olmos Casado

Gregorio Duro
Tecnico en licitaciones y Proyectos

APROXIMACIÓN AL CONCEPTO DE ENTROPÍA EN EL ENTORNO DE UN ANÁLISIS DE RIESGOS

En el artículo de este mes, quiero abordar el concepto de entropía en un análisis de riesgos. En este entorno, la entropía se refiere a la medida de incertidumbre o imprevisibilidad asociada a los eventos de riesgo dentro de un sistema. Cuanto mayor sea la entropía, mayor será la dispersión o variabilidad de los riesgos, lo que implica que los eventos son más difíciles de predecir y gestionar.

La entropía es un concepto que originalmente proviene de la termodinámica, donde se utiliza para medir el desorden o la dispersión de energía en un sistema. Fue introducido por el físico Rudolf Clausius en 1865 para describir cómo la energía en un sistema tiende a dispersarse y cómo este desorden aumenta a medida que un sistema se acerca al equilibrio. Posteriormente, el concepto de entropía fue adaptado por Claude Shannon en 1948 en el campo de la teoría de la información, donde la utilizó para cuantificar la incertidumbre o la cantidad de información necesaria para describir un evento o un mensaje. En este contexto, la entropía mide el resultado que se genera al observar un evento aleatorio ayudando a entender su imprevisibilidad y su variabilidad. Así, la entropía se ha extendido a diversas áreas, como la informática y el análisis de riesgos, donde sigue representando una medida de incertidumbre o aleatoriedad dentro de un sistema.

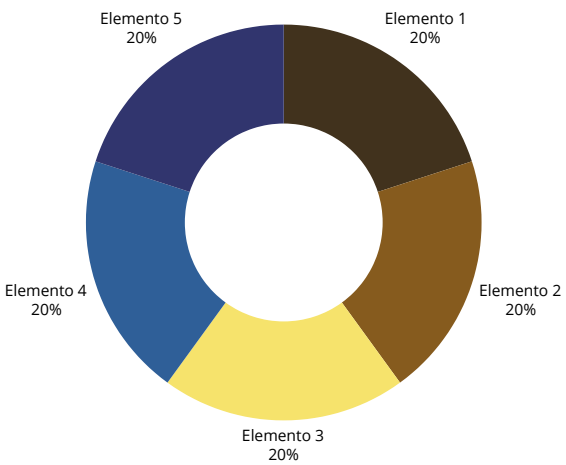
La entropía se calcula generalmente utilizando la fórmula de Shannon, que evalúa las probabilidades de manifestación de distintos eventos y permite cuantificar la cantidad de información necesaria (datos) para reducir la incertidumbre sobre los posibles riesgos, ayudando así en la toma de decisiones sobre cómo mitigar o gestionar esos riesgos. Integrar el concepto de entropía en un análisis de riesgos implica comprender cómo se refleja la incertidumbre o el desorden inherente a un conjunto de eventos o posibles resultados dentro de un sistema o entorno. La entropía permite cuantificar el grado de imprevisibilidad que existe en la ocurrencia de ciertos riesgos, lo cual resulta importante para gestionar la respuesta ante posibles amenazas. En este contexto, la entropía se calcula tomando en cuenta las probabilidades asociadas a cada riesgo, utilizando la fórmula de Shannon, que evalúa la dispersión o variabilidad en los posibles eventos, indicando cuánta información es necesaria para predecir con certeza el resultado.

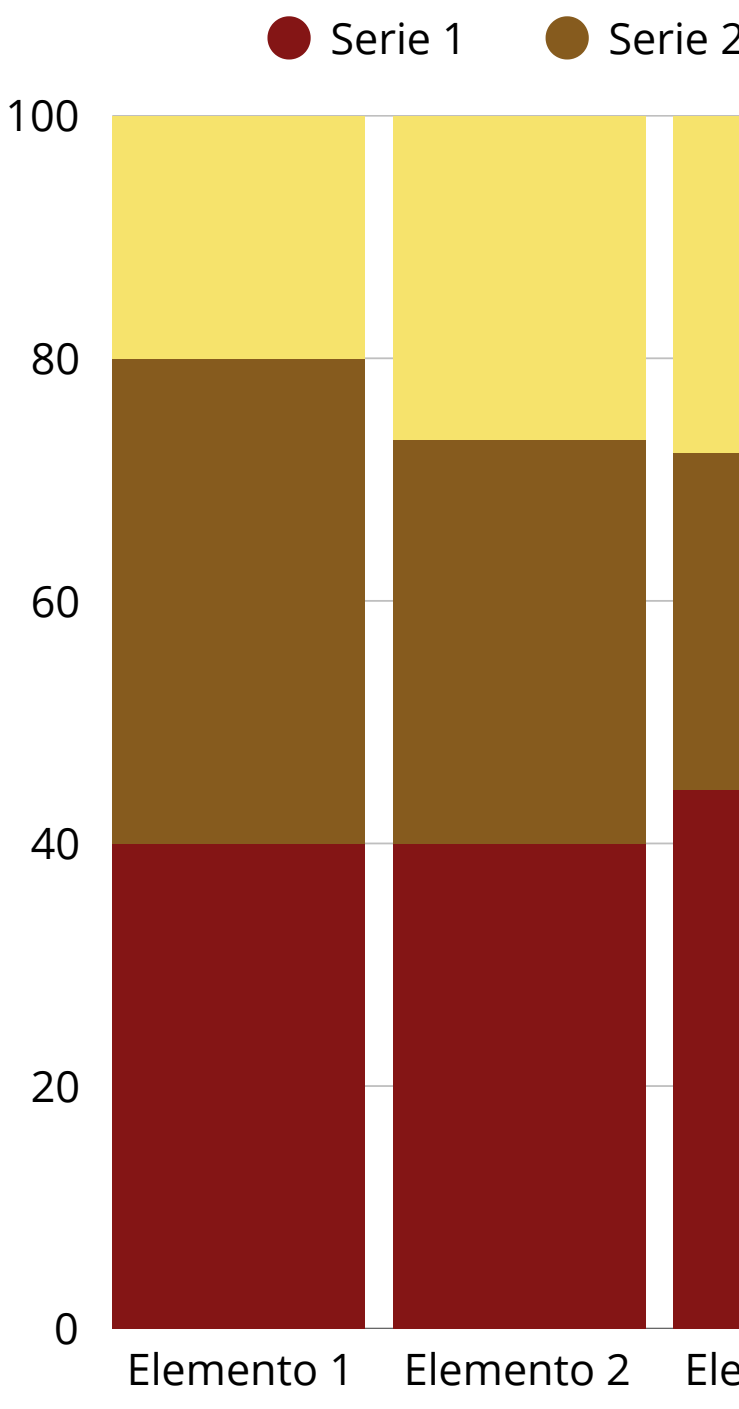
El cálculo de la entropía aplicado a un evento de riesgo se basa en la idea de medir la incertidumbre o el grado de desorden asociado a los posibles resultados de dicho evento. En un escenario de análisis de riesgos, como una evaluación de intrusión a un edificio, por ejemplo, se identifican distintos factores y variables (como el acceso por la puerta principal, por la ventana, por la cubierta o mediante un acceso no autorizado) y se asignan (en un cálculo previo) probabilidades porcentuales de ocurrencia a cada uno de ellos. Cuando un sistema presenta alta entropía, significa que los eventos de riesgo son extremadamente variados y la distribución de probabilidades entre ellos es casi uniforme, lo que resulta en una incertidumbre considerable sobre cuál de ellos se manifestará en un momento dado. Ello conlleva a que no existe un único riesgo predominante, sino múltiples amenazas con una probabilidad relativamente similar de ocurrir, lo que complica la identificación y priorización de medidas de mitigación. En estos casos, la gestión de riesgos debe ser abordada con un enfoque integral y flexible, que contemple la implementación de estrategias diversificadas que sean capaces de responder a una amplia gama de escenarios y contingencias, ya que la variabilidad inherente exige la preparación para eventos imprevistos y la adaptación constante de las medidas de seguridad. Por el contrario, cuando un sistema presenta baja entropía, la concentración de probabilidades en uno o pocos eventos específicos hace que estos sean más predecibles, permitiendo a los responsables de la gestión de riesgos focalizar sus esfuerzos y recursos en mitigar aquellas amenazas que tienen una mayor incidencia, optimizando así la asignación de recursos y reduciendo la incertidumbre en la toma de decisiones. En este contexto, la entropía se contempla como una herramienta estratégica fundamental, ya que al cuantificar la incertidumbre del sistema o entorno, proporciona una base objetiva para diseñar e implementar medidas preventivas, correctivas y de respuesta ante incidentes, facilitando la priorización de acciones y permitiendo a los equipos de seguridad anticipar y gestionar de manera más efectiva los riesgos, tanto en entornos con alta complejidad como en aquellos donde los riesgos son más específicos y concentrados.

El cálculo de la entropía en el análisis de riesgos no solo orienta la toma de decisiones a corto plazo, sino que también resulta fundamental para la formulación de planes estratégicos a largo plazo, al poner de manifiesto tendencias y patrones en la distribución de riesgos, lo que posibilita la actualización y mejora continua de las estrategias de seguridad en un entorno dinámico y en constante evolución. Al integrar la entropía en el análisis de riesgos, se logra identificar no solo cuáles son los riesgos más probables, sino también se obtiene una visión clara de lo dispersos o concentrados que están dichos riesgos, permitiendo así una gestión de recursos más eficiente y una planificación integral que abarca tanto la prevención como la mitigación de amenazas. Este enfoque cuantitativo proporciona una medida tangible de la incertidumbre y el desorden inherentes a un sistema, facilitando la comprensión de la cantidad de información necesaria para describir los fenómenos evaluados y cuantificar el grado de previsibilidad o caos en los eventos potenciales. Por ello, la entropía se convierte en una herramienta esencial para anticipar escenarios futuros, optimizar la asignación de recursos y desarrollar respuestas adaptables, contribuyendo de manera decisiva a la resiliencia del sistema y a la capacidad para hacer frente de forma proactiva a la complejidad y a la variabilidad de los riesgos.

Quiero expresar mi agradecimiento a Metrorisk por compartir mensualmente artículos de carácter técnico que contribuyen a la 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.

GOBERNANZA PARTICIPATIVA & CPTED

La prevención social de las violencias y la delincuencia es un desafío complejo que requiere un enfoque integral y colaborativo. En este contexto, la gobernanza participativa, entendida como la involucración activa de la ciudadanía y diversos actores sociales en el diseño, implementación y evaluación de políticas públicas, se erige como un pilar fundamental para el éxito de estas estrategias. Al integrar los principios de la Metodología Prevención del Delito mediante el Diseño Ambiental (CPTED), se potencia aún más la efectividad de las acciones, creando entornos más seguros y fomentando la cohesión social.

La gobernanza participativa implica la apertura de espacios de diálogo y colaboración entre el gobierno, la sociedad civil organizada, el sector privado, la academia y los propios ciudadanos. Esta participación asegura que las políticas y acciones implementadas respondan de manera más efectiva a las necesidades y realidades locales.

CPTED, por su parte, es una estrategia de prevención del delito que se centra en modificar el entorno físico para reducir las oportunidades de que ocurran delitos y el miedo a la delincuencia. Se basa en la idea de que un diseño ambiental adecuado puede influir en el comportamiento de las personas, disuadiendo a los posibles infractores y aumentando la sensación de seguridad de los ciudadanos.

La sinergia entre la gobernanza participativa y CPTED es poderosa. La participación ciudadana permite identificar de manera más precisa los puntos críticos y las características del entorno que contribuyen a la inseguridad, información crucial para la aplicación efectiva de los principios del CPTED. A su vez, la implementación de estrategias CPTED se puede generar un impacto positivo visible y tangible en la seguridad de las comunidades, lo que a su vez fortalece la confianza en las instituciones y fomenta una mayor participación ciudadana en los procesos de gobernanza.

La combinación de la gobernanza participativa y CPTED en las acciones de prevención social de violencia y delincuencia ofrece múltiples beneficios:

- Políticas más informadas y efectivas: la participación ciudadana aporta conocimiento local y experiencias valiosas que enriquecen el diagnóstico de los problemas de seguridad y la formulación de soluciones basadas en el CPTED.
- Mayor apropiación y sostenibilidad de las intervenciones: cuando las comunidades participan en el diseño e implementación de las mejoras en su entorno, se sienten más dueñas de los proyectos, lo que aumenta la probabilidad de su cuidado y sostenibilidad a largo plazo.
- Reducción del miedo y aumento de la seguridad: la aplicación de principios CPTED, como la mejora de la iluminación, la visibilidad y la delimitación de espacios, reduce las oportunidades para el delito y aumenta la percepción de seguridad de los habitantes y usuarios del territorio, validando la importancia de su participación.
- Fortalecimiento del tejido social y la confianza: los procesos participativos fomentan la colaboración y la comunicación entre vecinos y autoridades, fortaleciendo el tejido social y reconstruyendo la confianza en las instituciones.
- Transparencia y rendición de cuentas: la participación ciudadana exige transparencia en la gestión de los recursos y la rendición de cuentas por parte de las autoridades responsables de implementar las estrategias de prevención.
- Desarrollo de capacidades comunitarias: la participación en proyectos CPTED empodera a los ciudadanos, desarrollando sus habilidades para identificar problemas, proponer soluciones y colaborar en la mejora de su entorno.

Para integrar eficazmente la gobernanza participativa y CPTED, se pueden implementar diversos mecanismos:

- Diagnósticos participativos: involucrar a los residentes en la identificación de los puntos negros de inseguridad y las características del entorno que contribuyen a la delincuencia.
- Talleres de diseño participativo: organizar sesiones donde ciudadanos, expertos en CPTED y autoridades locales colaboren en el diseño de soluciones ambientales para mejorar la seguridad.
- Presupuestos participativos: destinar una parte del presupuesto público para proyectos de mejora del entorno propuestos y priorizados por los ciudadanos, aplicando principios CPTED.
- Observatorios ciudadanos de seguridad: crear espacios donde los ciudadanos puedan monitorear la implementación de las estrategias CPTED y evaluar su impacto en la seguridad.
- Campañas de sensibilización y educación: informar a la sociedad sobre los principios CPTED y la importancia de su participación en la prevención del delito y violencias.
- Mesas de trabajo intersectoriales: facilitar la colaboración entre autoridades locales, estatales, federales, policía, urbanistas, arquitectos, organizaciones de la sociedad civil y residentes para abordar los problemas de seguridad desde una perspectiva integral, con prevención y de

Si bien la integración de la gobernanza participativa y CPTED es prometedora, es importante considerar los siguientes desafíos:

- Garantizar la participación inclusiva: es crucial asegurar que todos los grupos de la comunidad, incluyendo los más vulnerables, tengan la oportunidad de participar en los procesos.
- Superar la desconfianza y el escepticismo: en algunos contextos, puede haber desconfianza hacia las instituciones, lo que dificulta la participación ciudadana. Es necesario construir puentes de confianza a través de la transparencia y la comunicación efectiva.
- Gestionar las expectativas: es importante comunicar claramente los alcances y limitaciones de las intervenciones CPTED y los procesos participativos.
- Sostenibilidad a largo plazo: asegurar la continuidad de los procesos participativos y el mantenimiento de las mejoras implementadas requiere un compromiso a largo plazo de todas las partes involucradas.
- Adaptación al contexto local: las estrategias CPTED deben adaptarse a las características específicas de cada comunidad, y la participación social es fundamental para asegurar esta adecuación.

La gobernanza participativa, al integrarse con los principios CPTED, se convierte en una herramienta poderosa para fortalecer las acciones de prevención social de las violencias y la delincuencia. Al involucrar activamente a la ciudadanía en la transformación de su entorno, se crean espacios más seguros, se fortalece el tejido social, se legitiman las políticas públicas y se construye una cultura de seguridad ciudadana más sólida y sostenible.

La clave reside en diseñar e implementar mecanismos participativos efectivos que permitan aprovechar el conocimiento y la experiencia de la comunidad para crear entornos que disuadan el delito y promuevan la convivencia pacífica. En todo contexto urbano, esta sinergia puede marcar una diferencia significativa en la construcción de comunidades más seguras y resilientes.

INTERNATIONAL
ICA
CPTED ASSOCIATION

LA OKUPACION. NOTAS DE LA ENTREVISTA EN COPE

Metro Risk

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

La okupación es algo que cada vez preocupa más a los propietarios. Así lo confirma Antonio Cozano, gerente de Cofer Seguridad, una empresa dedicada a la vigilancia y protección de bienes y servicios.

En una entrevista para COPE asegura que en los últimos meses la contratación de alarmas en ciudades como Málaga ha crecido de manera exponencial.

El experto indica qué tipo de casas son el objetivo de los okupas en España y ha detallado en esta radio su manera más frecuente de actuar.

El tipo de casas que son el objetivos de los okupas en España Antonio Cozano asegura que la gran mayoría de okupaciones «no se producen cuando alguien sale hacer la compra». El experto en seguridad explica cuáles son sus objetivos principales: **«Los okupas aprovechan para entrar en promociones nuevas antes de que se entreguen. Suelen ser viviendas que están pendientes de entrega».**

No obstante, el gerente de Cofer Seguridad avisa de que «también se dan casos en segundas viviendas». **«Vienen un par de meses en verano y no están el resto del año. Al no contar con sistemas de alarma, lo que ocurre es que como uno no percibe esa okupación, se encuentra con que no puede pedir que se marchen»,** comenta.

¿COMPLIANCE DE PAPEL O COMPLIANCE REAL?

Metro Risk

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

Sí, así lo vivimos quienes nos dedicamos a esto.
En muchas reuniones, nos llaman "asustadores profesionales".

Pero sinceramente, no me gusta sensibilizar ni divulgar desde el miedo.
Los que me conocéis lo sabéis.

Sin embargo, hoy te traigo una historia
—ficticia, pero más real de lo que parece—.
Una historia que va más allá de la mal llamada "cultura del miedo"...

Para que veas la realidad.

Luis Avila Suarez comparte una sentencia que lo deja claro:
los tribunales ya no se conforman con programas de compliance "de escaparate".

La STSJ CAT 9703/2024 marca un precedente:
una empresa de transporte intentó levantar una prohibición de contratar, pero su programa de compliance no convenció.

¿Por qué?
No supo demostrar lo que realmente importa:
que su cultura de cumplimiento es genuina y que su formación es efectiva.

Déjame contarte una historia.
Hace años, una empresa (llamémosla "Transporte Seguro")
decidió implementar su programa de compliance después de una sanción.

Lo hizo rápido, con asesoría externa y documentos bien estructurados.
Cumplía con todos los requisitos... en teoría era "casi perfecto"

✔ Tenía un código ético.
✔ Había realizado algunas formaciones.
✔ Contaba con un mapa de riesgos y un canal de denuncias.

Pero, cuando llegó la auditoría, encontraron un problema:

❌ No podían demostrar que sus empleados realmente habían sido formados.
❌ No había pruebas de evaluación o impacto real.
❌ El órgano de compliance no tenía formación específica en derecho de la competencia.

📌 Resultado: Su compliance fue visto como una simple formalidad.
📌 Consecuencia: Los tribunales no lo pasaron por alto y la sanción se mantuvo.

💡 Lección clave:
Compliance NO es un papel, ni un checklist, ni una mera formalidad.

SI es cultura, es prevención, es compromiso.
Y si no puedes demostrarlo, es como si no existiera.

¿Cómo evitar que tu programa de compliance sea solo un trámite?

✅ **Mide y prueba la formación: No basta con impartir cursos, hay que demostrar que han sido comprendidos y aplicados.**
✅ **Capacita al órgano de cumplimiento: Si no tienen formación especializada en la materia, ¿cómo van a liderar el cambio?**
✅ **Integra compliance en la cultura organizacional: Si tus empleados lo ven como una carga y no como un beneficio, algo falla.**
✅ **No te limites a asesores externos: Compliance no es solo una inversión en consultoría; requiere talento interno bien preparado.**

📢 **Los tribunales están poniendo los puntos sobre las íes.**

¿Lo hará también tu empresa?

C2C Consultoría&Compliance

CONSULTORÍA & COMPLIANCE

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

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

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

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

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

MEDIDAS PARA LA SEGURIDAD EN LA NUBE Y EN ENTORNOS HÍBRIDOS

Metro Risk

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

La adopción de servicios en la nube ha traído consigo ventajas significativas en términos de flexibilidad, escalabilidad y eficiencia, pero también ha introducido nuevos desafíos de seguridad. Por ello, es crucial establecer normas y prácticas que aseguren la protección de nuestros datos en los entornos híbridos que conforman la nube. A continuación, se presentan algunos ejemplos prácticos que pueden implementarse fácilmente:

Modelo de Responsabilidad Compartida Los proveedores de servicios en la nube son responsables de la seguridad de la infraestructura subyacente, mientras que el cliente debe gestionar la seguridad de los datos, las aplicaciones y las configuraciones. Por lo tanto, es fundamental comprender y aplicar este modelo para asignar correctamente las responsabilidades. Este modelo constituye la base de una estrategia de seguridad eficaz en la nube.

Gestión de Accesos e Identidades (IAM) Implementar políticas de IAM robustas para controlar quién tiene acceso a qué recursos, utilizando autenticación multifactor (MFA) y principios de mínimo privilegio.

Cifrado de Datos Ante el aumento de estafas y robos de información, debido a la vulnerabilidad de los sistemas y a la falta de precaución del usuario, es imprescindible adoptar el cifrado de datos como práctica habitual. Se recomienda:

- Cifrar datos en tránsito y en reposo.
- Utilizar claves de cifrado robustas y gestionarlas de forma segura.
- Monitorización y Gestión de Incidentes
- Establecer sistemas de monitorización continua para detectar actividades sospechosas y responder rápidamente a incidentes de seguridad.

Configuraciones Seguras y Automatización Automatizar la aplicación de configuraciones de seguridad para garantizar la consistencia y reducir errores humanos.

Seguridad en Entornos Híbridos Los entornos híbridos, que combinan infraestructuras locales con servicios en la nube, añaden una capa adicional de complejidad a la gestión de la seguridad:

- Integración Segura de Entornos: Asegurar la comunicación segura entre entornos locales y en la nube.
- Consistencia en Políticas y Controles: Aplicar políticas de seguridad uniformes en todos los entornos.
- Gestión de Vulnerabilidades y Parches: Mantener los sistemas actualizados con los últimos parches de seguridad.
- Cumplimiento Normativo y Gestión de Datos: Garantizar el cumplimiento de las regulaciones de protección de datos.
- Automatización y Orquestación: Utilizar herramientas de automatización para gestionar la seguridad de manera eficiente.

Tendencias y Desafíos Actuales en Seguridad en la Nube y en Entornos Híbridos Ciberseguridad

Basada en Inteligencia Artificial y Machine Learning: La aplicación de estas tecnologías permite detectar comportamientos anómalos y responder de forma proactiva en tiempo real, mejorando la capacidad de defensa en entornos híbridos. **Microsegmentación**: Dividir la red en segmentos pequeños y seguros para limitar el movimiento lateral ante brechas de seguridad. Esto es especialmente importante en entornos de nube híbrida, donde los niveles de exposición varían. **Zero Trust en la Nube Híbrida:** Adoptar una arquitectura Zero Trust, donde ningún usuario o dispositivo es de confianza por defecto, reforzando la seguridad mediante la verificación continua en ambos entornos. **Gestión de Identidades y Accesos Unificada**: Integrar la administración de accesos en ambos entornos, utilizando soluciones que centralicen el control y la auditoría de los accesos a la información crítica. La seguridad en la nube y en entornos híbridos es un tema dinámico y en constante evolución. Las organizaciones deben enfrentarse a desafíos complejos, que requieren un enfoque holístico que integre prácticas de gestión de identidades, cifrado, monitorización y automatización.

Mantenerse actualizado con las amenazas y adoptar un marco de seguridad unificado es esencial para proteger la infraestructura y los datos. Un enfoque unificado no solo fortalece la seguridad, sino que también potencia la agilidad y eficiencia operativa, elementos clave para la transformación digital de las organizaciones

BIG DATA Y SEGURIDAD PRIVADA: ¿ALIADO O RIESGO LEGAL?

Metro Risk

Rosa Fernandéz

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

ASUNTO: DERECHOS DIGITALES Y TECNOLOGÍA

Hoy vamos al lío con uno de esos términos que se instaló en nuestras vidas pero que ignoramos el alcance que puede tener para nuestra intimidad o privacidad. Señoras y Señores con ustedes ¡el Big Data!.

Big Data se refiere al procesamiento y análisis de grandes volúmenes de datos que se generan de forma masiva y a gran velocidad. Estos datos pueden provenir de múltiples fuentes, como redes sociales, cámaras de videovigilancia, dispositivos móviles, registros financieros y sensores inteligentes. Lo que hace especial al Big Data no es solo la cantidad de información, sino su capacidad para identificar patrones, predecir comportamientos y tomar decisiones automatizadas en sectores como la seguridad privada, la ciberinteligencia y la vigilancia. Sin embargo, su uso indebido puede vulnerar derechos fundamentales, por lo que debe cumplir con regulaciones como el RGPD para evitar el abuso de la privacidad y la discriminación.

El Big Data se ha convertido en una herramienta esencial en múltiples sectores, ya que permite procesar y analizar grandes volúmenes de información en tiempo real. En seguridad privada, se usa para identificar patrones de comportamiento en videovigilancia, aplicar reconocimiento facial y realizar investigaciones mediante OSINT. En el sector financiero, los bancos lo emplean para detectar fraudes y evaluar riesgos crediticios, mientras que las grandes plataformas tecnológicas lo utilizan para personalizar anuncios y predecir tendencias de consumo. En transporte y logística, ayuda a optimizar rutas y mejorar la eficiencia operativa, y en sanidad, permite predecir brotes epidémicos y personalizar tratamientos médicos. También en el comercio electrónico, el Big Data se aplica para analizar hábitos de compra y gestionar el inventario de manera eficiente. Sin embargo, su uso implica riesgos legales y éticos, por lo que las empresas deben garantizar el cumplimiento de normativas como el RGPD, protegiendo siempre la privacidad y los derechos de los ciudadanos.

⚖️ **El RGPD y la Protección de Datos en Seguridad Privada El Reglamento General de Protección de Datos (RGPD) es la normativa que regula el uso de información personal en Europa. Para el sector de seguridad privada, establece que no se puede recopilar y procesar datos sin justificación legal clara y sin respetar los derechos de los ciudadanos.**

¿Qué riesgos legales tiene el uso de Big Data en Seguridad?

PERFILES DE RIESGO SIN CONSENTIMIENTO Un aeropuerto usa un algoritmo para clasificar pasajeros en perfiles de riesgo basados en su nacionalidad o comportamiento en redes sociales. Esto puede ser ilegal si no existe una base jurídica clara para el tratamiento de esos datos. **VIGILANCIA MASIVA Y RECONOCIMIENTO FACIAL** Una empresa de seguridad instala cámaras con IA en un estadio de fútbol para detectar hooligans. El problema: Si la tecnología almacena datos biométricos de todos los asistentes sin su consentimiento, se está violando el **RGPD. USO INADECUADO DE OSINT** (Inteligencia de Fuentes Abiertas) Un detective privado usa software de rastreo para analizar los hábitos de un empleado sospechoso de fraude, revisando su geolocalización en redes sociales. Si el análisis no se hace con garantías legales, puede dar lugar a una denuncia por intromisión en la privacidad.

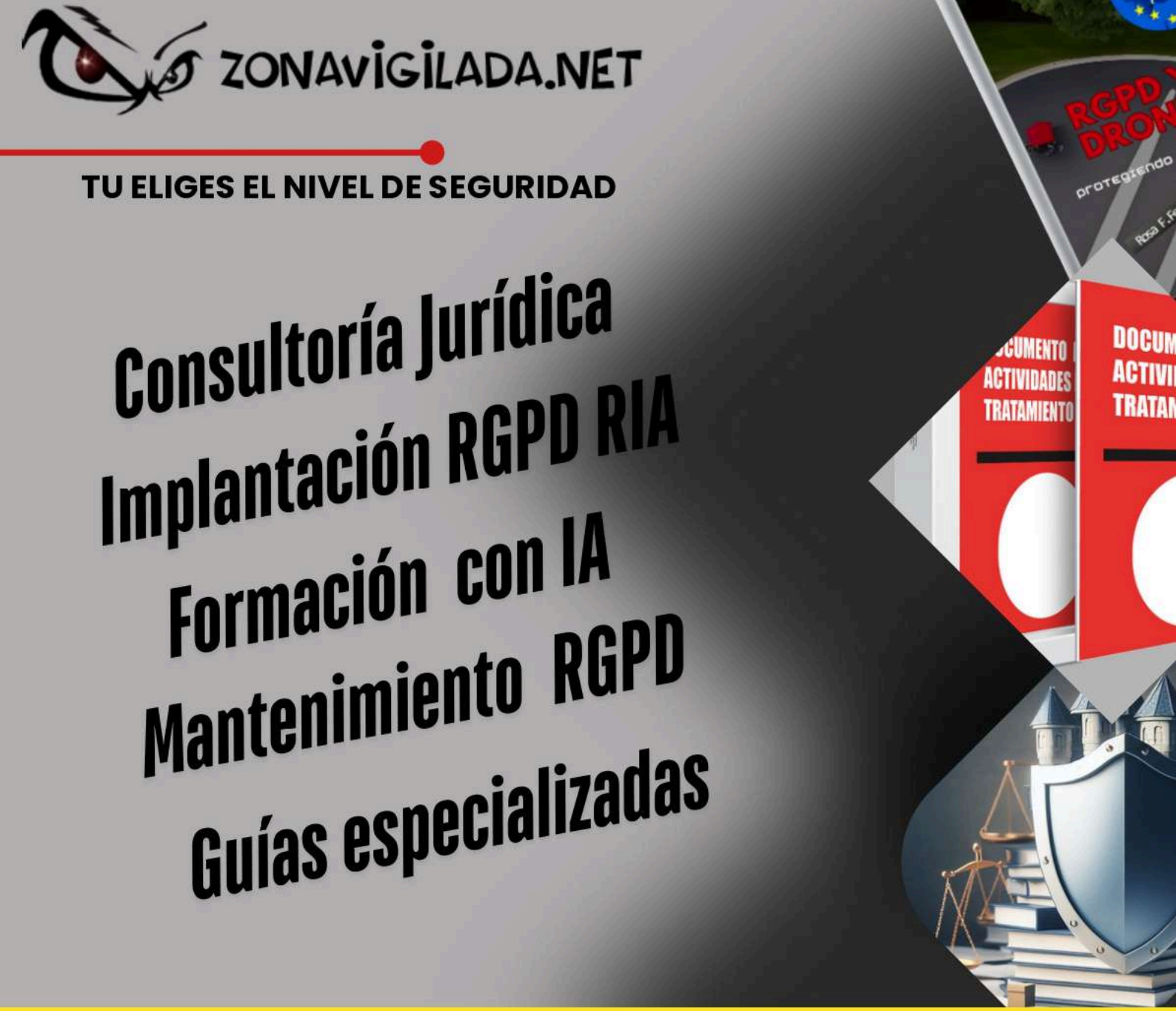
Cómo aplicar el RGPD en Seguridad Privada sin riesgos Las empresas del sector deben adoptar buenas prácticas para el uso de Big Data sin vulnerar derechos. Aquí algunos segurconsejos: Identifica la base legal del tratamiento: Antes de usar cualquier dato personal, pregúntate: ¿Tengo el derecho legal de procesar esta información? Justifícalo en base a interés legítimo o seguridad pública. Minimización de datos: No almacenes información innecesaria.

Si un dato no es imprescindible, bórralo. Consentimiento explícito: Para ciertos tratamientos, como la videovigilancia con reconocimiento facial, debes obtener el consentimiento expreso de las personas o asegurarte de que la base legal está bien definida. Auditoría constante: Revisa periódicamente que los datos que manejas cumplen con la normativa. Evita sorpresas en forma de sanciones o de denuncias de los interesados.

ZONAVIGILADA.NET

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.

ZONAVIGILADA.NET

*+ de 25 años formando a profesionales

LOS RETOS DE LA SEGURIDAD PRIVADA: UN SECTOR ESENCIAL EN BUSCA DE RECONOCIMIENTO

Carlos Serrano
Director de Contenidos de Seguridad y Empleo

La seguridad privada en España ha experimentado una evolución significativa en las últimas décadas, consolidándose como un elemento clave dentro del sistema integral de seguridad. Su presencia en infraestructuras críticas, centros de transporte, grandes eventos y espacios públicos es ya parte del paisaje habitual, desempeñando funciones de prevención, vigilancia y reacción ante situaciones de riesgo. No obstante, a pesar de su consolidación operativa, el sector sigue enfrentándose a desafíos estructurales que limitan su verdadero potencial.

Un sector estratégico, pero infravalorado La entrada en vigor de la Ley 5/2014 de Seguridad Privada representó un avance en el reconocimiento normativo del sector, ampliando funciones y reforzando la colaboración público-privada en materia de seguridad. Sin embargo, este marco legal aún no se ha traducido en una valorización social y económica acorde con la responsabilidad que asumen los profesionales del sector. Actualmente, persisten condiciones laborales por debajo del nivel de exigencia y responsabilidad del puesto, así como situaciones de intrusismo profesional por parte de empresas no habilitadas o servicios encubiertos. Este fenómeno no solo deteriora la imagen del sector, sino que además genera riesgos operativos y jurídicos considerables.

Formación y profesionalización: el eje pendiente La profesionalización del sector sigue siendo uno de los retos más relevantes. Aunque existen requisitos oficiales de acceso y una oferta formativa básica, el dinamismo del entorno actual exige una formación continua, especializada y adaptada a nuevos escenarios de amenaza: ciberseguridad, gestión de crisis, control de accesos mediante tecnologías avanzadas, detección de amenazas no convencionales, uso de drones, y atención a situaciones de alta complejidad social. En este sentido, resulta imprescindible que tanto el sector privado como las administraciones públicas articulen políticas de capacitación continua, incentiven la especialización y promuevan itinerarios profesionales que favorezcan la retención y el desarrollo del talento.

www.seguridadyempleo.com

Reconocimiento institucional y visibilidad pública *El fortalecimiento de la seguridad privada también pasa por un mayor reconocimiento institucional y social. A pesar de su rol preventivo y su impacto directo en la seguridad ciudadana, la figura del vigilante sigue siendo percibida de forma reduccionista por parte de la opinión pública. Esta visión limitada no solo desincentiva las vocaciones, sino que también dificulta la consolidación de una cultura de seguridad compartida. Resulta necesario, por tanto, impulsar campañas de visibilidad, reforzar el papel del sector en los foros de seguridad y establecer mecanismos de interlocución permanentes entre el ámbito público y el privado*

¿POR QUÉ CONTRATAR A UN CONSULTOR COMO DIRECTOR DE SEGURIDAD EXTERNO?

Metro Risk

Abraham Santana Herrera
Director de seguridad. Perito

En un contexto empresarial cada vez más complejo, donde los riesgos asociados a la seguridad física, organizacional y tecnológica aumentan de forma constante, muchas organizaciones se preguntan si es conveniente externalizar el rol del Director de Seguridad. La respuesta es sí, y no sólo es conveniente, sino que, en muchos casos, es una decisión estratégica.

El Director de Seguridad es responsable de supervisar, coordinar y optimizar todos los recursos, procesos y servicios relacionados con la protección de los activos de una organización. Su función va mucho más allá de gestionar la vigilancia física o controlar sistemas de acceso: implica diseñar políticas, prevenir amenazas, evaluar vulnerabilidades y garantizar el cumplimiento normativo en materia de seguridad.

Sin embargo, en muchas empresas, especialmente medianas o con estructuras dinámicas, no siempre es viable incorporar este perfil como parte del equipo interno. Aquí es donde surge la alternativa del consultor externo como Director de Seguridad funcional

Ventajas del Director de Seguridad externo

1. Independencia operativa: Uno de los principales beneficios es la independencia frente a los intereses de terceros. Cuando el Director de Seguridad no forma parte ni de la plantilla de la empresa de seguridad contratada ni del personal interno con posibles conflictos departamentales, su evaluación y toma de decisiones se basa exclusivamente en los intereses del cliente. Esto elimina interferencias y permite auditar de forma objetiva la eficacia del servicio de vigilancia y los sistemas implementados.

2. Mayor control y seguimiento: El consultor actúa como nexo entre la empresa y el proveedor de seguridad. Su labor incluye el seguimiento operativo diario, la evaluación del desempeño del personal de vigilancia, la verificación de cumplimiento de protocolos, y la emisión de informes periódicos con recomendaciones de mejora. Esto proporciona una visión clara, técnica y desinteresada del estado real de la seguridad corporativa.

3. Flexibilidad y especialización: Un consultor externo puede aportar una visión más actualizada y especializada, con conocimientos en normativas, ciberseguridad, CPTED (Prevención del Crimen a través del Diseño Ambiental), protección de infraestructuras críticas y planes de emergencia. Además, su contratación permite una adaptación del servicio según necesidades reales, sin asumir costes fijos o estructuras rígidas.

4. Auditorías e informes imparciales: La elaboración de auditorías internas y externas sobre los procedimientos de seguridad gana en credibilidad cuando es realizada por un profesional ajeno a las partes implicadas. Esta imparcialidad es fundamental para identificar debilidades, mejorar procedimientos y justificar decisiones ante la dirección, aseguradoras o autoridades.

Una fórmula eficiente y estratégica

En definitiva, contar con un consultor como Director de Seguridad externo no sólo es una forma eficiente de gestionar la seguridad de la empresa, sino también una estrategia para garantizar su continuidad operativa, proteger sus activos y cumplir con los requisitos legales y normativos sin caer en conflictos de intereses.

La seguridad no debe depender exclusivamente de quienes prestan el servicio, sino de quien tiene la visión global, técnica y estratégica para dirigirla.

RELACIÓN ENTRE SEGURIDAD Y SEGUROS

Metro Risk

Alina Rubio de las Casas
Experta en Seguros Generales

La relación entre seguridad y seguros es profunda y bidireccional. Ambas disciplinas están interconectadas en la gestión del riesgo y la protección de personas, bienes y activos...

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

A continuación, te explico los puntos clave de esta relación:

1. Gestión del Riesgo
• La seguridad busca prevenir y mitigar los riesgos mediante estrategias, medidas y tecnologías.
• Los seguros se enfocan en la transferencia del riesgo, compensando económicamente los daños cuando ocurren incidentes.

Ejemplo: Un edificio con un sistema de seguridad robusto (cámaras, control de accesos, alarmas) reduce el riesgo de robo o daño, lo que puede traducirse en primas de seguro más bajas.

2. Evaluación y Control del Riesgo
• Las aseguradoras dependen de análisis de seguridad para determinar el nivel de riesgo antes de emitir una póliza.
• Un lugar con bajas medidas de seguridad tendrá primas de seguro más altas o incluso puede ser rechazado por las aseguradoras.

Ejemplo: Un comercio con medidas de seguridad deficientes puede tener una prima más alta en un seguro contra robos.

3. Seguridad como Requisito para Asegurabilidad
• Algunas pólizas exigen protocolos de seguridad específicos para garantizar la cobertura.
• En ciertos casos, si no se cumplen las medidas de seguridad requeridas, la aseguradora puede negar la indemnización.

Ejemplo: Un seguro contra incendios puede requerir la instalación de detectores de humo y rociadores automáticos. Si el siniestro ocurre y no estaban instalados, el seguro podría no pagar.

4. Seguridad para Reducir el Costo de los Seguros
• Implementar buenas prácticas de seguridad reduce incidentes, lo que disminuye el número de reclamaciones.
• Menos reclamaciones significan costos más bajos para la aseguradora y primas más accesibles para el asegurado.

Ejemplo: En vehículos, instalar un rastreador GPS o sistemas antirrobo puede reducir la prima del seguro.

5. Seguros como Respaldo Financiero de la Seguridad
• A pesar de todas las medidas de seguridad, el riesgo nunca se elimina al 100%.
• Los seguros actúan como respaldo económico en caso de que las medidas de seguridad fallen o sean superadas.

Ejemplo: Un negocio con guardias de seguridad y CCTV aún puede ser víctima de un robo; el seguro cubre las pérdidas financieras.

GALINDO BENLLOCH

Somos expertos en compliance penal, prevención del blanqueo de capitales y seguridad de la información. Prestamos servicios de Cumplimiento normativo ofreciéndote la solución más eficaz, rentable y confidencial, a través de un equipo de profesionales que te acompañarán en todo momento.
Nuestra especialidad es la elaboración de informes periciales enfocados a la recuperación de activos sustraídos mediante técnicas de ingeniería social (estafas informáticas), tanto en dinero tradicional, como en Criptomonedas. Nuestros casos de éxito ante los tribunales de justicia nos avalan.
La orientación al cliente no es solo una palabra para nosotros, por eso siempre nos ajustaremos al presupuesto y tamaño de tu empresa.

Unidad de acción

CIERRA EL CÍRCULO CON GALINDO BENLLOCH

FORMACIÓN

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

PREVENCIÓN

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

DETECCIÓN

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

INVESTIGACIÓN

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

SEGURIDAD INTEGRAL

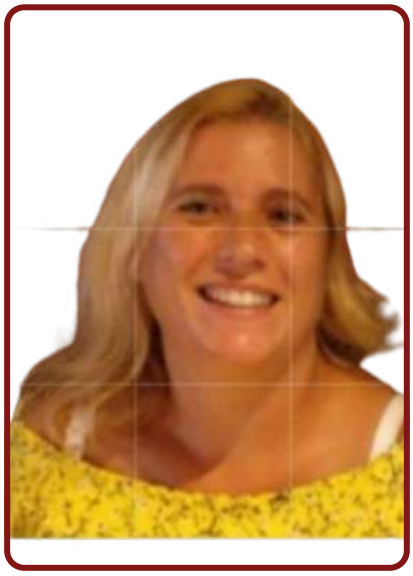
Realizamos consultoría de seguridad física, lógica y cibernética. Para nosotros la unidad de acción es un principio fundamental como prestadores de servicios. Uniendo en un solo proveedor los servicios de Ciberseguridad, seguridad física y lógica.

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

LAS SOMBRAS MÁS ALLÁ DE LAS LUCES EN TU ESTANCIA HOTELERA.

Metro Risk

Elena de la Parte



Más allá de la tarjeta de acceso a tu habitación vulnerabilidades palpables. La seguridad en los hoteles es un tema que trasciende más allá de la mera tarjeta de acceso a la habitación. En un mundo donde la movilidad y la conectividad son la norma, los hoteles son una esencia pura y cristalina que nos refleja. Una representación en miniatura de la sociedad.

¿Alguna vez te has detenido a considerar la complejidad de proteger un espacio que alberga a cientos, incluso miles, de personas cada día con datos sensibles circulando constantemente?

Los hoteles son espacios de convergencia. Albergan una diversidad de alojamientos y usos que se adaptan a las necesidades de un abanico amplio de huéspedes. Esta variedad, a su vez, implica una compleja dinámica de seguridad dada la constante afluencia de personas desconocidas. Las personas que trabajamos en el sector de la seguridad tenemos unas destrezas innatas, comportamientos heredados influenciados por situaciones e incidentes vividas, que a su vez nos forjan como personas y a su vez nos transmiten una necesaria desconfianza. Ante toda persona desconocida. Siempre estamos alerta, entras a un restaurante, te ubicas y con un simple vistazo. Miras las coordenadas y ubicación de las personas que están dentro del mismo local. ¿Es desconfianza? ¿Es protección? Afirmativo Sí. Ambas se cohesionan bien, pues cuando te alojas en un hotel tienes que tener, tus 5 sentidos activos y actuar con estos valores de protección

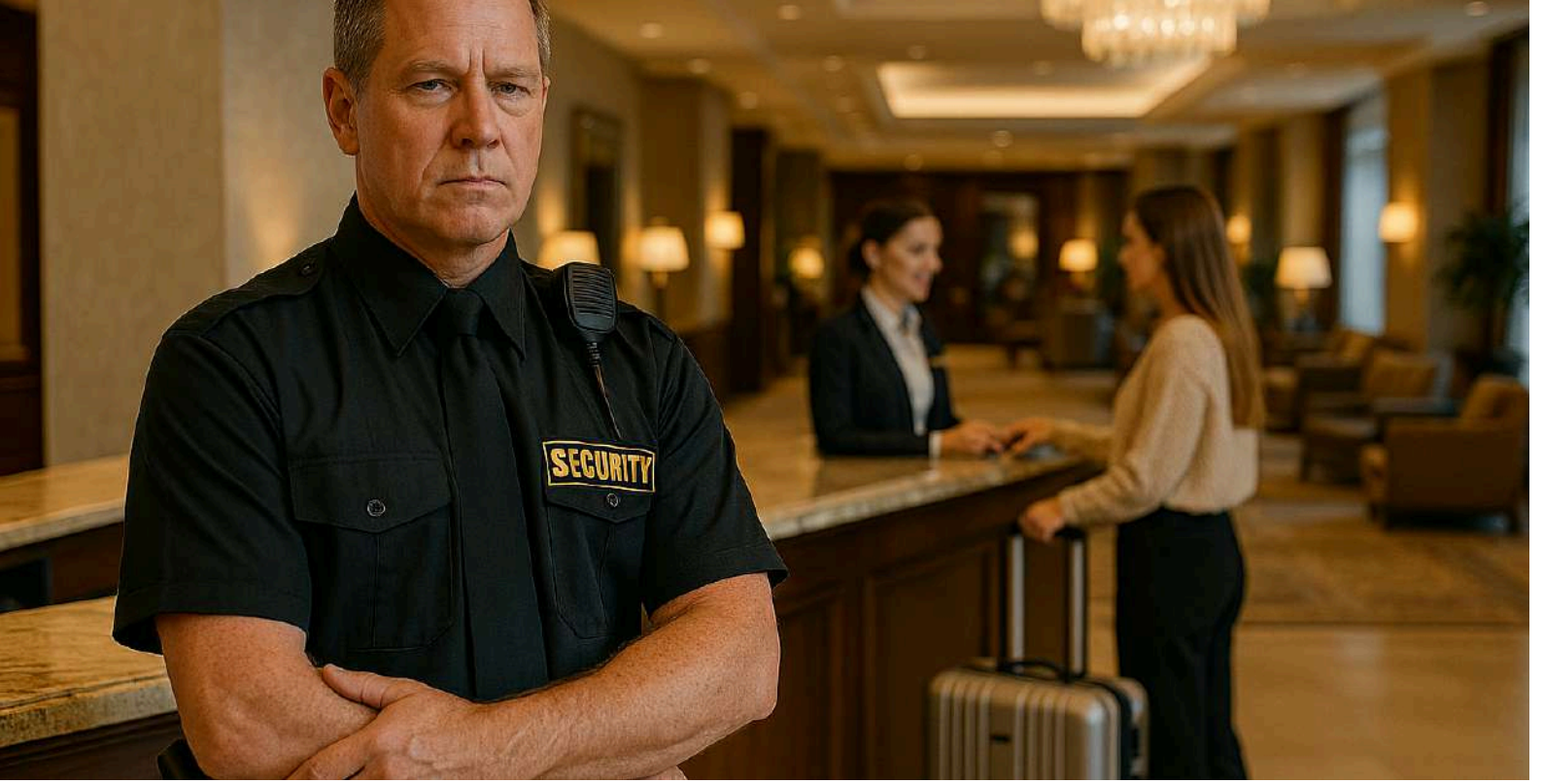
--- Ya, pero voy a. Un hotel para descansar, por cuestiones de trabajo ante las jornadas u conferencias de networking, desconectar, divertirme y pasar unas felices vacaciones. _Ya, pero no es desconfianza del mundo, es la pura realidad que nos rodea. Actualmente la mayoría disponemos de sistemas de CCTV en nuestro hogar. ¿Por protección, ¿verdad? Pues en un hotel la realidad es que la tarjeta de un hotel no es ni parecido a una alarma de seguridad. Sí, algún intruso accede a tu habitación. O te roban tu tarjeta de acceso. En el momento que tú estás dentro y te quitan la tarjeta, te quedas sin iluminación totalmente a oscuras en tu habitación. Es premisa fundamental la presencia de vigilantes de seguridad privada estratégicamente ubicados, capacitados y entrenados con un sistema de CCTV con cámaras de seguridad privada que monitoreen. Las zonas comunes, son elementos cruciales en la infraestructura de seguridad del hotel. Al igual, que en los espacios lúdicos y piscinas. Los socorristas, están capacitados para responder a emergencias médicas en zonas de estos espacios. lúdicos.

La sociedad y las políticas actuales son las que determinan la contratación. humana de estos imprescindibles y excelentes profesionales de seguridad privada con una óptima deontología profesional. La realidad es que en muchos servicios de seguridad privada se carece de binomio de seguridad, y luego vienen las lamentaciones y tragedias.

Sin embargo, la seguridad no recae únicamente en el personal del hotel. Estamos condicionados y cohesionados con las fuerzas y cuerpos de seguridad del Estado. (FFCCSE.) Estos colectivos, desempeñan un papel fundamental en la protección de los ciudadanos. Incluyendo a los huéspedes de los hoteles, su presencia y capacidad de respuesta son un pilar esencial para mantener el orden y la Seguridad Pública. Además, muchos hoteles cuentan con protocolos de seguridad y protección específicos diseñados para abordar los riesgos particulares de su ubicación, tamaño y tipo de clientela. Estos protocolos abarcan desde la gestión de accesos y la prevención de incendios hasta la respuesta de situaciones de emergencia en la Protección de datos personales. (LOPDGDD)., en España es la Ley Orgánica 3/2018, de 5 de diciembre

Aunque el turismo es una actividad en auge y que genera unos beneficios económicos crecientes a la vez que propician desarrollo a todos los niveles, su crecimiento y diversificación en los últimos años auspiciados por la tecnología siguen provocando grandes dudas y debates acerca de la sostenibilidad del sector.

Exploremos un poquitín las vulnerabilidades en la seguridad hotelera, desde los fallos en la señalización, hasta los riesgos cibernéticos y analizaremos cómo la combinación de seguridad privada, la intervención de las fuerzas y cuerpos de seguridad del Estado, FFCCSE., con sus protocolos internos de los hoteles contribuyen a crear un entorno seguro para huéspedes y personal. La diversidad de personas, que se hospedan en hoteles es notable. La cruda realidad es que, en los hoteles, si bien la mayoría de las estancias son pacíficas, es crucial reconocer que los hoteles pueden ser escenarios de comportamientos antisociales y situaciones de múltiples riesgos.



La realidad incómoda de violencia palpable y comportamientos destructivos, enumerando, por ejemplo; altercados y agresiones., comportamientos destructivos, acoso, violencia y agresiones de todo tipo. Como es bien sabido por la sociedad existen múltiples personas con intenciones maliciosas. Los hoteles pueden atraer a personas con intenciones delictivas como ladrones, secuestradores, estafadores o traficantes. La facilidad de acceso y la anonimidad relativa pueden facilitar la comisión de delitos. Al albergar tanta gente pueden ser un lugar donde, ocurran emergencias médicas y situaciones de vital riesgo. Al igual que pueden ocurrir situaciones de riesgo e incidentes y accidentes reales, como conatos de incendios, fugas de gas o amenazas de bombas

Es premisa fundamental que los hoteles se implementen con medidas de seguridad robustas que incluyan: Personal de seguridad capacitado: Vigilantes entrenados para detectar y responder a situaciones de riesgo. Personal capaz de mediar en conflictos y garantizar el cumplimiento de las normas y éticas del hotel. Protocolos de respuesta ante emergencias: Planes de evacuación claros y simulacros periódicos. Equipos de protección contra incendios en óptimas condiciones. Colaboración con las fuerzas y cuerpos de seguridad. Establecer canales de comunicación fluidos con la policía.

Y denunciar cualquier actividad delictiva o sospechosa y real. Es crucial que el personal del hotel esté entrenado para poder reconocer personas con comportamientos extraños o que puedan causar daños a terceros. La seguridad en los hoteles es una responsabilidad compartida. Los huéspedes también deben ser conscientes de los riesgos y tomar precauciones para protegerse a sí mismos, y a sus pertenencias. La seguridad en los hoteles es un tema que a menudo pasa desapercibido. Hasta que ocurre un incidente o accidente irreversible. ¿Alguna vez te has alojado en un hotel y has notado fallos en la seguridad?

Desde la señalización deficiente hasta la falta de accesibilidad, los equipos de protección contra incendios las vulnerabilidades pueden ser más comunes de lo que pensamos.

¿Experiencias reales, te identificas? Señalización: ¿has tenido dificultades para encontrar las salidas de emergencia en caso de un simulacro o una emergencia real? La falta de señalización clara y visible puede generar confusión, retrasos en la evacuación. Y desastres irreparables. Instalaciones de protección contra incendios. ¿Has notado extintores vencidos o mangueras contra incendios en mal estado y sin su optimo mantenimiento?

El mantenimiento inadecuado de estos equipos puede poner en riesgo la vida de los huéspedes y el personal. Accesibilidad a los equipos de protección contra incendios: ¿Has encontrado obstáculos que dificultan el acceso a los extintores o las salidas de emergencia? Los pasillos obstruidos y las puertas cerradas con llave pueden ser trampas mortales en caso de incendio. Recorridos de evacuación y dispositivos: ¿Has tenido que buscar salidas de emergencia en un pasillo a oscuras? La falta de iluminación adecuada y la ausencia de dispositivos de alarma audibles pueden dificultar la evacuación en situaciones de baja visibilidad.

¿Te han robado? Desafortunadamente, los robos en hoteles son más comunes de lo que se piensa. ¿Has sido víctima de un robo de pertenencias personales en tu habitación o áreas comunes? ¿Has visto alguna situación violenta o alguna situación de emergencia? Los altercados entre huéspedes, las emergencias médicas y otros incidentes pueden ocurrir en cualquier momento.

¿Has presenciado alguna situación que haya puesto en riesgo tu seguridad o la de otros? Vulnerabilidades físicas y cibernéticas: Además de las experiencias mencionadas, es importante considerar las vulnerabilidades físicas y cibernéticas que afectan al hotelería. Acceso no autorizado: La falta de control en los accesos, tanto a las habitaciones como a las áreas restringidas, facilita la entrada de intrusos. Robo y hurto: Las pertenencias de los huéspedes, así como los objetos de valor del hotel, están expuestos a robos y hurtos si no se implementan medidas de seguridad adecuadas.

Seguridad en áreas comunes: Las áreas comunes como vestíbulos, restaurantes y estacionamientos pueden ser puntos vulnerables si no se cuenta con vigilancia y sistemas de seguridad efectivos. Seguridad, riesgos de salud: Incendios, fugas de gas y otros riesgos de salud pueden poner en peligro la seguridad de los huéspedes y el personal. Ataques a redes Wifi: Las redes Wifi-públicas de los hoteles son, altamente vulnerables, a ataques de hackers, quienes pueden interceptar datos sensibles de los huéspedes. (Consejo NO te conectes a wifi públicas) Enumero las siguientes medidas de seguridad recomendadas, ya que tu seguridad es prioridad: Control de accesos: implementar sistemas de control de accesos con tarjetas con biometría, identificación y cámaras de seguridad en puntos estratégicos. Cajas fuertes en habitaciones: Proporcionar cajas fuertes en las habitaciones para que los huéspedes puedan guardar sus pertenencias de valor. Aunque cuidadin, estas también, pueden ser vulnerables. Ya que la quimera del riesgo cero no existe. Seguridad cibernética: Implementar medidas de seguridad cibernética robustas como Firewalls, Antivirus y sistemas de detección de intrusiones. Capacitación del personal y concienciación. Con los protocolos establecidos

La seguridad en los hoteles es una responsabilidad compartida. Seamos resilientes y empáticos. Precavidos y atentos a las vulnerabilidades y tomar medidas preventivas. Al implementar medidas de seguridad efectivas y fomentar la conciencia de los riesgos, se puede crear un entorno un poquitín más seguro y protegido para todos.

Si has notado fallos en la seguridad durante tu estancia, no dudes en informar al personal del hotel, al vigilante de seguridad o a las FFCCSE. Tu voz puede marcar la diferencia y salvar vidas.

Recuerda que la tarjeta de bienvenida del hotel. Incluye estas letras escritas:

” Bienvenido, deseamos que su estancia en este hotel sea inolvidable”

Consejo, la vida te puede cambiar en segundos.

Nunca bajes la guardia, que esa experiencia inolvidable, sea positiva. Y no lo contrario, y que estés con vida para poder contarla.

Prevaleceremos siempre la seguridad, ciberseguridad, la ética y la justicia.

ENTREVISTA PARA BOLETÍN METRORISK CARLOS MIGUEL ORTIZ

Metro Risk

¿Cuál es el recuerdo vívido de tu infancia que te ha moldeado como persona? La tecnología en general siempre me ha gustado; desde pequeño disfrutaba trasteando con todo tipo de herramientas, desmontando y explorando cómo funcionaban las cosas. Esa curiosidad me llevó a interesarme por la ingeniería, la innovación y, más tarde, por los drones y su impacto en la sociedad.

¿Tu medio de transporte preferido para viajar? Sin duda, el avión. No solo por la eficiencia y velocidad, sino porque siempre me ha fascinado la aviación y la perspectiva que ofrece desde el aire.

¿Si cambiaras de país para vivir? ¿A cuál irías? Me atrae mucho Canadá, por su combinación de tecnología, naturaleza y calidad de vida. Además, es un país con un gran desarrollo en el uso de drones para aplicaciones civiles.

¿Qué modificarías hoy en día en nuestro país si tú fueras el presidente del gobierno? Invertiría más en innovación y formación en nuevas tecnologías, especialmente en el sector de drones y ciberseguridad, ya que tienen un gran potencial para mejorar la seguridad, la productividad y la sostenibilidad en diferentes sectores

¿El mejor invento, para ti, de la historia? El autogiro sin duda alguna. Este invento revolucionó la aviación al abrir la puerta a los vuelos verticales, lo que ha sido clave para el desarrollo de helicópteros y otros vehículos aéreos verticales, incluidos los drones.

¿Un nuevo EPI para la seguridad de tu organización u empresa y para tu hogar, que no exista actualmente? Un sistema de monitoreo basado en drones de vigilancia autónomos que puedan detectar riesgos en tiempo real, tanto en el ámbito laboral como en la seguridad del hogar

¿Tu frase preferida? "Hazlo o no lo hagas, pero no lo intentes." – Yoda

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

Escoge 1 podcast para recomendar a tus seguidores. "Black Mango", un podcast con historias impactantes y un enfoque que engancha desde el primer minuto.

¿Cuál es la importancia de la ciberseguridad en tu organización? En el mundo de los drones, la ciberseguridad es clave. Desde la protección de los datos capturados hasta la prevención de accesos no autorizados a los sistemas de vuelo, es un aspecto fundamental para garantizar la operatividad y seguridad de cada misión.

¿Un superhéroe en el que te gustaría tener sus superpoderes? ¿Y por qué? No son superhéroes en el sentido tradicional, pero para mí, mis padres lo han sido. Con sus consejos, apoyo y ejemplo, me han ayudado a convertirme en la persona que soy hoy. Su paciencia, esfuerzo y enseñanzas han sido más valiosas que cualquier superpoder.

¿Si pudieras volver a vivir un año de tu vida, cuál sería y por qué? Quizá el año en el que empecé a trabajar con drones. Fue un momento de descubrimiento, de mucho aprendizaje y de ver cómo una pasión se podía convertir en un proyecto real con impacto.

¿Si pudieras aprender cualquier habilidad nueva en tu vida, cuál sería y por qué? Me gustaría aprender más sobre inteligencia artificial aplicada a drones. La combinación de IA con vuelo autónomo tiene un potencial increíble para múltiples sectores.

Si pudieras vivir en cualquier época histórica, ¿cuál elegirías y por qué? Me gustaría vivir en la época de la Revolución Industrial, para ver de primera mano cómo la tecnología comenzó a transformar la sociedad y comparar ese momento con la revolución digital que vivimos ahora.

Si tuvieras que elegir entre estas dos opciones, y solo te puedes quedar con una, ¿cuál seleccionas? ¿Compliance o ciberseguridad? Ciberseguridad. Sin una buena estrategia de ciberseguridad, el compliance se vuelve vulnerable, especialmente en el mundo digital en el que operamos hoy en día.

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

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

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

Colaboramos con MR-CONSULTING.

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

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

"RIESGOLOGÍA EMPRESARIAL: EL NUEVO PARADIGMA QUE REVOLUCIONA LA SEGURIDAD CORPORATIVA EN UN MUNDO DE AMENAZAS INTERCONECTADAS"

Metro Risk

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

Hermida Seguridad S.A.S.
Seguridad Corporativa Integral
www.hermidaseguridad.com

En un mundo donde los riesgos ya no se limitan a una sola área, las empresas están adoptando un enfoque revolucionario para gestionar sus amenazas: la Riesgología Empresarial. Este nuevo paradigma integra disciplinas tradicionalmente separadas, como la Seguridad y Salud en el Trabajo, la Seguridad Física, la Protección Civil, la Gestión de Emergencias y la Ciberseguridad, bajo una misma estrategia unificada.

La Riesgología Empresarial no solo busca prevenir incidentes, sino también crear organizaciones más resilientes y preparadas para enfrentar crisis complejas. Donde un ciberataque puede paralizar operaciones, un desastre natural puede afectar la salud laboral, y un error en la seguridad física puede comprometer datos críticos, este enfoque integral se convierte en una herramienta indispensable para la supervivencia y el éxito empresarial. ¿Por qué es relevante hoy? Según estudios recientes, el 60% de las empresas han enfrentado incidentes que involucran múltiples áreas de riesgo simultáneamente, y solo el 20% cuenta con un plan integral para gestionarlos.

La Riesgología no solo responde a esta necesidad, sino que también ofrece una ventaja competitiva al alinear la seguridad con los objetivos estratégicos de la organización. En este artículo, exploramos cómo este nuevo paradigma está transformando la seguridad corporativa, qué oportunidades ofrece a los líderes empresariales y por qué es crucial adoptarlo en un entorno cada vez más dinámico y desafiante. El Paradigma Tradicional de la Seguridad y la Necesidad de un Enfoque Integral

El paradigma tradicional de la seguridad en el ámbito empresarial ha estado históricamente fragmentado y orientado hacia la reactividad.

En este enfoque, cada área de seguridad (Seguridad y Salud en el Trabajo, Seguridad Física, Protección Civil, Gestión de Emergencias y Ciberseguridad) operaba de manera independiente, con sus propios protocolos, responsabilidades y objetivos. El modelo, aunque funcional en su momento, presenta limitaciones significativas en un mundo empresarial cada vez más complejo e interconectado.

Características del Paradigma Tradicional.

- Enfoque fragmentado: Cada área de seguridad trabaja de manera aislada, lo que genera duplicidad de esfuerzos y falta de coordinación.
- Reactividad: Las acciones se toman después de que ocurre un incidente, en lugar de prevenir riesgos de manera proactiva.
- Visión limitada: Se centra en cumplir normativas y estándares mínimos, en lugar de buscar la excelencia y la resiliencia organizacional.
- Falta de integración con la estrategia empresarial: La seguridad se ve como un costo operativo, no como un componente estratégico que puede agregar valor a la organización.

Las Limitaciones que presenta este Paradigma Tradicional son.

- Ineficiencia: La falta de coordinación entre áreas lleva a un uso ineficiente de recursos.
- Vulnerabilidad: Un enfoque fragmentado dificulta la identificación y gestión de riesgos interconectados, como un ciberataque que afecta la seguridad física o un desastre natural que impacta la salud laboral.
- Falta de resiliencia: Las organizaciones no están preparadas para enfrentar crisis complejas que requieren una respuesta integrada.
- Desconexión con la realidad empresarial: En un mundo donde los riesgos son cada vez más dinámicos y multidimensionales, el enfoque tradicional resulta insuficiente.

¿Por qué es Importante Cambiar a un Enfoque Integral? El cambio hacia un enfoque integral, como la Riesgología Empresarial, no es solo una mejora incremental, sino una transformación necesaria para que las organizaciones puedan sobrevivir y prosperar en un entorno empresarial cada vez más complejo. Este nuevo paradigma reconoce que los riesgos no existen en compartimentos estancos, sino que están interconectados y pueden tener impactos transversales en la organización.

Razones para Adoptar un Enfoque Integral. Interconexión de Riesgos: Los riesgos modernos rara vez se limitan a una sola área. Por ejemplo, un ciberataque puede afectar no solo los sistemas informáticos, sino también la seguridad física (por ejemplo, el bloqueo de sistemas de acceso) y la salud laboral (por ejemplo, el estrés generado en los empleados). Un enfoque integral permite identificar y gestionar estos riesgos de manera holística. Eficiencia y Optimización de Recursos: Al integrar las diferentes áreas de seguridad, se evitan duplicidades y se maximiza el uso de recursos humanos, tecnológicos y financieros. Resiliencia Organizacional: Un enfoque integral prepara a las organizaciones para enfrentar crisis complejas y recuperarse rápidamente, minimizando el impacto en sus operaciones y reputación.

Alineación con la Estrategia Empresarial: La seguridad deja de ser un costo operativo para convertirse en un componente estratégico que agrega valor a la organización. Por ejemplo, una gestión proactiva de riesgos puede mejorar la confianza de los clientes, inversores y reguladores. Cultura de Prevención: Un enfoque integral fomenta una mentalidad de prevención en todos los niveles de la organización, desde los empleados hasta la alta dirección. Esto no solo reduce la probabilidad de incidentes, sino que también mejora la moral y el compromiso del personal. Adaptabilidad a un Entorno Dinámico: En un mundo donde los riesgos evolucionan rápidamente (por ejemplo, nuevas amenazas cibernéticas o cambios en las normativas de salud laboral), un enfoque integral permite a las organizaciones adaptarse de manera ágil y efectiva.

La Riesgología Empresarial como Enfoque Integral. La Riesgología Empresarial es la evolución natural del paradigma tradicional de la seguridad. Este enfoque integra todas las disciplinas relacionadas con la gestión de riesgos (Seguridad y Salud en el Trabajo, Seguridad Física, Protección Civil, Gestión de Emergencias y Ciberseguridad) bajo un mismo marco conceptual y operativo. Su importancia radica en que: Unifica la visión de riesgos: Permite ver la organización como un todo interconectado, donde un riesgo en un área puede tener repercusiones en otras.

Promueve la proactividad: En lugar de esperar a que ocurra un incidente, se anticipa y previene. Facilita la toma de decisiones basada en datos: Utiliza herramientas como el análisis de datos y la inteligencia artificial para identificar y priorizar riesgos. Fomenta la colaboración interdepartamental: Rompe los silos y promueve la comunicación entre áreas. Agrega valor a la organización: No solo protege, sino que también contribuye a la sostenibilidad y el éxito empresarial

El cambio de paradigma de la seguridad tradicional a un enfoque integral como la Riesgología Empresarial no es solo una necesidad, sino una obligación estratégica para las organizaciones que buscan prosperar en un entorno lleno de incertidumbres. Este no solo mejora la eficiencia y la resiliencia, sino que también alinea la seguridad con los objetivos estratégicos de la empresa, convirtiéndola en un factor clave para la creación de valor. En un mundo donde los riesgos son cada vez más complejos e interconectados, la Riesgología es la respuesta para construir organizaciones más seguras, sostenibles y competitivas.

El Cambio de Paradigma de la Seguridad Integral a la Riesgología Empresarial En el mundo empresarial contemporáneo, la seguridad ha evolucionado de ser un conjunto de prácticas reactivas y aisladas a convertirse en una disciplina integral y proactiva que abarca múltiples dimensiones del riesgo. Este cambio de paradigma, que hemos denominado Riesgología Empresarial, representa una transformación profunda en la forma en que las organizaciones abordan la seguridad, no solo como un mecanismo de defensa, sino como una estrategia holística para gestionar riesgos y crear valor. Este enfoque integra disciplinas como la Seguridad y Salud en el Trabajo (SST), la Seguridad Física, la Protección Civil, la Gestión de Emergencias y, de manera crítica, la Ciberseguridad, bajo un mismo paraguas conceptual y operativo

Objetivos de la Riesgología Empresarial El principal objetivo de la Riesgología Empresarial es anticipar, prevenir y gestionar los riesgos de manera integral, considerando todas las áreas que pueden impactar la continuidad operativa, la reputación y la sostenibilidad de una organización. Esto implica: Identificar y evaluar riesgos: Desde los riesgos físicos y laborales hasta los cibernéticos, la Riesgología Empresarial busca crear un mapa completo de amenazas potenciales. Integrar disciplinas: Romper los silos entre las diferentes áreas de seguridad para crear un enfoque unificado y coherente. Fomentar una cultura de prevención: Educar y empoderar a los empleados y líderes para que comprendan y participen activamente en la gestión de riesgos. Optimizar recursos: Al integrar las diferentes áreas de seguridad, se evitan duplicidades y se maximiza la eficiencia en la asignación de recursos. Garantizar la resiliencia organizacional: Preparar a la empresa para responder de manera efectiva ante incidentes y recuperarse rápidamente.

Referencias Conceptuales La Riesgología Empresarial se basa en conceptos y marcos de referencia de diversas disciplinas, entre ellas: Gestión de Riesgos Corporativos (GRC): Un enfoque estructurado para alinear la gestión de riesgos con los objetivos estratégicos de la organización.
Seguridad y Salud en el Trabajo (SST): Normas y prácticas destinadas a proteger el bienestar físico y mental de los trabajadores. Protección Civil y Gestión de Emergencias: Protocolos para prevenir y responder a desastres naturales, accidentes y otras situaciones de crisis. Ciberseguridad: Protección de sistemas, redes y datos contra amenazas digitales. Seguridad Física: Medidas para proteger instalaciones, activos y personas contra riesgos físicos como robos, vandalismo o ataques.

Cambios que Conlleva la Riesgología Empresarial. El paso de la Seguridad Integral a la Riesgología Empresarial implica una serie de cambios significativos: De lo reactivo a lo proactivo: En lugar de esperar a que ocurra un incidente para actuar, la Riesgología Empresarial se enfoca en la prevención y la anticipación. Integración de disciplinas: Se supera la fragmentación tradicional entre áreas como SST, seguridad física y ciberseguridad, creando un enfoque unificado. Enfoque basado en datos: La toma de decisiones se sustenta en análisis de riesgos cuantitativos y cualitativos, utilizando herramientas como big data e inteligencia artificial. Cultura organizacional: Se promueve una mentalidad de riesgo en todos los niveles de la organización, desde los empleados hasta la alta dirección. Adaptabilidad: La Riesgología Empresarial reconoce que los riesgos son dinámicos y exigen una constante actualización de estrategias y protocolos

La Riesgología Empresarial en la Práctica. Seguridad y Salud en el Trabajo (SST)

La Riesgología en la SST ya no se limita a cumplir normativas legales. Se convierte en un pilar estratégico para identificar riesgos laborales que podrían afectar la productividad, la moral de los empleados y, en última instancia, la reputación de la empresa. Por ejemplo, un enfoque riesgológico podría incluir el análisis de datos de salud laboral para predecir y prevenir enfermedades profesionales o accidentes.

Seguridad Física y Protección Civil. La seguridad física y la protección civil se integran en un sistema único que no solo protege las instalaciones, sino que también prepara a la organización para enfrentar desastres naturales o emergencias. Esto incluye la implementación de planes de evacuación, simulacros y la utilización de tecnologías como sensores y cámaras inteligentes para monitorear riesgos en tiempo real

Ciberseguridad. Cada vez más digitalizado, la ciberseguridad es un componente crítico de la Riesgología Empresarial. Los líderes deben entender que un ciberataque no es solo un problema técnico, sino un riesgo empresarial que puede tener consecuencias financieras, legales y reputacionales devastadoras. La integración de la ciberseguridad en la Riesgología implica, por ejemplo, la capacitación de empleados para identificar phishing o la implementación de protocolos de respuesta ante brechas de datos.

Oportunidades para los Nuevos Líderes en Seguridad Corporativa.

Los líderes en seguridad corporativa que adopten el enfoque de la Riesgología Empresarial tienen la oportunidad de convertirse en agentes de cambio dentro de sus organizaciones. Para ello, deben: Dominar los conceptos básicos de cada disciplina: Entender los fundamentos de SST, seguridad física, protección civil y ciberseguridad es esencial para integrarlos de manera efectiva.

Desarrollar habilidades analíticas: La capacidad de analizar datos y prever escenarios de riesgo será una competencia clave.

Fomentar la colaboración interdepartamental: Romper los silos y promover la comunicación entre áreas es fundamental para una gestión integral de riesgos. Mantenerse actualizado: Los riesgos evolucionan rápidamente, especialmente en áreas como la ciberseguridad, por lo que los líderes deben estar al tanto de las últimas tendencias y tecnologías.

Promover una cultura de resiliencia: Los líderes deben inspirar a sus equipos a ver la gestión de riesgos no como una carga, sino como una oportunidad para fortalecer la organización.

La Riesgología Empresarial representa un cambio de paradigma en la forma en que las organizaciones abordan la seguridad. Al integrar disciplinas tradicionalmente separadas bajo un enfoque unificado, las empresas no solo pueden protegerse mejor contra amenazas, sino también crear valor y garantizar su sostenibilidad a largo plazo.

Para los nuevos líderes en seguridad corporativa, este enfoque ofrece una oportunidad única para destacarse como visionarios capaces de navegar en un mundo cada vez más complejo y lleno de riesgos. La Riesgología no es solo el futuro de la seguridad; es el presente de las organizaciones que buscan prosperar en un entorno empresarial dinámico y desafiante.

Hermida Seguridad S.A.S.

Seguridad Corporativa Integral

www.hermidaseguridad.com

EL SECUESTRO

Metro Risk

Carlos Tejada Morán
Asesor en seguridad personal y empresarial
CAPACITADO EN :

Criminalistica. Psicopatologia forense. Lavado de activos. inteligencia y contra inteligencia. Especialista contra el crimen organizado internacional. Especialista contra terrorismo y contra insurgencia. Dominación de inmuebles . Maniobras de vehículos blindados a alta velocidad

Cuando hablamos de Secuestro se nos viene a la mente la libertad de una persona por un tema de dinero político o venganza entre otros. Para los secuestradores el Secuestro se divide en 3 partes

- 1 la información de la víctima
- 2 la ejecución del Secuestro
- 3 el cobro del rescate

1 la información de la víctima

La información puede durar días y meses dependiendo de la importancia de la víctima. Casi siempre la información viene de gente conocida como amigos o empleados de la empresa. El gerente financiero etc. o de personas que venden información a cambio de un dinero. Esta información es total mente fidedigna ya que se sabe con exactitud que día tiene el dinero disponible para proceder con el secuestro de la persona.

2 la ejecución

La ejecución del Secuestro no se realiza cualquier día que la persona esté descuidada. El Secuestro se realiza un día antes de que la persona reciba una fuerte cantidad de dinero y tenga efectivo disponible para evitar dilatar el tiempo ya que los Secuestros exitosos no pueden durar más de 3 días porque los secuestradores tienen que aprovechar el pánico de la familia y sean más fácil de dominar.

El cobro de rescate es lo más fácil o difícil de efectuar, depende de cómo lo manejes. Si entrego la plata primero y después no me dan a la persona o si le doy a la persona y después no me dan la plata o una transferencia a un banco de otro país etc.

Es cuando entra a trabajar el negociador, quien es el que se canjea por la persona secuestrada, dependiendo de la situación del Secuestro. En estos temas hay muchas cosas más como cambios de identidad o lavar el dinero ilícito, donde ocultar a la victima, etc. Pero no se trata de formar secuestradores, se trata de tener una idea para que vean que si se puede rescatar a la víctima con éxito.

AGENDA

Metro Risk

Edición propiedad de @MetroRisk, asociación

RADIO

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

EL CANAL DEL CORONEL

LOS CONSEJOS DE CIBERSEGURIDAD DE ADOLFO GELDER.
en: www.linkedin.com/in/adolfo-gelder-b2327bb4/

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

Metrorisk

Proyecto Asociativo

www.metrorisk.es