

EDITORIAL MR

ENERO

AÑO
2025

La visión de un
Departamento de
Seguridad Cooperativa

Consideraciones Jurídicas
sobre el uso de la fuerza por
equipos caninos

La Necesidad de un
Departamento de Seguridad
en la Estructura Hotelera

El convenio colectivo y las
licitaciones públicas: un
sistema que estrangula a
vigilantes y empresas de
seguridad

Seguridad Inteligente:
Privacidad y Protección

¿RPO y RTO? ¿Sabes cuántos
minutos puede resistir tu
negocio sin sufrir una
catástrofe?

Más allá de las Luces: Los
Desafíos Ocultos de la
Seguridad Navideña

Sección Estudios Técnicos
D. Goyo Duro

Sección Prevención del Crimen. CPTED
Dra. Mercedes Escudero

CONOCE A:
Rafael Hernández

ASOCIACIÓN para la Investigación y la Divulgación de la Seguridad

Presidente:

D. Francisco Medina cruz

Vicepresidente Económico:

D. Abraham Santana Herrera

Vicepresidente Relaciones Institucionales:

D. Juan Carlos Galindo

Secretario General:

D. Emilio Piñeiro

Vocal Comunicación:

Dña. Elena González de la Parte

Vocal Temas Legales:

Dña. Rosa Fernández Fernández



MeTroRisk
Seguridad Patrimonial y CPTED



COLABORADORES



PATROCINADO POR LAS FIRMAS



BIENVENIDOS AL 2025

Fran Medina Cruz Director de MetroRisk

Un nuevo año siempre trae consigo una promesa de renovación y nuevas oportunidades, y el 2025 no es la excepción. Es el momento ideal para reflexionar sobre los aprendizajes del pasado y mirar hacia el futuro con optimismo y determinación. Al dar la bienvenida a este año, nuestro deseo principal es que esté lleno de salud, prosperidad y, sobre todo, seguridad para cada uno de nosotros y nuestras comunidades.

La seguridad se presenta como un elemento clave para garantizar que nuestras metas y sueños puedan desarrollarse en un marco de tranquilidad y confianza. En un mundo que avanza rápidamente en tecnología, innovación y desafíos globales, la seguridad debe ser entendida no solo como un concepto físico, sino como un compromiso integral que abarque todos los aspectos de nuestras vidas. Desde la protección de nuestras familias y comunidades, hasta la implementación de medidas que salvaguarden la información y los recursos en un entorno digital cada vez más complejo.

El 2025 nos invita a redoblar esfuerzos por construir un futuro más seguro y saludable. Esto significa trabajar juntos como sociedad, con la confianza de que la prevención, la educación y la colaboración son herramientas indispensables para hacer frente a cualquier desafío. Así como deseamos que este año sea una etapa de crecimiento y logros, también debemos comprometernos a ser agentes de cambio que contribuyan a un entorno más seguro y próspero para todos.

Que este nuevo año esté lleno de oportunidades para cuidarnos, protegernos y avanzar hacia un futuro más estable y esperanzador. ¡Feliz 2025! Que la salud, la seguridad y la motivación nos acompañen en cada paso de este emocionante viaje.



En 2025, la seguridad enfrenta una serie de desafíos complejos que requieren soluciones innovadoras y una colaboración efectiva. Estos desafíos abarcan tanto el ámbito físico como el digital, reflejando la creciente interconexión de nuestras sociedades y la evolución de las amenazas globales.

La digitalización de la vida cotidiana y los sistemas empresariales continúa exponiendo a gobiernos, empresas y particulares a riesgos cibernéticos. Desde ataques de ransomware y phishing más sofisticados hasta la manipulación de datos mediante inteligencia artificial, las organizaciones deben invertir en soluciones avanzadas de ciberseguridad. Además, la protección de infraestructuras críticas como redes eléctricas y sistemas de agua sigue siendo una prioridad global.

El crecimiento de las áreas urbanas y el aumento de eventos públicos masivos plantean desafíos logísticos y de seguridad. La gestión de multitudes, la vigilancia inteligente y la preparación ante emergencias son fundamentales para prevenir incidentes. Aquí, la inteligencia artificial y los sistemas de vigilancia avanzada desempeñan un papel clave, aunque deben equilibrarse con la protección de la privacidad individual.

Los conflictos geopolíticos y la inestabilidad en ciertas regiones siguen siendo una fuente importante de riesgo, desde amenazas terroristas hasta la proliferación de armas no convencionales. Esto afecta no solo a las fronteras internacionales, sino también a la seguridad nacional de muchos países. La cooperación internacional y el intercambio de inteligencia serán esenciales para abordar estos desafíos.

Si bien la IA ofrece soluciones revolucionarias, también plantea riesgos si no se implementa de manera ética y segura. Desde sistemas de reconocimiento facial hasta vigilancia predictiva, el desafío radica en utilizar estas herramientas sin comprometer la privacidad o los derechos humanos. Entre otros muchos desafíos de los que no debemos perder de vista





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.



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 VISION DE UN DEPARTAMENTO DE SEGURIDAD CORPORATIVA...

Francisco Javier Gonzales Fuentes
Presidente de ADISPO, AIMCSE y FIBSEM

....DESDE UN PUNTO DE VISTA HOLÍSTICO.

Muchos hemos avanzado en materia de Seguridad en España a través del tiempo, donde desde una perspectiva de la Seguridad física hemos sufrido algún cambio troncal en el ámbito normativo, pero vacío de reglamento que pueda desarrollar profesionalmente en materia de Seguridad Privada.

Mientras tanto la transformación 4.0 en materia de Seguridad Integral ha venido y ha pasado de la seguridad física a la Seguridad Corporativa, donde contemplamos como Directores de Seguridad todos los riesgos y amenazas existentes.

Contemplamos, los diferentes activos de nuestras entidades de manera singular usando todas las técnicas a nuestra disposición y cada vez más avanzada la formación especializada en nuevas tecnologías y nuevos riesgos y amenazas.

El trasiego de las personas con acceso cada vez más al manejo de informaciones y activos complejos y de las nuevas tecnologías, como directores de seguridad nos hace más competitivos en el desempeño de nuestras funciones en todas las áreas de la corporación



IntelForensic
G&F Soluciones

¿Cómo definimos seguridad corporativa?; no tenemos una definición estándar al respecto pero podemos definirla como el conjunto de políticas, procedimientos y recursos humanos, organizativos y técnicos destinados a proteger a las personas, a los activos tangibles e intangibles y a la reputación de una organización.

En nuestro caso, nos centramos en la elaboración de políticas de seguridad que puedan corregir malas conductas de los empleados que puedan repercutir en la corporación y los riesgos en distintas áreas y dimensiones que afectan a su actividad y la imagen ante la sociedad.

En estos tiempos aparecen nuevas técnicas de trabajo, por ejemplo y que se utilizan heredadas y en consonancia con el sector de la Seguridad las del ámbito operativo militar, como un binomio indispensable de la gestión en Seguridad Corporativa como es el caso de la Inteligencia corporativa, donde nos ayudará a tomar decisiones a todos los niveles de los departamentos directivos o de responsables de áreas, pero lo más importante de ese ciclo de Inteligencia es la toma de decisiones de la alta dirección. No está de más que el departamento de seguridad tenga analistas capacitados en esta materia o en los departamentos más pequeños el director de seguridad sea un buen analista de Inteligencia Corporativa.



Podemos trabajar en distintas áreas de manera integral y planificar actividades en las siguientes dimensiones;

RECURSOS HUMANOS:

- En el entorno socio laboral de la empresa buscando, quienes son las personas tanto de la estructura interna como externa que pueden con sus comportamientos y actitudes causar un perjuicio para la empresa y su imagen institucional.

MARKETING Y COMUNICACIONES:

-Trabajar especialmente sobre las informaciones y desinformaciones relevantes que pueden impactar sobre la repercusión corporativa de cara al exterior.

ORGANIZACION Y ADMINISTRACION:

Gestión documental, seguridad de la documentación utilizando los grados de clasificación, inventariado, controles de acceso de terceros, etc...

OPERACIONES

- Podemos incidir sobre operaciones de seguridad internacional en departamentos expatriados en el exterior, riesgos operacionales, gestión de crisis....

FINANCIERA

- Elección y perfilación de los intervinientes en contratos, operaciones financieras etc...

TECNOLOGICA

- Desarrollo de política IT, buenas prácticas ciberseguridad empleados... control seguridad servidores etc...

Para finalizar a nivel piramidal terminamos en nuestra planificación de medidas de seguridad con la;

DIRECCION

- Protección VIP, reconocimientos de zonas y de contactos de influencias, etc...

CONSIDERACIONES JURÍDICAS SOBRE EL USO DE LA FUERZA POR EQUIPOS CANINOS

José Ignacio Olmos Casado Presidente AEAS

Es de todos conocido que en las intervenciones de seguridad en las que es necesario hacer uso de la fuerza será primordial intentar ajustar ésta al ordenamiento jurídico, por las muchas implicaciones legales que pueden derivarse.

En los últimos años ha progresado mucho la formación del personal de seguridad, pública y privada, tanto en la perspectiva legal como en la operativa de las intervenciones, contando nuestro país con grandes docentes en una materia que tiene la dificultad añadida de tener que ajustarse a unas normas no pocas veces excesivamente proteccionistas con el sujeto pasivo de la intervención. Recientemente hemos tenido que ver cómo ante una agresión de un sujeto armado con un cuchillo una agente de la Policía de la Generalidad de Cataluña que usó su arma de fuego con efectos letales ha sido duramente criticada por todo tipo de "expertos" por no reducir al sujeto con menos lesividad.



Aún así, muy pocos trabajos creo que se han publicado en nuestro país sobre el uso de la fuerza por equipos caninos. Sin ser un experto desde el punto de vista operativo, si me gustaría abordar algunas cuestiones implícitas a estas actuaciones desde el punto de vista jurídico y de organización.

Además del uso múltiple que se hace tanto en unidades policiales como militares de los perros, quiero ceñirme al ámbito profesional de la seguridad privada, donde desde siempre han existido también servicios en los que el perro era elemento importante. En los albores de la seguridad privada moderna, desde finales de los años 70 del pasado Siglo aproximadamente, los servicios con perros eran usados ampliamente, desde grandes fábricas a grandes almacenes.

Con el gran auge del sector que se dio sobre todo a partir del año 92 su uso decayó notablemente. En los últimos años estamos viviendo un auge nuevamente de los servicios de caneros, como popularmente se conoce a los vigilantes de seguridad que actúan como guías, y no sólo en la especialidad más tradicionalmente utilizada de guarda y defensa, sino también en el ámbito de los perros detectores de explosivos, motivado por la situación de alerta terrorista a nivel internacional, con los atentados del 11 M en Madrid en particular, y con la aprobación en la normativa de la Unión Europea de los Equipos de perros detectores de explosivos de seguridad privada en los aeropuertos, modelo extrapolable a otras infraestructuras críticas que, incluso anticipándose a la existencia de normativa en su ámbito, ya exigen certificaciones similares, como la Autoridad Portuaria de Barcelona.

Son múltiples las virtudes de los perros en el trabajo de seguridad, desde su nivel de alerta con los sentidos (olfato-vista-oído) mucho más sensible y amplio que el de un humano, hasta su nivel de intimidación y su menor lesividad. Más adelante volveremos sobre estas cuestiones.

Inicialmente hay que abordar qué dice la normativa de seguridad privada al respecto de estos servicios, y la verdad es que decir, no dice prácticamente nada.

Este ha sido uno de los aspectos menos desarrollados y más tempranamente obsoletos. La única referencia aparece en el artículo 75 del aún vigente Reglamento de Seguridad Privada del año 94, que establece: "

1. Para el cumplimiento de sus funciones, los vigilantes de seguridad podrán contar con el apoyo de perros, adecuadamente amaestrados e identificados y debidamente controlados, que habrán de cumplir la regulación sanitaria correspondiente. A tal efecto, los vigilantes de seguridad deberán ser expertos en el tratamiento y utilización de los perros y portar la documentación de éstos.
2. En tales casos se habrán de constituir equipos caninos, de forma que se eviten los riesgos que los perros puedan suponer para las personas, al tiempo que se garantiza su eficacia para el servicio."

La actual Ley 5/2014, de seguridad privada, ni siquiera hace referencia al enumerar los distintos tipos de servicios a los realizados con perros. Los detalles principales a extraer del artículo 75 del Reglamento han sido pormenorizados también en unos pocos informes de la Unidad Central de Seguridad Privada del Cuerpo Nacional de Policía y de la Secretaría General Técnica del Ministerio del Interior:





- Posibilidad de que los vigilantes de seguridad puedan contar con el apoyo de perros para el desarrollo de sus funciones.
- Los perros deben estar amaestrados, identificados, controlados y observando la regulación sanitaria.
- Los vigilantes que realicen servicios de seguridad con apoyo de perros deberán acreditar una formación en el manejo y utilización de perros adiestrados. Se expedirá por el centro formador un diploma acreditativo del Curso y las horas impartidas.
- Tanto la formación del vigilante en el tratamiento y utilización de los perros, como el adiestramiento de éstos, corre a cargo de la empresa de seguridad.
- En cuanto a la obligación de llevar la documentación del perro, corresponde a la empresa hacer entrega al vigilante de dicha documentación. Por consiguiente, para que exista responsabilidad del vigilante ante la falta de documentación, la empresa deberá acreditar que, efectivamente, se entregó la documentación al vigilante-guía.
- La ley de Régimen de Tenencia de animales peligrosos 50/1999 de 23 de diciembre, en su artículo 1.2, excluye de su aplicación a los perros y otros animales pertenecientes a los cuerpos policiales y empresas de seguridad con autorización oficial.

A estas consideraciones habría que añadir que, respecto de la formación, no existía desarrollo normativo hasta la Resolución del Ministerio del Interior sobre formación de 12 de noviembre de 2012, donde, dando cumplimiento a la Orden INT 318/2011 sobre personal se establece en el Apéndice 11 la Formación específica para Vigilantes de Seguridad que presten servicio de vigilancia con perros, con una duración mínima de diez horas presenciales y determinados contenidos.

Esa formación deberá hacerse en Centros de Formación de seguridad privada; es curioso que así como en el caso de la galería de tiro y el gimnasio se menciona en la normativa la necesidad de contar con ellas en el centro de formación (generalmente no son instalaciones propias, sino externas que se utilizan mediante un convenio), nada se dice de instalaciones para la práctica con los perros (de hecho ni siquiera se exigen prácticas en ese Apéndice 11).

El Borrador del futuro Reglamento de Seguridad Privada que desarrolle la Ley de 2014 establece un artículo solamente al respecto:

“Artículo 128. Empleo de perros u otros animales.

1. En los servicios de seguridad privada de vigilancia y protección podrá emplearse, como complemento material del servicio, perros especialmente adiestrados. En estos casos, deberán constituirse equipos guía-perro que cumplirán los siguientes requisitos: a) El personal de seguridad privada deberá contar con la formación necesaria y los perros estar debidamente adiestrados para la prestación de los servicios. b) El perro deberá estar plenamente identificado y habrá de cumplir con los requisitos establecidos en la normativa de control sanitario. c) Durante la prestación del servicio de seguridad privada, el personal de seguridad privada que realice la función de guía canino deberá llevar la documentación acreditativa de los extremos contemplados en los párrafos anteriores.
2. Cuando en la práctica del servicio de seguridad privada se empleen otros animales como apoyo, éstos deberán cumplir con los requisitos de control sanitario y habrán de utilizarse de tal forma que no puedan ser percibidos como una amenaza para las personas.
3. En la prestación de los servicios de seguridad privada no podrán utilizarse animales que no se encuentren debidamente adiestrados, ni dejarse solos o sueltos en los lugares objeto de vigilancia y protección.”

Como vemos, se apunta en la misma línea de la doctrina establecida por la unidad de control administrativo, la cual por cierto, también dejó claro en uno de sus informes, que no cabe en nuestro país la posibilidad de que el guía canino sea una persona sin habilitación de vigilante de seguridad; habrá que poner en relación el uso del perro como instrumento por parte del vigilante, con las funciones que la Ley le atribuye (prevención, control de accesos...) Con esto cerraríamos la parte de normativa sobre esta cuestión en derecho administrativo especial.



Referido a cuestiones penales y procesales, como cualquier otra intervención de seguridad en la que se haga uso de la fuerza, habrá que considerar fundamentalmente:

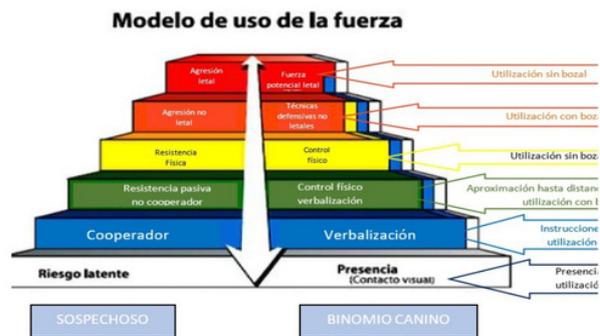
- Si existía necesidad de uso de la fuerza.
- Si la fuerza utilizada ha sido proporcional.
- Si, dentro de la necesidad de uso de la fuerza, se ha causado la menor lesividad posible.

Un sistema gradual del uso de la fuerza y sus técnicas deben adecuarse a una serie de principios básicos y fundamentales entre los cuales se debe hacer especial mención a:

- Adecuación al ordenamiento jurídico.
- Congruencia: adecuación de la técnica concreta a la situación dada.
- Oportunidad: adecuación al momento concreto de la intervención.
- Proporcionalidad: adecuación entre la técnica o medio empleado, el bien jurídico protegido y el resultado.
- Principio de efectividad: los medios empleados deben ser los suficientemente eficaces para conseguir los objetivos con el éxito y la seguridad precisa.

La propia Unidad Central de Seguridad Privada señala en uno de sus informes que "respecto a la posible responsabilidad del vigilante, en caso de que el perro causara lesiones, solamente cabría cuando aquél no hubiera actuado con la diligencia debida, en términos de una deficiente actuación profesional. Por último, y en el supuesto de que el perro causara lesiones al propio vigilante, estas deben ser consideradas como accidente de trabajo, debiendo responder la empresa".

El vigilante de seguridad no actúa en las intervenciones por libre, sino que siempre actúa "a demanda", en función de lo que se encuentra en frente. La relación entre el nivel de resistencia de los sujetos en sus acciones, la fuerza a utilizar por el personal de seguridad y el uso específico del perro como instrumento se representa en el siguiente esquema:



Como ya señalábamos al principio de este artículo, son múltiples, en mi modesta opinión, las ventajas de la utilización del perro en seguridad, y que pueden estar en relación directa con algunas de estas apreciaciones relativas a la ley penal.

Además de que, operativamente, el uso del perro es multidisciplinar y puede emplearse para vigilancia de grandes recintos con mayor efectividad que una patrulla compuesta sólo por vigilantes, como elemento de detección de personas ocultas (por ejemplo en accesos) y, obviamente para la detección de explosivos (especialidad que en principio no se utilizaría en intervenciones con fuerza), hemos de señalar que tanto para control de masas como para actuaciones reactivas el perro es un elemento con gran poder de disuasión y contención. Cuando el que realiza la intervención es un vigilante de seguridad o varios, los sujetos que están cometiendo (o pueden cometer) los ilícitos no siempre se retraen en su actuación ante la presencia de aquellos; sin embargo, el hecho de que exista el perro y levante la parte superior del morro es un elemento persuasivo importante, ya que el sujeto está pendiente de él y sabe de su contundencia; bastantes veces el delincuente piensa: "a ver si al vigilante se le va la cabeza y suelta al perro", o bien "a ver si se le escapa y aunque sea sin querer se me viene encima". La contundencia del perro como elemento de disuasión y control es innegable



SECURITY

Pero además, llegado el momento de tener que hacer uso de la fuerza a un cierto nivel, el perro bien entrenado y bien utilizado siempre será menos lesivo que el arma de fuego. Podemos también plantearnos que allí donde el vigilante no dispone de ese recurso, tener al perro le aportará mayor eficacia y mayor seguridad personal en sus actuaciones. Es más, en una intervención el arma del vigilante puede serle sustraída con el riesgo que entraña para él, por lo que el perro es un magnífico sustitutivo.

Como casi siempre es pieza fundamental la formación, tanto en el área jurídica como en el técnico profesional e instrumental, y, por supuesto, tanto en el plano teórico como en el práctico. Para estos servicios el recorrido formativo es largo e iría desde la selección del perro y su formación inicial hasta la formación del vigilante y de ambos juntos como binomio, amén de la formación periódica necesaria cada poco tiempo. A este respecto, con binomios operando en el transporte público, en estadios deportivos, etc, deberíamos preguntarnos si la formación práctica que se recibe es adecuada

La prestación de un servicio por un equipo canino no consiste en pasear cualquier perro con el vigilante que esté de turno. La óptima eficacia se obtendrá con el itinere que señaláramos antes y el desarrollo de supuestos prácticos: ¿sabe el vigilante qué hacer y dónde? ¿El perro está bien adiestrado? ¿Cómo se afronta la intervención? ¿Puede el guía cachear al sujeto o necesita de otro vigilante para hacerlo con garantías? ¿Cuántos guías manejan el perro? Todas estas cuestiones son esenciales.

Fundamental será también el material y el adecuado uso que se haga de él para llevar a buen puerto la intervención, tanto desde el punto de vista de la autoprotección como de la menor lesividad al sujeto pasivo de la misma. Los elementos de comunicación con el can (correa, trailla), los de control (collar, petral) y los de seguridad (bozal) deben ser revisados para culminar con éxito las actuaciones

Por último, señalar que, desde el punto de vista laboral, este desempeño del vigilante de seguridad ni constituye una especialidad ni se recoge en el Convenio Colectivo Nacional de empresas de seguridad, pagando muchas de ellas un plus al vigilante que hace esta función en torno al 10 % del salario base.

Deseo que estas reflexiones sirvan para promover trabajos técnicos de peso en este ámbito que puedan servir a los profesionales de la seguridad y, por ende, a toda la sociedad para la que trabajan, y me parece una excelente noticia que día a día aumenten los servicios de equipos caninos.

Es de justicia reconocer el asesoramiento para estas notas prestado por mi admirado F.J. Gil Acosta, Jefe de la Unidad Canina de la Central Nuclear de Cofrentes, profesional con una dilatada experiencia y con incipiente ánimo por seguir experimentando y evolucionando en su labor, cualidades que le hacen ser un absoluto referente en esta materia.



Gregorio Duro
Tecnico en licitaciones y Proyectos

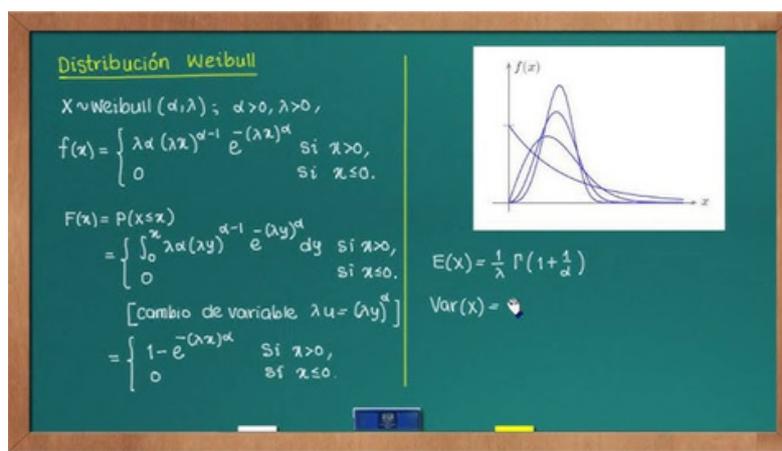
CÁLCULO DE LA PROBABILIDAD DE MANIFESTACIÓN DE EVENTOS DE RIESGO MEDIANTE MODELOS DE REDES NEURONALES

Un modelo de cálculo mediante redes neuronales es una representación computacional inspirada en el funcionamiento del cerebro humano, diseñada para resolver problemas complejos a través de un sistema de aprendizaje automatizado. Este modelo se compone de capas de entradas que simulan neuronas artificiales e interconectadas, donde cada entrada procesa y transmite información basada en funciones matemáticas. Las redes neuronales simulan el aprendizaje de tareas como clasificación, predicción o reconocimiento de patrones ajustando los valores de entrada de sus conexiones durante un proceso de entrenamiento, que utiliza grandes cantidades de datos para optimizar la precisión del modelo. Este enfoque se emplea ampliamente en campos como la inteligencia artificial, analítica de vídeo y procesamiento del lenguaje natural.

Un modelo de cálculo para un evento de riesgo basado en modelos de redes neuronales consiste en recopilar datos relevantes sobre el evento, entorno donde se puede materializar y factores que pueden influir o propiciar su manifestación, seleccionando características significativas que puedan influir en su ocurrencia o impacto. Estos datos se filtran, normalizan y estructuran para servir como entrada al modelo, que puede diseñarse con una red neuronal adecuada, como una red densa para predicción general o una red recurrente si el riesgo presenta dependencias temporales; el modelo se entrena utilizando algoritmos de optimización y funciones de pérdida que ajustan las entradas de las conexiones en repeticiones basadas en ejemplos etiquetados, y posteriormente se valida utilizando diversas métricas. Una vez validado se implementa en sistemas de evaluación de riesgos en tiempo real donde su desempeño se ajusta regularmente para garantizar su efectividad frente a cambios en los datos o en las condiciones del entorno. Este modelo se integra por varias variables clave: las entradas (X), que son los datos que alimentan la red y corresponden a las características del problema a resolver, como valores numéricos o categorías; los pesos (W), que determinan la influencia de cada entrada sobre las neuronas y se ajustan durante el entrenamiento; los sesgos (b), que permiten desplazar la activación de las neuronas para mejorar la flexibilidad del modelo; las activaciones (a), que son el resultado de aplicar una función matemática a la combinación de las entradas ponderadas y los sesgos, introduciendo no linealidades en el modelo; la salida (y), que es el resultado final del modelo y puede representar una predicción o clasificación; la función de pérdida (L), que mide el error entre la predicción y la realidad, guiando el ajuste de los pesos y sesgos; la tasa de aprendizaje (η), que controla la magnitud de los ajustes durante el entrenamiento; y el número de épocas, que define cuántas veces el modelo recorre los datos durante el entrenamiento para optimizar sus parámetros



Un ejemplo de cálculo mediante redes neuronales para detectar un evento de intrusión en un edificio podría basarse en un sistema de seguridad que registre los datos provenientes de múltiples fuentes, como intentos de acceso fallidos, registros de actividad de sensores de movimiento en áreas restringidas y la hora del día, factores relevantes que suelen correlacionarse con eventos de intrusión. Supongamos que el modelo tiene como entradas el número de intentos de acceso detectados (X1), la hora del día en formato 24 horas (X2) y la intensidad de actividad detectada por los sensores de movimiento (X3), valores que son procesados a través de una red neuronal con una capa oculta que contiene varias neuronas con funciones de activación. Durante el cálculo, cada entrada se multiplica por un peso (W), que inicialmente se asigna aleatoriamente y se ajusta durante el entrenamiento, y a este producto se le suma un sesgo (b) para generar una combinación lineal que se transforma mediante la función de activación para producir las salidas intermedias de la capa oculta (aj). Por ejemplo, si los valores de entrada son 4 intentos fallidos, hora 22 y una alta actividad de sensores representada por 1, las combinaciones lineales de las entradas con pesos como $W1=0.5$, $W2=-0.6$, $W3=0.2$ y un sesgo de 0.1 producen resultados que, al pasar por la función, generan activaciones entre 0 y 1, lo que refleja la relevancia de cada característica para el evento. Estas activaciones intermedias alimentan la capa de salida, que mediante otra combinación de pesos y sesgos calcula la probabilidad de que el evento sea una intrusión, con una salida final, por ejemplo, de $Y=0.87$, lo que indica una alta probabilidad de intrusión.





50
40
30
20
10
0

Este modelo se entrena con datos históricos de intrusiones reales y fallidas, utilizando una función de pérdida como la entropía cruzada binaria para comparar las salidas predichas con los valores reales, ajustando los pesos y sesgos para minimizar el error. El entrenamiento puede incluir diversas franjas temporales y una tasa de aprendizaje óptima para asegurar que el modelo se desarrolle correctamente. Finalmente, una vez entrenado y validado, el modelo se integra en el sistema de seguridad, donde se puede analizar constantemente las nuevas señales y emitir alertas automáticas en caso de detectar probabilidades significativas de intrusión, lo que permite una respuesta inmediata y eficiente de forma previa a la materialización del evento de riesgo. En definitiva y tras realizar una aproximación previa debido a su complejidad, el modelo de cálculo basado en redes neuronales para estimar la probabilidad de materialización de un evento de riesgo, como por ejemplo una intrusión en un edificio, es una herramienta fundamental que puede integrar datos de diversa naturaleza para detectar patrones complejos y generar predicciones precisas utilizando entradas relevantes, como registros de actividad, patrones horarios y señales de sensores (para este ejemplo concreto), que se procesan mediante capas de neuronas conectadas por pesos y sesgos ajustados durante el entrenamiento, permitiendo que la red aprenda a identificar correlaciones entre las características y la ocurrencia del evento. Mediante funciones de activación y una función de pérdida, el modelo optimiza su capacidad para distinguir eventos de riesgo reales de situaciones normales, garantizando alta precisión en entornos dinámicos. Una vez implementado, este sistema de predicción puede desarrollarse mediante un software específico y adaptarse de forma continuada a las nuevas condiciones que sean requeridas, proporcionando alertas precisas que permitan tomar decisiones informadas para mitigar el impacto de los riesgos, demostrando su utilidad y eficacia en la gestión proactiva de la seguridad

Elemento 1

Elemento 2

Elemento 3

Elemento 4

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



EL FUTURO DEL CPTED: CONVERGENCIA ENTRE TECNOLOGÍA, NORMATIVA ISO Y EL ANÁLISIS DE TERRITORIOS

“Cualquier actividad humana se realiza con base en la relación a una estructura física, incluyendo la calle, que se localiza en un territorio.”

Mercedes Escudero

La Prevención del Delito a través del Diseño Ambiental (CPTED, por sus siglas en inglés) ha evolucionado significativamente desde sus inicios. Originalmente centrado en principios de diseño físico, el CPTED se encuentra ahora en una encrucijada fascinante, impulsada por los avances tecnológicos en el análisis de territorios y comunidades, y respaldada por normativas internacionales como la ISO 22341:2021 y la ISO 22344:2024. Este artículo explora el futuro del CPTED, examinando cómo estas fuerzas convergen para crear entornos más seguros y resilientes.

La Revolución Tecnológica en el Análisis Territorial: Los avances tecnológicos están transformando radicalmente la forma en que entendemos y analizamos los territorios y las comunidades. Herramientas como:

- **Sistemas de Información Geográfica (SIG):** permiten mapear y analizar datos espaciales relacionados con el delito, la demografía, la infraestructura urbana, la iluminación, entre otros. Esto facilita la identificación de puntos críticos y la comprensión de patrones delictivos.
- **Análisis predictivo del delito:** utilizando algoritmos y modelos estadísticos, se pueden predecir zonas de alta probabilidad de delincuencia, permitiendo una intervención preventiva más efectiva.
- **Sensores y dispositivos IoT (Internet de las Cosas):** la instalación de sensores de movimiento, cámaras inteligentes, sistemas de iluminación adaptativa y otros dispositivos IoT proporciona datos en tiempo real sobre la actividad en un espacio, permitiendo una monitorización continua y una respuesta rápida ante incidentes.
- **Big Data y análisis de datos:** la recopilación y el análisis de grandes volúmenes de datos provenientes de diversas fuentes (redes sociales, informes policiales, datos de tráfico, etc.) ofrecen una visión integral de la dinámica social y delictiva en un territorio, en una comunidad, en una ciudad.
- **Realidad Virtual (RV) y Realidad Aumentada (RA):** permiten simular diferentes escenarios de diseño urbano y evaluar su impacto en la seguridad antes de la implementación física, optimizando así las intervenciones sociourbanas.

El Rol de las Normas ISO: ISO 22341:2021 e ISO 22344:2024 Las normas ISO proporcionan un marco de referencia estandarizado a nivel internacional para la implementación efectiva de la Metodología CPTED.

□ ISO 22341:2021 (Seguridad y resiliencia)

- Seguridad protectora

- Directrices para la prevención del delito a través del diseño ambiental); esta norma proporciona directrices para la aplicación del CPTED, abordando principios, elementos, estrategias y procesos para reducir el delito, incluyendo ciertos tipos de ataques terroristas. Se centra en la planificación urbana y el diseño de espacios públicos con visión social para mejorar la calidad de vida de las personas.

□ ISO 22344:2024 (Seguridad y resiliencia)

- Espacios seguros

- Directrices para el diseño de edificios residenciales): esta norma se centra específicamente en el diseño de edificios residenciales, considerando tanto los espacios públicos como privados. Ofrece recomendaciones para mejorar la seguridad en viviendas y conjuntos residenciales, en donde podríamos considerar estructuras donde las personas residimos de forma temporal para la realización de actividades laborales, sociales, culturales, económicas, comerciales, entre otras, que nos da la conectividad y movilidad social.

Estas normas son cruciales porque: □ Establecen un lenguaje común: facilitan la comunicación y la colaboración entre diferentes actores involucrados en la planificación, el diseño y la implementación de intervenciones sociourbanas.

-Promueven las mejores prácticas: ofrecen un conjunto de directrices basadas en la evidencia y la experiencia internacional.

-Aseguran la calidad y la consistencia: ayudan a garantizar que los proyectos CPTED se implementen de manera efectiva y sostenible; así como su evaluación de impacto





El Futuro del CPTED:

Una Visión Integrada El futuro del CPTED reside en la integración efectiva de la tecnología, las normativas ISO y un profundo análisis del contexto social y territorial. Esto implica:

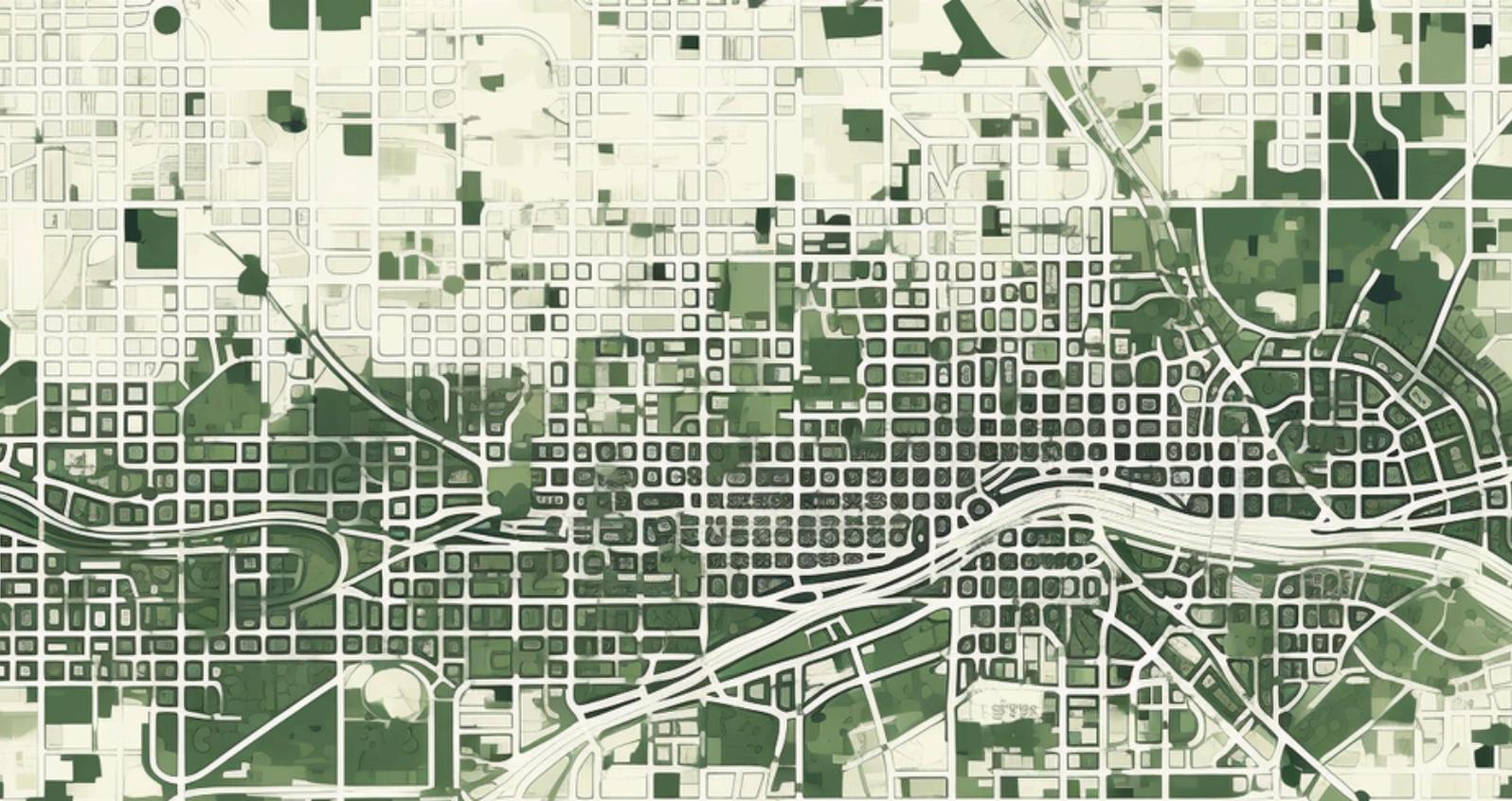
- **Enfoque basado en datos:** utilizar datos objetivos y análisis cuantitativos para respaldar las decisiones de diseño y las intervenciones.
- **Diseño centrado en el usuario:** considerar las necesidades y las percepciones de seguridad de los diferentes grupos de usuarios de un espacio.
- **Colaboración multidisciplinaria:** fomentar la colaboración entre arquitectos, urbanistas, criminólogos, policías, sociólogos, historiadores, administradores, etc., representantes de la comunidad y otros profesionales relevantes.
- **Evaluación continua y auditorías:** monitorear y evaluar el impacto de las intervenciones CPTED para realizar ajustes y mejoras.
- **Integración con otras estrategias de seguridad:** combinar CPTED con otras estrategias de prevención del delito, como la vigilancia policial, los programas sociales y la participación comunitaria.

La convergencia de CPTED amplía su alcance y eficacia al integrarlo con otros sistemas de gestión y enfoques. A continuación, se detalla la relación de CPTED con las normas ISO 18788:2015, ISO/IEC 27001:2022, ISO 39001:2012/Amd 1:2024, 28000:2022, 9001:2015/Amd 1:2024, 18091:2019, 37120:2018, 38122:2019, 37123:2019 y la 37124:2024.



Normas ISO que complementan el CPTED desde perspectivas específicas:

- **ISO 18788:2015 (Sistemas de gestión de operaciones de seguridad privada — Requisitos con orientación para su uso):** esta norma se centra en la gestión de las operaciones de seguridad privada. La convergencia con CPTED se da al considerar que el diseño ambiental puede influir en la eficiencia de las operaciones de seguridad optimizando el despliegue de recursos de seguridad privada. Además, la norma exige la identificación y gestión de riesgos, lo cual se alinea con el análisis de riesgos previo a la implementación CPTED.
- **ISO/IEC 27001:2022 (Sistemas de gestión de la seguridad de la información):** aunque se enfoca en la seguridad de la información, esta norma es relevante para CPTED en contextos donde se utilizan tecnologías de seguridad, como sistemas de videovigilancia, control de accesos electrónicos o sensores; y de forma operativa por la geolocalización y los espacios públicos como las calles que son conectores sociales. La ISO 27001 asegura que la información recopilada y gestionada por estos sistemas se proteja adecuadamente, evitando accesos no autorizados o fugas de datos. En residenciales habitacionales, centros comerciales, empresas, escuelas, etc., es decir, cualquier estructura física que conforman a las ciudades inteligentes, la integración de CPTED con sistemas de gestión de la información seguros es crucial porque la información de las personas que participan en un proyecto de intervención otorgan sus información y geolocalización de sus casas, lugares de trabajo, etc
- **ISO 39001:2012/Amd 1:2024 (Sistemas de gestión de la seguridad vial):** si bien se centra en la seguridad vial, esta norma puede ser relevante para proyectos CPTED que involucran el diseño de espacios públicos con alta afluencia de vehículos, como calles, estacionamientos o zonas de carga y descarga. La aplicación de principios CPTED puede mejorar la seguridad de peatones y conductores en estos espacios, reduciendo el riesgo de accidentes, robos, violencia, entre otras situaciones.



□ **ISO 28000:2022 (Sistemas de gestión de la seguridad para la cadena de suministro):** en el contexto de CPTED, puede ser relevante para el diseño de infraestructuras críticas, como puertos, aeropuertos o centros de distribución, donde la seguridad de la cadena de suministro es fundamental. CPTED puede contribuir a fortalecer la seguridad física de estas instalaciones, previniendo robos, sabotajes o actos terroristas porque se analiza el territorio, su desarrollo social, urbano y económico.

□ **ISO 18091:2019 (Sistemas de gestión de la calidad:** directrices para la aplicación de la norma ISO 9001 en los gobiernos locales) proporciona un marco para la gestión de la calidad que puede ser aplicado a cualquier servicio o proceso que ofrecen los gobiernos locales, incluyendo las políticas públicas relacionadas con la seguridad, la prevención del delito y participación ciudadana.

□ **ISO 37120:2018 (Desarrollo sostenible de las comunidades — Indicadores para los servicios de las ciudades):** esta norma define los indicadores para medir el desempeño de los servicios urbanos, incluyendo la seguridad. Por ello, al utilizar la ISO 22341 CPTED se deben considerar los indicadores de la ISO 37120, ya que proporciona un marco para evaluar el impacto de las intervenciones sociourbanas en la calidad de vida de los habitantes de un Territorio.

□ **ISO 37122:2018 (Ciudades inteligentes — Indicadores para ciudades inteligentes):** Similar a la ISO 37120, pero enfocada específicamente en ciudades inteligentes, esta norma define indicadores para evaluar el desempeño de las ciudades en diversas áreas, incluyendo la seguridad. CPTED, al integrarse con las tecnologías de las ciudades inteligentes debe considerar los indicadores de seguridad y resiliencia urbana.

□ **ISO 37123:2018 (Desarrollo sostenible de las comunidades — Indicadores para ciudades resilientes):** esta norma se centra en la resiliencia de las ciudades, es decir, su capacidad para resistir y recuperarse de situaciones de crisis. CPTED, al contribuir a la prevención del delito y la mejora de la seguridad, fortalece la resiliencia urbana al reducir la vulnerabilidad de las comunidades ante actos delictivos o situaciones de emergencia.

□ **ISO 37124:2024 (Ciudades y comunidades sostenibles — Guía para el uso de ISO 37120, ISO 37122 e ISO 37123),** esta norma proporciona orientación sobre cómo utilizar un conjunto de indicadores para evaluar el desempeño de las ciudades en diversas áreas, con un enfoque en la sostenibilidad y la resiliencia. Ofrece orientación sobre cómo elegir los indicadores más relevantes según las necesidades y prioridades específicas de cada ciudad. No todas las ciudades necesitarán utilizar todos los indicadores de las tres normas.

□ **ISO 9001:2015/Amd 1:2024 es una enmienda a la norma ISO 9001:2015 (Sistemas de Gestión de la Calidad (SGC)).** Es importante entender que no es una nueva versión de la norma, sino una modificación que se añade a la versión 2015. Introduce modificaciones 3 y aclaraciones a la norma ISO 9001:2015, principalmente en relación con el cambio climático. Su objetivo principal es asegurar que las organizaciones consideren el impacto del cambio climático en sus sistemas de gestión de la calidad, es importante ya que en la ISO 22341 se considera la integración de principios de sostenibilidad ambiental y diseño ecológico en las estrategias CPTED





Cómo convergen estas normas con las Normas ISO CPTED

La convergencia por la transversalidad de las Normas se manifiesta en:

□ **Enfoque holístico de la seguridad:** se pasa de un enfoque centrado en el diseño físico y social a una visión más amplia que considera la gestión de la seguridad, la seguridad de la información, la seguridad vial, la seguridad de la cadena de suministro y la resiliencia urbana.

□ **Integración con sistemas de gestión:** la Metodología CPTED se integra con los sistemas de gestión definidos por las normas ISO, lo que facilita su implementación, seguimiento y mejora continua.

□ **Medición del impacto:** las normas de indicadores (37120, 37122, 37123) permiten evaluar el impacto de las intervenciones de CPTED en la seguridad y la calidad de vida de las personas en un territorio determinado, proporcionando datos objetivos para la toma de decisiones.

□ **Gestión de riesgos integral:** se amplía la gestión de riesgos a diferentes ámbitos, incluyendo la seguridad de la información, la seguridad vial y la seguridad de la cadena de suministro, complementando la gestión de riesgos específico de CPTED para dar paso a un Sistema de Gestión de Riesgos Sociourbanos.

□ **Las auditorías CPTED (con la ISO 19011:2018):** que proporciona directrices para la realización de auditorías de sistemas de gestión, incluyendo la planificación, ejecución, informe y seguimiento de las auditorías. En el contexto del CPTED, la ISO 19011 asegura que las auditorías urbanas se realicen de manera sistemática, objetiva y profesional, siguiendo un proceso estructurado que incluye:

o Gestión del programa de auditoría: define la planificación, los recursos y las responsabilidades para las auditorías.

o Realización de la auditoría: describe las etapas de la auditoría, desde la reunión de apertura hasta el informe final.

o Competencia de los auditores: establece los requisitos de competencia para los auditores, asegurando la calidad de las auditorías.

o Enfoque basado en riesgos: incorpora el enfoque basado en riesgos en todas las etapas de la auditoría, alineándose con la ISO 31000

Beneficios adicionales de la convergencia ampliada:

□ **Mayor integralidad en la gestión de la seguridad:** se aborda la seguridad desde múltiples perspectivas, considerando tanto los aspectos físicos como los tecnológicos, organizativos y sociales.

□ **Mejora de la eficiencia y la eficacia de las intervenciones:** la integración con sistemas de gestión y la medición del impacto permiten optimizar los recursos y obtener mejores resultados.

□ **Mayor adaptabilidad a diferentes contextos:** la convergencia en la trazabilidad con normas específicas permite adaptar CPTED a diferentes tipos de proyectos y entornos, desde edificios residenciales (habitacionales y donde se reside para actividades laborales, 4 comerciales, sociales, culturales y económicas) hasta infraestructuras críticas o ciudades inteligentes.

□ **Verificación del cumplimiento de los principios CPTED:** la ISO 19011:2018 proporciona las herramientas para auditar si el diseño del entorno cumple con los principios de la ISO 22341, lo cual asegura que las estrategias CPTED se implementen correctamente.

□ **Identificación de riesgos específicos:** la auditoría, guiada por la ISO 19011 y utilizando los criterios de la ISO 22341, permite identificar riesgos de seguridad específicos relacionados con el diseño del entorno que puedan facilitar la comisión de delitos.

□ **Evaluación de la eficacia de las medidas CPTED:** la ISO 19011 permite auditar la eficacia de las medidas CPTED implementadas. Se evalúa si las medidas han logrado reducir los riesgos identificados y mejorar la seguridad del entorno.

□ **Priorización de acciones:** la auditoría, al identificar y evaluar los riesgos, permite priorizar las acciones de mejora, con lo cual se deben enfocar los recursos en las áreas que presentan mayor riesgo y donde las intervenciones CPTED tendrán un mayor impacto.

□ **Integración con otros sistemas de gestión:** la ISO 19011 facilita la integración de la gestión de la seguridad, basada en CPTED, con otros sistemas de gestión de la organización, como la gestión de la calidad (ISO 9001:2015/Amd 1:2024), la gestión ambiental (ISO 14001:2015/Amd 1:2024) y fundamental la gestión de riesgos (ISO 31000:2018).

22344.2024

LA NECESIDAD DE UN DEPARTAMENTO DE SEGURIDAD EN LA ESTRUCTURA HOTELERA

Abraham santana Herrera
Director de seguridad. Perito

....UN PILAR PARA LA PROTECCIÓN Y LAS BUENAS PRÁCTICAS

En el sector hotelero, garantizar la seguridad de los huéspedes, empleados y activos no solo es una responsabilidad ética, sino también una necesidad estratégica para el éxito y la sostenibilidad del negocio. La creación de un departamento de seguridad dentro de la estructura organizativa del hotel se ha convertido en un requisito imprescindible para enfrentar los crecientes desafíos del entorno actual. Desde la protección frente a riesgos físicos y cibernéticos hasta el cumplimiento de normativas y la promoción de buenas prácticas, este departamento desempeña un papel fundamental en la operación diaria y en la reputación de la empresa.



Un hotel es un espacio dinámico que alberga a personas de diferentes orígenes, culturas y propósitos. Este carácter heterogéneo lo convierte en un entorno susceptible a riesgos como robos, incidentes de emergencia, ataques cibernéticos o incluso amenazas terroristas. Además, la creciente sofisticación de los clientes exige estándares de seguridad más altos que garanticen tanto su bienestar como la protección de sus datos personales.

Para abordar estas amenazas de manera efectiva, el establecimiento de un departamento de seguridad permite una gestión integral y proactiva de los riesgos, con estrategias específicas adaptadas al contexto de cada hotel.

En el centro de este departamento se encuentra el Director de Seguridad, una figura clave cuya responsabilidad va mucho más allá de la supervisión básica. Este profesional no solo lidera al equipo de seguridad, sino que también actúa como un enlace estratégico entre la alta dirección y las operaciones diarias. Sus funciones incluyen:

- Evaluación de Riesgos: Identificar vulnerabilidades dentro del hotel, desde accesos físicos hasta sistemas tecnológicos.
- Cumplimiento Normativo: Asegurar que el hotel cumpla con las leyes y regulaciones locales, nacionales e internacionales, especialmente en áreas como prevención de incendios, evacuaciones y protección de datos.
- Diseño de Protocolos: Desarrollar y actualizar procedimientos de seguridad que abarquen desde la vigilancia hasta la respuesta ante emergencias.
- Gestión de Crisis: Liderar las acciones durante incidentes críticos, asegurando una comunicación clara y decisiones rápidas.
- Capacitación del Personal: Garantizar que todo el equipo, no solo el de seguridad, esté preparado para actuar ante diversas situaciones de riesgo.

La seguridad es un componente esencial del éxito en la industria hotelera, y un departamento de seguridad bien establecido es la mejor inversión para garantizar la tranquilidad de los huéspedes, el personal y los propietarios.

El entorno regulatorio del sector hotelero es cada vez más complejo, abarcando normativas que van desde la seguridad física hasta la protección de datos de los clientes. Un departamento de seguridad bien estructurado, liderado por un Director de Seguridad capacitado, asegura que el hotel opere dentro de los marcos legales, evitando sanciones y preservando su reputación.

Asimismo, la implementación de buenas prácticas, como la incorporación de tecnología avanzada para el control de accesos o la instalación de sistemas de videovigilancia integrados, no solo mejora la seguridad, sino que también refuerza la percepción de los huéspedes sobre la calidad del servicio.

Más allá de la protección, la seguridad también es un elemento diferenciador en el mercado hotelero. Los clientes valoran la tranquilidad de saber que su bienestar y sus pertenencias están en buenas manos. Esto puede traducirse en una ventaja competitiva, fomentando la fidelidad de los huéspedes y atrayendo a nuevos clientes que priorizan la seguridad al elegir un alojamiento.

Además, un enfoque sólido en seguridad reduce los costos asociados con incidentes, como indemnizaciones, interrupciones operativas o daños a la reputación, lo que impacta positivamente en la rentabilidad del hotel.



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, cibercrimes y delitos económicos.

DETECCIÓN

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

INVESTIGACIÓN

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

SEGURIDAD INTEGRAL

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

SEGURIDAD INTELIGENTE: PRIVACIDAD Y PROTECCIÓN

Rosa Fernández

ASUNTO: SEGURIDAD 360º

¿Empezamos el año como lo terminamos?. ¿Sigues sin tener claro si tienes protección, si tu documentación te protege, si estás trabajando con legalidad? No te preocupes, para eso estamos. Para recordarte lo importante que es para ti y tus clientes que cumplas con la normativa vigente, no sólo la de tu sector, sino esa normativa universal que protege derechos fundamentales. Si, esa. El RGPD y la LOPDGD.

Es muy importante que la tengas en el radar porque el mundo está muy tecnologizado y tu entorno de trabajo más: dispositivos por todos lados que tratan datos, procesan información con la que se obtienen datos que hay que protege

Así que ten en cuenta esto: Seguridad 2025, Esencial para Pequeñas Empresas como la tuya, para tu proyecto o para tu actividad como profesional altamente competente y responsable. La protección de datos y la privacidad ya no son conceptos reservados para grandes corporaciones o empresas tecnológicas.

En 2025, pequeñas empresas, especialmente las dedicadas a la seguridad privada, enfrentan desafíos únicos en un mundo donde los dispositivos cotidianos como drones, videovigilancia y sistemas biométricos son herramientas clave de trabajo. Estos avances traen consigo grandes oportunidades, pero también responsabilidades ineludibles en materia de privacidad y cumplimiento normativo. Gestiona confianza con la privacidad.

La privacidad no es solo un requisito legal, es un elemento de confianza que puede marcar la diferencia entre ganar o perder un cliente. Por ejemplo, cuando una empresa de seguridad utiliza drones para patrullar una propiedad o gafas grabadoras para documentar eventos en tiempo real, los clientes esperan que sus datos estén protegidos y que las grabaciones solo se utilicen para los fines acordados. La normativa de protección de datos, como el RGPD, establece obligaciones claras para el uso de estos dispositivos, incluyendo la necesidad de informar a las personas afectadas, garantizar la seguridad de las grabaciones y definir límites claros sobre su uso.

Dispositivos Cotidianos y Retos de Privacidad Aquí te comparto unos cuantos ejemplos de lo que puedes usar tu, tu empresa o tus clientes para tener un entorno seguro. No se trata sólo de la protección física, sino también tienes que cumplir con la protección legal del uso y la finalidad de estas herramientas para tu trabajo, así que no pierdas de vista que: Los dispositivos de captura de imágenes y video, como drones, sistemas de videovigilancia, gafas grabadoras y cámaras corporales, son herramientas fundamentales en la seguridad privada, pero implican riesgos asociados a la grabación no autorizada de personas o propiedades fuera del objetivo establecido.



Los dispositivos de captura de audio, como los registros de voz, su uso sin el debido consentimiento puede infringir derechos de privacidad. Por otro lado, los dispositivos de identificación y autenticación, como los sistemas de accesos biométricos y reconocimiento facial, manejan datos altamente sensibles que requieren medidas avanzadas de protección. Los dispositivos de supervisión física, como las mirillas periscópicas, presentan riesgos de intrusión en espacios privados si no se utilizan con precaución. Finalmente, los dispositivos digitales y conectados, como los dispositivos móviles corporativos y los sensores IoT, implican riesgos relacionados con el almacenamiento y transmisión segura de datos, además del riesgo de accesos no autorizados.

Aplica las estrategias adecuadas a cada herramienta con la que trabajes, y no te olvides, que también tienes que proteger los datos que te confía su propietario.

Consultora jurídica. ©2024
Miembro del Comité Técnico de
MetroRisk, área de seguridad
jurídica y derecho tecnológico





ZonaVigilada

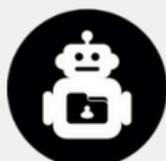
Nuestros servicios de **CONSULTORÍA, ASESORAMIENTO, FORMACIÓN Y AUDITORÍA** te permiten aplicar el cumplimiento digital (RGPD, LOPDgdd, ePrivacy, Redes, Cloud...) en tu empresa, aumentando la reputación y la confianza y evitando sanciones. Trabaja con nosotros y entra en ZonaVigilada, tu Agencia de Seguridad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



Documento de
Actividades del
Tratamiento



Contratos y Protocolos



Cumplimiento Digital



Asesoramiento y
Soporte RGPD



Vigilancia Legislativa

<https://futurasoluciones.es/rgpd-zonavigilada/>

Rosa 6.0 Código Experiencia



Consultora Sr Calidad (ISO, EFQM, 5S)

Consultora Sr Tecnología y Privacidad (RGPD.LOPDgdd)

Formadora veterana*

Diseñadora de material didáctico

Desarrollo de contenidos y redactora

Diplomada en Derecho, Tecnología e Innovación

Miembro Comité Técnico en MetroRisk

Socia de ENATIC, asociación de Abogacía Digital

Competencias técnicas:

WORDPRESS, PRESTASHOP, PREZI, POWTOON, DOODLY,
AUDACITY, MOODLE, OBS, VIMEO.



*+ de 20 años formando a profesionales



EL CONVENIO COLECTIVO Y LAS LICITACIONES PÚBLICAS: UN SISTEMA QUE ESTRANGULA A VIGILANTES Y EMPRESAS DE SEGURIDAD

Carlos Serrano
Director de Contenidos de Seguridad y Empleo

La seguridad privada en España, un pilar esencial para garantizar la protección de personas e instalaciones, atraviesa una crisis estructural que amenaza su sostenibilidad. En el epicentro de este problema se encuentran las licitaciones públicas, que priorizan el precio más bajo, y un convenio colectivo incapaz de adaptarse a las necesidades actuales del sector. Este cóctel explosivo deja a los vigilantes con salarios precarios y a las empresas al borde de la viabilidad económica.

La precarización institucionalizada El sistema de licitaciones públicas, diseñado para optimizar los recursos del Estado, ha terminado convirtiéndose en un arma de doble filo. Las adjudicaciones basadas exclusivamente en el precio más bajo no solo comprometen la calidad del servicio, sino que también imponen condiciones insostenibles para los trabajadores y las empresas. La búsqueda de ahorro inmediato se está asfixiando a un sector que requiere estabilidad para cumplir su función social. Un ejemplo ilustrativo es el coste que supone un equipo de cinco vigilantes operando las 24 horas del día: más de 141.000 euros al año, incluyendo pluses de nocturnidad y trabajo en fines de semana. Sin embargo, los contratos adjudicados apenas permiten a las empresas cubrir estos gastos, dejando márgenes de beneficio ínfimos y ningún espacio para mejorar las condiciones laborales o invertir en innovación

El convenio colectivo: una herramienta desfasada En teoría, el convenio colectivo debería ser un escudo protector para los derechos de los trabajadores. En la práctica, ha quedado obsoleto, atrapando tanto a empleados como a beneficios en una trampa económica. Mientras los vigilantes se resignan a salarios mínimos, las empresas se enfrentan a un panorama financiero crítico, con beneficios que rara vez superan el 6%. Este margen, insuficiente para cubrir imprevistos o invertir en formación y tecnología, condena al sector a una precariedad crónica.

Un círculo vicioso sin salida La interacción entre licitaciones públicas restrictivas y un convenio colectivo desfasado ha creado un círculo vicioso. Las empresas, incapaces de asumir costes adicionales, no pueden ofrecer salarios competitivos ni mejorar sus servicios. Esto genera una espiral descendente en la que los vigilantes ven limitada su progresión profesional, y los clientes, ya sean instituciones públicas o privadas, reciben servicios cada vez más limitados

¿Es posible revertir la situación? A pesar del sombrío panorama, existen propuestas viables para rescatar al sector. Entre las más destacadas se encuentran:

1. Revisar los criterios de adjudicación : Incorporar la calidad del servicio como elemento clave, no solo el costo económico.
2. Ampliar los márgenes empresariales : Ajustar las licitaciones para garantizar un equilibrio entre precio y sostenibilidad.
3. Revisar el convenio colectivo : Modernizarlo para que refleje las realidades actuales del sector y permita la mejora de condiciones laborales. Estas no solo permitirían la supervivencia de las empresas, sino que también dignificarían el trabajo de los vigilantes, cuyo papel resulta imprescindible para la seguridad en nuestra sociedad



www.seguridadyempleo.com

C2C Consultoría&Compliance



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



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

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

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

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

¿RPO y RTO? ¿Sabes cuántos minutos puede resistir tu negocio sin sufrir una catástrofe?

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

Imagina que el peor escenario golpea tu empresa: ciberataques, desastres naturales o fallos críticos....

El reloj empieza a correr 🕒 y cada segundo cuenta.

📄 **RPO** (Recovery Point Objective):

¿Cuánto puedes perder antes de que te falten los datos críticos?

⌚ **RTO** (Recovery Time Objective):

¿En cuánto tiempo puedes estar de vuelta sin perder clientes, ingresos y reputación?

👉 ¿Por qué importa esto?

Porque la diferencia entre una empresa resiliente y una que desaparece en el caos es la capacidad del plan para la continuidad de negocio.

Datos Impactantes:

Más del 60% de las empresas sufrieron incidentes de seguridad solo en un año.

🔒 ¿Ransomware?

Una organización atacada puede perder días... incluso semanas de operaciones.

🔗 Hoy, no tener un Plan de Continuidad de Negocio (ISO 22301) es como navegar en alta mar sin salvavidas.

"La resiliencia no es una opción, es la garantía de que cuando todo falle, tú no fallarás." - Emilio Piñero

✅ De riesgos sabe mucho mi estimado David Méndez Piffault.

David, me encantaría conocer tu opinión:

¿Qué es lo primero que debe analizar una organización cuando quiere prepararse para lo inevitable?

¿Listos para evitar que el negocio se detenga?



Figura 11. Descripción gráfica de RTO

Fuente: <https://ciberseguridad.blog/conceptos-basicos-de-plan-de-continuidad-de-negocio-rpo-rto-wrt-mtd/>

Punto Objetivo de Recuperación (RPO), describe el tiempo del último punto de restauración que se haya generado, es decir, la tolerancia que el negocio puede permitir para continuar sus actividades con el último respaldo.



Figura 12. Descripción gráfica de RPO

Fuente: <https://ciberseguridad.blog/conceptos-basicos-de-plan-de-continuidad-de-negocio-rpo-rto-wrt-mtd/>

MÁS ALLÁ DE LAS LUCES: LOS DESAFÍOS OCULTOS DE LA SEGURIDAD NAVIDEÑA

Elena de la Parte

La Navidad, para algunos es sinónimo de alegría, reuniones familiares y consumismo, también representa un período de alta vulnerabilidad en términos de seguridad.

Para otros sectores profesionales, que trabajan a turnos y a cuadrante anual, como la seguridad privada y sus especialidades. Extendido también a otros sectores profesionales como; las emergencias las FCSE, LA UME, LOS TECNICOS SANITARIOS Las Emergencias Sanitarias (TES) los bomberos, médicos etc. la navidad se puede convertir en días de múltiples caos, incidentes, accidentes y otras circunstancias improvisadas inesperadas e indeseadas.



Más allá de las luces y los adornos, se esconde un complejo entramado de riesgos que van desde lo físico hasta lo cibernético, pasando por lo sociopolítico.

Este artículo profundiza en los principales desafíos que enfrentan empresas, gobiernos y ciudadanos durante esta temporada, y propone estrategias para garantizar unas fiestas un poquitín más seguras y tranquilas.

Los Riesgos Escondidos de la Navidad La temporada navideña, marcada por un aumento significativo en la actividad económica y social, se convierte en un blanco atractivo para diversos actores malintencionados. Los riesgos se multiplican y se entrelazan, creando un panorama complejo que exige una respuesta integral.

· **Seguridad Física y Ambiental:** · Aumento de la criminalidad: Robos, hurtos y atracos se incrementan debido a la mayor afluencia de personas en espacios públicos y privados. · Amenazas terroristas: Lugares concurridos como mercados navideños y centros comerciales se convierten en blancos potenciales para ataques. · Desastres naturales: Eventos climáticos extremos, cada vez más frecuentes, pueden interrumpir las festividades y causar daños significativos. · Incendios: El uso indiscriminado de velas, luces navideñas y otros elementos inflamables aumenta el riesgo de incendios en hogares y establecimientos comerciales.

· **Seguridad Tecnológica:** · Ciberataques: El comercio electrónico y las transacciones en línea se multiplican, creando oportunidades para cibercriminales que buscan robar datos personales y financieros. · Phishing y estafas: Los correos electrónicos y mensajes fraudulentos se vuelven más sofisticados, engañando a usuarios desprevenidos. · Ransomware: El bloqueo de sistemas informáticos a cambio de un rescate se ha convertido en una amenaza constante para empresas de todos los tamaños. · Phishing y fraude del CEO: Engaños a empleados para obtener acceso ilegítimo a sistemas y fondos. · Denegación de servicio (DoS) es una ciberamenaza que tiene como objetivo principal hacer inaccesible un servicio o recurso de red a sus usuarios legítimos. En términos más simples, es como inundar un servidor con tanto tráfico que se "ahoga" y deja de responder a las solicitudes normales.

· **Seguridad Sociopolítica y Económica:** · Inestabilidad geopolítica: Conflictos internacionales y tensiones comerciales pueden afectar las cadenas de suministro y generar escasez de productos. · Desigualdad social: Las protestas y manifestaciones sociales pueden intensificarse durante la Navidad, generando tensiones y alteraciones del orden público. · Desinformación: La propagación de noticias falsas y teorías conspirativas puede exacerbar divisiones sociales y socavar la confianza en las instituciones

Un Enfoque Integral para la Seguridad Navideña Ante la creciente complejidad de los riesgos, es necesario adoptar un enfoque integral que combine medidas preventivas, tecnológicas y de colaboración. Algunas recomendaciones clave incluyen: · Fortalecer la colaboración público-privada: Una estrecha cooperación entre gobiernos, empresas y ciudadanos es fundamental para compartir información, coordinar acciones y responder de manera efectiva ante incidentes. · Invertir en tecnología: El uso de sistemas de vigilancia inteligentes, análisis de datos y ciberseguridad avanzada puede ayudar a detectar y prevenir amenazas. · Concientizar a la población: Campañas de sensibilización sobre los riesgos más comunes pueden ayudar a los ciudadanos a adoptar medidas de autoprotección. · Preparar planes de emergencia: Empresas y gobiernos deben contar con planes detallados para responder a incidentes de seguridad, incluyendo simulacros

La Navidad, más allá de ser una época de celebración, plantea desafíos importantes en materia de seguridad. Al comprender los riesgos y adoptar un enfoque proactivo, podemos garantizar unas fiestas seguras y tranquilas para todos. La seguridad navideña no es solo una responsabilidad de las autoridades, sino de cada uno de nosotros. Desde esta redacción y editorial de MetroRisk os deseamos, los mejores deseos en Navidad, esperamos que estas fiestas les traigan mucha alegría. Un agradecimiento especial a todos los colegas que trabajan durante estas fechas navideñas. Les enviamos un abrazo y les deseamos un buen servicio y sin novedades. "La Navidad es un libro abierto. Cada página cuenta una historia diferente. ¡Leamos nuestro propio capítulo y celebremos la diversidad de esta festividad!" "La Navidad es un mosaico de historias. ¡Añade la tuya!"

Rafael Hernández
Asesor de Seguridad en Segurma S.A

LA IMPORTANCIA DE LOS SISTEMAS CCTV.

Los sistemas de Circuito Cerrado de Televisión, por sus siglas CCTV (Closed Circuit Television), tienen una importancia vital y son un complemento ideal dentro de los Sistemas de Seguridad. Lo más habitual es enfocarlos en la evaluación y comprobación en un salto de alarma, ya que podemos actuar con mayor rapidez y evitar falsas alarmas, además de proporcionarnos una respuesta rápida, pero tiene otras importantes ventajas. Algunas ventajas son las siguientes:



«El trabajo en equipo es la habilidad de trabajar juntos con un objetivo en común. La habilidad de lograr logros personales relacionados con los objetivos empresariales. Es la gasolina que permite a la gente común lograr resultados no comunes»



- Tiene un gran efecto disuasorio, ya que un posible delincuente, al saberse que lo están grabando, opte por no cometer ningún delito.
- Podemos comprobar y vigilar en tiempo real cualquier tipo de incidencia que acontezca en nuestras instalaciones, ya sea un robo, un hurto, un incendio, una inundación, un altercado o disputa de empleados o clientes etc...
- Podemos realizar rondas de vigilancia en cualquier momento.
- En caso de emergencia, podemos dirigir a las personas a la salida más segura en una evacuación de emergencia.
- La supervisión de empleados y clientes en tiempo real.
- Corregir fallos de producción.
- Los fotogramas. La tasa de fotogramas (FPS) debe permitirnos el seguimiento y ubicación del objetivo de la grabación dentro del espacio vigilado. Para una buena identificación es aconsejable utilizar una tasa superior de 6 fotogramas por segundo.
- La compresión. El objetivo es no disminuir la calidad de la imagen, o lo que es lo mismo, la compresión exacta para para no influir negativamente en la calidad.
- La iluminación evitando zonas donde se produce un exceso de luz (contraluces) o en caso contrario (en lugares con poca luz) utilizar iluminación alternativa.

Independientemente de la tecnología que utilicemos para estos sistemas (IP o analógicos), debemos tener claro lo que queremos visualizar, no es lo mismo querer observar una vista general o algo más concreto con todo detalle.

Por lo tanto, no tenemos que instalar el mismo tipo de cámara con las mismas características. Para instalar la cámara adecuada debemos conocer lo siguiente:

- La resolución que nos va a aportar la capacidad para ver con detalle lo que queremos observar, posiblemente lo más importante. a la LOPD.

Por último y no menos importante, disponer de un grabador en zona segura, con acceso restringido, actualizado, con fecha y hora correctos, con capacidad de grabación como mínimo de 15 días y con un máximo de 30 días (según normativa no se debe guardar más tiempo las grabaciones), y cumplir con las Normativa Vigente en cuanto



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

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

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

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

Colaboramos con MR-CONSULTING.



Asesoramiento Técnico

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

En el Ámbito de la:

- Seguridad Privada, Balística Forense.
Ciberseguridad, Inteligencia y
Geopolítica.
- Seguros de Embarcaciones Recreo.
Grafología, Documentoscopia,
Grafopsicopatología Criminal y
Forense.
- Due Diligence (Debida Diligencia).

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

AGENDA

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 INTERECONOMIA VALENCIA PARA TODA ESPAÑA.**



Profesorado

Compuesto fundamentalmente por profesores colaboradores del Sector especializados en relaciones internacionales, seguridad pública, inteligencia, así como juristas, miembros de las Fuerzas Armadas, de las Fuerzas y Cuerpos de Seguridad y profesionales de la Seguridad Privada, dando así un carácter multidisciplinar y global al Curso en todas sus materias.

Sistema de enseñanza

Metodología **ONLINE**, avanzar a lo largo del itinerario de aprendizaje y finalmente realizar con éxito la evaluación final, en la que el alumno/a deberá completar todos los ejercicios propuestos en el curso con más de un 50% de aciertos para superarlo.

Nuestra trayectoria

AIMCSE es una Asociación Internacional que se constituyó en el año 2013 en España, para aunar los intereses de los profesionales de todos los cuerpos de seguridad y emergencias.

Patrocinan:



Contáctanos

Calle Espoz y Mina, 2-1º
28012 Madrid (Spain)

info@aimcse.org
www.aimcse.org

VI Edición Curso Online Superior Universitario

SEGURIDAD INTERNACIONAL INTELIGENCIA Y GEOPOLÍTICA

Curso 2025

★ La Salle
Escuela de Posgrado

PROTEGENS MUNDI
AIMCSE
www.aimcse.org

web somosdirectores.es



Aquí es donde comienza nuestra lucha por la dignificación y profesionalización del **DIRECTOR DE SEGURIDAD**

Con la denominación **ASOCIACIÓN PARA LA PROFESIONALIZACIÓN Y DIGNIFICACIÓN DEL DIRECTOR DE SEGURIDAD**, se constituye una asociación al amparo de la Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación, y normas complementarias, con personalidad jurídica y plena capacidad de obrar, careciendo de ánimo de lucro.

MR Consulting, de METRORISK en YouTube

www.youtube.com/channel/UCyKvr4HvT52sCiIzI7wrxjQ

No te pierdas los blogspot de:



WWW.ALBERTORAY.COM

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



LOS CONSEJOS DE CIBERSEGURIDAD DE ADOLFO GELDER.

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

DESDE 2014

SEGURIDAD Y EMPRESAS GRUPO SEGURIDAD Y EMPLEO

Seguridad y Empresa
Los mejores servicios para
empresas y particulares.

Especialidades
cursos, servicios jurídicos,
telefonía, kit digital,
colaboraciones, sistemas de
seguridad, gestión
subvenciones,, asesoría
formación y seguros



Metrorisk

Proyecto Asociativo

www.metrorisk.es