EDITORIAL MR

FEBRERO

AÑO 2025

Fran Medina Cruz Francisco Javier Gonzales Fuentes José Ignacio Olmos Casado Fernando Montoya Cerio Gregorio Duro Mercedes Escudero Carmona Antonio Pérez Cala Emilio Piñeiro Rosa Fernández Carlos Serrano Abraham Santana Herrera Elena de la Parte Edgar Octavio Herrera Rodríguez Jonathan Hermida Sosa Cristóbal Granados Sánchez y Carlos Miguel Ortiz

ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

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

COLABORADORES

PATROCINADO POR LAS FIRMAS

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

DONDE NO LLEGA LA SEGURIDAD PÚBLICA, LLEGA LA SEGURIDAD PRIVADA

Metro Risk

Fran Medina Cruz
Director de MetroRisk

.En el panorama actual de la seguridad, la colaboración entre los sectores público y privado se ha convertido en una necesidad creciente. La expansión de las ciudades, el aumento de los riesgos y la complejidad de los entornos urbanos han puesto de manifiesto las limitaciones de los recursos públicos para garantizar la protección de todos los ciudadanos. Aquí es donde entra en juego la seguridad privada, que no solo complementa, sino que en muchos casos lidera la respuesta frente a amenazas específicas.

La modernización de la seguridad privada es clave en este proceso. El uso de tecnologías avanzadas como la inteligencia artificial, los sistemas de videovigilancia inteligentes y los drones de patrullaje ha permitido una respuesta más rápida y eficiente a los incidentes. Estas herramientas no solo mejoran la prevención, sino que también facilitan la investigación y disuasión de delitos. Sin embargo, este crecimiento debe ir de la mano de una regulación estricta y adecuada.

Es esencial que los marcos legales no solo definan las competencias de los actores privados, sino que también protejan los derechos de los ciudadanos, evitando excesos o abusos. La regulación actúa como el puente que garantiza una convivencia armónica entre el deber público y la actividad privada.

Por último, la formación profesional es un pilar imprescindible. Los profesionales de la seguridad privada deben estar preparados para enfrentar desafíos complejos, combinando conocimientos técnicos con habilidades humanas como la comunicación y la gestión de conflictos. Certificaciones actualizadas y programas de capacitación continua aseguran que estos agentes sean verdaderos aliados en la construcción de entornos seguros.

En definitiva, la seguridad privada no es un sustituto, sino un complemento estratégico de la seguridad pública. Su modernización, regulación y profesionalización son los cimientos para garantizar que este sector contribuya eficazmente a la protección de la sociedad en conjunto

La Importancia de Establecer Protocolos de Seguridad en Espacios Públicos y Privados

La seguridad es un derecho fundamental que debe ser garantizado en todos los entornos donde confluyen personas, ya sea en espacios públicos como colegios y hospitales o en lugares privados como aviones y trenes. En un mundo cada vez más complejo y globalizado, los protocolos de seguridad no solo son necesarios, sino que su obligatoriedad debería estar respaldada por una legislación moderna y efectiva.

Cuando se habla de espacios donde se concentra un número significativo de personas, como aeropuertos, estaciones de tren, instituciones educativas o centros sanitarios, es fundamental contar con protocolos de seguridad claros y eficaces. Estos deben contemplar medidas preventivas, sistemas de respuesta ante emergencias y mecanismos de supervisión para garantizar la integridad de quienes los frecuentan. La obligatoriedad de estos protocolos por ley sería un paso esencial para establecer un marco normativo uniforme y garantizar su aplicación en todos los sectores. El sector de la seguridad privada juega un papel crucial en este contexto. Sin embargo, para responder a los desafíos actuales, es imprescindible una modernización integral que abarque los siguientes aspectos:

1. **Formación Obligatoria y Continuada**
2. **Dotación y Uniformidad**
3. **Auditorías Regulares**

Una normativa moderna debe abordar las necesidades del sector con una perspectiva garantista tanto para los usuarios como para los trabajadores. Esto incluye:

- **Establecer requisitos mínimos exigentes para acceder a la profesión en todas sus categorías.**
- **Crear órganos de dirección colegiados e independientes que regulen el sector de manera efectiva.**
- **Promover la investigación y el desarrollo de tecnologías que mejoren los sistemas de seguridad.**

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 TRANSVERSALIDAD DE LA SEGURIDAD INTEGRAL Y CORPORATIVA

Metro Risk

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

En el entorno corporativo moderno, la seguridad integral y corporativa se ha convertido en una prioridad fundamental.

Esta disciplina no solo abarca la protección física y digital de los activos, sino que también se extiende a todas las áreas funcionales de una organización. La transversalidad de la seguridad implica que esta debe ser considerada en todas las etapas de operación y desarrollo de la empresa, integrándose de manera holística y estratégica. No solo en esa línea, desde la perspectiva de la empresa, si no que ya sale del marco jurídico del concepto "Seguridad Privada" y con el tiempo obtiene una mayor transversalidad , como parte troncal de Seguridad Integral . Como principio jurídico y constitucional, valor primario de cualquier sociedad moderna , la Seguridad Integral , ocupa diferentes dimensiones en el plano social , empresarial y en las instituciones públicas y privadas.

IntelForensic
G&F Soluciones

El modelo Español, referente a nivel Europeo en un marco regulatorio donde existe la Ley de Seguridad Privada, Ley 5/2014, de 4 de abril, de Seguridad Privada. Queda latente que las organizaciones y usuarios, necesitan un producto de seguridad que abarca una extensión que superan las fronteras de la propia ley, donde esa transversalidad multifuncional, nos lleva a intercambiar para los profesionales, los Técnicos en Seguridad, en la implantación y desarrollo de planes de seguridad más complejos, con riesgos y amenazas cada vez mas estratégicas que afectan de lleno a cualquier organización (pública y privada intersectorial). Planes de Autoprotección, colaboración de los técnicos en los planes de emergencias, participación de la Dirección de Seguridad en la toma de decisiones... Y un sinfín de ramas que exponemos a continuación.

Para ello, tenemos que definir los conceptos de Seguridad Integral y Seguridad corporativa.

Concepto de Seguridad Integral y Corporativa

La seguridad integral se refiere a un enfoque amplio y completo que abarca la protección de todas las dimensiones de una empresa: física, lógica, operativa y de recursos humanos. Esto incluye la prevención de riesgos, la gestión de crisis, la ciberseguridad, la seguridad física y la continuidad del negocio.

La seguridad corporativa, por su parte, se enfoca en proteger los intereses de la empresa, sus empleados, activos y datos. Incluye la implementación de políticas, procedimientos y tecnologías que aseguren la integridad, confidencialidad y disponibilidad de la información y los recursos.

Transversalidad en la Seguridad Integral

1. Ciberseguridad: La protección de la información digital es una de las áreas más críticas.
2. Seguridad Física: La protección de las instalaciones, equipos y personal es fundamental.
3. Gestión de Riesgos: La identificación, análisis y mitigación de riesgos debe ser una práctica continua y transversal.
4. Seguridad de la Información: Más allá de la ciberseguridad, esto incluye la protección de documentos físicos, la gestión adecuada de registros y la confidencialidad de la información sensible.
5. Seguridad de Recursos Humanos: La seguridad en la gestión de personal implica desde el cumplimiento de normas laborales hasta la implementación de políticas de prevención de acoso y manejo de conflictos.

Transversalidad en la Seguridad Integral

1. Políticas y Procedimientos
2.Formación y Concienciación
3.Tecnología y Herramientas
4.Evaluación y Mejora Continua

La transversalidad de la seguridad integral y corporativa es esencial para proteger a las empresas, instituciones públicas y privadas, en definitiva a cualquier activo social, en un entorno cada vez más complejo y dinámico. Integrar la seguridad en todas las áreas y niveles de la organización no solo mejora la protección de los activos, sino que también fortalece la resiliencia y competitividad de las organizaciones. Adaptarse a esta visión holística de la seguridad es clave para el éxito y la sostenibilidad a largo plazo.

Dentro siempre de un marco regulatorio, que marque todos los objetivos sectoriales y profesionales en el plano profesional y académico.

Mtro. Francisco Javier González Fuentes

LA CONVERGENCIA DE LAS SEGURIDADES Y LA SEGURIDAD INTEGRAL

Metro Risk

José Ignacio Olmos Casado
Presidente AEAS

Mucho se habla en los últimos tiempos de la convergencia entre la seguridad lógica y la seguridad física como eje fundamental de la propia seguridad en el contexto actual y el futuro inmediato. Y lo cierto es que, aunque mucho se habla y todos estamos de acuerdo en la necesidad de alcanzar esa convergencia, también son muchas las voces críticas que señalan que aún nos encontramos muy lejos de esa convergencia; sin ir más lejos algún colega comentaba hace no mucho en un evento que "llevamos media década hablando de la convergencia y en términos generales no hemos conseguido nada de eso".

La cuestión en sí es compleja debido a múltiples factores como las estructuras de las propias compañías y sus organigramas, lo que ha venido representando en ellas la seguridad física y el papel fundamental que representa ya hace tiempo la seguridad lógica

Sin embargo, no aspiro a hablar de algo tan complejo en este artículo aunque sí de algo tan importante: la seguridad integral. Hoy día no podemos entender la seguridad si no es de forma integral.

Esa integralidad, bajo mi punto de vista, tiene dos acepciones. La primera de ellas es que la seguridad se debe abordar como un todo, puesto que las corporaciones pueden ver amenazados sus activos por una multiplicidad de riesgos con origen diverso; de nada sirve protegerse en un ámbito si el activo se pierde por falta de protección en otro.

Hoy se impone, y desde luego me parece lo más acertado, la versión anglosajona del security management, que no es otra que la del gestor de riesgos, más allá de lo que la propia normativa española de seguridad privada establezca para un director de seguridad. La segunda acepción es que para la protección de esos activos el tratamiento de los riesgos lo realizamos, entre otras formas, mediante su gestión a través de medidas, es decir, lo que conocemos como sistema integral de seguridad.

Esas medidas, que sólo pueden ser de tres tipos (técnicas, humanas y organizativas) son uno de los pilares esenciales de ese sistema. Generalmente al hablar de medidas pensamos sobre todo en medios técnicos (sobre todo los activos) o en el elemento humano; aquí podemos hacer también dos precisiones: es imprescindible buscar la complementariedad entre tecnología y elemento humano en búsqueda de la eficacia y la eficiencia del sistema, pero además, no podemos dejar de lado los medios técnicos pasivos que son fundamentales en ese sistema integral de seguridad. Pero además, hay que llamar la atención sobre el tercer aspecto, que son las medidas organizativas, aspecto que, con mucha habitualidad es dejado de lado como menos importante.

INo seré yo quien diga que un protocolo es más importante que un medio técnico o que uno humano, pero sí quien recuerde que esas medidas organizativas tienen, , al menos, tanta importancia como las otras dos, entre otras cosas porque son las que las dotan de cohesión. No nos olvidemos que, nuestro sistema, no es una cámara de CCTV, ni tampoco un vigilante de seguridad, ni aún siquiera un protocolo; mi sistema es un vigilante de seguridad bien formado y motivado con una buena cámara y las directrices adecuadas para utilizarla. Y si me falta una de las tres cosas, la hemos fastidiado.

En mi práctica profesional habitual, al realizar auditorías, me resulta demasiado habitual encontrar que los procedimientos brillan por su ausencia. Pensemos que, dentro de las medidas organizativas, y junto con la importancia que tiene casi siempre la normativa, es imprescindible que dispongamos de ese Plan de Seguridad Integral, que incluirá aquellos planes específicos que sean necesarios. Y la forma de llevar éstos a término es con los adecuados procedimientos.

De tal manera que, y resumiendo mucho, los procedimientos:

- Deben existir
- Deben ser los adecuados (para lo cual habrá que comprobar su eficacia)
- Deben implantarse (darse a conocer a todos los implicados)
- Deben probarse (¿por qué sólo hacemos simulacros en aspectos de safety y prácticamente nunca de security?)

El procedimiento ayuda a dar la mejor solución a una problemática y a que la respuesta ante problemáticas sea uniforme, sobre todo cuanto más grave y menos rutinario sea el problema.

Y no debemos olvidar que un procedimiento es algo que debe facilitar el trabajo, no entorpecerlo; por eso un procedimiento no puede ser una carpeta de anillas rebosante de documentos…

Comenzábamos expresando la dificultad que entraña incardinar seguridad física y lógica y apuntando que se deben abordar de forma conjunta todas las seguridades; si lo primero es complicado, ¿Cuál es el grado de dificultad de lo segundo? Bueno, nadie dijo que fuese fácil… por eso algunos locos elegimos ser directores de seguridad

LA SEGURIDAD FACTOR FUNDAMENTAL PARA EL TURISMO

Fernando Montoya Cerio
Presidente de AIMCSE

SI NOS ATENEMOS A LOS DATOS FACILITADOS POR LA ALIANZA PARA LA EXCELENCIA TURÍSTICA (EXCELTUR), EL TURISMO, EN EL EJERCICIO DE 2024, SE HA CONSOLIDADO COMO EL PRINCIPAL MOTOR DE LA ECONOMÍA ESPAÑOLA, APORTANDO CERCA DE 208.000 MILLONES DE EUROS, UN 6,5% MÁS QUE HACE UN AÑO.

Por otra parte, en el año de referencia (2024), el sector turístico generó más de 72.000 nuevos empleos, lo que supone un incremento del 3,2%, y ha aportado 32.854 millones de euros para la financiación de la Seguridad Social, rebajándose simultáneamente la temporalidad al 7,8% por el aumento de la contratación indefinida, con 69.000 trabajadores más.
Las previsiones para el año 2025 no pueden ser mejores: el turismo seguirá siendo uno de los pilares económicos con un crecimiento real del 4% lo que supone una desviación al alza, respecto al estimado por el banco de España para el PIB nacional (2,5%); el sector de viajes y turismo se consolida con el 17,5% de la fuerza laboral en España

En resumen, el sector turístico es un verdadero motor de crecimiento económico y de la creación de empleo.

Hasta aquí, puros datos que incluso podrían llegar a ser debatidos, en cuanto al contenido de sus cifras, dependiendo de la fuente en la que nos fijemos. Pero, en cualquier caso, lo que sí es definitivo es que la importancia del sector turístico para una economía como la española es determinante. Pero el turismo, tanto nacional como internacional, va unido indefectiblemente al factor SEGURIDAD.

Seguridad para los potenciales viajeros y de las empresas que proveen estos servicios. Seguridad personal y seguridad de empresa, ramas ambas a las que el Estado debe de contribuir para preservar unos ingresos que ayudan a equilibrar sus cuentas nacionales.

También los empresarios del sector tienen que hacer sus deberes para proteger sus propias inversiones mediante acciones directas que salvaguarden la integridad del turista a través de una política próxima de seguridad, de unos planes integrales de seguridad y de una cultura de seguridad de todos los trabajadores del sector.

La figura del turista debe de ser la de una persona despreocupada con su día a día ante un ambiente desconocido y que en ningún caso le pueda de ser hostil. Naturalmente que el turista tiene unas vulnerabilidades y corre unos riesgos, en ocasiones de modo consciente o como consecuencia de imprudencias o simplemente por desconocimiento, entre los que podríamos hacer constar los que generan los estafadores, los robos y hurtos propiciados por los carteristas y los agresores sexuales.

En cualquier caso, pequeños incidentes que, sin llegar a mayores, pueden ahogar las expectativas de unas vacaciones, y de unos servicios hoteleros, y que sin duda alguna repercutirán de modo directo en la credibilidad en la seguridad del país que le acoge y eso, en última estancia, quebrará las cuentas de resultados de la máquina del turismo.

Lo anterior nos obliga a estar en disposición de saber manejar prudentemente los riesgos a través de los conocimientos y cómo no, de las previsiones. Y en esta tarea se reparten por igual las responsabilidades y obligaciones a lo largo de toda la cadena turística:

a. Los Grandes Operadores Turísticos, facilitando cuanta información sea precisa para el turista sobre el país y lugar de acogida, incluidos sus comportamientos sociales, lo que podría definirse como INTELIGENCIA ANTICIPADA.
b. El Estado receptor está obligado a mantener, en estado óptimo, la seguridad ciudadana generando una suerte de confianza al turista potencial, abarcando desde la prevención de incidentes hasta el apoyo, información y ayuda si se ha llegado a producir.
c. También a los establecimientos turísticos se les tiene que asignar tareas como la de garantizar la seguridad de su propio establecimiento y negocio, y asesorar, de modo complementario al que llevan a cabo las Fuerzas y Cuerpos de Seguridad del Estado, apoyar y ayudar a tramitar incidentes, desde el relleno de simples formularios ad – hoc hasta acompañamiento a comisarías o lugares establecidos para formular las denuncias pertinentes, y sobre todo apoyo al turista una vez que el incidente se ha producido.

El incidente es incierto y no fácil de prevenir, pues garantizar una seguridad al cien por cien no es posible, pero las acciones posteriores marcarán la diferencia entre uno y otro establecimiento hotelero

En este orden de ideas, la dirección debe de disponer de planes perfectamente planificados tanto preventivos como reactivos, políticas de seguridad integral así como de gestión de amenazas y riesgos, y normas de autoprotección para los clientes. Vistas las responsabilidades de la industria hotelera parece necesario recomendar la necesidad de que cada uno, cuente con unos servicios pasivos y activos de seguridad, cuya dimensión la marcará el tamaño del hotel y en este sentido los profesionales del sector de la seguridad mucho tienen que aportar a través de sus estudios y experiencias.

De cualquier modo, una industria tan frágil, tan a merced de las circunstancias y de los escenarios nacionales e internacionales, precisa una atención preferente en toda su cadena.

La palabra FIDELIZAR al cliente – turista, debe de ser una máxima permanente. Conviene también tener muy presente que en muchas ocasiones un turista puede convertirse en un potencial inversor y eso nos tiene que obligar a ser proactivos y a tener un sentido prospectivo. En definitiva, podemos afirmar, que la seguridad integral es un problema de cultura empresarial, constituye el pilar del negocio turístico, y que no lo habrá si se carece de seguridad y esta únicamente se conseguirá a través de la plena integración de profesionales cualificados y tecnología.

Gregorio Duro
Tecnico en licitaciones y Proyectos

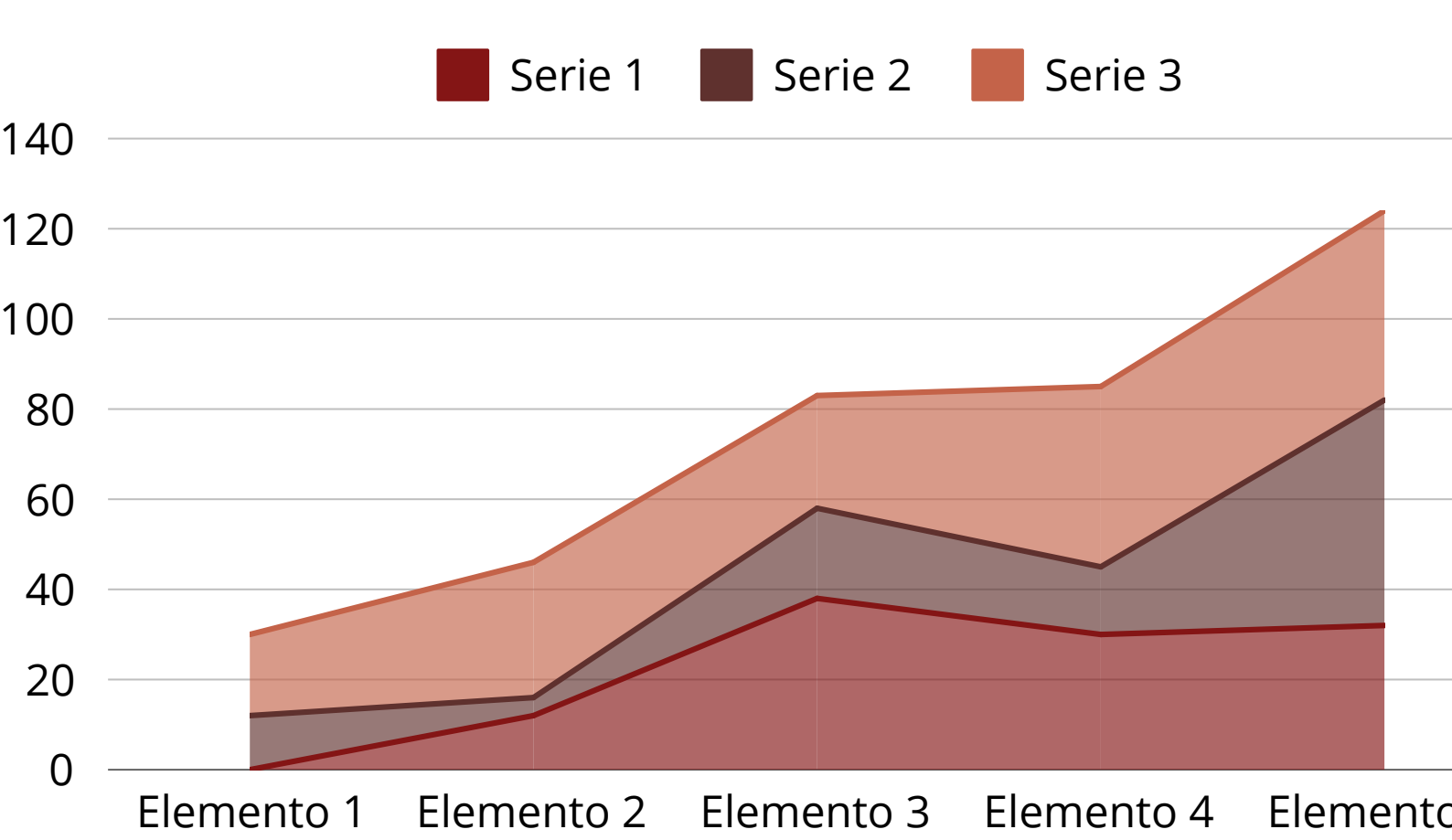
VIGENCIA DEL MÉTODO MOSLER EN EL CONTEXTO ACTUAL

En el artículo de este més, analizaré la vigencia del método Mosler, ampliamente utilizado para el análisis de riesgos en el sector de la seguridad. El método de análisis de riesgos Mosler, desarrollado en una época donde los riesgos eran más previsibles y los entornos organizacionales y tecnológicos menos complejos, bajo mi punto de vista se ha vuelto obsoleto en el contexto actual debido a múltiples deficiencias relacionadas con sus variables limitadas, su rudimentaria forma de cálculo y su inherente simplicidad. Estas características, aunque en su momento lo hicieron accesible y funcional para cualquier profesional, hoy en día restringen gravemente su capacidad para abordar los desafíos de un mundo donde los riesgos son cada vez más complejos, dinámicos y se encuentran más interconectados.

Este método se basa en la utilización de matrices simples que evalúan los riesgos a través de dos variables principales: la probabilidad de ocurrencia y el impacto del evento. Si bien esta aproximación puede ser adecuada para escenarios lineales y predecibles, su diseño falla al intentar capturar la complejidad inherente a los sistemas modernos, donde los riesgos suelen estar interrelacionados, evolucionar rápidamente y generar consecuencias imprevistas debido a su naturaleza multidimensional. La forma de cálculo del método Mosler asigna valores subjetivos a la probabilidad e impacto para luego combinarlos de manera lineal y producir una clasificación de riesgos, lo que resulta demasiado básico para reflejar adecuadamente la realidad actual. Este enfoque no solo ignora la posibilidad de interacciones entre diferentes riesgos, sino que también subestima el impacto acumulativo de eventos secundarios, lo que puede llevar a decisiones mal fundamentadas. Este aspecto es particularmente crítico en sectores donde los riesgos son altamente dinámicos, como la ciberseguridad o la logística entre otros, donde la falta de herramientas avanzadas para modelar escenarios, simular probabilidades o analizar dependencias puede dar lugar a resultados erróneos. La metodología del método Mosler no contempla mecanismos para incorporar variables adicionales que resultan fundamentales en la evaluación de riesgos modernos, como el tiempo de exposición a un riesgo específico, la capacidad de respuesta de la organización ante un evento adverso, o incluso el análisis costo□beneficio de las medidas de mitigación, lo que la coloca en clara desventaja frente a metodologías más robustas como el Enterprise Risk Management (ERM) o el análisis de redes de riesgo (Risk Network Análisis). Otra limitación significativa del método Mosler radica en su dependencia de evaluaciones cualitativas y subjetivas, un enfoque que, aunque fácil de implementar, es propenso a errores humanos y sesgos cognitivos. Esto contrasta marcadamente con los enfoques actuales que emplean inteligencia artificial y aprendizaje automático para procesar grandes volúmenes de datos históricos y patrones emergentes, eliminando en gran medida los sesgos y ofreciendo un análisis más objetivo y preciso.

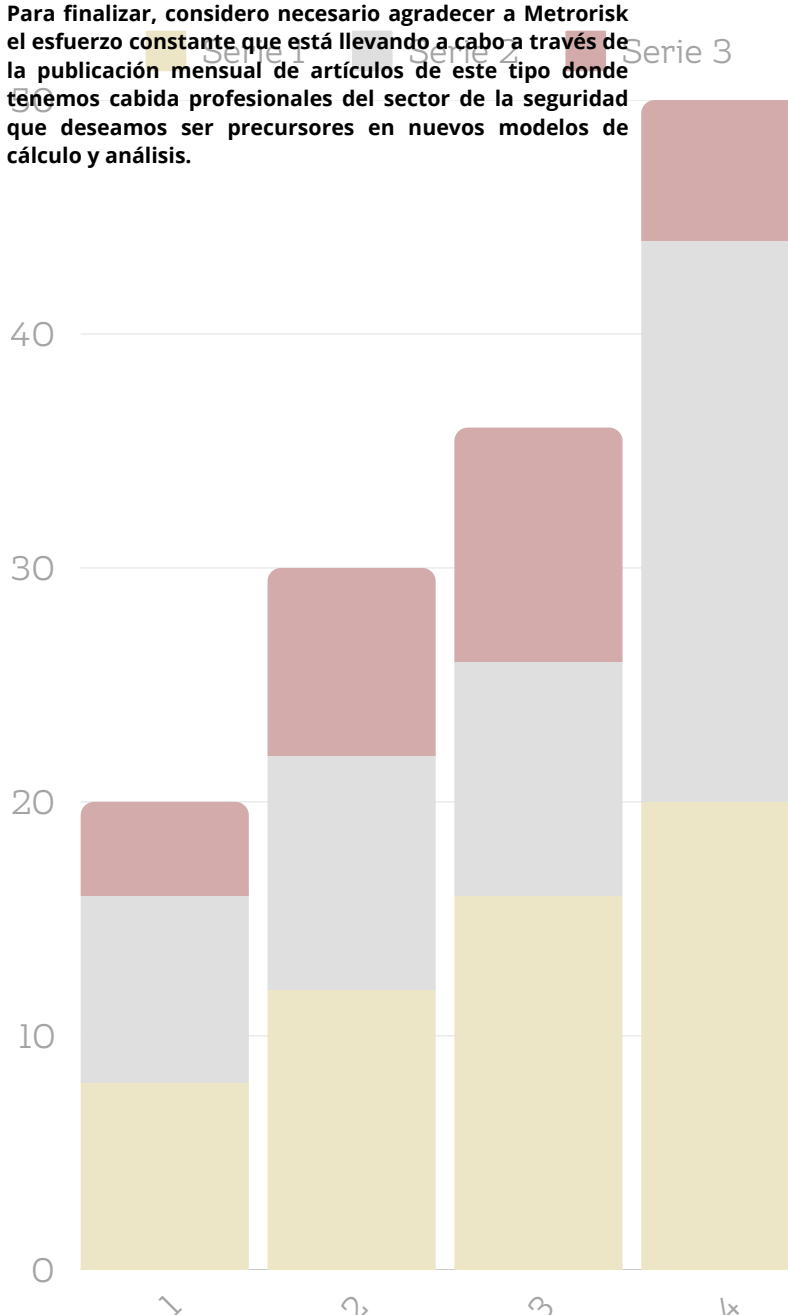
Estos métodos modernos, que integran big data y tecnologías avanzadas, no solo permiten prever riesgos con mayor exactitud, sino que también posibilitan el modelado dinámico y en tiempo real, características indispensables para abordar escenarios de incertidumbre extrema o eventos de alto impacto.

Adicionalmente, la escasa complejidad del método Mosler no solo limita su aplicabilidad, sino que también lo vuelve incapaz de adaptarse a los contextos específicos que exigen un análisis más detallado. Por ejemplo, los riesgos relacionados con el cambio climático, la sostenibilidad y la gobernanza corporativa requieren enfoques más integradores que consideren múltiples variables y la interacción entre factores económicos, sociales y medioambientales, aspectos que están completamente fuera del alcance del método Mosler. El método de análisis de riesgos Mosler, aunque útil en su época, se considera anticuado hoy en día debido a varias limitaciones que lo hacen menos efectivo en comparación con métodos más modernos. Una de las principales críticas es su enfoque en matrices simples que evalúan los riesgos basándose únicamente en las dos variables que he comentado con anterioridad:



Ela probabilidad de ocurrencia y el impacto del evento. Este enfoque puede resultar insuficiente para capturar la complejidad y la interconexión de los riesgos en los entornos empresariales actuales. Además, la asignación de valores en el método Mosler puede ser subjetiva, ya que depende de la opinión de la persona que lo realiza, lo que introduce sesgos y limita la objetividad del análisis. En contraste, los métodos actuales de análisis de riesgos incorporan técnicas avanzadas como simulaciones de Monte Carlo, análisis de escenarios y herramientas de big data, que permiten una evaluación más precisa y dinámica de los riesgos. Estas metodologías modernas no solo consideran una gama más amplia de variables, sino que también facilitan la adaptación a contextos específicos y la identificación de riesgos emergentes en tiempo real. Por otro lado, la persistencia en el uso del método Mosler por parte de algunos profesionales puede atribuirse a una formación deficiente que limita su conocimiento de métodos de cálculo más avanzados. Esta falta de cualificación adecuada impide la adopción de enfoques más sofisticados y eficaces en la gestión de riesgos, lo que subraya la necesidad de una educación continua y actualizada en este campo para enfrentar los desafíos de un entorno empresarial en constante evolución. Aunque el método Mosler representó un avance importante en su época, su diseño simplista, su incapacidad para manejar la interdependencia y dinamismo de los riesgos modernos, y su enfoque basado en pocas variables lo convierten en una herramienta anticuada que no puede competir con los métodos actuales, mucho más avanzados, dinámicos y apoyados en tecnologías de vanguardia. La superación de estas limitaciones exige no solo la adopción de nuevas metodologías, sino también un compromiso con la educación y capacitación continua para garantizar que los profesionales de la gestión de riesgos estén preparados para hacer frente a los desafíos de un mundo en constante transformación.

Para finalizar, considero necesario agradecer a Metrorisk el esfuerzo constante que está llevando a cabo a través de la publicación mensual de artículos de este tipo donde tenemos cabida profesionales del sector de la seguridad que deseamos ser precursores en nuevos modelos de cálculo y análisis.



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

LA COPRODUCCIÓN DE SEGURIDAD: UN ENFOQUE PARA CONSTRUIR COMUNIDAD Y CULTURA DE SEGURIDAD

""TE NECESITAMOS PARA CREAR COMUNIDADES Y CIUDADES SEGURAS Y EN PAZ"

Mercedes Escudero

La Seguridad Ciudadana es un bien público que trasciende las acciones del Estado. Su construcción requiere de la participación activa de las personas, en lo que se conoce como coproducción de seguridad. Este enfoque, sitúa a los ciudadanos como actores protagónicos en la construcción de entornos seguros con empoderamiento ciudadano, ha cobrado relevancia en los últimos años.

La Coproducción de Seguridad es un modelo de gestión que promueve la corresponsabilidad entre los gobiernos y la ciudadanía en la construcción de entornos seguros y pacíficos. Implica la participación de las personas en la identificación de problemas, la búsqueda y diseño de soluciones; la implementación de acciones para mejorar la seguridad en sus comunidades y la evaluación.

Beneficios de la Coproducción de Seguridad:

- Mayor eficacia en la prevención del delito: al conocer de cerca las problemáticas de sus comunidades, las personas pueden identificar los factores de riesgo y proponer soluciones más efectivas.
- Fortalecimiento del tejido social: la participación ciudadana fomenta la cohesión social y el sentido de pertenencia a la comunidad.
- Legitimidad de las acciones de seguridad: al involucrar a las personas en la toma de decisiones, se aumenta la legitimidad de las acciones de las autoridades y se reduce la desconfianza.
- Mayor eficiencia en el uso de recursos: la coproducción en materia de Seguridad permite optimizar el uso de los recursos públicos, al canalizarlos hacia las acciones que realmente tienen un impacto positivo en la seguridad.

Para la implementación de la coproducción de seguridad se requiere de un enfoque holístico que incluya las siguientes acciones:

- Creación de espacios de participación ciudadana: establecer mecanismos formales e informales para que los ciudadanos puedan expresar sus opiniones, inquietudes y propuestas en materia de seguridad.
- Capacitación de los ciudadanos: es necesario capacitar a los ciudadanos en temas de seguridad, prevención del delito y resolución de conflictos para que puedan participar de manera efectiva.
- Fortalecimiento de las organizaciones comunitarias: se debe apoyar la creación y fortalecimiento de organizaciones comunitarias que trabajen en temas de Seguridad.
- Co-creación de políticas públicas: las autoridades gubernamentales deben involucrar a las personas en la elaboración y evaluación de las políticas públicas en materia de Seguridad.
- Uso de tecnologías: puede facilitar la participación de las personas, por ejemplo, a través de plataformas digitales para la denuncia y la colaboración.

Ejemplos de Coproducción de Seguridad:

- Consejos vecinales: permiten a los vecinos organizarse y participar en la toma de decisiones sobre la Seguridad en sus comunidades.
- Rondas vecinales: la vigilancia vecinal es una forma de participación ciudadana que contribuye a prevenir el delito y las violencias.
- Programas de prevención del delito: los programas de prevención del delito deben involucrar a toda la Comunidad y se pueden realizar desde las escuelas. La mediación escolar es ejemplo de coproducción de Seguridad.

La implementación de la coproducción de seguridad enfrenta diversos desafíos, como la falta de confianza en las instituciones gubernamentales, la desigualdad social, la falta de recursos y el desinterés de las personas.

ACUERDO MARCO, PARA LOS SERVICIOS DE SEGURIDAD EN LA JUNTA DE ANDALUCÍA.

Metro Risk

Antonio Pérez Cala
Director de Seguridad.

BREVE RESUMEN DE CÓMO LA JUNTA DE ANDALUCÍA PARA REALIZAR SUS CONTRATACIONES DE LOS SERVICIOS DE SEGURIDAD, HA REALIZADO UN ACUERDO MARCO PARA LA UNIFICACIÓN DE ESTOS.

La Junta de Andalucía, desde la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, a través de su departamento de la Secretaría de Interior, declaró la necesaria uniformidad a la hora de la contratación de los servicios de vigilancia, de mantenimiento de sistemas de seguridad y gestión de alarmas (conexión a Central Receptora de Alarmas (CRA) + respuesta ante alarmas) quedando los mismos formalizados dentro del Acuerdo Marco, 23 de febrero de 2024. (Excluidos contratos menores con respeto a los presupuestos y límites que establece el artículo 118 y concordantes de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público)

Estructuraron 72 lotes teniendo en consideración los tipos de servicios mencionados anteriormente, quedando los mismos referenciados como sigue, M1 instalaciones que solo requieren servicios de Vigilancia, M2 instalaciones que requieren servicios de Vigilancia y a su vez se conectarán a CRA y tendrán su mantenimiento correspondiente, M3 instalaciones que requieren servicios de Vigilancia (24/7) a su vez se conectarán a CRA y tendrán su mantenimiento. Establecen también una gradación económica del valor de los contratos, teniendo en cuenta los tramos de menos de 100.000 euros, de 100.000 a 500.000 euros y un tercer tramo de valor superior a los 500.000 euros. Se presentaron para optar a las licitaciones unas 26 empresas de seguridad, según los tipos de servicios que optarían cada una de ellas, quedando finalmente siete empresas autorizadas. El Acuerdo Marco, tendrá una duración de dos años, las empresas han sido sometidas a un proceso de selección en el que valoraron:

1. Los estudios presentados para los tipos de activos cuya seguridad interior constituye el objeto de los lotes en cuestión (Calidad, tipos de activos en función de riesgos, mapa de riesgos, medidas técnicas, medidas organizativas, etc.)
2. La temprana percepción de sus haberes en los trabajadores adscritos, condición especial de ejecución exigible también a subcontratistas, la acreditación del pago de los salarios del personal adscrito con antelación de 4 días antes de que finalice el mes.
3. El precio, que garantice estabilidad y cumplimiento de Convenio Colectivo en vigor.

Los precios máximos para un servicio básico de cada modalidad que incluye:

- Costes directos de mano de obra (sueldo base, pluses y complementos fijos y SS).
- Costes directos de materiales o equipos.
- Costes indirectos.
- Gastos generales.
- Beneficio industrial

Respecto a la parte que es de las más preocupantes para el personal de seguridad, la Junta de Andalucía a la hora de realizar las Licitaciones, tiene en cuenta los siguientes conceptos mínimos para el presupuesto de licitación:

- Precio: Costes directos de mano de obra, pluses fijos y SS. Costes directos de materiales o equipos. Costes indirectos. Gastos generales. Beneficio Industrial.
- Complementos: Antigüedad del puesto de trabajo. Gratificaciones (navidad, julio y marzo) Plus de distancia, transporte, vestuario.
- Pluses: Peligrosidad. Responsable Equipo. Radioscopia Básica. Trabajo Nocturno. Fines de Semana y Festivos. Noche Vieja y Noche Buena.

Una vez finalizado este breve resumen obviando la parte más técnica en referencia a cómo los técnicos de la Junta realizan las baremaciones de lo presentado por parte de las empresas, en las que el porcentaje del criterio de calidad será del 60%, parece al fin, que las empresas presentadas a cada licitación están a niveles de negocios con los que poder afrontar los pagos a los trabajadores evitando así casos como los sucedidos en contrataciones anteriores

¿Y SI TE DIJERA QUE INTENTAR "ENCERRAR LA LUZ" ES COMO MATAR EL POTENCIAL DE TU EQUIPO?

Metro Risk

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

De adolescente me hice esta pregunta

¿Qué pasaría si enciendo una luz dentro de un cubo sellado con espejos perfectos y luego la apago?

Imaginé que podría atrapar esa energía para siempre, creando una especie de "bomba fotónica" lista para Liberarla con todo su poder.

Pero la realidad me enseño algo muy diferente y valioso Por más perfecta que sea la caja, la luz interactúa con su entorno.

Los electrones y protones absorben Parte de su energía, transformándola en calor y liberándola poco a poco, otra nueva forma.

La luz como las ideas y la creatividad no puede ser encarcelada. Y en esa transformación está su verdadero poder.

En el mundo empresarial ¿cuántas veces intentamos sellar la innovación, retener el talento o encapsular problemas?

Creemos que podemos contenerlos, pero lo único que hacemos es apagar la chispa.

Las ideas, los equipos y las oportunidades no se atrapan: se potencian, se dejan fluir.

La clave está en reflejar y amplificar la luz, no en atraparla.

Los grandes líderes entienden esto. inspiran, transforman y permiten que la energía fluya libremente. ?

Si estás "encerrando luz" en tu organización, estás perdiendo mucho más de lo que crees. ¿Listo para romper ese cubo y dejar que las ideas brillen?

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

¿SEGURIDAD INTELIGENTE O RIESGO OCULTO?

Metro Risk

Rosa Fernandéz

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

ASUNTO: SEGURIDAD 360º

¿Te gusta saber y estar al día de las últimas novedades, tendencias y herramientas? ¿Quieres conocer cómo la tecnología afecta a tu empresa de seguridad o a tu actividad profesional en este sector?

Si la respuesta es sí, estás en el sitio adecuado, así que sigue leyendo, por favor. La seguridad privada se encuentra en un momento de transformación impulsada por avances tecnológicos que redefinen sus métodos y herramientas. Sin embargo, las innovaciones con las que trabajamos cada día, presentan desafíos significativos en términos de cumplimiento normativo, especialmente con el Reglamento General de Protección de Datos (RGPD).

Te traigo por aquí algunas de las tendencias emergentes en Seguridad Privada y el Impacto que tiene en la Protección de Datos, datos que por supuesto tu empresa tiene la obligación de proteger. IA.

Como no, nuestra querida IA que está revolucionando el sector mediante herramientas como sistemas de videovigilancia inteligente realizando análisis en tiempo real para la detección de comportamientos sospechosos. O sistemas de reconocimiento facial, permitiendo la Identificación de personas en tiempo real en eventos masivos o áreas restringidas. Estas herramientas son muy útiles, pero comportan riesgos importantes si el Compliance RGPD no está bien llevado en la empresa.

Proteger el perímetro de la privacidad que afecta a los derechos del interesado es la prioridad, y por eso hay que conocer el impacto que estas herramientas tiene en esa privacidad para poder gestionarlo adecuadamente y poder realizar un tratamiento legal y legitimado.
¿Cómo lo hago?

• Pide el consentimiento explicito de los interesados
• Realiza evaluaciones de impacto relativas a la protección de datos (EIPD)
• Aplica medidas técnicas para garantizar la arnonimización o pseudonimización de los datos.

DRONES. Los drones son cada vez más populares en el sector, proporcionando una visión aérea y acceso a áreas de difícil alcance. Una herramienta muy práctica, que permite a las empresas de seguridad dar un valor añadido importante a la relación con los clientes, ampliando el alcance de sus servicios y competencias.

Pero al igual que pasa con la IA, esto comporta riesgos si el Compliance RGPD no está bien adaptado e implantado, ya que pueden captarse imágenes no deseadas, hacer capturas inadvertidas de imágenes o información personal de terceros no implicados. invadir espacios no consentidos, o adolecer de falta de transparencia en el tratamiento de los datos captados por drones. Todo ello es un reto de cumplimiento para la empresa.

¿Cómo lo hago? Entre otras medidas te sugiero estas:

• Informar adecuadamente mediante carteles o avisos cuando se utilicen drones en áreas aero videovigiladas.
• Asegurar que las grabaciones se eliminen cuando ya no sean necesarias para el propósito previsto.
• Puedes realizar el curso RGPD y DRONES.

INTERNET DE LAS COSAS (IOT) (MÁS BIEN LAS COSAS EN INTERNET) Y DISPOSITIVOS CONECTADOS

Suena mucho en la publicidad de una empresa de seguridad un avance que puede ser revolucionario: la cerradura inteligente. Si te fijas, todo en el SXXI es inteligente, y eso nos obliga a ponernos en guardia. Cámaras, alarmas y otros dispositivos IoT conectados a redes o a aplicaciones de las que no sabemos tan siquiera ni quien es la empresa ni dónde están sus servidores que almacenarán los datos que vamos tratando en nuestra operativa. Todas estas soluciones están permitiendo una seguridad más eficiente, pero también aumentan las vulnerabilidades ante ciberataques y los riesgos en la protección al tener a los datos viajando por el ciberespacio, y alojándose no se sabe dónde.

Por un lado estas soluciones aumentan la “seguridad” o la percepción de seguridad en el cliente, pero tienen un lado oscuro: una vez que capturamos el dato (que no es nuestro) no sabemos ni quien lo maneja, ni dónde lo aloja, ni si lo cede o no. Es decir, abrimos la puerta a usuarios no autorizados que ponen en riesgo los datos de nuestros clientes, con lo cual nuestra seguridad o al menos los servicios de seguridad que les prometemos no son todo lo seguros que deberían, ni protegen todo lo que deberían de proteger.

Ponemos en riesgo los datos de nuestros clientes y colaboradores, ¿Cómo evitarlo?

-Seguridad por diseño y por defecto: Los dispositivos deben incorporar medidas de ciberseguridad desde su desarrollo.
-Supervisar la transferencia de datos en tiempo real para prevenir filtraciones.
-Identificar a los proveedores de esta tecnología y tener formalizados con ellos contratos de encargados del tratamiento: eso legitima el procesamiento de los datos.

MORALEJA.

Una empresa de seguridad privada que no cumple con el RGPD no solo arriesga su operatividad legal y económica, sino también la confianza de sus clientes, lo que puede llevar a su pérdida de competitividad en el mercado. Como alternativa, esta empresa debería invertir en un programa sólido de cumplimiento normativo y seguridad de datos para garantizar la protección de sus clientes y su sostenibilidad en el tiempo.

Nuestros servicios de **CONSULTORÍA, ASESORAMIENTO, FORMACIÓN Y AUDITORÍA** te permiten aplicar el cumplimiento digital (RGPD,LOPDgdd, ePrivacy, Redes, Cloud...) en tu empresa, aumentando la reputación y la confianza y evitando sanciones. Trabaja con nosotros y entra en ZonaVigilada, tu Agencia de Seguridad y Protección.

Zonavigilada y MetroRisk se han unido para ofrecerte una protección
¡Protege tu negocio con Suscripción MetroRisk por solo 35€/mes!
Un blindaje integral en un solo servicio
En un mundo donde la protección de datos es una prioridad y las sanciones por incumplimientos pueden ser devastadoras, Suscripción MetroRisk te ofrece la tranquilidad de un cumplimiento RGPD 360º, diseñado para que te centres en lo que importa: tu negocio.

¿Por qué elegir la Suscripción MetroRisk?
1. Cumplimiento normativo garantizado: Nos aseguramos de que tu empresa cumpla con todas las exigencias del RGPD, desde evaluaciones de impacto hasta protocolos de tratamiento de datos.
2. Asesoramiento experto: Accede a profesionales especializados que resolverán tus dudas y te guiarán paso a paso.
3. Monitorización continua: Supervisamos el cumplimiento en tiempo real para prevenir riesgos antes de que se conviertan en problemas.
4. Protección integral: Cobertura completa que incluye documentos legales, formación y medidas técnicas.

Beneficios que marcan la diferencia
- Evita sanciones que pueden alcanzar millones de euros.
- Refuerza la confianza de tus clientes al garantizar la seguridad de sus datos.
- Simplifica la gestión del RGPD con soluciones claras y personalizadas.

Por solo 35€ al mes, obtendrás una solución integral que protege tu negocio, tu reputación y tus clientes.
Suscripción MetroRisk: La tranquilidad de estar siempre protegido.
¿Listo para llevar la seguridad al siguiente nivel?
suscríbete ahora.
MetroRisk transforma el cumplimiento normativo en tu mejor estrategia de seguridad. ¿Estás listo para blindar tu negocio?

MeTroRisk™

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

LA SEGURIDAD DISCONTINUA SEGÚN LA LEY DE SEGURIDAD PRIVADA 2014

Metro Risk

Carlos Serrano
Director de Contenidos de Seguridad y Empleo

www.seguridadyempleo.com

La Ley 5/2014 de Seguridad Privada, en su artículo 41, establece los distintos tipos de servicios que pueden ofrecer las empresas del sector. Entre ellos, una modalidad que ha suscitado interés y debate es la de los servicios de vigilancia discontinua. Estos servicios, definidos en el apartado e) del mencionado artículo, consisten en la realización de rondas o visitas intermitentes y programadas a diferentes puestos o lugares objeto de protección.

Aunque a primera vista esta modalidad podría parecer secundaria frente a los servicios de vigilancia permanente, su relevancia operativa y estratégica ha ido ganando peso en el sector, especialmente en contextos donde la optimización de recursos y la adaptación a las necesidades del cliente son prioritarias. ¿Qué es la seguridad discontinua?

La seguridad discontinua se refiere a los servicios intermitentes y planificados que realiza el personal de seguridad privada en diferentes puntos establecidos previamente. Este modelo no implica una vigilancia estática o continua, sino rondas o inspecciones periódicas en lugares concretos, que suelen incluir:

Edificios o instalaciones con baja actividad nocturna.
Urbanizaciones residenciales.
Polígonos industriales o almacenes.
Oficinas o locales comerciales en horarios no operativos

El principal objetivo de este tipo de vigilancia es prevenir riesgos mediante la presencia puntual del vigilante, quien puede detectar incidentes, disuadir actos delictivos y garantizar la protección de bienes o instalaciones sensibles. Ventajas de la seguridad discontinua para empresas y clientes La seguridad discontinua ofrece múltiples beneficios tanto para las empresas del sector como para los clientes que contratan estos servicios:

1. Optimización de recursos: Permite distribuir al personal de seguridad de manera más eficiente, cubriendo múltiples ubicaciones con un coste operativo menor que el de la vigilancia permanente.
2. Reducción de costes para el cliente: Este servicio resulta más económico para empresas pequeñas, comunidades de vecinos o propietarios de instalaciones con necesidades puntuales de seguridad.
3. Flexibilidad operativa: La modalidad discontinua se adapta fácilmente a las necesidades del cliente, permitiendo ajustar horarios, rutas y frecuencia de visitas según las exigencias específicas de cada caso.
4. Efecto disuasorio: Aunque no implica una presencia constante, la realización de rondas aleatorias o programadas genera incertidumbre en potenciales infractores, aumentando la sensación de seguridad.

Desafíos operativos y normativos para las empresas de seguridad A pesar de sus ventajas, la implementación de servicios de seguridad discontinua presenta desafíos específicos que las empresas del sector deben gestionar con especial cuidado:

1. Coordinación logística: Diseñar rutas eficientes y garantizar que los vigilantes cumplan con los horarios establecidos requiere una planificación precisa y herramientas tecnológicas avanzadas, como sistemas de geolocalización o gestión de rondas.
2. Cumplimiento normativo: Según la Ley 5/2014, estos servicios deben ser prestados por personal habilitado y cumplir con los requisitos generales de la seguridad privada, lo que incluye formación adecuada, uso de equipos homologados y coordinación con las fuerzas de seguridad pública en caso necesario.
3. Garantía de efectividad: A diferencia de la vigilancia permanente, la seguridad discontinua puede ser percibida como insuficiente si no se comunica claramente al cliente el alcance y los objetivos del servicio.
4. Adaptación a incidentes: Al tratarse de un servicio no permanente, la capacidad de reacción ante un incidente puede ser más limitada, lo que exige a las empresas tener protocolos bien definidos para responder a emergencias.

Impacto en la percepción de la seguridad Un aspecto fundamental de la seguridad discontinua es cómo esta modalidad afecta la percepción de la seguridad en las áreas protegidas. Aunque no implica una presencia constante, los servicios intermitentes pueden generar una sensación de control y vigilancia suficiente, siempre que se ejecuten de manera profesional y bien organizada.

Por otro lado, es importante que los clientes comprendan que este modelo no sustituye a la vigilancia permanente en contextos de alta criticidad, como infraestructuras críticas o eventos masivos, sino que actúa como un complemento estratégico en situaciones de menor riesgo. El futuro de la seguridad discontinua En un sector en constante evolución, la seguridad discontinua se perfila como una solución cada vez más demandada por su capacidad para equilibrar eficiencia operativa y reducción de costes. Sin embargo, su consolidación requiere que las empresas del sector inviertan en: Tecnología de gestión: Aplicaciones móviles, software de control de rondas y sistemas de verificación en tiempo real.

LA SEGURIDAD PRIVADA EN EL CONTEXTO GEOPOLÍTICO ACTUAL

Metro Risk

Abraham Santana Herrera
Director de seguridad. Perito

En un mundo donde los conflictos geopolíticos están en constante evolución, la seguridad privada ha emergido como un actor clave para mitigar riesgos y ofrecer soluciones en escenarios donde los estados no pueden o no quieren intervenir directamente. Desde la protección de infraestructuras críticas hasta la asesoría en zonas de conflicto, la seguridad privada desempeña un papel crucial en este contexto global de tensiones y conflictos

Los conflictos actuales, caracterizados por su naturaleza híbrida y asimétrica, han ampliado las demandas sobre la seguridad privada:

• Protección de Infraestructuras Estratégicas: Empresas de seguridad privada son contratadas para resguardar instalaciones críticas como oleoductos, redes eléctricas y centros de datos, especialmente en áreas con inestabilidad política.
• Seguridad de Cadenas de Suministro: En un contexto donde las guerras y sanciones afectan las rutas comerciales, las empresas privadas aseguran el transporte de bienes esenciales, desde alimentos hasta tecnología.
• Servicios en Zonas de Conflicto: Compañías especializadas despliegan personal para proteger instalaciones corporativas, embajadas y misiones humanitarias en regiones afectadas por conflictos.

La seguridad privada en este contexto abarca diferentes áreas:
• Asesoría estratégica: Consultoras en seguridad privada analizan riesgos específicos de cada región, desde amenazas terroristas hasta conflictos locales, para asesorar a sus clientes.
• Ciberseguridad: Dado el auge de la guerra híbrida, las empresas privadas juegan un papel esencial en proteger infraestructuras digitales contra ciberataques.
• Formación y entrenamiento: Empresas de seguridad ofrecen capacitación a fuerzas locales y privadas en técnicas avanzadas de defensa, manejo de crisis y uso de tecnología de punta.

A pesar de su importancia, la seguridad privada enfrenta varios desafíos en este contexto:
• Regulación Internacional: La falta de normativas claras y unificadas dificulta la supervisión de actividades, especialmente en zonas de conflicto donde las empresas privadas actúan como intermediarias.
• Reputación y Ética: Operar en áreas de guerra puede implicar dilemas éticos relacionados con la legitimidad de las operaciones y el respeto a los derechos humanos.
• Competencia por Recursos Humanos: La necesidad de personal altamente capacitado genera una competencia feroz por talentos, incrementando los costos y la necesidad de formación continua.

Por otro lado, el contexto geopolítico actual también abre oportunidades:
• Demanda en Crecimiento: La expansión de conflictos genera un aumento en la demanda de servicios especializados.
• Innovación Tecnológica: Las empresas privadas lideran el desarrollo de herramientas avanzadas, como drones, sistemas de vigilancia basados en inteligencia artificial y plataformas de análisis de riesgos.

En un escenario donde los recursos públicos a menudo son insuficientes, la cooperación entre gobiernos y empresas de seguridad privada se ha vuelto esencial:

• Contratos Públicos: Los gobiernos recurren a empresas privadas para complementar las operaciones de seguridad nacional, especialmente en áreas remotas o de alto riesgo.
• Intercambio de Información: Las empresas privadas proporcionan inteligencia valiosa sobre amenazas locales y globales, alimentando la toma de decisiones a nivel estatal.
• Gestión de Crisis: En situaciones de evacuación o desastre, estas compañías ofrecen soporte logístico y operacional.

En un mundo cada vez más interconectado y volátil, la seguridad privada continuará evolucionando. La integración de tecnologías disruptivas, el establecimiento de estándares globales y la profesionalización del sector serán claves para que este actor siga desempeñando un rol estratégico en el marco geopolítico actual

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

LA REVOLUCIÓN DIGITAL EN EL DEPORTE: UNA NECESIDAD PARA TODOS LOS PROFESIONALES

Metro Risk

Elena de la Parte

En la era digital, la tecnología y los datos se han convertido en pilares fundamentales para el éxito en todos los sectores, y el deporte no es una excepción. La integración de estas herramientas ha transformado la manera en que las entidades deportivas, desde clubes de fútbol hasta organizaciones olímpicas, gestionan sus recursos, optimizan el rendimiento de sus atletas, se conectan con los aficionados y mejoran la eficiencia en todas las áreas

Este artículo explora las vastas oportunidades que ofrecen estas innovaciones en el ámbito deportivo y destaca la importancia crucial de que todos los profesionales dentro de una entidad deportiva se sumerjan en este mundo digital. La transformación tecnológica y la aplicación del análisis avanzado de datos no se limitan al terreno de juego ni a los expertos en tecnología; abarcan cada aspecto y talento dentro de una organización, desde la gestión institucional hasta el marketing, la comunicación y el departamento legal.

"La tecnología y el análisis de datos ofrecen un valor estratégico en el deporte, accesible a todos los profesionales, desde la alta dirección hasta los departamentos legal, marketing y comunicación. Comprender y aprovechar estas herramientas es clave para optimizar el rendimiento y alcanzar el éxito en cada área."

¿Por qué es esencial que todos los profesionales deportivos comprendan el potencial de los datos y la tecnología? Para mantenerse competitivas en este nuevo panorama digital, las entidades deportivas y sus integrantes deben adoptar plenamente la tecnología y los datos, explotando al máximo su potencial para impulsar cada área de gestión. Ventajas clave de la tecnología y los datos en el deporte:

- Potencial deportivo: La tecnología y el análisis de datos han abierto nuevas fronteras en el rendimiento deportivo. Desde el monitoreo de la salud de los atletas hasta el análisis avanzado de video para perfeccionar tácticas y estrategias, estas herramientas proporcionan a entrenadores y deportistas una ventaja competitiva sin precedentes.
- Ciencia del Deporte y Fisiología: Los profesionales de estas áreas pueden utilizar los avances tecnológicos y el análisis de datos para realizar un seguimiento más preciso del rendimiento físico de los atletas, identificar áreas de mejora y diseñar programas de entrenamiento más efectivos. Los dispositivos portátiles que rastrean el rendimiento físico en tiempo real permiten a los entrenadores ajustar los entrenamientos con precisión para maximizar el progreso y minimizar el riesgo de lesiones.
- Análisis de rendimiento en tiempo real: Los avances tecnológicos permiten un análisis detallado del rendimiento de los atletas durante la competición en tiempo real. Esto proporciona a los entrenadores información valiosa sobre el desempeño de sus equipos y les permite realizar ajustes tácticos sobre la marcha, optimizando las posibilidades de alcanzar sus objetivos.
- Desarrollo de talentos: Los responsables de descubrir, identificar y desarrollar nuevos talentos pueden utilizar la tecnología para evaluar el potencial de los jóvenes deportistas, analizar su progreso y proporcionarles el apoyo necesario para alcanzar su máximo rendimiento.

El impacto en las distintas áreas de una entidad deportiva:

- Alta Dirección: Los líderes deben comprender cómo las últimas tendencias tecnológicas pueden impactar en la estrategia global de la institución, mejorando la eficiencia operativa, aumentando los ingresos y fortaleciendo la posición competitiva. Estas herramientas brindan una visión más detallada y precisa para la toma de decisiones estratégicas.
- Recursos Humanos: El departamento de recursos humanos puede utilizar herramientas tecnológicas para gestionar el reclutamiento, la contratación y el desarrollo del personal, así como para mejorar la comunicación interna.
- Marketing y Comunicación: La transformación tecnológica ofrece nuevas oportunidades para llegar de manera más efectiva a los aficionados y crear experiencias únicas que generen engagement y fidelidad a la marca. La tecnología también brinda oportunidades para monetizar contenidos y aumentar el fan engagement.
- Departamento Legal: En un entorno cada vez más regulado, el departamento legal juega un papel crucial en la implementación de tecnologías y el manejo de datos, garantizando el cumplimiento normativo y mitigando el riesgo legal, incluyendo la prevención de fraudes y la protección de la integridad deportiva.
- Innovación y Desarrollo: Los profesionales responsables de la innovación y el desarrollo estratégico deben mantenerse actualizados con las últimas innovaciones tecnológicas para identificar nuevas oportunidades de negocio y mejorar los procesos internos. La investigación y desarrollo de nuevas tecnologías deportivas son cruciales para mantener a la entidad a la vanguardia.

Desde la optimización del rendimiento deportivo hasta la conexión con los seguidores, estas herramientas han demostrado ser fundamentales en la evolución del deporte. Es crucial que todos los profesionales dentro de una entidad deportiva reconozcan el potencial de la tecnología y los datos, y se comprometan a mantenerse actualizados en este ámbito en constante cambio. Solo así podrán aprovechar plenamente las oportunidades que ofrecen estas innovaciones y mantener la competitividad en un panorama deportivo cada vez más exigente y digitalizado.

Cuando hablamos de gestión de seguridad deportiva nos referimos a la seguridad en aquellos eventos deportivos en los cuales se prevé un gran desplazamiento masivo, encuentros eliminatorios, eventos con antecedentes, eventos con amenazas. La gestión integral de la seguridad deportiva se basa en la preparación de medidas preventivas y reactivas que abarcan diversas fases, garantizando una cobertura completa.

"Tras 20 años dedicados al arbitraje de Fútbol Sala, desde categorías Base hasta crono en Nacional B, puedo afirmar que esta experiencia ha dejado una huella imborrable en mi vida. Me ha permitido crecer como profesional y como persona, fortaleciendo mi resiliencia y asertividad, además de transmitirme valores, principios y una sólida disciplina deportiva que forman parte integral de mi ser."

Todo colectivo arbitral, necesita una protección y tener una sensación de seguridad, en fases de; prepartido. Durante el encuentro e incluso y no por esto menos importante, la protección de todo el colectivo arbitral, después de finalizar un encuentro-Al igual que la protección de los medios de transporte en los que realizan sus desplazamientos. ¿Como funcionan las nuevas tecnologías para los árbitros? La seguridad para los árbitros consta de un dispositivo de localización

El sistema de protección para árbitros consiste en un dispositivo de localización portátil, integrado en un reloj de muñeca, que incorpora un pulsador de emergencia (SOS). La activación de dicho pulsador genera una señal de alarma que es recibida por un Centro de Operaciones de Seguridad (SOC). Los operadores del SOC establecen una comunicación de audio bidireccional con el árbitro para la verificación de la incidencia. En caso de confirmación, se procede a la notificación a las Fuerzas y Cuerpos de Seguridad del Estado.

Con este artículo, os invito a realizar una reflexión, de resiliencia, empatía sobre todo de respeto a todos los sectores profesionales. Con humanidad y solidaridad. Recordando la cohesión y colaboración de la seguridad privada, las FFCSE los deportistas, los árbitros. Con el lema principal, que debemos tener marcado a fuego que; “Mas allá del resultado en toda competición predomina la deportividad "considero bajo mi punto de vista, que la deportividad y la educación se debe inculcar en edades tempranas.

Edgar Octavio Herrera Rodríguez

LAS FUNCIONES DEL AGENTE DE SEGURIDAD PRIVADA: UN PILAR ESENCIAL EN EL ESQUEMA DE SEGURIDAD

El rol del agente de seguridad privada ha evolucionado significativamente en las últimas décadas, adaptándose a las demandas de una sociedad cada vez más compleja y globalizada. En el contexto de Guatemala, la seguridad privada se ha convertido en un elemento esencial para la protección de bienes, recursos humanos y activos intangibles. Experimentado un crecimiento significativo en las últimas décadas, convirtiéndose en un componente esencial para la protección de bienes y personas en diversas organizaciones. Los agentes de seguridad privada desempeñan un papel fundamental en este esquema, enfrentando múltiples desafíos que van desde condiciones laborales precarias hasta riesgos inherentes a su labor. Este ensayo analiza las funciones de estos agentes, su preparación, los incidentes que los afectan y la situación actual de las empresas de seguridad en el país.

La preparación del agente de seguridad privada

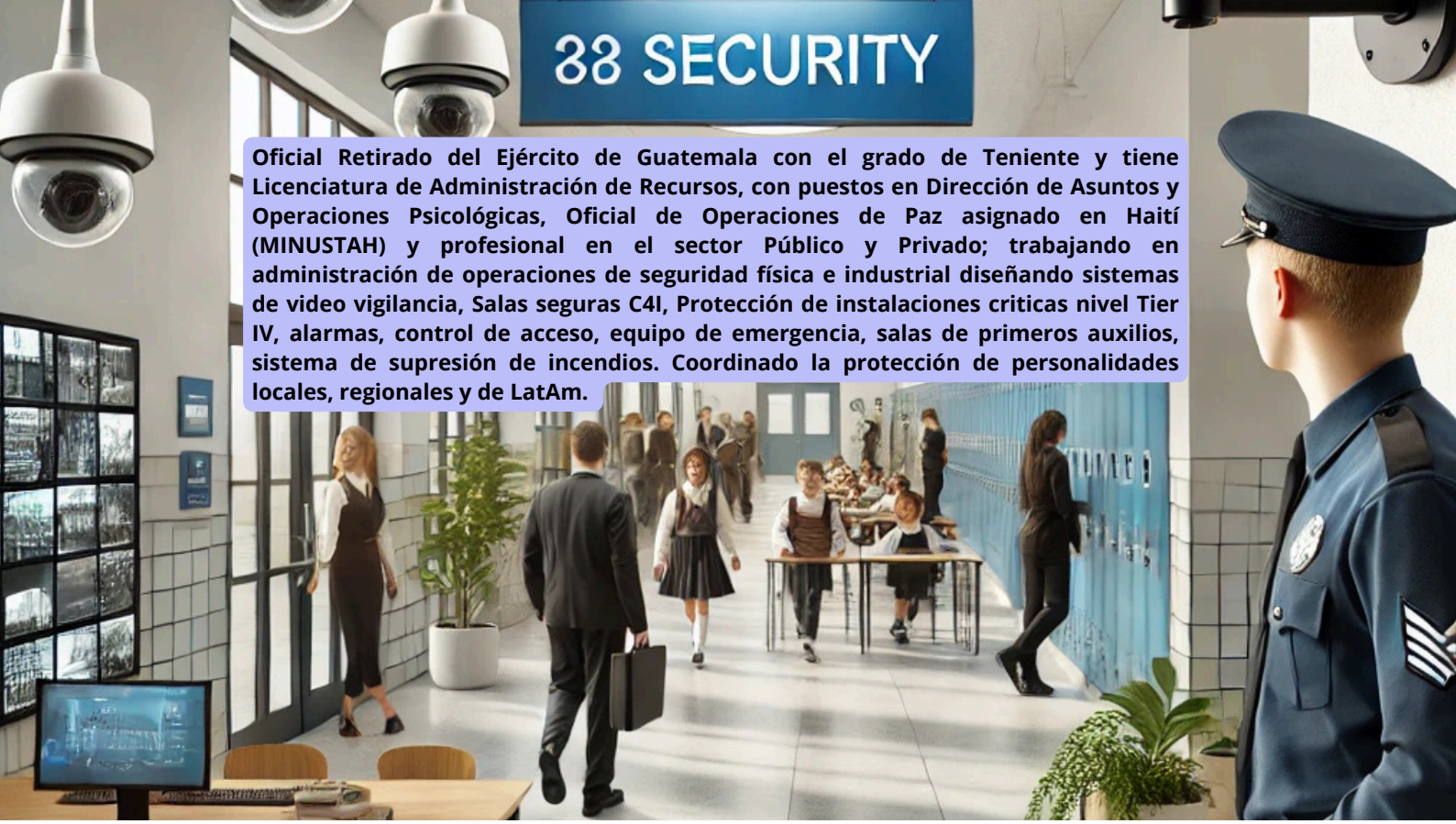
La preparación de los guardias de seguridad es un tema crucial y complejo que varía según la región, la legislación local y las decisiones comerciales tanto del cliente como del proveedor y que influye directamente en su desempeño. En Guatemala, la Dirección General de Servicios de Seguridad Privada (DIGESSP) es la entidad encargada de regular y supervisar a las empresas de seguridad privada. Según datos de la DIGESSP, hasta febrero de 2023, existían 250 entidades autorizadas para operar en el país y empleando a más de 42,000 agentes registrados. Sin embargo, el cumplimiento de los requisitos legales y la capacitación obligatoria son retos persistentes

La preparación de los guardias de seguridad es un tema que debe ir más allá de los aspectos técnicos, incluyendo competencias interpersonales y conocimiento del entorno organizacional donde se desempeña el agente. En este sentido, la formación debe abordar también los factores culturales y sociales que afectan su trabajo, especialmente en regiones como Latinoamérica, donde la violencia y el crimen organizado plantean retos únicos. Sin embargo, en la práctica, a menudo se le asignan tareas adicionales ajenas a la seguridad, como recepción, atención de pedidos o labores de conserjería, lo que puede desviar su atención de sus responsabilidades principales

Roles y funciones principales del guardia de seguridad
El agente de seguridad uniformado es el eslabón fundamental dentro del sistema de protección. Sus funciones pueden clasificarse en tres categorías principales:

1. Prevención y disuasión:
   - o Control de accesos para evitar intrusiones no autorizadas.
   - o Supervisión de áreas críticas mediante rondas de vigilancia.
   - o Identificación de comportamientos sospechosos para prevenir incidentes.
2. Protección de bienes y recursos:
   - o Salvaguardar activos tangibles e intangibles.
   - o Monitorear sistemas de seguridad electrónica, como cámaras de vigilancia y alarmas.
3. Atención y servicio al cliente:
   - o Actuar como el primer punto de contacto en las instalaciones.
   - o Brindar información y asistencia al personal y visitantes.
   - o Gestionar situaciones de emergencia con profesionalismo.

Los desafíos del agente de seguridad El documento también aborda las dificultades que enfrentan los guardias al desempeñar funciones ajenas a su rol principal, como recepción, jardinería o mensajería. Esto no solo disminuye su capacidad para cumplir con las tareas de seguridad, sino que también genera una percepción errónea de su valor dentro de la organización. Además, la rotación frecuente de personal y la falta de reentrenamiento adecuado contribuyen a la desvalorización de la profesión. Según un informe de la Federación de Empresas de Seguridad de Centroamérica y Panamá (FEDECASP), solo el 40% de los agentes en Guatemala recibe capacitación continua, lo que impacta negativamente en la calidad del servicio



Oficial Retirado del Ejército de Guatemala con el grado de Teniente y tiene Licenciatura de Administración de Recursos, con puestos en Dirección de Asuntos y Operaciones Psicológicas, Oficial de Operaciones de Paz asignado en Haití (MINUSTAH) y profesional en el sector Público y Privado; trabajando en administración de operaciones de seguridad física e industrial diseñando sistemas de video vigilancia, Salas seguras C4I, Protección de instalaciones criticas nivel Tier IV, alarmas, control de acceso, equipo de emergencia, salas de primeros auxilios, sistema de supresión de incendios. Coordinado la protección de personalidades locales, regionales y de LatAm.

Crecimiento de la industria de seguridad privada en Guatemala En los últimos cinco años, la industria de la seguridad privada en Guatemala ha experimentado un crecimiento significativo. Según datos de la DIGESSP, el número de empresas registradas aumentó en un 15% entre 2018 y 2023. Este crecimiento refleja la creciente demanda de servicios de protección en un país donde los índices de criminalidad siguen siendo altos.

Estadísticas recientes indican que el 65% de los negocios en el país contratan servicios de seguridad privada, lo que subraya su importancia como un pilar en la economía nacional. Sin embargo, también pone de manifiesto la necesidad de una regulación más estricta y de mecanismos de supervisión para garantizar la calidad del servicio.

Condiciones Laborales y Riesgos Las condiciones laborales de los guardias de seguridad en Guatemala son, en muchos casos, precarias. Largas jornadas laborales, salarios bajos y falta de garantías legales son algunas de las problemáticas que enfrentan. Entre 2010 y julio de 2018, se registraron 21,314 denuncias contra empresas privadas de seguridad ante el Ministerio de Trabajo, evidenciando las malas condiciones laborales en el sector. Además de las condiciones laborales, los agentes de seguridad están expuestos a diversos riesgos. Por ejemplo, se han reportado incidentes donde delincuentes han intoxicado a guardias de seguridad para perpetrar robos en las instalaciones que custodian Estos hechos ponen de manifiesto la vulnerabilidad a la que están expuestos en el ejercicio de sus funciones.

La percepción del servicio de seguridad Un aspecto clave es la percepción de los usuarios respecto a los agentes de seguridad. En un estudio realizado por la Cámara de Comercio de Guatemala en 2022, el 70% de los encuestados afirmó que el desempeño de los guardias era adecuado, pero el 45% consideró que las empresas proveedoras no invertían lo suficiente en su capacitación. Esto refleja la necesidad de un enfoque más integral que combine la preparación profesional con una mejor valoración del rol de los agentes.

Esto además que, en los últimos años, el número de empresas de seguridad privada en Guatemala ha aumentado considerablemente. Según datos del Registro Nacional de Empresas, Personal y Equipo de Seguridad Privada, en los últimos cinco años se ha registrado un incremento en el número de empresas, sin embargo, la informalidad en el sector es considerable, con numerosas empresas irregulares que representan una competencia desleal para aquellas que operan legalmente.

La DIGESSP reporta que, hasta enero de 2022, había 140 empresas autorizadas para prestar servicios de seguridad privada y 68 en proceso de adecuación. No obstante, estimaciones de la Cámara de Seguridad y Gremial de Empresas de Seguridad Privada sugieren que el número real de agentes de seguridad privada podría ser hasta cinco veces mayor que las cifras oficiales, lo que indica la existencia de un mercado informal significativo.

Desafíos y Retos del Sector El sector de la seguridad privada en Guatemala enfrenta varios desafíos. La proliferación de empresas "piratas" o no registradas complica la supervisión y regulación efectiva del sector. Estas empresas suelen evadir responsabilidades laborales y fiscales, afectando tanto a los trabajadores como a la calidad del servicio ofrecido. Además, la falta de capacitación continua y adecuada para los agentes de seguridad limita su eficacia en la prevención y respuesta ante incidentes. La DIGESSP ha implementado programas de capacitación para instructores y directores de agentes de seguridad privada, buscando mejorar la calidad del servicio y las condiciones laborales de los agentes.

Recomendaciones para mejorar el esquema de seguridad

1. **Capacitación continua**
2. **Supervisión efectiva**
3. **Reconocimiento profesional**
4. **Colaboración público-privada**

CONOCE A...

Metro Risk

Jonatthan Hermida Sosa. SAPPC, SFPC, DAS, CPO, ISOC, GER, CRASE.

LOS RETOS DE LA CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL EN LAS MIPYMES Y PYMES MEXICANAS

En un mundo cada vez más digitalizado, las micro, pequeñas y medianas empresas (mipymes y pymes) en México enfrentan un panorama complejo. Aunque estas empresas representan más del 90% del total de unidades económicas del país y generan aproximadamente el 72% de los empleos, también son uno de los sectores más vulnerables a los riesgos cibernéticos. La incorporación de tecnologías avanzadas, como la inteligencia artificial (IA), puede ofrecer soluciones clave, pero también plantea nuevos desafíos.

La vulnerabilidad de las mipymes y pymes en México Las mipymes y pymes mexicanas suelen operar con presupuestos limitados, lo que restringe su capacidad para invertir en tecnologías de seguridad y capacitación del personal. Además, la percepción de riesgo en ciberseguridad es baja, lo que las deja expuestas a amenazas como:

- Ransomware: Los ciberdelincuentes bloquean los sistemas de las empresas y exigen un rescate por su liberación.
- Phishing: Las pequeñas empresas son objetivo fácil de correos electrónicos fraudulentos que buscan robar información confidencial.
- Ataques internos: La falta de protocolos claros y supervisión puede facilitar el robo de datos por parte de empleados.

Según un informe reciente, más del 40% de las mipymes en América Latina no cuentan con una estrategia de ciberseguridad, y el 60% de las que sufren un ataque cibernético cierran operaciones en menos de seis meses. En México, donde el uso de tecnología ha crecido aceleradamente, estas cifras son alarmantes.

La inteligencia artificial como aliada y reto La IA puede ser un arma de doble filo para las mipymes y pymes. Por un lado, ofrece herramientas potentes para prevenir y mitigar riesgos cibernéticos; por otro, puede ser explotada por ciberdelincuentes para realizar ataques más sofisticados. Los beneficios potenciales de la IA incluyen:

1. Detección proactiva de amenazas: Los sistemas de IA pueden identificar patrones anómalos en tiempo real, detectando intentos de intrusión antes de que causen daños significativos.
2. Automatización de tareas de seguridad: La IA puede encargarse de tareas repetitivas, como el monitoreo de redes, lo que libera tiempo para que los equipos humanos se concentren en actividades estratégicas.
3. Análisis predictivo: Mediante el análisis de grandes volúmenes de datos, la IA puede predecir futuros riesgos y recomendar medidas preventivas.

Sin embargo, también existen barreras para la adopción de la IA en este sector:

- Costo: Muchas soluciones de IA requieren una inversión inicial elevada que puede estar fuera del alcance de las mipymes y pymes.
- Falta de conocimiento: La adopción de IA requiere personal capacitado, algo que escasea en muchas organizaciones
- Amenazas avanzadas: Los ciberdelincuentes también están utilizando IA para desarrollar ataques más difíciles de detectar.

Estrategias para enfrentar los retos Para que las mipymes y pymes mexicanas puedan beneficiarse de la ciberseguridad y la IA sin comprometer su estabilidad financiera, es fundamental implementar estrategias adaptadas a sus capacidades. Algunas recomendaciones clave incluyen:

1. Conciencia y capacitación: Fomentar una cultura de ciberseguridad dentro de la organización. Esto incluye educar a los empleados sobre buenas prácticas, como la detección de correos sospechosos y el uso de contraseñas seguras.
2. Soluciones escalables: Optar por herramientas de ciberseguridad asequibles y escalables que puedan crecer junto con el negocio. Muchas plataformas ofrecen soluciones adaptadas para mipymes.
3. Colaboración con expertos: Subcontratar servicios de ciberseguridad o colaborar con startups especializadas puede ser una opción viable para acceder a tecnología avanzada sin incurrir en altos costos.
4. Uso de IA accesible: Aprovechar herramientas de IA de bajo costo o gratuitas que estén diseñadas para pequeñas empresas. Por ejemplo, sistemas de monitoreo básico que utilicen IA para detectar riesgos.
5. Políticas claras: Establecer y comunicar políticas de ciberseguridad claras para minimizar los riesgos de ataques internos y externos.

El impacto en las empresas familiares y emprendedores Las empresas familiares y los emprendedores enfrentan desafíos particulares dentro del contexto de la ciberseguridad y la transformación digital. Estos negocios, que muchas veces operan con estructuras administrativas menos formales, son especialmente vulnerables a los riesgos digitales debido a factores como:

1. Falta de recursos especializados: Las empresas familiares suelen contar con personal limitado y polifuncional, lo que dificulta la implementación de medidas de ciberseguridad robustas.
2. Dependencia de confianza personal: Muchas decisiones se basan en relaciones personales, lo que puede llevar a subestimar amenazas como el phishing o ataques internos.
3. Infraestructura tecnológica básica: Estas empresas tienden a operar con tecnología desactualizada o soluciones poco seguras debido a restricciones presupuestarias.

Para los emprendedores, el panorama es igualmente complejo. Mientras intentan ganar terreno en mercados competitivos, enfrentan riesgos que pueden comprometer su crecimiento, como:

- Robo de propiedad intelectual: Los proyectos innovadores pueden ser blanco de ciberdelincuentes interesados en apropiarse de ideas o datos.
- Ataques de denegación de servicio (DDoS): Páginas web de startups pueden ser desactivadas por ataques que buscan sobrecargar sus servidores

Estrategias específicas para empresas familiares y emprendedores

1. Implementar herramientas gratuitas o de bajo costo
2. Capacitar a todos los miembros
3. Asegurar la infraestructura digital
4. Crear un plan de respuesta a incidentes

El camino hacia un futuro más seguro La transformación digital en México es inevitable, y las mipymes y pymes deben adaptarse para no quedarse rezagadas. La adopción de tecnologías no solo es una ventaja competitiva, sino una condición necesaria para la supervivencia en un mercado globalizado.

Sin embargo, esta transformación debe ser acompañada de un enfoque estratégico en seguridad. En primer lugar, es esencial que los líderes empresariales reconozcan la importancia de la ciberseguridad como un componente integral de su operación diaria.

Esto implica no solo invertir en tecnología, sino también en la capacitación continua de su personal para que puedan identificar y responder a las amenazas emergentes. Además, el fortalecimiento de la colaboración entre los sectores público y privado es crucial para combatir los retos compartidos. Programas de apoyo gubernamental que promuevan la adopción de herramientas de ciberseguridad e inteligencia artificial pueden marcar una diferencia significativa. Iniciativas como subsidios tecnológicos, capacitaciones gratuitas y plataformas de comunicación entre empresas podrían allanar el camino para una mayor resistencia ante ataques cibernéticos. Finalmente, la sostenibilidad tecnológica debe estar en el centro de esta transformación.

Las mipymes y pymes deben adoptar soluciones que sean escalables y accesibles, asegurándose de que el crecimiento tecnológico no comprometa su viabilidad económica. Esto incluye la implementación de tecnologías de código abierto y la exploración de modelos de negocio que integren la seguridad digital desde el diseño. Aunque el camino hacia un futuro más seguro está lleno de desafíos, también está repleto de oportunidades para innovar y fortalecer las bases del sector empresarial en México. Con la combinación adecuada de conciencia, inversión y colaboración, las mipymes y pymes mexicanas tienen el potencial de liderar una nueva era de resiliencia digital.

Cinco metodologías adaptables al análisis de retos y oportunidades de ciberseguridad e inteligencia artificial en pequeñas y microempresas mexicanas.

1. Metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) Diseñada por el Gobierno de España, MAGERIT se enfoca en identificar y gestionar los riesgos relacionados con los sistemas de información. Esta metodología es ideal para pequeñas y microempresas mexicanas, ya que permite analizar el impacto de los riesgos tecnológicos y establecer prioridades para proteger los activos más valiosos, como los datos de clientes o inventarios digitales.
2. Marco de Ciberseguridad para Pequeñas Empresas del NIST Este marco simplificado, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), está diseñado específicamente para pequeñas empresas con recursos limitados. Proporciona un enfoque práctico para identificar vulnerabilidades, priorizar medidas de protección y responder a incidentes de seguridad cibernética sin necesidad de una gran inversión.
3. Modelo CIS Controls (Center for Internet Security Controls) Los "Controles CIS" son un conjunto de 18 prioritarias que permiten medidas para proteger los activos tecnológicos contra ciberamenazas. Su aplicación es especialmente útil para pequeñas empresas, ya que establece una guía clara y accesible para fortalecer la seguridad con recursos limitados. Ejemplo: implementar la autenticación multifactor y restringir el acceso a datos sensibles.
4. Metodología Agile aplicada a la Ciberseguridad Agile, tradicionalmente utilizada en desarrollo de software, se adapta al contexto de ciberseguridad para pequeñas empresas al permitir una respuesta flexible y rápida a los riesgos. La metodología fomenta la implementación de mejoras en ciclos cortos

Referencias que pueden ser útiles para profundizar en el análisis de los retos y oportunidades de la ciberseguridad e inteligencia artificial en las pequeñas y microempresas mexicanas:

Libros y publicaciones

1. "Ciberseguridad para PyMEs" Autor: Francisco Acosta López Editorial: Alfaomega Descripción: Este libro se centra en las principales vulnerabilidades de las pequeñas empresas y proporciona estrategias prácticas para protegerse contra amenazas cibernéticas.

2. "Conceptos básicos de inteligencia artificial: una introducción no técnica" Autor: Tom Taulli Editorial: Apress Descripción: Introduce los conceptos clave de la inteligencia artificial y cómo las pequeñas empresas pueden implementarlos para mejorar la eficiencia y la seguridad.

3. "Gestión de riesgos en seguridad de la información" Autor: Vicente Aceituno García Editorial: Ra-Ma Descripción: Este texto explica cómo evaluar y gestionar riesgos en el ámbito de la ciberseguridad, con ejemplos aplicables a micro y pequeñas empresas. Artículos y reportajes

4. Reporte "Estado de la Ciberseguridad en las PYMES en América Latina y el Caribe" Publicado por: Organización de los Estados Americanos (OEA) y el Banco Interamericano

Respetuosamente: Lic. en Seguridad Pública y Criminología.
Jonatthan Hermida Sosa.
SAPPC, SFPC, DAS, CPO, ISOC, GER, CRASE.

Cristóbal Granados Sánchez
Carlos Miguel Ortiz

Empresa destacada

Metro Risk

DRONES: UN CAMBIO REAL EN LA SEGURIDAD

Fijémonos en los drones ¿se han vuelto algo casi cotidiano? Ya no son un juguete caro o una herramienta exclusiva para cine, son un elemento clave en áreas donde nunca habríamos imaginado que llegarían, especialmente en la seguridad. Podemos grabar increíbles paisajes o entregar paquetes, salvar vidas, proteger propiedades y cambiar la manera en que entendemos la seguridad pública y privada. Y lo mejor es que no estamos hablando de algo futurista, sino de una realidad, gracias a empresas como Ritrac International, que lidera la integración de drones en diversos sectores, incluyendo la seguridad.

La Seguridad Pública: Protegernos con Ojos en el Cielo Si pensamos en el trabajo que hacen los cuerpos de seguridad, nos damos cuenta de que siempre han tenido una tarea compleja: responder rápido, cubrir grandes áreas y minimizar riesgos. Aquí es donde los drones han llegado como una herramienta revolucionaria.

1. Vigilancia Más Eficiente Pensemos en eventos como festivales, partidos de fútbol o manifestaciones. Garantizar la seguridad del evento, implica desplegar un montón de personal, cámaras y recursos. Con el dron sobrevolando proporcionaremos imágenes en tiempo real de todo lo que sucede. Desde el aire detectar situaciones de riesgo, como aglomeraciones peligrosas o comportamientos sospechosos, es más ágil y fácil.

Un valor añadido de los drones equipados con cámaras térmicas y visión nocturna es que no tienen limitaciones de luz. Incluso de noche pueden identificar movimientos, personas o puntos de interés que pasarían desapercibidos para una cámara convencional.

Ritrac International, empresa especializada en drones con tecnología térmica y multiespectral, esta transformando la manera en que las fuerzas de seguridad operen. Cuenta con pilotos e instructores certificados en todo el país, aseguran que estas herramientas sean utilizadas de forma eficiente y profesional.

2. Emergencias : Respuesta Rápida Ante un desastre natural, como un terremoto o una inundación. Es primordial localizar personas atrapadas o evaluar daños, pero es una tarea difícil. Los drones equipados con cámaras térmicas, pueden localizar a personas incluso bajo escombros o entre la vegetación densa. Un ejemplo que me impactó fue el uso de drones para coordinar rescates durante incendios forestales.

Mientras los bomberos trabajan en tierra, los drones identifican los puntos calientes y trazan rutas seguras. Es como si el equipo tuviera un mapa en vivo del incendio, ayudándolos a ser más efectivos y seguros

3. Delitos : Patrullaje y Prevención En muchas ciudades del mundo los drones están patrullando ya las calles. Disuaden a los delincuentes, permiten una respuesta más rápida en caso de incidentes. Si algo ocurre, el dron puede ser el primero en llegar al lugar, enviando imágenes al equipo de seguridad mientras llegan refuerzos.

Ritrac International ha trabajado en la formación de pilotos especializados que colaboran con cuerpos policiales y de emergencias, integrando esta tecnología en su día a día. Esto no solo mejora la vigilancia, sino que también protege a los agentes al minimizar su exposición en situaciones de alto riesgo.

Tecnología al Servicio de Todos: La Seguridad Privada Tan importante es la seguridad pública como la privada. Proteger nuestras casas, empresas o eventos siempre ha sido un desafío, pero los drones están cambiando las reglas del juego

1. Vigilancia de Propiedades Grandes ¿Te preocupa tu empresa con un almacén enorme o una finca en una zona rural? Los drones son perfectos para patrullar grandes extensiones de terreno en poco tiempo. Un dron puede moverse libremente, inspeccionando cada rincón y detectando cualquier anomalía.

Ritrac International ofrece soluciones específicas para este tipo de necesidades, incluyendo formación personalizada para garantizar que cualquier equipo pueda operar los drones de forma autónoma y profesional.

2. Supervisión de Eventos Privados En eventos privados, como bodas, conferencias o fiestas exclusivas, los drones ofrecen una capa adicional de seguridad. No solo monitorizan desde el aire, sino que también permiten grabar lo que sucede, ayudando a documentar cualquier incidente para futuras investigaciones.

3. Adaptabilidad en Zonas Complejas Los drones llagan a lugares donde los sistemas tradicionales de seguridad tienen problemas. Por ejemplo, en terrenos montañosos, bosques densos o áreas industriales con obstáculos, los drones pueden navegar fácilmente, proporcionando una vista aérea que ningún otro sistema puede igualar.

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

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

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

Colaboramos con MR-CONSULTING.

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

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

AGENDA

Metro Risk

RADIO

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

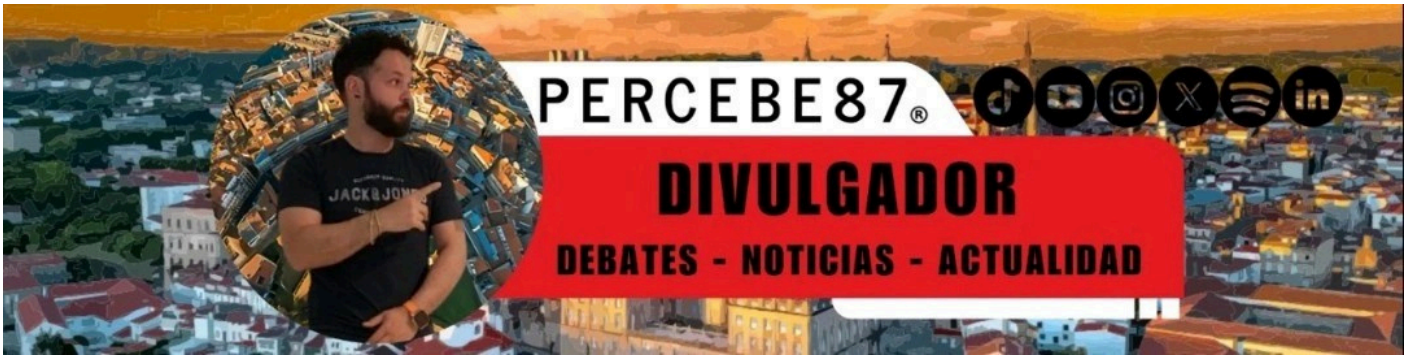
WORLD COMPLIANCE ASSOCIATION

Conoce a los expertos que participarán en el III Congreso Internacional de Compliance Officers!

🎬 Mesa temática: "El lobo de Wall Street" (2 de abril, Barcelona, 15:10)

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