EDITORIAL MR

MARZO

AÑO 2025

Fran Medina Cruz | Francisco Javier Gonzales Fuentes | José Ignacio Olmos Casado | Gregorio Duro
Mercedes Escudero Carmona | Antonio Cozano Fernández | Emilio Piñeiro | Adolfo M. Gelder
Rosa Fernández | Carlos Serrano | Abraham Santana Herrera | Elena de la Parte | 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.

A SEGURIDAD PRIVADA Y LA IMPORTANCIA DEL RELATO.

Metro Risk

Fran Medina Cruz
Director de MetroRisk

En el sector de la seguridad privada, la narrativa juega un papel esencial en la percepción y efectividad de sus actores. Desde la formación de los vigilantes y mandos intermedios hasta la regulación y la estructura empresarial, el relato que se construye en torno a la seguridad privada determina tanto la calidad del servicio como su legitimidad en el tejido social y económico. Sin embargo, esta narrativa se encuentra fragmentada, con un marcado énfasis en el negocio sobre los efectivos, una regulación estancada y un ingreso al sector cada vez más desprotegido y vulnerable.

Uno de los pilares fundamentales de la seguridad privada es la formación de sus efectivos. Un vigilante bien capacitado no solo representa un recurso eficiente para la empresa que lo contrata, sino que además actúa como un verdadero profesional capaz de reaccionar adecuadamente ante cualquier contingencia. No obstante, el relato institucional y empresarial ha ido relegando la formación a un papel secundario. En lugar de un proceso riguroso de selección y capacitación, se ha priorizado una entrada masiva y poco filtrada al sector, lo que compromete la calidad y profesionalismo de los servicios prestados. El resultado de esta falta de filtros y exigencias formativas es evidente: vigilantes de seguridad con una comprensión limitada de sus funciones y derechos, así como una menor capacidad para gestionar crisis de manera efectiva. A su vez, esto impacta negativamente en la imagen de la seguridad privada, reduciendo su credibilidad ante el público y las fuerzas del orden.

Las empresas de seguridad privada, como cualquier otra entidad comercial, buscan rentabilidad. Sin embargo, la tendencia actual en el sector apunta a una visión puramente mercantilista, donde la reducción de costos y la maximización de beneficios han tomado prioridad sobre la calidad del personal y el servicio. La rotación laboral, los bajos salarios y la sobrecarga de funciones son síntomas claros de una industria que ha optado por la rentabilidad inmediata en lugar de la sostenibilidad y el prestigio a largo plazo. Esta lógica empresarial también se traduce en una narrativa donde el vigilante es visto como un recurso desechable, más que como un profesional imprescindible. A esto se suma una competencia feroz en el sector, donde el abaratamiento del servicio se ha convertido en la estrategia predominante para ganar contratos, muchas veces a costa de la seguridad real que se ofrece.

La seguridad privada opera dentro de un marco normativo que, en teoría, debería garantizar la calidad del servicio y la protección de sus agentes. Sin embargo, la realidad es que muchas regulaciones han quedado obsoletas o simplemente no se aplican de manera efectiva. La falta de actualización legislativa en relación con los nuevos desafíos en seguridad, la ausencia de mecanismos de control eficientes y la permisividad con prácticas empresariales poco éticas han generado un entorno donde la precarización laboral y la falta de garantías legales son moneda corriente.

En este punto, surge una pregunta clave: ¿Por qué los gobiernos no han impulsado una regulación más estricta y efectiva para el sector? La respuesta podría estar en la relación de conveniencia que muchas veces existe entre la seguridad privada y los intereses políticos. Un sector fragmentado y precarizado es más fácil de controlar y manipular, ya que no representa una amenaza real para otros sectores de poder ni exige cambios estructurales que podrían afectar a ciertos intereses económicos.

Por último, la apertura descontrolada del sector a nuevos miembros sin filtros adecuados ha generado una fuerza laboral frágil y vulnerable. La facilidad para obtener acreditaciones y acceder a puestos de vigilancia sin una preparación real pone en riesgo no solo a los propios vigilantes, sino también a la sociedad que depende de sus servicios. Además, la precariedad laboral y la falta de incentivos para el desarrollo profesional han convertido a la seguridad privada en una opción de empleo de última instancia, en lugar de una carrera con proyección y prestigio.

Si queremos que la seguridad privada sea vista como un sector profesional y confiable, es fundamental cambiar el relato que la rodea. Esto implica reforzar la formación de los efectivos, mejorar las condiciones laborales, actualizar la regulación y exigir a las empresas un compromiso real con la calidad del servicio. La seguridad privada no puede seguir siendo un sector donde el negocio prima sobre la protección, donde la falta de regulación favorece el deterioro de sus condiciones y donde la narrativa empresarial minimiza el papel fundamental de sus agentes. Solo a través de una transformación profunda podremos construir un relato que dignifique la labor de los profesionales de la seguridad privada y garantice un servicio eficaz para la sociedad.

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

EL DIRECTOR DE SEGURIDAD COMO CONSULTOR: CLAVE PARA LA GESTIÓN INTEGRAL DE RIESGOS EN LAS PYMES

Metro Risk

Francisco Javier Gonzales Fuentes
Presidente de ADISPO y FIBSEM

...En el mundo empresarial actual, caracterizado por su dinamismo y complejidad, la figura del Director de Seguridad ha evolucionado más allá de la supervisión operativa para convertirse en un asesor estratégico clave. Este papel consultivo en materia de seguridad integral permite a las organizaciones anticiparse, prevenir y responder eficazmente a los diversos riesgos que pueden amenazar su continuidad y reputación. Esta evolución resulta especialmente relevante para las pequeñas y medianas empresas (PYMES), que enfrentan desafíos particulares en la gestión de sus recursos y en la protección de sus activos.

IntelForensic
G&F Soluciones

Las PYMES, a menudo centradas en el crecimiento operativo, pueden subestimar la importancia de una gestión integral de la seguridad. Aquí es donde la figura del Director de Seguridad, actuando como consultor profesional autónomo, cobra un valor esencial. Este profesional ofrece a las PYMES un servicio personalizado y flexible, adaptado a sus necesidades específicas, sin que ello suponga la carga económica de mantener un departamento de seguridad interno. A través de un enfoque consultivo, el Director de Seguridad identifica vulnerabilidades, evalúa riesgos y propone soluciones prácticas y rentables que fortalecen la resiliencia empresarial. El Director de seguridad no solo está enfocado a la Seguridad Privada, también de manera transversal como profesional autónomo puede ofrecer sus servicios de consultoría a cliente y empresas.

Tradicionalmente, la seguridad en las organizaciones se limitaba a la vigilancia física y al control de accesos. Sin embargo, las PYMES también se enfrentan a amenazas como el cibercrimen, la protección de datos, los fraudes internos y las emergencias/ crisis. El consultor en seguridad para PYMES no solo aborda estas problemáticas, sino que además ofrece un acompañamiento estratégico, integrando la seguridad física, lógica y humana en la toma de decisiones corporativas. Esto se traduce en la elaboración de planes de contingencia, formación para el personal, diseño de protocolos de emergencia y la implementación de tecnologías adecuadas a cada entorno.

La contratación de un Director de Seguridad como consultor autónomo brinda a las PYMES múltiples beneficios. Permite la toma de decisiones informadas que reducen pérdidas económicas, evita sanciones derivadas del incumplimiento normativo y promueve un entorno laboral seguro que mejora la productividad y la confianza del equipo de trabajo. Asimismo, contribuye a fortalecer la reputación empresarial frente a clientes, proveedores e inversores, quienes valoran positivamente las organizaciones que priorizan la seguridad y la gestión responsable de sus riesgos.

El éxito de este enfoque consultivo radica en la capacidad del profesional para comprender la realidad operativa de las PYMES, ofreciendo soluciones viables que no impliquen inversiones desproporcionadas. La clave está en priorizar acciones de alto impacto, aprovechando los recursos disponibles y sensibilizando a la dirección sobre la importancia de integrar la seguridad en su estrategia de negocio. Además, la flexibilidad que ofrece un consultor autónomo permite a las empresas contar con asesoría continua o puntual según sus requerimientos y presupuestos.

Para desempeñar esta función con eficacia, el Director de Seguridad debe poseer competencias en análisis de riesgos, gestión de crisis, normativas legales aplicables y liderazgo organizacional. La empatía, la comunicación efectiva y la adaptabilidad son cualidades esenciales para lograr una relación de confianza con las PYMES, entendiendo sus limitaciones y oportunidades. Este acompañamiento cercano permite que las empresas pequeñas y medianas se sientan respaldadas en la toma de decisiones críticas que pueden marcar la diferencia entre la continuidad o el fracaso ante situaciones adversas.

El papel del Director de Seguridad como consultor profesional autónomo representa una oportunidad estratégica para las PYMES que buscan crecer de forma sostenible y segura. Más allá de proteger activos, su intervención ayuda a crear una cultura organizacional consciente de los riesgos y preparada para enfrentarlos. Apostar por la seguridad no solo es una inversión en protección, sino en la proyección y competitividad futura de la empresa

Mtro. Francisco Javier González Fuentes

SEGURIDAD, ¿PÚBLICA O PRIVADA?

Metro Risk

José Ignacio Olmos Casado
Presidente AEAS

...La cuestión que plantea el título de este artículo es un debate abierto que nos encontramos en la sociedad actual.

Este debate no sólo está presente en el ámbito de la seguridad, sino también en otros como la educación o la sanidad; y es un debate lícito, actual y hasta considero que sano y necesario.

La cuestión no es baladí y trasciende la discusión coloquial y, posiblemente incluso la académica, puesto que, en nuestro caso concreto hablamos de un derecho fundamental, base además para el desarrollo de las libertades individuales y también de la vida social.

Por ello no sólo hemos de tener en cuenta jurisprudencia y doctrina, sino también ámbitos reales y más prácticos como problemáticas sociales, demandas de los ciudadanos e índices delincuenciales.

La existencia de seguridad privada puede históricamente remontarse muy atrás en unos u otros formatos, y, en la sociedad actual, está presente con distintos alcances en todos los países de nuestro entorno.

En el caso concreto de España el fundamento jurídico tenemos que buscarlo en el más alto nivel normativo: el artículo 17 de la Constitución. Dicho artículo establece que "toda persona tiene derecho a la libertad y a la seguridad".

Por tanto la primera precisión a realizar es que, jurídicamente, la seguridad se configura como un derecho de los ciudadanos, y no como cualquier derecho, sino como un derecho fundamental, con todas las garantías que le asisten.

Dado que la seguridad es un derecho, como con cualquier otro, el Estado es el encargado de intentar garantizar el libre ejercicio de los derechos por parte de los ciudadanos, disponiendo para ello como instrumento de las Fuerzas y Cuerpos de Seguridad, como así establece el artículo 104.1 de nuestro texto constitucional.

Hasta aquí, como vemos, no aparece la seguridad privada; pero, ¿cuál es la razón de que exista esa seguridad privada? Por un lado hay que pensar que los recursos de que dispone el Estado son siempre limitados, por lo que él mismo viene a considerar que si alguien quiere disponer de más seguridad que la que puede ofrecer, lo va a permitir. Por otro lado, existirían esferas de actividad más estrictamente privadas (y que posiblemente puedan influir menos en la seguridad ciudadana); aquí el Estado vuelve a adoptar la misma postura: si quieres seguridad para tus cosas lo permito, con coste a tu cargo

En ambos casos, no sólo es que el Estado permita esa seguridad privada, sino que la autoriza, dice cómo debe ser en todos los ámbitos, cómo deben desarrollarse todos los servicios, tiene la postestad de controlarlos e inspeccionarlos, e incluso, si hay anomalías, bien no autorizarlos o fundamentalmente proponer para sanción e incluso finalizarlos

De cualquier manera, y volviendo a la legitimación estricta de la seguridad privada, la existencia de ésta se basa, al final, en que el titular de ese derecho fundamental es el ciudadano, no el Estado, y por tanto el propio Estado no puede negarme ese derecho a la seguridad si soy yo el que quiere intentar garantizárselo, sólo supervisarlo y darlo forma. La seguridad privada es, como no puede ser de otra manera, una de las actividades más intervenidas desde el punto de vista administrativo.

La propia Ley 5/2014, de seguridad privada establece que la seguridad privada es complementaria de la pública. Esto nos lleva a establecer que en España la fórmula jurídica de la seguridad se articula como la suma de la seguridad pública y de la privada. De alguna manera y por expresarlo de una forma más gráfica y menos jurídica, en virtud de ese artículo 104.1 de nuestra Carta Magna, la parcela de la seguridad pertenecería a la seguridad pública, pero una parte de ella es arrendada a la seguridad privada; por eso cuando alguien (empresa o personal) quieren acceder a esa parcela necesitan primero de su autorización; una vez que están dentro de ella, los titulares de la parcela (las Fuerzas de Seguridad) son los que vigilan si son buenos inquilinos, y en caso contrario puede llegar a producirse la expulsión de la misma. Progresivamente, además, la seguridad privada viene ocupando cada vez más terreno en esa parcela

AEAS
Asociación Española de Auditores de Seguridad

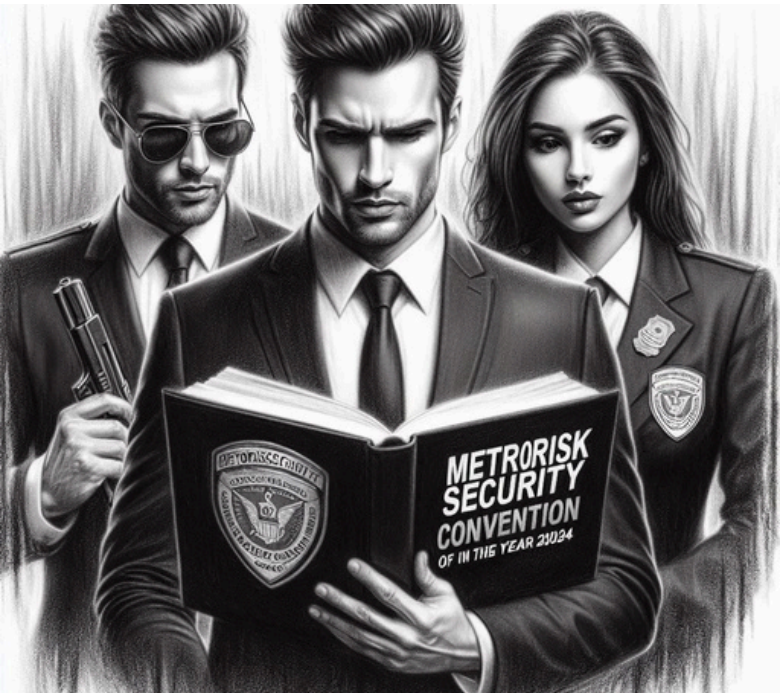
La normativa de seguridad privada española, que ya fue avanzada en su momento y modelo para otros países con la Ley 23/92, sigue siéndolo con la actual Ley 5/2014, de seguridad privada; en particular comentaremos alguno de los nuevos servicios que en ella se establecieron:

"Artículo 41. Servicios de vigilancia y protección.

3. Cuando así se decida por el órgano competente, y cumpliendo estrictamente las órdenes e instrucciones de las Fuerzas y Cuerpos de Seguridad, podrán prestarse los siguientes servicios de vigilancia y protección:

a) La vigilancia perimetral de centros penitenciarios.
b) La vigilancia perimetral de centros de internamiento de extranjeros.
c) La vigilancia de otros edificios o instalaciones de organismos públicos. d) La participación en la prestación de servicios encomendados a la seguridad pública, complementando la acción policial.

La prestación de estos servicios también podrá realizarse por guardas rurales." Los nuevos servicios que aparecen en este apartado tercero del artículo 41 fueron muy polémicos ya desde antes de la aprobación de la Ley De él, podemos hacer una división en dos partes: los tres primeros apartados, que pueden tener ciertas similitudes, y el último.



De los tres primeros, posiblemente el más destacado sea el apartado a), pues en su puesta en marcha se alzaron muchas voces con opinión contraria, desde partidos políticos a asociaciones de Guardias Civiles, sindicatos policiales o meros ciudadanos.

Ante esas voces podemos hacer algunas argumentaciones, no ya como profesionales de la seguridad, sino simplemente como ciudadanos:

- Las funciones que desempeñan las Fuerzas y Cuerpos de Seguridad en esos servicios no son particularmente sofisticadas.
- Con la formación adecuada la seguridad privada puede prestarlas (si ha aprendido un funcionario público, casi seguro que yo también puedo aprender).
- Posiblemente el coste de la prestación del servicio por parte de seguridad privada sea más económico.

Al final, vemos que lo primordial es la capacitación adecuada del personal, y, por supuesto, la seriedad y el control de las administraciones públicas tanto en las licitaciones como en el seguimiento de los contratos. Yo, particularmente, como ciudadano, no me gasto el dinero que cuesta formar un Guardia Civil, por ejemplo, en que esté visionando cámaras en un cuarto de control, porque eso lo puede hacer perfectamente un vigilante de seguridad con infinitos menos costes; yo me gasto el dinero en un Tedax, un Geo, o la Policía Científica, por poner algunos ejemplos, pero no en eso. Criterios económicos, de funcionalidad y de optimización de recursos e inversiones

Con la ya señalada disminución de efectivos que acusa progresivamente la seguridad pública, por mucho que deseásemos que la película fuese otra, es la que es, y en muchos casos no se garantiza correctamente el derecho a la seguridad de los ciudadanos. Patrullas nocturnas turnándose vehículos en capitales de provincia, patrullas a pie porque no pueden realizarse los mantenimientos oportunos de los vehículos o llenarse de combustible, fotocopias por cortesía del ayuntamiento porque ya no tenemos para tóner o tiempos de respuesta aumentados porque los funcionarios que quedan son escasos, son algunas de las situaciones vividas en los últimos tiempos.

Realmente como ciudadanos estamos muy orgullosos de nuestras Fuerzas de Seguridad, las instituciones más valoradas siempre en todas las encuestas, y reputadísimas a nivel mundial, trabajando muchas veces con recursos, medios, sueldos y apoyos ínfimos obtienen resultados impresionantes. Nos encantaría tener más como ellos...pero no los tenemos, y es un problema a abordar. En esta misma situación el Estado se ha encontrado ya varias veces. Echando la vista atrás todos recordamos cómo se modificó la Ley cuando ETA extendió su amenaza a colectivos como periodistas o jueces y el Estado institucionalizó las escoltas privadas.

Cuando antes comentábamos los servicios en centros penitenciarios me venía a la cabeza el caso de los Aeropuertos: llegó un momento en que el tráfico aéreo se disparó y la Guardia Civil no tenía suficientes efectivos ni suficientemente formados, y AENA, como gestor de la mayoría de los aeropuertos le pidió una solución al Ministerio del Interior como competente para prestar la seguridad. Solución, la misma, firma en 1.999 de un Convenio para permitir los servicios de seguridad privada supervisados por la Guardia Civil. ¿En qué nivel estaba la seguridad privada en los aeropuertos con anterioridad a esa fecha y dónde se encuentra ahora?; no hay ni que explicarlo, porque nadie se cuestiona la capacidad y profesionalización de los vigilantes de seguridad en los aeropuertos.

Son sólo algunos ejemplos.

Más polémico aún es el apartado d) de ese artículo 41, pues posibilitaría que la seguridad privada realizase servicios como patrullaje en vías públicas o reforzar a las unidades antidisturbios en manifestaciones o similares. Sinceramente, aunque la Ley lo autorice, no creo que lo veamos a corte o medio plazo, porque ningún grupo político se atrevería a ello y, aunque se han hecho algunos servicios en este ámbito, como patrullas en pequeños municipios asimilables a policías locales, creo que aún nos queda mucho por andar y que, para algunos de esos servicios, la capacitación del personal de seguridad privada debería ser otra

Algunas voces dicen que la seguridad privada sólo beneficia a unos pocos y que no se debería entrar en lo público, pero, ¿dónde está la frontera de lo público?, ¿qué es?. Empresarialmente la seguridad privada como cualquier otra actividad económica está regulada y sometida a la ley, parte por la cual no hay nada de particular que alegar. Si una patrulla de seguridad privada que presta servicio en un polígono industrial detiene a una banda de butroneros, ¿cuál es la diferencia con que la detenga una patrulla de la seguridad pública?: ninguna, pero hay tres delincuentes menos en la calle. Si los vigilantes de seguridad del Santiago Bernabéu impiden un atentado terrorista, el beneficio para quién es, ¿para Florentino Pérez?¿Para el Real Madrid? O tal vez para los ciudadanos que se encontraban en el estadio y no lo han sufrido. El beneficio social de la seguridad privada está más que demostrado. No olvidemos que en numero de efectivos, son más que Cuerpo Nacional de Policía o que Guardia Civil, y me parece muy acertado que los ciudadanos podamos aprovecharnos directa o indirectamente de esos recursos

Como ciudadano, cuando voy a un hospital no me fijo en el rótulo de la entrada ni en el color de la bata del médico; deseo que me atiendan bien, rápido, no me corten la pierna equivocada y, si además le cuesta poco dinero al Estado mejor que mejor. Con la seguridad privada hemos de pensar lo mismo, pública o privada no son más que apellidos que contribuyen a garantizar ese derecho tan preciado por el ciudadano

Gregorio Duro
Tecnico en licitaciones y Proyectos

DIAGRAMA DE SECUENCIA DEL ADVERSARIO (DSA)

En el artículo de este mes, trataré el concepto teórico del Diagrama de Secuencia del Adversario (DSA), el cual se configura como una herramienta analítica esencial en los campos de la seguridad física y la ciberseguridad, cuyo propósito principal es modelar, de manera estructurada y detallada, las posibles vías que un adversario o atacante podría seguir para vulnerar un sistema de protección. Esta herramienta se utiliza para simular y representar las acciones secuenciales que un intruso llevaría a cabo con el objetivo de acceder a una instalación o vulnerar un sistema de seguridad.

En este contexto, el DSA no solo visualiza las etapas de la intrusión, sino que también considera las posibles contramedidas que se activarían en cada una de estas fases, permitiendo identificar los puntos vulnerables que pueden ser explotados por un atacante y evaluar la efectividad de las barreras de seguridad. El análisis mediante un DSA es, por lo tanto, una forma de anticipar cómo un adversario podría aprovechar las debilidades de un sistema de protección, lo cual es esencial para la toma de decisiones en la mejora de la infraestructura de seguridad y para el diseño de estrategias preventivas reforzadas. Uno de los aspectos más importantes del DSA es su capacidad para integrar y detallar diversos factores clave, como el tiempo de ejecución de cada acción del adversario, la probabilidad de detección de cada paso y las interacciones con los diversos sistemas de seguridad. Estos elementos son fundamentales para simular el comportamiento del adversario en situaciones de alta incertidumbre, en las cuales es difícil predecir con precisión el curso exacto de un ataque. El DSA toma en cuenta la respuesta humana ante eventos de intrusión, lo cual supone un factor determinante que puede influir tanto en la detención del ataque como en su éxito. Por ejemplo, la intervención de personal de seguridad o la activación de un protocolo de emergencia pueden alterar significativamente la evolución del ataque, lo que añade complejidad al análisis La variabilidad de los eventos que podrían modificar el resultado de cada intento de ataque, como el comportamiento del adversario ante una situación sobrevenida o error, es otra capa de incertidumbre que el DSA ayuda a modelar y gestionar.

El DSA no solo se limita a representar las acciones de un único adversario; una de sus características más importantes es su capacidad para simular diferentes escenarios de ataque, adaptándose a diversas condiciones y objetivos, lo que es esencial para anticipar múltiples estrategias de los atacantes. Esto permite a los analistas de seguridad y a los diseñadores de sistemas comprender de forma más profunda las diferentes tácticas que un intruso podría utilizar, evaluando qué contramedidas pueden ser más efectivas en cada caso específico.

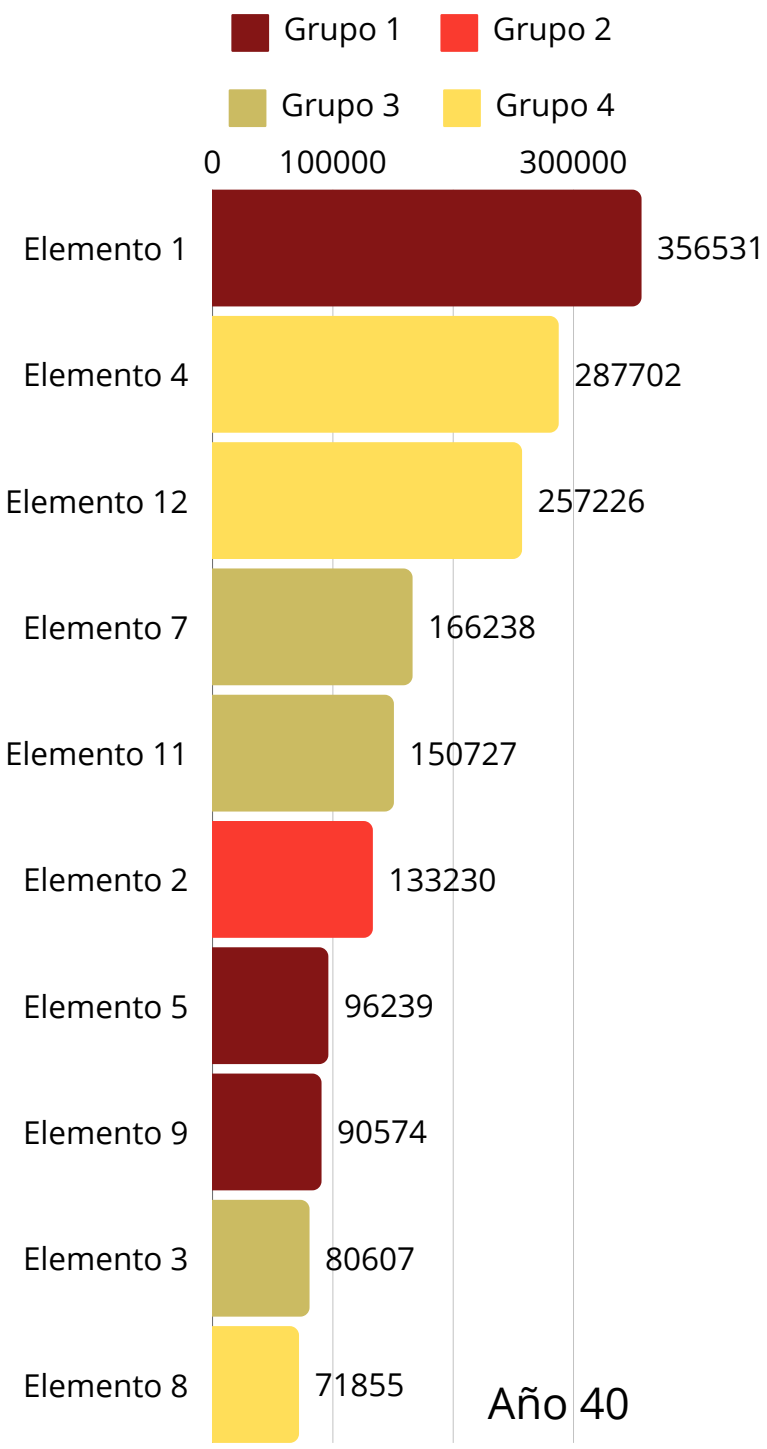
La simulación de varios escenarios de ataque proporciona una forma adecuada de probar la resiliencia del sistema ante situaciones imprevistas, y permite hacer ajustes proactivos a las políticas de seguridad en función de la evolución de las amenazas. Al proporcionar una aproximación al nivel de riesgo, el DSA ayuda a las organizaciones a optimizar los recursos destinados a la seguridad, permitiendo priorizar las mejoras en aquellas áreas donde el impacto potencial de un ataque podría ser mayor, y al mismo tiempo minimizando la probabilidad de éxito de una intrusión. Este enfoque basado en la simulación de ataques reales, con un alto grado de detalle, facilita la identificación de los puntos críticos en un sistema de protección y mejora la comprensión general de los factores humanos, tecnológicos y operacionales involucrados en la seguridad. Por ejemplo, un DSA puede revelar fallos en la coordinación entre diferentes sistemas de seguridad o identificar problemas en el entrenamiento y formación del personal de seguridad, factores que de otro modo podrían pasarse por alto en un análisis convencional.

En comparación con otros métodos de análisis de riesgos, como los análisis cualitativos o cuantitativos simples, el DSA ofrece una ventaja significativa al incorporar la incertidumbre y la variabilidad inherentes tanto en el comportamiento del adversario como en la respuesta del sistema. Los métodos tradicionales suelen centrarse en la probabilidad de que ocurra un evento, sin tener en cuenta los aspectos dinámicos y adaptativos de un ataque real, lo que puede hacer que la evaluación del riesgo sea menos precisa y confiable. El DSA permite un enfoque más dinámico y realista en la evaluación del nivel de riesgo, ya que tiene en cuenta múltiples variables interdependientes que afectan el curso de un ataque y la defensa. De esta forma, no solo proporciona un análisis más completo y detallado, sino que también permite identificar las brechas de seguridad que pueden ser aprovechadas por un atacante, ayudando a los departamentos de seguridad a mejorar sus defensas de manera más efectiva.

Otra de las grandes ventajas del DSA es su capacidad para ser utilizado como herramienta de capacitación y entrenamiento. Al proporcionar un marco visual y estructurado de las posibles secuencias de un ataque, los equipos de seguridad pueden practicar y mejorar sus protocolos de respuesta en un entorno controlado y predecible. La visualización de diferentes escenarios permite familiarizarse con las decisiones que deben tomar ante situaciones de emergencia y mejorar sus tiempos de reacción, lo que puede marcar la diferencia en la mitigación de un ataque real. Este tipo de simulaciones permite identificar de manera temprana déficits en la capacitación o en la preparación operativa, optimizando los procesos de formación y garantizando que los equipos de seguridad estén mejor equipados para hacer frente a cualquier amenaza.

El Diagrama de Secuencia del Adversario (DSA) no solo es una herramienta técnica para simular la secuencia de un ataque, sino que representa una estrategia integral de análisis de riesgo, planificación de defensa y capacitación. Al ofrecer una visión detallada de cómo un adversario podría vulnerar un sistema de protección, el DSA permite a los departamentos de seguridad anticipar y predecir amenazas de manera más precisa, identificar puntos débiles en sus estrategias de seguridad y mejorar sus respuestas ante incidentes. Esto no solo incrementa la efectividad de las medidas preventivas y de protección, sino que también optimiza los recursos y mejora la resiliencia general de las infraestructuras ante posibles ciberataques o intrusiones físicas. Con la creciente complejidad de las amenazas y la rapidez con la que evolucionan los métodos de ataque, herramientas como el DSA son esenciales para proporcionar una defensa proactiva y adaptativa, que esté a la altura de los desafíos actuales en seguridad. Para finalizar, agradecer a Metrorisk la difusión mensual de artículos de carácter técnico que puedan aportar una mejora y desarrollo en el conocimiento de nuestro sector

Gregorio Duro Navarro
Técnico de Licitaciones y Proyecto



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

LA RESILIENCIA URBANA, AMBIENTAL & CPTED

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

Mercedes Escudero

Actualmente, las ciudades se erigen como centros de innovación, cultura y progreso. Sin embargo, también se encuentran en la primera línea de una creciente serie de desafíos, desde desastres naturales, crisis económicas hasta pandemias y tensiones sociales. En este contexto, el concepto de resiliencia urbana emerge como un faro de esperanza, representando la capacidad de una ciudad para no solo sobrevivir a la adversidad, sino también para aprender, adaptarse y prosperar.

CPTED ha evolucionado a lo largo del tiempo, adaptándose a los cambios sociales, climáticos y comprendiendo la complejidad de la seguridad en las ciudades.

- Primera Generación: se centraba en el diseño físico del entorno para disuadir la comisión de delitos. Principios como la vigilancia natural, el control de accesos, la territorialidad y el mantenimiento eran fundamentales.
- Segunda Generación: amplió el enfoque al reconocer la importancia de los factores sociales y la participación ciudadana. Se buscaba fortalecer el sentido de comunidad y la cohesión social como elementos clave para la prevención del delito.
- Tercera Generación: integra los principios de las generaciones anteriores y añade un enfoque en la sostenibilidad, la salud pública y el bienestar comunitario. Se busca crear entornos que promuevan la calidad de vida y el desarrollo integral de las personas.

Definiendo la Resiliencia Urbana: Más Allá de la Supervivencia La resiliencia urbana se define como la capacidad de una ciudad para prevenir, resistir, absorber, adaptarse y recuperarse de una amplia gama de impactos y tensiones. Estos pueden ser de naturaleza:

- Física: terremotos, inundaciones, incendios, olas de calor extremo.
- Económica: crisis financieras, recesión, desempleo masivo.
- Social: disturbios civiles, conflictos, migración masiva.
- Ambiental: contaminación, escasez de agua, cambio climático.

Una ciudad resiliente no solo sobrevive a estos desafíos, sino que también aprende y se fortalece a partir de ellos, emergiendo con una mayor capacidad de adaptación y preparación para el futuro.

Sus pilares son multifacéticos y están interconectados para reforzar:

- 1. Infraestructura Robusta: las ciudades resilientes invierten en infraestructuras críticas que sean capaces de resistir y recuperarse rápidamente de los impactos. Esto incluye sistemas de transporte, energía, agua, comunicaciones y edificios.
- 2. Economía Diversificada: una economía local diversificada, con múltiples sectores y fuentes de empleo, es menos vulnerable a las crisis económicas. Fomentar la innovación y el emprendimiento también contribuye a la resiliencia económica.
- 3. Cohesión Social: una comunidad unida y organizada, con fuertes lazos sociales y participación ciudadana, es más capaz de enfrentar los desafíos y recuperarse de los impactos.
- 4. Planificación y Gobernanza: las ciudades resilientes cuentan con planes de contingencia y estrategias de adaptación para diferentes tipos de impactos. Una gobernanza transparente y participativa es fundamental para la implementación exitosa de dichos planes.
- 5. Medio Ambiente Sostenible: la protección de los ecosistemas urbanos, la gestión sostenible de los recursos naturales y la adaptación al cambio climático son esenciales para la resiliencia a largo plazo.

Ante este panorama, la Metodología de Prevención del Delito a Través del Diseño Ambiental (CPTED), la Resiliencia Urbana y Resiliencia Ambiental son conceptos interrelacionados que buscan crear ciudades más seguras, sostenibles y capaces de enfrentar los desafíos futuros. La norma ISO 22341:2021 proporciona un marco de referencia valioso para integrar estos conceptos, ofreciendo directrices para la implementación de estrategias de CPTED que contribuyan a la resiliencia urbana y ambiental.

CPTED de Tercera Generación: La tercera generación de CPTED representa un cambio de paradigma en la forma de entender y abordar la seguridad urbana. Al integrar los principios de las generaciones anteriores y añadir un enfoque en la sostenibilidad, la salud pública y el bienestar comunitario, con lo cual se puede lograr un impacto positivo en la calidad de vida de las personas y construir ciudades más seguras, justas y sostenibles para todos.

Gregory Saville y Mateja Mihinjac en su artículo Third-Generation Crime Prevention Through Environmental Design (CPTED) nos invitan a repensar la seguridad desde una perspectiva más amplia, donde el diseño urbano se convierte en una herramienta poderosa para construir comunidades más resilientes y promover el desarrollo integral de las personas.

CPTED, en su tercera generación, y la resiliencia urbana comparten objetivos comunes, como la creación de entornos más seguros, saludables y sostenibles. Al aplicar sus principios se pueden fortalecer los pilares de la resiliencia urbana, tales como:

- Infraestructura Robusta: el diseño de espacios públicos seguros y bien iluminados, así como la implementación de sistemas de control de acceso, contribuyen a la seguridad de la infraestructura urbana.
- Cohesión Social: CPTED promueve la creación de espacios públicos que fomenten la interacción social, la participación ciudadana y el sentido de comunidad, fortaleciendo la cohesión social.
- Medio Ambiente Sostenible: CPTED de tercera generación incorpora criterios de sostenibilidad en el diseño urbano, como el uso de energías renovables, la gestión eficiente de los recursos naturales y la protección de los ecosistemas urbanos, contribuyendo a la resiliencia ambiental.

Al aplicar los principios de CPTED, se pueden fortalecer los pilares de la resiliencia ambiental, tales como:

- Reducción de la Vulnerabilidad a Desastres: el diseño de espacios públicos seguros y bien iluminados, así como la implementación de sistemas de alerta temprana y evacuación, pueden reducir la vulnerabilidad de las comunidades ante desastres naturales.
- Uso Eficiente de los Recursos: CPTED de tercera generación promueve el uso de materiales de construcción sostenibles, la implementación de sistemas de recolección de agua de lluvia y la creación de espacios verdes que contribuyan a la eficiencia energética y la gestión sostenible de los recursos.
- Protección de la Biodiversidad: el diseño de espacios públicos que fomenten la biodiversidad, como parques y jardines, puede mejorar la calidad del aire, reducir el efecto isla de calor y promover la salud de los ecosistemas urbanos.
- Adaptación al Cambio Climático: CPTED puede contribuir a la adaptación al cambio climático mediante el diseño de infraestructuras resilientes a eventos climáticos extremos, como inundaciones y olas de calor.

La ISO 22341: Un Marco para la Integración La norma ISO 22341:2021, "Seguridad y resiliencia - Seguridad protectora - Directrices para la prevención del delito a través del diseño ambiental", proporciona un marco de referencia valioso para integrar los principios de CPTED en la construcción de ciudades más resilientes. La norma aborda los principios, elementos, estrategias y procesos para reducir el delito, incluyendo ciertos tipos de ataques terroristas, a través del diseño ambiental.

Asimismo, destaca la importancia de considerar el contexto ambiental de los factores de riesgo de la delincuencia y la seguridad sociourbana, las causas de las vulnerabilidades y los niveles de riesgo. La ISO 22341 enfatiza la necesidad de involucrar a todas las partes interesadas en el proceso de diseño e implementación de estrategias de CPTED, incluyendo a los residentes, las autoridades, los planificadores urbanos y los profesionales de la seguridad.

La integración de CPTED, la resiliencia urbana y la resiliencia ambiental, guiada por la ISO 22341, representa un enfoque prometedor para la construcción de ciudades más seguras, sostenibles y capaces de enfrentar los desafíos del futuro. Al adoptar un enfoque holístico que considere los factores físicos, sociales, económicos y ambientales, se pueden crear entornos urbanos que promuevan la calidad de vida, el bienestar y la seguridad de todos los habitantes.

MÁS DE 30 AÑOS DEDICADOS A LA SEGURIDAD PRIVADA

Metro Risk

Antonio Cozano Fernández
CEO Cofer Seguridad.

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

D. Antonio Cozano Fernández

Treinta años pueden parecer un suspiro cuando se miran con la perspectiva de quien ha dedicado su vida a construir, aprender y evolucionar. Sin embargo, en el mundo de la seguridad, donde la responsabilidad y el compromiso son el eje central de cada decisión, tres décadas representan mucho más que una cifra: simbolizan constancia, visión y una pasión inquebrantable.

Iniciar un camino en el mundo empresarial nunca es fácil. Requiere coraje, determinación y, sobre todo, la capacidad de adaptarse a los cambios. La seguridad, como sector, ha evolucionado enormemente en los últimos años, desafiando a quienes la integran a reinventarse constantemente. Pero hay algo que permanece inalterable: el propósito. Proteger, anticiparse y crear soluciones que salvaguarden a personas y bienes es más que un trabajo; es una vocación.

A lo largo de estos más de 30 años, la ilusión intuyo que fue el motor que ha impulsado cada decisión. No ha sido solo cuestión de experiencia o conocimiento, sino de esa chispa que permite visualizar oportunidades donde otros ven obstáculos. Pero la ilusión, por sí sola, no es suficiente. Es la disciplina la que ha marcado la diferencia: la constancia en el esfuerzo diario, el aprendizaje continuo, la resiliencia ante los momentos difíciles y la voluntad de seguir adelante cuando las circunstancias parecían adversas.

Y sí, siempre se dice que la suerte juega un papel en la vida. Quizás haya tenido su parte en este recorrido, pero la realidad es que la suerte suele encontrarse con quienes están preparados para recibirla. La perseverancia, la visión y la capacidad de no rendirse son los verdaderos imanes que atraen esas oportunidades que parecen casuales, pero que en el fondo son el resultado del esfuerzo y la preparación.

Hoy, después de más de tres décadas en este apasionante camino, es momento de celebrar no solo los logros, sino también los retos superados, las personas que han formado parte de esta historia y el legado construido con dedicación.

Homenaje de esta EDITORIAL para Antonio Cozano.

Porque los sueños sí se cumplen, pero solo cuando se persiguen con determinación, pasión y ese toque de fortuna que recompensa a quienes nunca dejaron de creer.

EL 75% DE LOS RIESGOS DE TU EMPRESA VIENEN DE LA GESTIÓN DE TERCEROS.

Metro Risk

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

El dato:
3 de cada 4 empresas han ignorado este dato hasta que fue demasiado tarde.

Si un proveedor falla, el problema es suyo... hasta que deja de serlo.

👉 Si no controlas los #riesgos en tu #cadenadesuministro, no controlas tu #negocio.

¿Qué está en juego?

🔹 DORA y cambio de reglas:

La gestión de terceros no es solo una buena práctica, es requisito regulatorio en la UE para el sector financiero y tecnológico.

🔹 ISO 27001:

Refuerza el control sobre proveedores: No basta con cumplir internamente, ahora la seguridad debe extenderse a toda la cadena de valor.

El impacto real de no gestionar bien a terceros:
según los datos de incidentes de ciberseguridad,
el 70% de los ataques recientes explotaron
debilidades en proveedores
o socios tecnológicos.

Dónde están los mayores riesgos?

El DORA Assessment deja clara la dirección que deben tomar las empresas:

✅ Evaluar y monitorear proveedores de tecnología en tiempo real.
✅ Incluir controles de ciberseguridad y compliance en los contratos.
✅ Tener planes de respuesta ante fallos de terceros.
✅ Asegurar que cada proveedor cumpla con ISO 27001 y otros marcos internacionales.

No se trata de si habrá un problema, sino de cuándo.
Y cuando ocurra, no podrás decir que no lo viste venir.

¿Cómo responder a esto?

Empieza por la foto real de tu empresa.
¿Tienes identificados los riesgos de tus proveedores críticos?
Auditoría y seguimiento continuo.

DORA exige pruebas de resiliencia operativa, no palabras.

No basta con "tener un plan", hay que aplicarlo.
De nada sirve una ISO 27001 si no se ejecutan sus controles.

La imagen de este post lo dice todo:
la mayoría de las empresas siguen ciegas ante su mayor vulnerabilidad.

DORA no deja margen a la improvisación.
Si no tienes una estrategia real, es momento de replantearlo.

Hablemos claro:

¿En tu empresa ya hay un plan real de gestión de terceros?
¿Tienes identificados los riesgos que podrían impactar en tu operación?

Si la respuesta es sí, coméntalo y compartamos mejores prácticas.
Si la respuesta es no, es momento de actuar antes de que sea demasiado tarde.

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 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

CIBERSEGURIDAD: UN JUEGO DE ESTRATEGIAS EN EL MUNDO DIGITAL

Metro Risk

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

Hace poco estaba leyendo información en Twitter (o mejor dicho, ahora conocida como X) y me llegó un anuncio de unas clases que ofrecían sobre la teoría de los juegos. Me llamó la atención y decidí indagar un poco más sobre esto. Resulta que la teoría de los juegos es un área de las matemáticas que utiliza modelos para estudiar interacciones en estructuras formalizadas de incentivos y llevar a cabo procesos de decisión.

Es decir, en un juego, varios jugadores toman decisiones que afectan los resultados de todos los participantes. La teoría de juegos analiza las estrategias óptimas que los jugadores pueden tomar para maximizar sus ganancias o minimizar sus pérdidas, teniendo en cuenta las acciones de los demás.

Esto me hizo recordar el libro Padre Rico, Padre Pobre, donde el autor Robert Kiyosaki recomienda el juego de mesa Cashflow como una metáfora para explicar cómo los ricos adquieren riqueza. En este juego, los jugadores ganan comprando propiedades, cobrando alquileres e invirtiendo en mejoras.

Tomando en consideración todo esto, considero que la ciberseguridad es precisamente un juego estratégico entre los atacantes y los defensores, o mejor dicho, los hackers y las empresas, organizaciones y usuarios. Es decir, ellos contra nosotros. Pero, ¿cómo puede la teoría de los juegos ayudar a comprender y mejorar la ciberseguridad? Tanto los atacantes como los defensores actúan como jugadores que buscan maximizar sus beneficios o mitigar, tal vez minimizar, sus pérdidas. Día a día nos encontramos con distintas maneras en las cuales los ciberdelincuentes logran estafar a empresas o personas.

Estas estrategias pueden incluir ataques de denegación de servicio, phishing o sencillamente el uso de malware para obtener su recompensa, tal como el robo de datos, la interrupción de servicios y el botín final: los costos de recuperación. Mientras tanto, las personas que nos dedicamos a defender a los usuarios y las organizaciones utilizamos firewalls, sistemas de detección de intrusiones, contraseñas robustas, entre otros métodos.

Podría citar varios métodos para que las personas que capacitan tomen en consideración:

- Juegos cooperativos: Explorar cómo las empresas pueden colaborar para compartir información sobre amenazas y mejorar sus defensas en conjunto.
- Juegos no cooperativos: Analizar cómo los atacantes y defensores interactúan en un entorno competitivo, donde cada uno busca su propio beneficio.
- Juegos de suma cero: Describir cómo en algunos casos (como el robo de información), la ganancia de un jugador (el atacante) implica una pérdida equivalente para el otro jugador (la víctima).

Pero más allá de esta dinámica, la verdadera razón de enseñar mediante estos juegos es conocer conceptos clave para incluir la teoría de los juegos en la ciberseguridad:

- El dilema del prisionero: Este concepto puede ilustrar la dificultad de la cooperación en ciberseguridad. Describe una situación donde dos o más personas pueden obtener beneficios individuales al cooperar, pero la falta de confianza puede llevar a resultados peores para todos.
- La estrategia dominante: Describe cómo los jugadores pueden identificar estrategias que siempre les darán el mejor resultado, independientemente de lo que haga el otro jugador.
- El equilibrio de Nash: Este puede ayudar a identificar situaciones en las que ningún jugador tiene incentivos para cambiar su estrategia, dado lo que están haciendo los demás. En otras palabras, nadie ganará nada si decide cambiar su estrategia bajo el supuesto de que los demás individuos no cambian la suya.

Estos conceptos son interesantes y vitales para comprender el comportamiento de los mercados de ciberseguridad, donde se compran y venden herramientas y servicios de protección. De esta manera, se podrán abordar los desafíos de la ciberseguridad de una manera más dinámica y actualizada.

¿SEGURIDAD O FIABILIDAD?

Metro Risk

Rosa Fernandéz

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

ASUNTO: NIVEL DE SEGURIDAD

¿Cuándo hablamos de seguridad siempre pensamos en tres elementos básicos: tecnológico, humano y organizativo. Combinar estos elementos resulta esencial para conseguir un sistema de seguridad sólido y fiable, capaz de proteger la información y salvaguardar la continuidad de la actividad o del negocio.

Pero también sabemos -como la realidad y la casuística nos han demostrado en más de una ocasión que la cadena siempre se rompe por el eslabón más débil.

Por ejemplo, hay quien compra un arma para protegerse, pero no aprende a utilizarla. En lugar de potenciar su seguridad, esa decisión aumenta el riesgo de sufrir un accidente. Del mismo modo, la adopción de aplicaciones de IA sin la formación adecuada puede dejar a empresas y profesionales expuestos a vulnerabilidades no previstas.

El dilema de la alta seguridad sin fiabilidad
Pensemos en las cerraduras digitales que se activan únicamente con el teléfono móvil. A primera vista, ofrecen comodidad y un alto grado de seguridad. Sin embargo, ¿qué ocurre cuando la aplicación falla, se pierde el teléfono o surge un imprevisto que impide el acceso a la aplicación? En esos casos, la "solución" se convierte en problema. La seguridad vale y es eficaz, pero solo si va acompañada de mecanismos de fiabilidad: un doble factor de autenticación, una llave física de emergencia o un protocolo de recuperación de accesos. Comprar la "herramienta más avanzada" (ya sea un software de encriptación, una cerradura inteligente o un sistema de IA) no garantiza la protección si no se dispone de los procedimientos y la formación necesaria para usarla correctamente.

El factor humano: ¿formado o punto débil? En materia de protección de datos y uso de inteligencia artificial, la normativa —como el RGPD en Europa— exige no solo instalar medidas de seguridad tecnológicas, sino también formar y concienciar a quienes intervienen en el tratamiento de la información (empleados, proveedores, colaboradores, etc.).

Personal sin formación: Es un cable suelto y una vulnerabilidad para tu empresa. Porque si un miembro de tu equipo carece de conocimientos básicos en protección de datos, puede cometer errores elementales (enviar información sensible a un destinatario equivocado, almacenar contraseñas en lugares inseguros o hacer clic en enlaces maliciosos). Malas prácticas que comprometen a tu negocio.

Personal con formación adecuada: Son un pilar solido porque entienden la importancia de cumplir procedimientos, protegen el acceso físico y digital de los datos, utilizan contraseñas robustas o sistemas de autenticación y, sobre todo, participan activamente en la cultura de seguridad. Trabajan en modo dato, protegiendo tu empresa y tu negocio desde su puesto de trabajo.

Sin formación no hay transformación.

Claves para lograr seguridad con fiabilidad: tu combinación ganadora

- 1.Formación continua Formar a todo el personal en aspectos fundamentales de protección de datos, ciberseguridad e inteligencia artificial. Mantén una vigilancia que te permita estar preparado ante nuevas amenazas y cambios normativos.
- 2.Plan B Disponer de planes de contingencia para responder rápidamente ante un fallo de la aplicación o pérdida de credenciales.
- 3.Evaluación y mejora constante Realizar auditorías para identificar vulnerabilidades. Incorporar protocolos de revisión y mejora tras cada incidente o anomalía detectada.
- 4.Tecnología complementada con supervisión humana Contar con sistemas de IA y protección de datos que actúen como primera línea de defensa. Garantizar la supervisión por parte de profesionales que sepan detectar irregularidades, interpretar resultados y tomar decisiones informadas.
- 5.Cumplir con la normativa Adoptar las obligaciones del RGPD y demás regulaciones (RIA, LOPDGDD, LSICE), de modo que la organización respalde el derecho a la privacidad y gestione los datos de forma responsable.

Para que la seguridad sea lo menos falible posible, necesitamos un enfoque integral que ponga la formación como un pilar básico sobre el que podrás trabajar con la tecnología que necesites.

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

SEGURIDAD PRIVADA EN ESPAÑA: UN PILAR FUNDAMENTAL PARA LA PROTECCIÓN CIUDADANA

Metro Risk

Carlos Serrano
Director de Contenidos de Seguridad y Empleo

La seguridad privada en España juega un papel clave en la protección de bienes, personas e infraestructuras críticas. Aunque muchas veces pasa desapercibida, es un sector en constante evolución que complementa el trabajo de las fuerzas y cuerpos de seguridad del Estado. Desde vigilantes de seguridad en centros comerciales hasta escoltas y expertos en ciberseguridad, la seguridad privada es un pilar fundamental en la tranquilidad de la sociedad.

Un Sector en Crecimiento y Regulación Estricta

La seguridad privada en España está regulada por la Ley 5/2014, de 4 de abril, de Seguridad Privada , que establece los requisitos y competencias de los profesionales del sector. Esta normativa busca garantizar que las empresas y los trabajadores de seguridad cumplan con estándares de profesionalidad y respeto a los derechos de los ciudadanos. Actualmente, hay más de 1.500 empresas de seguridad privada en el país, empleando a más de 80.000 profesionales , lo que convierte a España en uno de los países europeos con mayor presencia en este sector.

www.seguridadyempleo.com

Principales Ámbitos de Actuación

Los profesionales de la seguridad privada desempeñan múltiples funciones, entre las que destacan:

- Vigilancia y protección : En centros comerciales, aeropuertos, hospitales y eventos masivos.
- Transporte de fondos y valores : Seguridad en el traslado de dinero y objetos valiosos.
- Escoltas privadas : Protección de personas con riesgo elevado, como empresarios o figuras públicas.
- Ciberseguridad : Prevención y gestión de ataques informáticos en empresas e instituciones.

Desafíos y Futuro del Sector

A pesar de su importancia, la seguridad privada enfrenta varios desafíos:

1. Intrusismo laboral : El ejercicio ilegal de actividades de seguridad sin la formación ni acreditación necesarias.
2. Condiciones laborales : En algunos casos, los profesionales denuncian bajos salarios y largas jornadas.
3. Adaptación a nuevas amenazas : El auge de la ciberseguridad y el uso de tecnologías como la inteligencia artificial requiere

EL PERITAJE DESDE LA SEGURIDAD PRIVADA

Metro Risk

Abraham Santana Herrera
Director de seguridad. Perito

Hoy en día, existe la figura del Perito Judicial en Seguridad Privada, a pesar de que no es una especialidad dentro de la Ley ni el Reglamento de seguridad privada, y aún menos en el convenio colectivo de nuestro sector. Pero no cabe duda que es una figura, interesante no solo para los Juzgados españoles, sin incluso para las compañías aseguradoras, y en este último quiero centrar la figura del profesional de seguridad privada. Debemos de recordar, que cuando surge legalmente la figura del director de seguridad, había que darle forma a su formación, teniendo en cuenta que la máxima de su labor, es la prevención, anulación o minimización de cualquier riesgo, que ponga en peligro la vida humana, el patrimonio o la imagen de la corporación a la que represente. Es por ello, que la base de la formación de un director de seguridad, haya nacido de las premisas de las compañías de seguro, donde vale más la pena prevenir que curar. De hecho, muchos directores de seguridad utilizan análisis de riesgos, desarrolladas por compañías aseguradoras, para clasificar y cuantificar los diversos riesgos.

Las compañías aseguradoras, cuentan en su mayoría con gabinetes de peritos subcontratados, para analizar y evaluar dentro de las garantías de las pólizas que ofrecen a sus clientes, los diferentes siniestros que afectan a los usuarios de seguros. Estos gabinetes de peritajes, evidentemente cuentan con grandes profesionales, de diferentes sectores, que en su mayoría son especialistas en edificación, en especial, arquitectos técnicos o ingenieros, o incluso, profesionales que pueden acreditar un alto conocimiento en su materia. He ahí donde entra los profesionales de la seguridad privada, y en especial todo aquél que cuente con la habilitación de director de seguridad. Debemos de partir, que el director de seguridad, intrínsicamente es un perito en seguridad privada, más allá, si está registrado o no en un Juzgado, ya que, un director de seguridad puede ejercer como perito privado para una compañía de seguros. Otra cosa, es que un Juzgado, te asigne un caso para dar luz a un proceso judicial, donde sí debes estar debidamente registrado.

Desde mi experiencia, el director de seguridad tiene los conocimientos específicos en la materia de seguridad privada, sobre el perito de IRD. La línea principal de investigación dentro de los siniestros en las compañías de seguros, es la determinar la viabilidad de un hurto o robo, y el porqué fallaron los sistemas electrónicos de detección de intrusión. El análisis de la composición del entorno siniestrado, y de los objetos sustraídos. Para ello, el director de seguridad necesita un amplio conocimiento de toda la legislación en seguridad privada.

Recientemente, hablando con un amigo, que trabaja en las Fuerzas y Cuerpos de seguridad del Estado, me preguntó si ese tipo de investigación no entra en conflicto con la investigación pública.

Como le comenté en su momento, el perito en seguridad privada, no investiga para dar con lo Causantes del siniestro, sino lo que hace es verificar la veracidad de los hechos y detectar las posibles fallas de seguridad. Si las medidas tomadas, eran las adecuadas para aquello que se pretendía proteger, y si la hubiese, por qué no funcionaron.

Así mismo, debemos de recordar que el director de seguridad no es un detective, ni tiene cualificación ni preparación como tal, a no ser que independientemente de la TIP, haya realizado el curso y también posea la TIP de detective privado, con lo cual no deja de ser un extra que lo cualifica doblemente. Por lo tanto, el director de seguridad, tiene más campos en los que es posible poner de manifiesto que tiene una utilidad en diversos campos

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

MAS ALLÁ DEL ALGORITMO: LA INTUICIÓN HUMANA EN EL TABLERO DE LA ÉTICA CON LA IA

Metro Risk

Elena de la Parte

La IA la inteligencia artificial está transformando a pasos agigantados el panorama profesional, automatizando tareas repetitivas y optimizando los procesos. No obstante, es crucial comprender sus limitaciones y valorar las habilidades humanas, que siguen siendo esenciales.

La Inteligencia artificial (IA), se ha integrado en múltiples aspectos de nuestra vida, incluyendo el ámbito profesional. ¿Ese software que te ayuda a generar informes mensuales? Probablemente utiliza la IA y el Big data para analizar y monitorizar grandes cantidades de datos. ¿Las plataformas que surgieren candidatos para un puesto de trabajo? Se basan en algoritmos de IA y aprendizaje automático para filtrar perfiles. Incluso es posible que uses herramientas con IA generativa para redactar correos electrónicos profesionales o presentaciones.

Y en base a esto reflexionemos un poquitín… ¿Dónde establecemos el límite? Si la IA puede ejecutar tareas monótonas y repetitivas, e incluso generar contenido a una velocidad que supera con creces las capacidades humanas, ¿Cuál es entonces nuestro rol? ¿Es realmente indispensable la "perspectiva humana" para el éxito de una organización? Pensemos en el ajedrez.

La IA puede calcular millones de movimientos por segundo, evaluando combinaciones con una precisión asombrosa. Podría decirse que es invencible en el cálculo bruto. Sin embargo, ¿quién concibe la estrategia general de la partida, la visión a largo plazo que sacrifica una pieza menor para obtener una ventaja posicional decisiva? ¿Quién interpreta el lenguaje corporal del oponente, detectando una vacilación o una señal de confianza que escapa al análisis puramente numérico?

Ahí reside la intuición humana, la comprensión del contexto y la capacidad de adaptación estratégica que aún diferencian a un gran mentor y maestro de una máquina. Profundicemos entonces en los beneficios, desafíos y riesgos de elegir al mejor contendiente (¿o deberíamos decir "jugador"?) para el tablero: ¿un autómata o un humano?

Sin embargo, un análisis más profundo introduce ambigüedades en el panorama generando contradicciones. Si bien es cierto que los sistemas de IA pueden reducir los errores derivados de la fatiga y la falta de concentración, no son inmunes a equivocaciones. La IA también comete errores y “alucinar”, es decir presenta información falsa con total convicción, especialmente si existen deficiencias en los datos con los que fue entrenada o /y / el propio algoritmo.

Es decir, la eficacia de los sistemas de IA depende directamente de la calidad de datos con los que se les entrena, lo cual exige experiencia y supervisión humana.

Siguiendo con la analogía del ajedrez, imaginemos un IA diseñada para jugar al más alto nivel de “Experto”. Se alimenta con millones de partidas históricas, analizando cada movimiento, cada estrategia. En teoría debería ser imbatible. Sin embargo, si en ese conjunto de datos se incluyen partidas con errores estratégicos sistemáticos, o incluso partidas fraudulentas, la IA podría aprender y replicar esos errores, creyendo que son válidos. Podría, por ejemplo, "aprender" que sacrificar la reina en el tercer movimiento es una estrategia brillante, basándose en una serie de partidas amañadas donde ese movimiento condujo a la victoria (debido a la trampa, no a una estrategia legítima).

En este caso, la IA estaría "alucinando", presentando una falsedad como una verdad, debido a la deficiente calidad de los datos de entrenamiento. De igual manera, un error en la programación del algoritmo, como una mala ponderación de ciertos valores posicionales, podría llevar a la IA a sobrevalorar la ganancia material por encima de la seguridad del rey, cometiendo errores tácticos graves. Por lo tanto, incluso en un juego tan lógico como el ajedrez, la supervisión humana y la curación de los datos son cruciales para evitar que la IA aprenda y perpetúe errores.

La IA puede amplificar los sesgos presentes en los datos. Para ilustrar esto con el ajedrez, imaginemos una IA entrenada solo con partidas ganadas por el jugador de las fichas blancas. Está podría sobrevalorar las aperturas y subestimar las de las piezas negras, generando un sesgo en su juego.

Si bien la IA busca objetividad, los datos con, los que se entrena pueden introducir a la subjetividad. Un jugador humano (“persona”), puede preferir un estilo de juego “gambito” o un juego de ataque directo al Rey. Mientras que la IA entrenada con datos diversos debería ser neutral en su estrategia

MetroRisk
EDITORIAL AND MAGAZINE

Por lo tanto, garantizar la equidad y la objetividad en los sistemas de IA, incluso en un dominio tan aparentemente objetivo como el ajedrez, requiere un esfuerzo constante en la curación de datos, el diseño de algoritmos y el monitoreo continuo. No basta con alimentar a la IA con "muchos datos"; es esencial asegurar que esos datos sean representativos, equilibrados y libres de sesgos para que la IA pueda alcanzar su máximo potencial como herramienta objetiva.

Es premisa fundamental, garantizar la equidad y la objetividad en los sistemas de IA requiere un esfuerzo continuo en la curación de datos, el diseño de algoritmos y el monitoreo continuo. Garantizar la equidad y la objetividad en los sistemas de IA requiere un esfuerzo continuo en la curación de datos, el diseño de algoritmos y el monitoreo continuo.

Dado que la IA se basa en el procesamiento de volúmenes masivos de datos, surge una preocupación fundamental en materia de privacidad y cumplimiento normativo. La ingesta y el tratamiento de datos sensibles, especialmente aquellos que contienen Información Personal Identificable (PII), incrementan la superficie de ataque y exigen un riguroso cumplimiento del Reglamento General de Protección de Datos (RGPD) y otras normativas análogas. Actores maliciosos, aprovechando vulnerabilidades en la infraestructura o deficiencias en los controles de acceso, podrían explotar estas extensas bases de datos para realizar exfiltraciones de información, comprometiendo la confidencialidad, integridad y disponibilidad de los datos.

Si bien existen técnicas como el cifrado de datos en reposo y en tránsito, la anonimizarían, la seudonimización y el uso de entornos de ejecución confiables (TEE) para mitigar estos riesgos, las organizaciones deben implementar un robusto marco de ciberseguridad que abarque:

Evaluaciones de Riesgos de Privacidad (PIA): Para identificar y mitigar los riesgos específicos asociados al tratamiento de datos personales por sistemas de IA.

Controles de Acceso Basados en Roles (RBAC) y el principio de mínimo privilegio: Para restringir el acceso a los datos solo a personal autorizado y con la necesidad legítima de procesarlos.

Monitoreo continuo de la actividad y detección de anomalías: Para identificar y responder a posibles incidentes de seguridad en tiempo real.

Pruebas de penetración (Pentesting) y análisis de vulnerabilidades: Para identificar y corregir debilidades en los sistemas antes de que sean explotadas.

Implementación de un Security Information and Event Management (SIEM): Para la correlación de logs y la detección temprana de incidentes.

Formación continua en concienciación en ciberseguridad y privacidad: Para el personal que interactúa con los sistemas de IA.

"Además de la formación es premisa fundamental la concienciación de los trabajadores, ya que, si existe formación actualizada, pero si esta NO se lleva a cabo, carece de sentido"

Cumplimiento con marcos de trabajo como NIST Cybersecurity Framework o ISO 27001: Para asegurar la adopción de buenas prácticas en seguridad de la información.

En definitiva, la adopción de IA exige una postura proactiva en ciberseguridad y cumplimiento normativo. La gestión diligente de los datos y la implementación de controles robustos son cruciales para prevenir brechas de seguridad, proteger la privacidad de los individuos y evitar sanciones regulatorias. La superficie de ataque se expande con la IA, y las organizaciones deben fortalecer sus defensas en consecuencia.

LA REVOLUCIÓN DE LOS DRONES CON IA EN LA SEGURIDAD

Metro Risk

Carlos Miguel Ortiz
Delegado Regional
Comunidad Autónoma de Madrid
Piloto remoto UAS certificado EASA
Instructor-examinador UAS certificado RITRAC

Ritrac International UAS professional services worldwide RUPSW

Correo electrónico:	cmiguel@ritrac.eu
Móvil/Whatsapp:	+34 685040875
Sitio web:	https://ritrac.eu
Plataforma formación:	https://remotepilot.online
Reuniones telemáticas:	http://webex.ritrac.eu

La seguridad es un reto en constante cambio, y la tecnología ha jugado un papel clave en su evolución. Entre las innovaciones más prometedoras, los drones equipados con inteligencia artificial (IA) están marcando un antes y un después en la vigilancia, la prevención y la respuesta ante amenazas. Su capacidad para operar de manera autónoma y analizar grandes volúmenes de datos en tiempo real los convierte en aliados fundamentales para mejorar la eficiencia en la seguridad pública y privada

Drones Inteligentes: Más Allá de la Vigilancia Tradicional El uso de drones en seguridad ya es una realidad, con aplicaciones que van desde la supervisión de espacios sensibles hasta el apoyo en emergencias. Sin embargo, cuando se combina con IA, su potencial se dispara. Los drones pueden operar de manera autónoma, analizar datos en tiempo real e incluso detectar comportamientos sospechosos antes de que representen un peligro. Gracias a los avances en inteligencia artificial, estas aeronaves pueden reconocer rostros, identificar objetos peligrosos e interpretar situaciones de riesgo con gran precisión. Esto no solo alivia la carga de los operadores humanos, sino que permite una respuesta más rápida y eficaz en caso de necesidad. Además, pueden operar en condiciones extremas, como en incendios, tormentas o zonas de difícil acceso, donde la presencia humana resultaría peligrosa o inviable. Otra de sus ventajas es la capacidad de realizar patrullajes preventivos sin descanso, lo que reduce los costos de seguridad y aumenta la cobertura de vigilancia en comparación con los métodos tradicionales. Su integración con otros sistemas de seguridad, como cámaras de vigilancia fijas y centros de control, optimiza la toma de decisiones en situaciones de emergencia.

Aplicaciones en Diferentes Ámbitos

- 1.Vigilancia en Espacios Públicos: Durante eventos multitudinarios, los drones con IA pueden monitorear la situación, identificar posibles altercados y ayudar a las autoridades a intervenir de manera oportuna y efectiva. Su capacidad para transmitir imágenes en vivo permite una supervisión detallada de los eventos, minimizando riesgos y facilitando una rápida actuación.
- 2.Prevención y Control de Incendios: Mediante sensores térmicos y algoritmos avanzados, estos dispositivos pueden detectar focos de incendio antes de que se propaguen, permitiendo actuar con rapidez y minimizar daños. Además, pueden mapear áreas afectadas, facilitando la coordinación de los equipos de emergencia y reduciendo el tiempo de respuesta.
- 3.Protección de Infraestructuras Críticas: Instalaciones estratégicas, como plantas energéticas, aeropuertos y centros de datos, pueden contar con drones patrullando sus perímetros, detectando intrusiones y alertando sobre cualquier anomalía. Su capacidad de respuesta inmediata ante intentos de sabotaje o actos vandálicos refuerza la seguridad sin necesidad de exponer al personal de vigilancia.
- 4.Búsqueda y Rescate: En situaciones de emergencia, los drones con IA pueden cubrir grandes extensiones de terreno en poco tiempo, identificando a personas atrapadas mediante cámaras térmicas y otras tecnologías. En casos de desastres naturales, como terremotos o inundaciones, su uso permite localizar supervivientes con mayor rapidez, optimizando los esfuerzos de rescate y aumentando las posibilidades de salvar vidas.
- 5.Apoyo en Operaciones Policiales y Militares: En el ámbito de la seguridad pública, los drones pueden ser utilizados para realizar operaciones de reconocimiento en zonas peligrosas, evitando poner en riesgo la vida de agentes. También son útiles en la persecución de sospechosos, proporcionando imágenes aéreas que ayudan a coordinar las acciones policiales. En el ámbito militar, su uso para la vigilancia de fronteras y la detección de amenazas potenciales es cada vez más común.

Desafíos y Consideraciones Éticas

A pesar de sus ventajas, esta tecnología no está exenta de desafíos. La privacidad es una preocupación clave, ya que la vigilancia automatizada puede generar inquietudes sobre el uso indebido de los datos recopilados. Si bien la IA permite una identificación rápida y eficiente de amenazas, su uso inadecuado podría derivar en vigilancia masiva sin controles adecuados, lo que pondría en riesgo los derechos de las personas. Para evitar esto, es esencial establecer límites claros sobre la recopilación, almacenamiento y uso de la información obtenida por estos dispositivos. El riesgo de errores en la identificación de amenazas sigue siendo un tema delicado.

La posibilidad de que un algoritmo identifique erróneamente a una persona como sospechosa puede derivar en problemas legales y sociales. Un falso positivo podría desencadenar intervenciones innecesarias por parte de las fuerzas del orden, afectando la vida de ciudadanos inocentes y debilitando la confianza en estas tecnologías. Es crucial que los sistemas de IA utilizados en drones sean rigurosamente entrenados y sometidos a pruebas constantes para minimizar estos errores. También es fundamental establecer regulaciones claras para garantizar un uso responsable de estos sistemas, evitando su aplicación en contextos que puedan vulnerar derechos fundamentales o generar un exceso de control sobre la población.

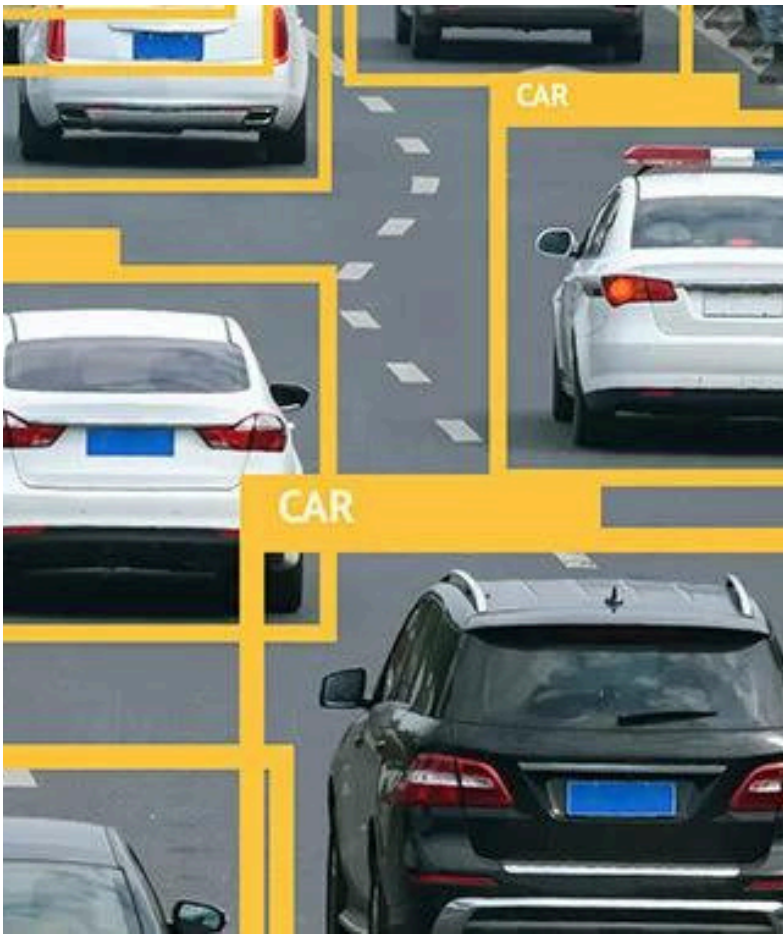
La transparencia en el uso de drones y el acceso a la información recopilada deben ser aspectos prioritarios para evitar abusos y garantizar que su implementación beneficie a la sociedad en su conjunto. Otro punto a considerar es la ciberseguridad. Como cualquier dispositivo conectado, los drones con IA pueden ser vulnerables a ataques informáticos, lo que representa un riesgo en términos de seguridad y privacidad. Un hacker podría tomar el control de un dron con fines malintencionados, comprometiendo la integridad de la información recopilada e incluso utilizando el dispositivo para actividades delictivas. Para mitigar estos riesgos, es crucial desarrollar sistemas robustos de protección, aplicar actualizaciones de software frecuentes y garantizar que solo personas autorizadas puedan operar y acceder a los datos generados por los drones.

Además, se debe analizar el impacto laboral que esta tecnología podría tener en el sector de la seguridad. Si bien los drones con IA pueden optimizar la vigilancia y reducir costos, también podrían desplazar a trabajadores humanos que desempeñan funciones similares.

Es necesario encontrar un equilibrio que permita la convivencia de la tecnología con el empleo humano, promoviendo la capacitación en nuevas habilidades y generando oportunidades en el desarrollo y mantenimiento de estas soluciones.

Conclusión

Los drones con IA están transformando la seguridad, ofreciendo herramientas más eficaces para la protección de personas y bienes. No obstante, su implementación debe ser cuidadosa y regulada para equilibrar los beneficios tecnológicos con la protección de la privacidad y los derechos individuales. Además, se debe trabajar en normativas que aseguren su uso ético y transparente. Si se desarrolla con responsabilidad, esta innovación promete mejorar significativamente la manera en que enfrentamos los desafíos de seguridad en el futuro. En los próximos años, veremos cómo esta tecnología se integra cada vez más en la vida cotidiana, redefiniendo la forma en que protegemos nuestro entorno y a quienes nos rodean. Sin duda, los drones inteligentes han llegado para quedarse, y su impacto en la seguridad será cada vez más evidente



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

Edición propiedad de @MetroRisk, asociación

RADIO

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

Feria Internacional de Seguridad, Defensa y Emergencias

Se trata de una iniciativa de la Feira Internacional de Galicia ABANCA junto con la Asociación de Directivos de Seguridad Integral (ADSI), la Asociación Nacional de Profesores Acreditados de Seguridad Privada (ANPASP), la Asociación Internacional de Miembros de Cuerpos de Seguridad y Emergencias (AIMCSE) y el consultor y asesor de seguridad y defensa D. Luis Martínez Gavilán

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