

ESPECIAL

y su industria de la protección



www.conseguridadmagazine.com



HIKVISION®



Guanlan

To understand the nature and movement of water, one must observe its waves.



Protección perimetral Impulsado por Hik iA

De 1 m a 100 km con protección precisa en cualquier entorno.

Nuestras soluciones perimetrales combinan **inteligencia artificial con tecnología avanzada** para proteger de forma precisa cualquier tipo de espacio: fábricas, puertos, granjas, residencias, fronteras y más.

Incluso bajo lluvia intensa, niebla o viento fuerte, la seguridad no se detiene.



IA con 99.9% de precisión.



Estabilidad en condiciones climáticas adversas.



Cobertura desde 1 m hasta 100 km.



Alertas inmediatas y verificación en tiempo real.



@HikvisionMx
www.hikvision.com/mx

Hikvision México
sales.mexico@hikvision.com

Colombia y sus diferentes rostros de la seguridad privada

En Colombia actualmente, la industria de la seguridad privada enfrenta diferentes desafíos ante la ola de inseguridad que impera en ese país. Por ello, los diferentes gremios no se detienen, deben proteger a los ciudadanos, esto con base en la estructura de diversas organizaciones del sector.

Su ecosistema laboral es complejo y en expansión con una estructura diversa en sus nichos como el blindaje, vigilancia presencial, transporte de valores, seguridad electrónica y consultoría estratégica. La industria de la seguridad se ha consolidado como una de las principales fuentes de empleo del país.

Algunos de los porcentajes del aporte económico del sector en Colombia, ronda el 1.2% del Producto Interno Bruto (PIB), con una participación aproximada de 10.5 billones de pesos colombianos en 2022. El 95% de la actividad aún corresponde a vigilancia presencial, mientras que el componente electrónico representa solo el 5% en línea con una transición gradual hacia modelos tecnológicos.

La regulación del sector está a cargo del Ministerio de Defensa a través de la Superintendencia de Vigilancia y Seguridad Privada, bajo el marco del Decreto 356 de 1994. En este marco legal y operativo actúan diversas organizaciones gremiales que representan hoy los intereses de empresas y trabajadores del sector; de las cuales apreciable lector, podrá conocer lo que cada uno está haciendo desde su trinchera en pro del país.

Este panorama general permite comprender la magnitud, diversidad y responsabilidad que implica el sector de la seguridad privada en Colombia. Cada una de las asociaciones que la conforman, representan una visión particular del oficio, una agenda gremial y un compromiso con la legalidad, profesionalización y adaptación a nuevos desafíos tecnológicos y sociales. 🌐

CON SEGURIDAD Magazine Latam

DIRECCIÓN GENERAL

HUMBERTO MEJÍA, DSE, CPSI, CIEIE
NORTEAMÉRICA / ESPAÑA
hmejia@conseguridad.com

ALFREDO YUNCOZA, CSSM, CPOI, CPO
CENTRO / SUDAMÉRICA
ayuncoza@conseguridad.com

DIRECCIÓN COMERCIAL

MARÍA ANTONIETA JUÁREZ CARREÑO
DIRECCIÓN COMERCIAL Y RELACIONES PÚBLICAS
marieclaira@conseguridad.com

COORDINACIÓN EDITORIAL

BEATRIZ CANALES HERNÁNDEZ
COORDINACIÓN EDITORIAL
edicion@conseguridad.com

COORDINACIÓN DISEÑO

SERGIO GIOVANI REYES POZO
COORDINACIÓN DISEÑO
diseno@conseguridad.com

MARKETING LATAM

SARA MEJÍA CASTRO
DESARROLLO DE NEGOCIOS LATAM
negocios@conseguridad.com

CORRESPONSAL

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@conseguridad.com

ADMINISTRACIÓN Y CONTABILIDAD

OSCAR TENORIO COLÓN
ADMINISTRACIÓN Y CONTABILIDAD
contabilidad@conseguridad.com

CONTACTO

Tel: +52 55 1607 1398 (México)
WhatsApp: +58 424 1390 359 (Venezuela)
WhatsApp: +52 55 1894 7067 (México)
asistencia@conseguridad.com

- 6 Gemelos digitales de Hikvision
- 7 Ajax realiza 7° Ajax Special Event
- 8 Ofrece Motorola seguridad con Pelco
- 16 Nuevo libro de Inteligencia Cuántica
- 18 **La otra fuerza del orden en Colombia**
- 26 Impulsa IAAPA seguridad en parques de diversiones
- 28 Paneles INSPIRE de Honeywell
- 19 México se suma al ICC



HERACRON®

KOLON INDUSTRIES

La Aramida de Clase MUNDIAL.

“Heracron® Ofrece protección de grado profesional validada en zonas reales de conflicto y bajo normas internacionales.

Sus filamentos creados específicamente para el blindaje, tienen mayor tenacidad, versatilidad para vehículos y silueta personal además de mayor resistencia térmica..”



La Nueva Elite del Blindaje en México.

Solicita ya tus láminas de 9 y 11 capas para niveles NIJ II y IIIA.



CONTACTO:
www.heracron.mx
www.prorescue.mx
contacto@prorescue.mx



El Profesional

Doctorando en Estudios Políticos (Universidad Externado de Colombia). Maestría en Estrategia y Geopolítica (Escuela Superior de Guerra de las FFMM). Especialización en Administración de la Seguridad (Universidad Militar Nueva Granada). Profesional en Ciencias Militares (Escuela Militar de Cadetes). Certificado internacional de seguridad CPP por ASIS International. Certificado internacional en Operaciones de Seguridad CPO por IFPO. Miembro del Consejo Consultivo Latino de IFPO.

Con más de 30 años de experiencia profesional en consultoría, asesoría e investigaciones para la prevención y control del fraude, consultoría y asesoría de seguridad corporativa para empresas locales y multinacionales, análisis y evaluación de información de interés para el desarrollo de las operaciones de las compañías clientes, planeamiento y desarrollo de investigaciones corporativas y gerenciamiento de incidentes, de crisis, desarrollo e implementación de los planes de continuidad de negocio y recuperación del desastre; manejo de relaciones y coordinación de apoyos con las autoridades de cada región.

Docente universitario para los posgrados en Administración de Seguridad de la Universidad Militar Nueva Granada y la Escuela de posgrados de la Policía Nacional.



Ramiro Díaz Carreño



Colombia

Su decisión inteligente.

WSO
WORLDWIDE SECURITY OPTIONS

Protección ejecutiva
Protección electrónica
Seguridad física
Gestión de riesgos
Seguridad robótica
Servicios de inteligencia

WSO SIAT

WSO SECURITY

wso-security.com

info@wso-security.com

Tour Internacional 2026

CON SEGURIDAD
Magazine Latam



AJAX

DOMINA TU ESPACIO

Detectores inalámbricos de incendio con
sensores de calor, humo y monóxido de
carbono



FireProtect 2
Protección contra todo tipo de amenazas incluso las
invisibles como el (CO)



Dónde comprar
www.ajax.systems

Futuro impulsado por modelo virtual de gemelos digitales de **HIKVISION**

- El ecosistema proporciona a las universidades una estrategia para optimizar operaciones y elevar la calidad educativa.
- Desde reducción de costos hasta la mejora de la experiencia de aprendizaje, beneficios innovadores y de gran impacto.

Las tecnologías digitales están transformando la educación superior, brindando a las instituciones una ventaja competitiva y moldeando el futuro del aprendizaje. Entre las innovaciones emergentes, destacan los gemelos digitales (réplicas virtuales de un sistema físico), que están transformando seguridad, operaciones y experiencias educativas del campus. Al integrar estos sistemas con cámaras inteligentes y tecnologías modernas para las aulas, las universidades están creando campus más inteligentes, seguros y eficientes.

"Un gemelo digital es un modelo detallado de un campus —incluyendo sus edificios, aulas e infraestructura— creado en una computadora. Aunque aún no se ha desarrollado plenamente el potencial de esta nueva tecnología, los gemelos digitales ya ofrecen diversas aplicaciones que pueden revolucionar los entornos y los resultados educativos", destaca Miguel Arrañaga, director Regional de Ventas de Hikvision México.

Comenta que los métodos tradicionales de gestión de campus se basan en cámaras anticuadas y sistemas independientes. Por ello, suelen ser inadecuados y costosos, sobre todo para universidades en crecimiento con decenas de aulas. Además, los sistemas de control de acceso que dependen de lectores de tarjetas aislados suelen complicar los procesos de seguridad. Por otro lado, las aulas convencionales con pizarras básicas y proyectores de baja resolución no consiguen captar la atención de los estudiantes y suponen una carga para los docentes.

Estos sistemas ineficientes y desconectados, dice, ya no satisfacen las demandas de un campus moderno a gran escala. Es aquí donde la tecnología de gemelos digitales puede marcar una diferencia tan significativa.

Beneficios de aplicar gemelos digitales a instituciones educativas

Los gemelos digitales conectan los entornos físicos y digitales para mejorar los servicios, entornos y procedimientos educativos. Algunos beneficios clave:

- **Permiten** la monitorización y el análisis en tiempo real de los espacios físicos. Los administradores pueden optimizar la distribución de las aulas, el equipamiento y los flujos de trabajo para ofrecer una experiencia de aprendizaje fluida desde el momento en que los estudiantes entran al campus hasta que salen. Se benefician de entornos más inteligentes y tecnológicos, lo que fomenta la participación y la eficiencia.
- **Integran** diversos sistemas de gestión, mejorando la precisión de los datos y la visibilidad operativa, lo que a su vez optimiza la prestación de servicios educativos. Esta composición proporciona una visión integral de las operaciones del campus, permitiendo a los administradores supervisar y gestionar diversos aspectos del campus, como la seguridad, el mantenimiento y la asignación de recursos, desde una plataforma centralizada. Al optimizar estos procesos, los gemelos digitales reducen las ineficiencias operativas y los costos.
- **Promueven** la responsabilidad ambiental al monitorear el uso de recursos, como energía y agua. Las universidades pueden usar la información para reducir su huella ecológica, por ejemplo, identificando ineficiencias en los sistemas de iluminación o climatización y reasignando recursos físicos para evitar el desperdicio.

"Tenemos un ejemplo claro de su uso en la Universidad Qassim de Arabia Saudita que, en colaboración con Hikvision, desarrollamos un ecosistema de gemelos digitales de realidad aumentada (RA) que abarca sus 30 edificios. Cuenta con un modelo 3D detallado con más de 6000 cámaras inteligentes. Con un panel de control intuitivo y centralizado, los administradores pueden supervisar fácilmente la distribución y las estructuras interiores, lo que garantiza un entorno más seguro para todos en el campus".

Arrañaga detalla que los educadores se han beneficiado de sistemas mejorados de programación y gestión de asistencia, lo que les permite centrarse más en la interacción estudiantil y la calidad de la enseñanza, ofreciendo una educación transfronteriza. Las aulas con tecnología avanzada promueven el aprendizaje activo y ofrecen a los estudiantes una experiencia más ágil en el campus. Para los administradores, las plataformas centralizadas simplifican las operaciones complejas, mejorando la eficiencia en áreas clave como el comedor, las residencias estudiantiles y las comunicaciones del campus.

El ecosistema de gemelos digitales ofrece a las universidades una hoja de ruta para operaciones más inteligentes y resultados educativos superiores. Desde la reducción de costos operativos hasta el enriquecimiento de las experiencias de aprendizaje, las posibilidades son inmensas. 🌐



AJAX presentó nuevas soluciones en el 7º Ajax Special Event: Atrévete a ser el primero

Ajax Systems anunció la 7ª muestra anual **Ajax Special Event: Atrévete a ser el primero**. La empresa exhibió soluciones que revolucionan el sector y abren nuevas oportunidades para los partners, profesionales y usuarios de Ajax. La presentación se retransmitió en línea el pasado 21 de noviembre de 2025 en los canales de YouTube de la empresa.

El Ajax Special Event: Atrévete a ser el primero es el evento más importante del sector. Reveló los nuevos dispositivos de protección contra incendios, de videovigilancia, contra intrusiones, y las formas de combinarlos en un único sistema integrado. La presentación mostró cómo los Servicios Ajax pueden aumentar la satisfacción de los clientes y cómo el software Ajax, en constante evolución, aporta ventajas a los usuarios más experimentados y a los PRO.



Con el lema Atrévete a ser el primero, el equipo de Ajax anima al sector a enfrentarse una vez más a lo desconocido con la emoción de las nuevas innovaciones, superando retos de siempre, mejorando la experiencia tanto de los profesionales como de los usuarios y estableciendo nuevos puntos de referencia en la industria.



La presentación en línea se transmite en todo el mundo en más de 20 idiomas con locución y subtítulos. Siga el enlace para inscribirse en la presentación en línea del Ajax Special Event: Atrévete a ser el primero y mantenerse al día con las últimas noticias de la compañía. 🌐

AJAX

SPECIAL EVENT

DARE TO BE FIRST
NOVEMBER 21

Ofrece **MOTOROLA SOLUTIONS** seguridad robusta para infraestructura crítica con **Pelco**

- Nuevo portafolio innovador de dispositivos de Pelco impulsados por IA.
- Las tecnologías de vanguardia de Pelco ofrecen un rendimiento confiable en condiciones extremas y una fácil integración con sistemas de gestión de video existentes.

Chicago, EE.UU.- Motorola Solutions anunció el nuevo portafolio innovador de dispositivos impulsados por Inteligencia Artificial Pelco, diseñados específicamente para empresas que operan en algunos de los entornos más desafiantes, como petróleo y gas, o puertos. Respaldo por la profunda experiencia en ingeniería de la compañía y significativas inversiones en investigación y desarrollo, la línea de dispositivos de Pelco incluye cámaras fijas, cámaras robustas y de largo alcance, sensores inteligentes y análisis de Inteligencia Artificial (IA) que se integran fácilmente con una amplia gama de sistemas de gestión de video (VMS) de terceros.

Desde la adquisición de Pelco en 2020, Motorola Solutions ha transformado completamente la línea de cámaras, que se ha duplicado desde que la compañía trajo a casa áreas de ingeniería y diseño. Bajo una nueva y moderna marca Pelco, el portafolio reúne tecnologías de seguridad especializadas de las adquisiciones estratégicas de Videotec, IP Video y Silent Sentinel.

"Pelco proporciona a los operadores de seguridad soluciones robustas de seguridad impulsadas por IA, capaces de funcionar en una amplia gama de condiciones ambientales", dijo Hamish Dobson, vicepresidente corporativo de Pelco. "Hemos creado Pelco con el propósito de combinar hardware resistente, detección de última generación y análisis impulsados por IA para un portafolio de dispositivos agnóstico al VMS que está impulsando estándares más altos en la seguridad de la infraestructura crítica".



Las expansiones del portafolio amplían las oportunidades de crecimiento con empresas e industrias de infraestructura crítica como el transporte, la aviación, el sector marítimo y los servicios públicos. Tales operaciones soportan rutinariamente condiciones climáticas extremas, elementos corrosivos y otras condiciones peligrosas donde las cámaras y dispositivos de seguridad estándar se dañan rápidamente.

El nuevo portafolio especializado de Pelco incluye:

- **Cámaras Anti-corrosión Espirit:**

Pueden soportar los duros elementos oceánicos de los entornos marítimos.

- **Cámara fija ExSite Enhanced**

Thermal 2: proporciona a sitios peligrosos como centrales eléctricas una cámara de seguridad de imágenes térmicas con certificaciones globales a prueba de explosiones.

- **Sensor Halo Smart:** un sensor inteligente todo en uno que ofrece seguridad sin video, protegiendo la privacidad mientras detecta instancias como vapeo, disparos, ruidos anormales, movimiento y palabras clave de emergencia como "ayuda".

- **Cámaras Aeron y Jaehar**

ofrecen capacidades de detección a distancias de hasta 32 kilómetros en entornos extremos asociados con los sectores militar, aviación, marítimo e infraestructura crítica.

Todos los dispositivos Pelco cuentan con el respaldo de Elevate, una plataforma de soporte de cámaras basada en la nube. Evalúa la salud de las cámaras y amplía las capacidades de detección con IA basada en la nube. Los dispositivos Pelco están diseñados para ser compatibles con sistemas Open Network Video Interface Forum (ONVIF) lo que simplifica la instalación, permite integraciones flexibles y mitiga las costosas renovaciones del sistema. Las cámaras IP de Pelco permiten el cumplimiento normativo con las reglas actuales de la Sección 889 de la Ley de Autorización de Defensa Nacional (NDAA) para la adquisición de equipos seguros. 

Lanza **AXIS** COMMUNICATIONS reporte en la industria de la videovigilancia

- El reporte destaca que el reconocimiento facial se ha adoptado en muchos países, respaldado por nuevas regulaciones para la aplicación de esta tecnología de manera ética.

La empresa mundial del sector de la videovigilancia, Axis Communications, ha publicado su último informe, "El estado de la IA en la videovigilancia", que explora las perspectivas del sector sobre el uso de la IA en la seguridad, la protección y más allá. El informe revela los principales conocimientos críticos sobre las tecnologías de IA, su integración y las oportunidades y desafíos con respecto a la seguridad, inteligencia, inteligencia empresarial y la eficiencia operativa.

El despliegue de la IA se ha disparado en los últimos dos años, sobre todo debido al aumento de las demandas de los clientes, la mejora del conocimiento de las aplicaciones y la aparición de nuevos casos de uso.

Mats Thulin, director de soluciones de IA y análisis de Axis Communications, comentó: "La IA sigue siendo una de las tecnologías más potentes y transformadoras dentro de la industria de la videovigilancia. Esta nueva investigación revela que, si bien existen oportunidades significativas para que la IA mejore la seguridad, la eficiencia operativa y la inteligencia empresarial, debe haber un enfoque en la implementación ética y las integraciones significativas que generen valor".

A través de entrevistas de investigación cualitativa con expertos en IA de la red global de socios de Axis, en este nuevo informe se descubrieron varias ideas temáticas sobre las tecnologías de IA.

Transición de la IA en la nube y en el borde sigue acelerándose

Los resultados de la investigación destacan que el paso de los sistemas de servidores locales a las arquitecturas híbridas continúa a buen ritmo. Este desarrollo está impulsado por la necesidad de una mayor escalabilidad, un procesamiento más rápido y un mejor uso del ancho de banda. El modelo híbrido, que combina las capacidades de procesamiento inmediato de la IA periférica en las cámaras con la escalabilidad y el almacenamiento de datos a largo plazo de la nube, se está convirtiendo en el enfoque preferido por muchos. Este equilibrio permite a las organizaciones aprovechar las fortalezas de ambas tecnologías.

Integración de diversas fuentes de datos

Los encuestados de la investigación coincidieron en que la integración de datos sensoriales adicionales, como el audio y los factores ambientales contextuales, para complementar los datos de video mejorará la conciencia situacional, proporcionará

información más profunda y procesable, y ofrecerá una comprensión más completa de los eventos. En última instancia, esto revolucionará la seguridad y la protección, al tiempo que elevará las capacidades de inteligencia empresarial.

La combinación de múltiples flujos de datos permite una detección y predicción más precisas de posibles amenazas. Por ejemplo, en escenarios de emergencia, la combinación de datos visuales con análisis de audio puede permitir a los equipos de seguridad responder de forma más rápida y precisa.

Reconocimiento facial gana terreno

La investigación también destacó que el reconocimiento facial parece haberse adoptado más ampliamente en muchos países, respaldado por la introducción de nuevas regulaciones para ayudar a aclarar cómo se puede aplicar esta tecnología de manera ética y proporcionar un marco para su uso responsable.



Los expertos entrevistados predijeron que el reconocimiento facial seguirá ganando terreno a nivel mundial, pero primero debe haber una alineación con las regulaciones de privacidad y transparencia sobre cómo funciona la tecnología. Las consideraciones éticas en torno al uso del reconocimiento facial siguen siendo un foco central, especialmente en regiones con leyes de privacidad estrictas.

¿QUIENES SOMOS?

Somos una empresa fundada en República Dominicana especializada en consultoría y desarrollo de proyectos de seguridad integral, cubriendo protección (security) y seguridad (safety). Con experiencia nacional e internacional, diseñamos e implementamos soluciones personalizadas, efectivas y cuantificables, optimizadas continuamente para garantizar alta calidad y eficiencia, adaptándonos a las necesidades específicas de nuestros clientes en cualquier contexto geográfico.

SERVICIOS QUE OFRECEMOS A NUESTROS CLIENTES EN EL AREA DE CONSULTORÍA

Auditorías de seguridad, Análisis de riesgos, Evaluación de amenazas, Análisis de vulnerabilidades, Análisis de entorno, Medición de cultura organizacional orientada a la seguridad, Diseños de política de seguridad, Diseño de implementación y mantenimiento de sistemas de seguridad: barreras físicas, controles de acceso, videovigilancia y otras tecnologías básicas, medias y avanzadas, Planificación de emergencias, Diseño de planes de evaluación, Diseño de planes de gestión de crisis y continuidad de negocios, Consultoría en ciberseguridad, Consultoría de seguridad de la información, Consultoría de inteligencia artificial aplicada a la gestión de riesgos de seguridad, Consultoría en debida diligencia (Compliance), Investigación de incidentes, Evaluación y optimización de recursos de seguridad y Capacitación en seguridad.

Redefine **HID** la integración de la seguridad física y digital

- Nueva plataforma de servicios de integración como servicio (IPaaS), concebida para desarrolladores de aplicaciones, integradores de soluciones y proveedores de software.
- HID Integration Service responde a las exigencias cada vez más complejas en la gestión de infraestructuras de seguridad.

Austin, Texas. - HID, firma mundial en soluciones confiables de gestión de acceso e identidades, anunció el lanzamiento de HID Integration Service, una plataforma que integra la seguridad física, ciberseguridad y gestión de identidades digitales.

Esta plataforma de integración como servicio (IPaaS) fue concebida para que desarrolladores de aplicaciones, integradores de soluciones y proveedores de software puedan integrar de forma ágil y sin complicaciones las soluciones esenciales de seguridad física, simplificando los procesos y mejorando la interoperabilidad de los sistemas. Al hacerlo, la plataforma busca aliviar la carga de mantenimiento y actualizaciones que conlleva la gestión y puesta en marcha de integraciones entre los sistemas de seguridad física y la ciberseguridad, generando así un ahorro de costos, operaciones más eficientes y una significativa disminución en los tiempos de implementación.

"Las organizaciones llevan mucho tiempo lidiando con integraciones inestables y complejas, además de los elevados costos que implica su mantenimiento", explicó Martin Ladstaetter, vicepresidente sénior y responsable de la división de Soluciones de Gestión de Identidad y Acceso de HID. "HID Integration Service resuelve estos problemas al proporcionar una plataforma de integración que conecta los productos de seguridad física y digital, lo que reduce el tiempo de lanzamiento al mercado para nuestros socios desarrolladores, quienes están creando una nueva generación de soluciones de seguridad con mayor velocidad, calidad, resiliencia y valor para el usuario".

HID Integration Service se enfoca directamente en los principales beneficios que buscan los responsables de la seguridad en las organizaciones al adoptar soluciones de gestión unificada —mejorar la eficiencia, simplificar la gestión y obtener un panorama completo de los procesos—, ayudándolos a:

- Reducir la complejidad operativa y los costos de mantenimiento.
- Implementar con mayor rapidez nuevas prestaciones de seguridad en soluciones adaptadas a cada sector.
- Simplificar los puntos de interacción con los sistemas de seguridad mediante experiencias de uso más ágiles y sin complicaciones.

Las siguientes son las principales características de la solución:

- Una capa unificada de integración que abarca desde conexiones punto a punto hasta integraciones con múltiples plataformas y usuarios.
- Integraciones preconfiguradas que agilizan la implementación y reducen los costos de desarrollo.
- Escalabilidad y seguridad que se adaptan a las necesidades cambiantes de su organización.

HID tiene el privilegio de contar con varios usuarios pioneros que ya están implementando la plataforma. Cada uno de ellos aporta una amplia trayectoria y sólidas funcionalidades en diversas tecnologías, mercados verticales y ámbitos de seguridad.

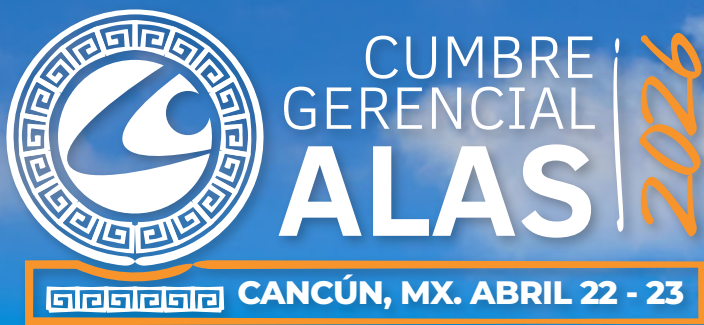
"Estamos entusiasmados con las nuevas posibilidades que ofrece la plataforma de integración de HID, pues creemos que fortalecerá aún más la capacidad de SwiftConnect para responder a las expectativas y necesidades cada vez más amplias de nuestros clientes en el sector inmobiliario comercial y empresarial", señaló Matt Kopel, cofundador y codirector ejecutivo de SwiftConnect. "La coincidencia de visión y dirección entre ambas compañías potenciará y amplificará los cambios corporativos que nuestros clientes desean implementar", añadió Kopel.

"Imaginamos un mundo en el que las fotografías de identificación lleguen mágicamente a su destino, sin intervención humana", afirmó Luke Rettstatt, director ejecutivo de CloudCard. "Para hacer realidad esta visión, debemos desarrollar y mantener numerosas integraciones, algo que supone una gran carga de trabajo para un equipo pequeño. HID Integration Service nos permite concentrarnos en el flujo de trabajo impulsado por IA de RemotePhoto, en lugar de destinar tiempo y recursos al desarrollo y mantenimiento de integraciones certificadas con terceros".

Esta demanda cada vez de mayor integración y eficiencia se ve reflejada en el Informe sobre el estado de la Seguridad y la Identidad de 2025. Según este estudio, el 67% de los encargados de la protección están migrando hacia soluciones basadas en software, mientras que casi tres cuartas partes de las organizaciones consideran fundamental para sus operaciones la recopilación unificada de datos. 📊

alas-la.org/cumbre-gerencial-alas

El 2026 llega con el mayor Encuentro de
Líderes de la Seguridad en LATAM - Únete a la
Cumbre Gerencial ALAS Cancún



Factores de riesgos psicosociales en las fuerzas de seguridad en Latinoamérica



Guillermo Fogelman
Licenciado en Seguridad Pública.
Vicepresidente IFPO Comunidad Argentina.

Articulista invitado



Buenos Aires, Argentina. - El suicidio en las fuerzas de seguridad constituye un problema creciente y crítico de salud pública. La incidencia es mayor que en la población general, fenómeno agravado en los últimos años y potenciado tras la pandemia de COVID-19 (Clavijo Ruiz, 2022). Los factores de riesgo psicosocial —desconexión social, falta de apoyo organizacional, ausencia de reconocimiento social, frustración crónica y estrés prolongado— se constituyen como disparadores directos de conductas autolesivas.

Los riesgos psicosociales en la región se explican por desigualdades estructurales, precarización laboral, migraciones internas, déficit habitacional y exclusión educativa. Todo ello genera un entramado social frágil que afecta de manera particular a los cuerpos policiales. El aislamiento percibido, la falta de empatía institucional y la desvalorización social de la función policial refuerzan la sensación de vulnerabilidad y soledad de los agentes.



La "cuestión social policial" refleja esta paradoja: los uniformados forman parte de un estrato social, pero se sienten divorciados de él. Esto produce desconexión, frustración y consumo de sustancias, y en muchos casos, la decisión de recurrir al suicidio como mecanismo último frente a un dolor insostenible.

A nivel global, se estima que alrededor de un millón de personas se suicidan anualmente, representando el 1,5% de las muertes en el mundo. En 2019, fue la principal causa de fallecimiento en jóvenes de 15 a 29 años (Naghavi et al., 2019). Los métodos más frecuentes son la asfixia, armas de fuego, intoxicación con drogas y envenenamiento, que representan el 91% de los casos (OPS, 2023).

En Estados Unidos, un estudio del Instituto Nacional de Seguridad y Salud Ocupacional reveló que la tasa de suicidios en policías es 3,5 veces mayor que la de otros trabajadores, y que entre 2003 y

2010 los agentes tenían hasta 2,4 veces más probabilidades de morir por suicidio que por homicidio (Tiesman et al., 2015).

En Ecuador, por contraste, la incidencia es baja, con apenas tres casos reportados en 2022 (López, citada en fuentes locales). En Brasil, en cambio, una investigación sobre la policía del estado de Río Grande (2006–2016) reportó una tasa anual de 12,5 suicidios por cada 100.000 agentes, frente a 4,9 en la población general. La tasa fue de 18,5 entre menores de 40 años y de 7,3 entre mayores. Por género, las mujeres alcanzaron 18,8/100.000 y los hombres 11,9/100.000, lo que evidencia un riesgo particularmente alto en mujeres jóvenes (Gomes, de Araújo & Gomes, 2018).

La evidencia demuestra que la problemática es multifactorial y exige un abordaje integral. Las políticas públicas deben reconocer la centralidad de los factores psicosociales, incorporando diagnósticos tempranos, estrategias personalizadas de prevención, acompañamiento institucional y acciones de posversión para los supervivientes (Grande Ratti et al., 2024). Asimismo, resulta indispensable fortalecer las habilidades blandas y la inteligencia emocional en los liderazgos, junto con medidas de apoyo socioeconómico y cultural que reconstruyan los lazos de pertenencia.

La prevención eficaz requiere superar el estigma y visibilizar el problema en toda su magnitud. Reconocer los factores de riesgo psicosocial como detonantes del suicidio en las fuerzas de seguridad es el primer paso para diseñar políticas efectivas que protejan la vida de quienes dedican la suya a proteger a la sociedad. 🌐



Los ejecutivos y la divulgación inadvertida de la información sensible de la organización



Ramiro Días Carreño
CPP. CPO. Miembro por Colombia al Consejo Consultivo Latino de IFPO.

Articulista invitado



Bogotá, Colombia.- El mundo corporativo cada vez más competitivo y exigente hace que los ejecutivos y/o directivos de manera inadvertida e inconsciente y en ocasiones consciente, pero sin medir las consecuencias en el negocio, divulgan información sensible de las empresas, facilitado por el inmediato acceso a medios de comunicación masivo como las redes sociales o los canales de difusión internos de cada empresa.

Los atacantes también cada vez más sofisticados acuden entre otros a los anuncios de viajes de negocio, visitas a grandes clientes o competidores, fotos, bocetos y videos de novedosos productos o servicios, propuestas de nuevos organigramas con sus responsables, acceso a áreas restringidas, contraseñas visibles en tableros, entre muchas otras formas que inadvertidamente se convierten en vulnerabilidades.

Entre las modalidades más utilizadas por los atacantes están la suplantación de identidad física o digital, la ingeniería social, las contraseñas fáciles de descubrir o inferir, los seguimientos al entorno digital de cada persona objetivo y de la misma empresa, los malware en los sistemas informáticos de equipos de cómputo y móviles, el fácil acceso a las basuras de las áreas sensibles e incontables maneras de lograr los objetivos de los atacantes.



Dado lo anterior, es relevante concientizar periódicamente a todos los empleados, contratistas y en especial a los directivos de la organización en las diferentes formas en que puede divulgarse inadvertidamente la información sensible y de la misma manera como tomar medidas preventivas y correctivas, de manera decidida y consciente.

Considerando lo previamente mencionado, es imperioso realizar un diagnóstico de seguridad que permita identificar las debilidades y exposiciones que pueden presentar la empresa, los directivos y empleados con cargos sensibles y de alta visibilidad en la organización; para ello se hace necesario analizar y evaluar entre otros aspectos los siguiente:

Análisis del contexto externo:

Mapeo de la huella digital, donde se revisa y analiza la información pública con el objeto de identificar información sensible expuesta y vulnerable.

Las políticas corporativas para el acceso y uso de las redes sociales, buscando identificar la claridad, la pertinencia legal, el cubrimiento, los niveles de difusión, el acceso y, por ende, las restricciones o prohibiciones en el manejo de la información.

Capacitar a todos los directivos y empleados con cargos sensibles y de alta visibilidad en la organización, ofreciendo formación regular, especializada y actualizada sobre los riesgos y las diferentes modalidades de ataque, y a su vez, dar a conocer e implementar las mejores prácticas para el uso responsable de las redes sociales.

Monitoreo permanente de las redes sociales, a través de herramientas especializadas que identifiquen y alerten sobre actividades que puedan representar una amenaza para la seguridad y la reputación de la organización.

Análisis del contexto interno

Identificación y clasificación de datos sensibles, a través de un inventario de la información confidencial para la organización, donde se detalle entre otros, la relación de los clientes, la propiedad intelectual, nuevos productos, secretos comerciales, organigrama, la nómina, procesos internos con información sensible. A su vez la clasificación de la información, donde se detalle entre otros aspectos si la información es pública, interna, privada, restringida, confidencial o muy alta confidencialidad.

La accesibilidad a la información donde se detalla quién o quiénes tienen acceso a la información sensible, las herramientas y privilegios de acceso a la información para los empleados, sistemas de autenticación robustos como la autenticación de dos factores, restricción de dispositivos de almacenamiento de información o de conexión.

Auditorías periódicas para identificar y hacer seguimiento al tráfico de la red informática, a patrones sospechosos como los accesos en horario no laboral, acceso a información no autorizada, cambios inusuales en los puertos de conexión, transferencia de datos inusuales o no autorizados, entre otros.

Alertas y notificaciones con el objeto de detectar en tiempo real actividades sospechosas relacionadas con la información clasificada como sensible, quienes reciben y tramitan las alertas.

Planes de respuesta a incidentes y recuperación de la información con el apoyo forense para los casos que lo ameriten.

Implementar un programa de lecciones aprendidas, con el objeto aprender de las vulnerabilidades aprovechadas por los atacantes o por los descuidos al interior de la organización.

¿Malware autónomo e IA generativa: la nueva frontera del cibercrimen en América Latina?

¿Alguna vez has imaginado un malware (software malicioso, a menudo llamado "virus informático") capaz de gestionarse a sí mismo, crear nuevas estrategias ofensivas, generar deepfakes de voz y video y, además, adaptar sus tácticas al comportamiento de la víctima? ¡Entonces sabe que esto ya está ocurriendo!



Antonio Celso Ribeiro Brasiliano
PhD, Doctor en Filosofía en Ciencias de la Seguridad Internacional, Cambridge International University, Inglaterra.
Presidente de Brasiliano INTERISK.
abrasiliano@brasiliano.com.br

Articlista invitado



São Paulo, Brasil. - Debemos entender que, en lugar de que un único código malicioso ejecute un ataque aislado, ahora hay grupos de agentes especializados trabajando juntos. Entre los componentes principales de este nuevo modelo de ataque, podemos destacar:

- Análisis de víctimas (Agente de análisis): Recopila y estudia información sobre el objetivo y el vector de ataque;
- Agente de vulnerabilidades de explotación: Localiza fallos y ejecuta exploits de forma automatizada;
- Ingeniería social avanzada (Agente de Ingeniería Social): Utiliza deepfakes de voz y video para estafas muy convincentes;

- Mapeo de A a Z Agente: Calcula el camino más eficiente entre diferentes sistemas y dispositivos, hasta que se traza la ruta de invasión;
- Agente de invisibilidad/ocultación: Borra registros y utiliza cifrado, dificultando la detección por parte de los defensores;
- Comunicación segura (Agente de Comunicaciones y Cifrado): Garantiza que todos los agentes intercambien datos de forma confidencial;
- Autonomía y adaptación (Agente de Actualización del Agente): Monitoriza las defensas del objetivo y actualiza el malware en tiempo real, eludiendo contramedidas.

El impacto en América Latina: ¿por qué es crítica esta amenaza?

América Latina es uno de los continentes más afectados por estafas digitales y ataques de ingeniería social. La situación tiende a empeorar a medida que surge malware autónomo, haciendo que el fraude sea aún más sofisticado.

La situación es mucho más vulnerable en Los Ángeles debido a la legislación obsoleta, la falta de concienciación, la falta de recursos, tanto para empresas privadas/públicas como para instituciones estatales que luchan contra el cibercrimen. El escenario prospectivo no es el mejor, creando grandes brechas para que los ataques sean prometedores.



Medidas preventivas y de mitigación que las empresas e instituciones deberían practicar como una biblia:

1. Educación y concienciación

- Formación recurrente en ingeniería social y técnicas avanzadas de intrusión, utilizando recursos humanos como vectores estratégicos, tanto para los empleados de la empresa como para la población general que se encuentra en casa sin acceso a entornos corporativos; en este caso, las instituciones financieras, las redes sociales y la prensa desempeñan un papel fundamental.

- Simulaciones realistas de phishing e ingeniería social destinadas a poner a los recursos humanos en contacto con la realidad, preparando a los usuarios para contraataques cada vez más convincentes.

2. Herramientas inteligentes de seguridad

- Soluciones de detección y respuesta basadas en IA que analizan comportamientos y patrones de red, capaces de identificar proactivamente amenazas.

- Software actualizado continuamente, que se adapta rápidamente a nuevas variantes de malware.

3. Acciones estratégicas para la base de conocimiento

- Alianzas nacionales e internacionales, facilitar la cooperación en el aprendizaje con institutos nacionales e internacionales, intercambio de conocimientos.

- Integración con empresas tecnológicas, proporcionando acceso a herramientas avanzadas de monitorización y respuesta.

- Colaboración entre empresas, gobierno y academia para intercambiar conocimientos e inteligencia sobre amenazas.

- Adopción de modelos de defensa colaborativos, con ejercicios y simulaciones de respuestas integradas.

Conclusión

Inteligencia Artificial – La IA debe estar vinculada a la inteligencia criminal de combate. Hoy en día, los ciberdelincuentes avanzan cada día, con innovaciones continuas y sucesivas. La ciberseguridad debe estar atenta y preparada para competir, conociendo profundamente el perfil, el modus operandi, las capacidades de nuestros adversarios, de lo contrario seremos simples piezas en el tablero del crimen. 🌐

¿Tiene que ser la IA un pilar central de la ciberseguridad en cualquier tipo de empresa? ¿Tendremos éxito?



Nuevo

La computación cuántica ya dejó de ser una promesa futurista para convertirse en un factor estratégico de seguridad nacional, poder tecnológico y ventaja competitiva. En **“Del Bit al Qubit: Hacia la Era de la Inteligencia Cuántica”**, Eddie Velásquez Ortiz y Félix A. Reyes Gutiérrez presentan una obra excepcional en español que explica, con claridad y rigor, cómo este nuevo paradigma transformará la defensa, la ciberseguridad y la industria global en la próxima década.

El libro conduce al lector desde los principios fundamentales del qubit, la superposición y el entrelazamiento, hasta las tecnologías reales que hoy desarrollan potencias como Estados Unidos, China y la Unión Europea. Expone la relevancia de los procesadores NISQ, los algoritmos cuánticos aplicables en 2025 —como QAOA— y el camino hacia la inteligencia cuántica híbrida que marcará la próxima ola de innovación.

Una de sus contribuciones más críticas es la explicación del riesgo cuántico sobre RSA, ECC y las infraestructuras gubernamentales y empresariales que dependen de ellas. La obra detalla la urgencia de migrar hacia esquemas de Criptografía Post-Cuántica basados en los estándares NIST y alerta sobre el escenario “harvest now, decrypt later”, ya empleado por adversarios estratégicos.

El texto también aborda el renovado tablero geopolítico: la carrera cuántica, las inversiones militares, las implicaciones para inteligencia y disuasión, y el posible impacto en comunicaciones, satélites, logística y sistemas autónomos. Para las instituciones de defensa y seguridad, el libro funciona como una guía ejecutiva para anticipar la transición.

“Del Bit al Qubit” es, sin duda, uno de los textos más completos, actuales y estratégicos publicados en español sobre el tema. Para más información: eddievelasquez.com



Libro



Eddie Velásquez Ortiz



Felix Reyes Gutiérrez





ReputationUP, expertos
en defender el activo
más frágil: **la reputación.**

REPUTATIONUP.COM

La otra **fuerza del orden** en **Colombia**: gremios, cifras y rostros de la **seguridad privada**

- Protección que no se detiene y cuida a ciudadanos y propiedades, gremios que sostienen la seguridad de un país.

Beatriz Canales Hernández

Bogotá, Colombia.- La industria de la seguridad privada en el país está conformada por una estructura diversa de gremios —lo que en otras naciones se denomina nichos, sectores o verticales— que articulan un ecosistema laboral complejo y en expansión. Entre blindaje, vigilancia presencial, transporte de valores, seguridad electrónica o consultoría estratégica, el sector se ha consolidado como una de las principales fuentes de empleo del país.

Actualmente, según cifras de la Superintendencia de Vigilancia y Seguridad Privada, cerca de 390 mil personas trabajan de manera directa en esta industria, entre guardias, escoltas, técnicos e ingenieros. El aporte económico del sector ronda el 1.2% del Producto Interno Bruto (PIB), con una participación aproximada de 10.5 billones de pesos colombianos en 2022. El 95% de la actividad aún corresponde a vigilancia presencial, mientras que el componente electrónico representa solo el 5% en línea con una transición gradual hacia modelos tecnológicos.

La regulación de la industria está a cargo del Ministerio de Defensa a través de la Superintendencia de Vigilancia y Seguridad Privada bajo el marco del Decreto 356 de 1994. Esta normativa contempla modalidades como vigilancia fija, móvil, protección de bienes, personas y comunidades, así como blindaje, monitoreo electrónico y capacitación profesional. En este marco normativo y operativo actúan diversas organizaciones gremiales que representan los intereses de las empresas y trabajadores del sector.

Asociación Colombiana de Seguridad (ASOSEC). Conformada por alrededor de 30 empresas y cerca de 30 mil empleados a nivel nacional, Promueve el desarrollo del sector mediante eventos como el Congreso Nacional de Seguridad —donde se reconocen los méritos de los guardas y se impulsan alianzas con entidades como la Superintendencia y la Policía Nacional— y campañas de liderazgo, inclusión y profesionalización.

Consejo Nacional de Seguridad Privada (CNSP). Este gremio representa a empresas de vigilancia, ofreciendo asesoría jurídica, representación institucional y coordinación de eventos como congresos sectoriales. Busca consolidar un liderazgo intergremial que impulse mejores prácticas en distintas regiones del país.

Asociación Colombiana de Empresas de Seguridad (ACES). Establecida sin ánimo de lucro con cinco capítulos regionales, Apunta a fortalecer la sostenibilidad y rentabilidad de sus afiliados, posicionarse como referente consultor nacional, impulsar la digitalización y cuidados ambientales, y ofrecer capacitación, convenios y representación gremial ante el Estado.

Federación Colombiana de Empresas de Vigilancia y Seguridad Privada (FECOLSEP). Con casi tres décadas de trabajo desde su fundación en 1996, fortalece a sus miembros mediante investigación aplicada, formación continua, asesoría técnica y proyección nacional e internacional, con un enfoque en sostenibilidad, innovación y ética profesional.

Confederación Nacional del Gremio de Vigilancia Privada (CONFVIP), organización que defiende los intereses del gremio ante entidades públicas y privadas. Ha consolidado eventos internacionales, como congresos de seguridad, busca representar de forma sólida los intereses de sus afiliados.

Federación Colombiana de Empresas de Vigilancia y Seguridad Privada (FEDESEGURIDAD), agrupa a las principales organizaciones del país dedicadas a supervisión, protección electrónica y transporte de valores. Su misión es promover el desarrollo sostenible del sector y el bienestar del talento humano, impulsando iniciativas de modernización y comunicación pública del gremio.

Asociación Latinoamericana de Seguridad (ALAS), Comité Colombia. En términos regionales, cuenta con una trayectoria de más de 28 años, específicamente en el mercado de la seguridad, y para poder desarrollar su misión y su visión de forma local, permite crear comités nacionales. Cuya función es la de desarrollar valores y estrategias diseñadas a nivel regional para expandir más la asociación y respaldar a los profesionales de la seguridad.

Este panorama general permite comprender la magnitud, diversidad y responsabilidad que implica el sector de la seguridad privada en Colombia. Cada una de las asociaciones aquí mencionadas representan una visión particular del oficio, una agenda gremial y un compromiso con la legalidad, la profesionalización y la adaptación a nuevos desafíos tecnológicos y sociales.

A través de ellas se articula una industria que custodia bienes e infraestructuras, y protege vidas, construye confianza ciudadana y genera miles de empleos formales. Colombia es un referente en la materia para América Latina. 🌐





impulsa integración tecnológica y profesionalización en la seguridad de Colombia

- Comité Colombia reúne a más de 100 socios entre fabricantes, integradores y usuarios finales.
- Inteligencia Artificial y analítica de datos marcan la evolución de la industria.
- La asociación fortalece alianzas con gremios, universidades y entidades públicas.

Bogotá, Colombia.- La Asociación Latinoamericana de Seguridad (ALAS) Comité Colombia, es el punto de encuentro entre fabricantes, integradores, distribuidores y usuarios finales para impulsar el desarrollo del sector. Con más de 28 años de trayectoria regional, el Comité Colombia, presidido por Daniela Cajamarca, agrupa a cerca de 100 socios nacionales y forma parte de una red de 800 miembros en América Latina.

El Comité colombiano estructura su labor en vicepresidencias temáticas que abarcan entre otras infraestructura crítica, banca, capacitación, membresías, comunicación y videovigilancia. Cada área desarrolla estrategias para que los afiliados accedan a capacitaciones y herramientas que fortalezcan su operación.

“El objetivo es que nuestros socios mejoren su desempeño profesional y aprovechen las tendencias tecnológicas para incrementar su competitividad”, señala Daniela Cajamarca.

Entre sus miembros se encuentran empresas fabricantes de cámaras, plataformas de control de acceso y sistemas de gestión, así como integradores y consultores especializados, entre otros.



La presidenta destaca el valor de contar con usuarios finales, quienes aportan retroalimentación directa sobre necesidades reales en materia de seguridad, ayudando a fabricantes e integradores a diseñar soluciones más efectivas.

El impacto de tecnologías como la Inteligencia Artificial y la analítica de datos han redefinido las prioridades del sector. Daniela Cajamarca subraya que el reto no solo es integrar herramientas innovadoras, sino utilizarlas para fortalecer la seguridad física y generar información estratégica para la toma de decisiones.

“La demanda está enfocada en obtener datos precisos que permitan anticipar y prevenir riesgos”, añade.

ALAS Comité Colombia mantiene un calendario de actividades. Entre ellas, ferias digitales, encuentros tecnológicos presenciales —como el realizado en Medellín con más de 120 asistentes—, webinars y mesas de trabajo sobre ciberseguridad, IA y tendencias globales. En agosto de 2025, el Comité participó en la Feria Internacional de Seguridad en Bogotá, con paneles como *Looking to the future*, enfocado en las tendencias del mercado, y debates sobre el impacto de la reforma laboral en la industria tecnológica.



Las alianzas estratégicas son otro pilar de trabajo. El Comité ha establecido vínculos con organizaciones como COLADCA, CONFEVIP, Policía Nacional, ASIS, el Clúster de Seguridad de Bogotá y la Asociación Colombiana de Arquitectos. Estos acuerdos permiten capacitar a profesionales y estudiantes en temas como prevención de riesgos en edificaciones, rutas de evacuación y manejo del fuego.

Daniela Cajamarca resalta que, aunque los Comités nacionales enfrentan problemáticas distintas, comparten retos comunes como la adopción de Inteligencia Artificial y el fortalecimiento de la colaboración público-privada.

“La riqueza de ALAS está en reunir a todos los actores para compartir experiencias y construir soluciones”, concluye.



Daniela Cajamarca
presidenta del Comité ALAS Colombia.

ASOSEC

ASOCIACIÓN COLOMBIANA DE SEGURIDAD

impulsa transformación tecnológica, cohesión gremial y profesionalización

● Colombia afina su músculo estratégico en seguridad privada ante desafíos crecientes.

Barranquilla, Colombia.- Las empresas de seguridad privada en el país se han visto obligadas a reinventarse en medio de un panorama político cambiante y un entorno regulatorio que exige respuestas cada vez más ágiles. El sector, que hoy genera más de 400 mil empleos formales y representa un componente clave del Producto Interno Bruto (PIB) nacional, atraviesa un proceso de adaptación profunda.

Al frente de este esfuerzo se encuentra la Asociación Colombiana de Seguridad (ASOSEC), una de las organizaciones más activas y comprometidas con la transformación gremial en el país.

"Colombia enfrenta una coyuntura compleja que demanda fortalecer nuestras capacidades de análisis, reacción y planeación estratégica", explica Gabriel Berrío, presidente de ASOSEC.

Desde su sede en Barranquilla, la organización trabaja en múltiples frentes para acompañar a las empresas afiliadas frente a los retos del presente: demoras administrativas por la rotación de funcionarios en la Superintendencia de Vigilancia y Seguridad Privada, riesgos como el lavado de activos y el financiamiento del terrorismo, y una presión creciente para incorporar tecnologías disruptivas como la Inteligencia Artificial, drones y soluciones de ciberseguridad.

Como una asociación en movimiento, ASOSEC ha establecido alianzas estratégicas con universidades, cámaras de comercio y entidades públicas clave, promoviendo proyectos de formación y asesoría técnica para sus miembros. Además, ha establecido una interlocución constante con organismos como la Policía Nacional, el Ejército, la Fiscalía General y el Congreso, con el fin de participar activamente en la construcción de políticas públicas y marcos regulatorios adecuados.



Uno de los principales hitos anuales de la organización es el Congreso Nacional de Seguridad, que se ha convertido en un punto de encuentro para líderes gremiales, representantes de entidades gubernamentales y especialistas internacionales. En este espacio se abordan temas como el cumplimiento normativo, la gestión del riesgo y las nuevas tendencias tecnológicas, todo desde una perspectiva de formación, análisis y networking.

A esto se suman diplomados, talleres técnicos, foros temáticos, asesorías personalizadas y sesiones mensuales que ASOSEC realiza de forma sostenida: "Los beneficios para los afiliados son

concretos: acompañamiento permanente, actualización normativa, capacitación constante y representación ante los entes rectores", detalla Berrío.

Según datos de la Superintendencia de Vigilancia y Seguridad Privada, entre 2017 y 2025 el número total de servicios de seguridad privada pasó de 6,171 a 15,387, lo que representa un crecimiento del 149%. Los mayores incrementos se observaron en los rubros de vigilancia sin armas con el 103%, consultoría e investigación casi el doble, y servicios de asesoría y arrendamiento.

Uno de los principales obstáculos que enfrenta el gremio es su fragmentación. Actualmente existen más de 14 asociaciones en el país, lo que diluye la capacidad de interlocución frente al gobierno: "Necesitamos consolidar una voz común. Sin cohesión, es difícil incidir en las políticas públicas que afectan a nuestro sector", afirma el dirigente.

ASOSEC ha emprendido mesas de trabajo con los gremios más representativos para articular una gran alianza nacional. La meta: lograr un reconocimiento institucional que corresponda al peso económico y social del sector, y fortalecer su papel estratégico en la seguridad del país.

Colombia y México: caminos paralelos

En su visión como empresario y dirigente gremial, Gabriel Berrío considera que Colombia sigue siendo un referente en la región gracias a su marco normativo robusto y su capacidad de resiliencia. Pero también reconoce en México a un socio valioso y una industria hermana. "Las amenazas y los riesgos que enfrentamos son similares. El profesional mexicano es altamente competente, y las empresas están a la vanguardia en tecnologías aplicadas a la seguridad y la logística", destaca.



Gabriel Berrío
presidente de ASOSEC.

ANDEVIP
ASOCIACIÓN NACIONAL DE ENTIDADES
DE SEGURIDAD PRIVADA

por la formalidad y alianzas regionales en Colombia

- La asociación representa a más de 150 empresas de seguridad privada, cooperativas y academias en todo el país.
- Alerta por los efectos económicos de la reforma laboral y el crecimiento de la informalidad.
- Mantiene una agenda internacional activa como única agremiación colombiana en la Federación Panamericana de Seguridad.

Bogotá, Colombia.- Desde su fundación en 1983, la Asociación Nacional de Entidades de Vigilancia Privada (ANDEVIP), es la organización gremial más antigua y representativa del sector en Colombia. Con 155 afiliados distribuidos en Bogotá, Medellín, Cali, Bucaramanga y otras ciudades, la organización agrupa a empresas de vigilancia, cooperativas de seguridad, academias y compañías blindadoras, entre otros.



Rodolfo Tamayo Neira, presidente de ANDEVIP, expuso los retos actuales de la industria, los beneficios que representa estar agremiado y la estrategia de fortalecimiento de la asociación en marcha, tanto en el plano nacional como internacional.

De acuerdo con Tamayo Neira, el auge de nuevas asociaciones gremiales ha fragmentado la representación del sector: "Hoy existen al menos 17 gremios en Colombia, muchos nacidos desde ANDEVIP. Pese a ello, somos referente, con una estructura sólida y legalmente constituida que permite interlocución directa con la Superintendencia de Vigilancia y Seguridad Privada, y otras entidades del gobierno".

Uno de los principales beneficios para sus afiliados es el acompañamiento frente a trámites ante las autoridades, muchas veces afectados por lentitud tecnológica o carga burocrática. Además, la asociación participa activamente en la discusión normativa, como ocurrió con la Ley Lorenzo sobre vigilancia con medio canino o con la aplicación gradual de la Ley 2101 que reduce la jornada laboral.

Tamayo advierte que la nueva reforma laboral, junto con la reducción de jornada que entró en vigor el 15 de julio de 2025, tendrá un efecto económico significativo sobre las empresas formales: "Los turnos de 12 horas pueden mantenerse, pero el recargo nocturno se amplía y los costos para los empresarios se elevan más de lo que pueden trasladar en la tarifa. La facturación solo podrá subir un 1.64%, pero los costos crecerán mínimo un 4%. Esa brecha es crítica".

El sector, que ya opera con tarifas reguladas, teme que este desbalance favorezca la aparición de empresas informales que ofrecen servicios por debajo del precio legal, muchas veces vulnerando derechos laborales. "Calculamos que la ilegalidad ya supera el 40% del mercado", denuncia el directivo.

Aunque ANDEVIP no otorga capacitaciones directamente, sí organiza foros, cumbres y congresos donde reúne a empresarios con expertos en tecnología, normatividad y tendencias globales en seguridad. Estos encuentros abordan temas como vigilancia remota, Inteligencia Artificial, nuevas modalidades de servicio y aplicación de normativas recientes.

Entre sus actividades de 2025 destacaron dos grandes eventos: una Cumbre Nacional en Cartagena de Indias organizada en alianza estratégica, y un foro en Bogotá: "Hace tres años fuimos pioneros en unir gremios para realizar congresos conjuntos. En nuestra última edición reunimos a más de 500 empresarios", recuerda.

Proyección internacional y reconocimiento regional

ANDEVIP es actualmente el único gremio colombiano con vicepresidencia ejecutiva en la Federación Panamericana de Seguridad (FEPASEP). Participa anualmente en encuentros internacionales: en 2023 estuvo en México, este año en Paraguay, y ya se prepara para los eventos de 2026 en Brasil y 2027 en Uruguay: "Representamos a Colombia ante otros países y participamos en las decisiones de la región", afirma Rodolfo Tamayo.

El objetivo a corto y mediano plazo es fortalecer la unión gremial para mejorar la percepción institucional del sector y proteger a los empresarios, en especial a las MiPyMEs: "El derecho a agremiarse es esencial. Las reformas afectarán a todos, pero golpearán con más fuerza a las pequeñas y medianas empresas. La unión gremial es lo único que puede garantizar sostenibilidad". ANDEVIP por la formalidad, robustece alianzas regionales para enfrentar cambios laborales en Colombia.



Rodolfo Tamayo Neira
presidente de ANDEVIP.

Por la integración y profesionalización en Colombia, apuesta el



- Representan a más de 37 empresas con alta presencia territorial y enfoque en seguridad residencial.
- Lideran el Congreso de Seguridad de las Américas con alianzas regionales y respaldo de gobiernos.
- Defienden la representación real de las medianas y pequeñas empresas del sector.

Bogotá, Colombia.- En esta nación, más del 90% de las empresas de seguridad privada pertenecen al sector mediano y pequeño, históricamente un grupo poco representado ante las instituciones. Con esa premisa, nació el Consejo Nacional de Seguridad Privada (CNSP), organización gremial que impacta las necesidades reales de ese amplio segmento, fortaleciendo su capacidad de diálogo con el Estado, promoviendo profesionalización y propiciando espacios de integración regional.

César Rodríguez, presidente del organismo, conversa sobre los orígenes del Consejo, el papel que desempeñan empresas asociadas y los alcances de su más reciente iniciativa: el Congreso de Seguridad de las Américas.

"Colombia pasó de tener una sola agremiación fuerte a estar atomizada en más de 10, muchas creadas por intereses políticos o grupos económicos particulares", explica Rodríguez. "Frente a eso, decidimos crear un Consejo que represente verdaderamente a las medianas y pequeñas empresas colombianas, que son la gran mayoría del sector".

Actualmente, el CNSP cuenta con 37 empresas agremiadas, con operaciones en Bogotá, Antioquia, Los Llanos Orientales y otras regiones del país. La mayoría se dedica a seguridad residencial, propiedad horizontal, centros comerciales y contratación pública, además de servicios en instalaciones estratégicas como minas, aeropuertos y plantas petroleras.

El Consejo opera como un organismo articulador: representa al sector frente a la Superintendencia de Vigilancia y Seguridad Privada, al Congreso y otras entidades, asesora a sus miembros en temas jurídicos, normativos y operativos: "No impartimos formación directamente, pero sí articulamos con firmas expertas. Por ejemplo, con la empresa Godoy Córdoba organizamos un webinar gratuito sobre la nueva reforma laboral, al que asistieron más de 430 empresas del sector", relata Rodríguez.

Además, el CNSP desarrolla alianzas con proveedores para facilitar compras colectivas y acuerdos preferenciales en certificaciones, capacitaciones y equipamiento.

Congreso de Seguridad de las Américas, un llamado a la integración

Como parte de su proyección regional, el Consejo organizó por primera vez el Congreso de Seguridad de las Américas, evento académico en la ciudad de Panamá con participación de gremios de México, Centroamérica y el Caribe, así como representantes gubernamentales y expertos en tecnología, Inteligencia Artificial y seguridad pública.

"Queremos que los países empiecen a hablar el mismo idioma en materia de seguridad. No se trata de competir, sino de compartir

buenas prácticas. Lo que México vive hoy, Colombia lo vivió en los 80's y 90's, hay mucho que aprender mutuamente. El evento contó con el respaldo del Ministerio de Seguridad de Panamá", subraya Rodríguez.



También, a corto plazo, el Consejo continuará trabajando por la integración gremial, el fortalecimiento jurídico de sus miembros y la capacitación profesional del sector. Según datos de la Superintendencia, más de 400 mil personas trabajan hoy en seguridad privada en Colombia, lo que implica un impacto social directo en más de un millón de personas.

"Queremos ser asesores también de los gobiernos. Muchos Ministerios de Seguridad en Centroamérica no cuentan con formación ni estructura. Colombia y México ya están a la vanguardia, pero podemos y debemos acompañar a la región en la construcción de una seguridad profesional y sostenible", concluye César Rodríguez.



César Rodríguez
presidente del CNSP.



SERCOPP

SERVICES & CONSULT

Servicios de consultoría y
personal profesional

Sercopp asesora activamente en las operaciones que involucran activos virtuales, así como en la asesoría a entidades en la adopción de políticas internas que permiten cumplir con las nuevas regulaciones que se expanden sobre la materia, y los representa mediante un servicio **BPO** de **COMPLIANCE OFFICER**, quien se encarga de liderar su Unidad de Cumplimiento.

- ESTUDIOS DE CONFIABILIDAD
- OFICIAL DE CUMPLIMIENTO
- SERVICIO DE POLIGRAFÍA
- SEGURO DE RESPONSABILIDAD CIVIL
PROFESIONAL RCP
- AUDITORÍAS INTEGRALES DE SEGURIDAD

 Dg. 81i #74C-19, Bogotá, D.C. Colombia
 +57 3108052421
 gerenciasercopp@gmail.com

www.sercopp.com



Los jóvenes autistas y la seguridad



Herbert Calderón Alemán

Oficial retirado de la Marina de Guerra. Magister en Seguridad y Defensa Nacional, Master en Criminología, Master en Seguridad Laboral, actualmente Doctorando en Criminología. Triple certificado en ASIS Internacional

Articulista invitado



Lima, Perú.- El autismo o Trastorno del Espectro Autista, denominación utilizada actualmente, se refiere a un conjunto de trastornos relacionados entre sí que se desarrollan en la infancia y a una serie de características y dificultades en el desarrollo del niño que pueden mantenerse durante toda su vida.

El Trastorno del Espectro Autista (TEA) es un trastorno neurobiológico del neurodesarrollo presente desde el nacimiento o durante la primera infancia. Se manifiesta en el trayecto vital de la persona a través de una variedad de grados de vulnerabilidad de capacidades cognitivas, adaptativas, motoras, integrativas, comunicativas y relacionales. En consecuencia, este puede abarcar y subyacer todas las singularidades culturales y sociales.

En el ámbito laboral, la inclusión y aceptación de personas con diversidad funcional están sujetas a muchas variaciones entre países e industrias. En EE.UU., un 17% de las industrias observaban un crecimiento en la contratación de personas con alguna discapacidad, mientras que un 17% también reportaba haber implementado programas específicos para trabajadores con discapacidad. Sin embargo, más de un 52% de los sectores no contemplaban en sus estrategias a estos trabajadores.

Algunas de las ventajas que aporta este enfoque de diversidad funcional en las empresas son la variedad y opiniones diferentes, adaptabilidad frente la diversidad, captar otros públicos que incrementan el mercado, valiosas capacidades, crecimiento personal, mayor conexión emocional y finalmente, un mejor desempeño.



La profesión de "seguridad" está centrada en resguardar la vida, la integridad y los bienes de las personas y las instituciones. Es una labor exigente que requiere la implementación y control de sistemas de protección constantemente en el tiempo, que debe estar atenta frente a las diferentes situaciones críticas y potencialmente adversas que puedan tener lugar. Implica políticas de prevención y gestión frente a incidentes graves y delitos como hurtos, incendios e inclusive desastres naturales.

Para que la misión de proteger se cumpla, el recurso humano constituido por los profesionales del área tiene una fuerte influencia en los resultados. Dentro de los parámetros que actúan con mayor relevancia destacan las habilidades y capacidades de los funcionarios de seguridad. Con estas habilidades de alta calidad y en continuo desarrollo, junto a equipos tecnológicos de alto perfil, se conforman "los sistemas de seguridad".

El autismo, particularmente dentro del espectro del Trastorno del Espectro Autista (TEA), puede aportar una serie de ventajas en profesiones relacionadas con la seguridad, dependiendo del perfil específico de la persona y del tipo de trabajo. Aquí algunas ventajas potenciales que pueden ser especialmente valiosas en este ámbito:

1. Atención al detalle. Muchas personas autistas tienen una capacidad sobresaliente para notar patrones, errores o anomalías que podrían pasar desapercibidos para otros. Esto es clave en: Monitoreo de cámaras de vigilancia, revisión de documentos o registros, detección de comportamientos inusuales.

2. Pensamiento lógico y estructurado. El pensamiento sistemático y ordenado es útil en tareas que requieren seguir protocolos de seguridad, analizar riesgos, o resolver situaciones de forma objetiva.

Ideal para tareas de evaluación de riesgos o cumplimiento de normas. Útil en ciberseguridad, donde se requiere análisis lógico constante.

3. Preferencia por rutinas y cumplimiento de normas. Muchos autistas encuentran comodidad en las rutinas y en el seguimiento de reglas claras, lo cual encaja perfectamente en profesiones de seguridad que requieren procedimientos estrictos y protocolos fijos.

4. Fuerte sentido de la justicia y responsabilidad. Algunas personas autistas tienen un alto compromiso con lo que consideran correcto, lo cual puede traducirse en una ética profesional fuerte y en una actitud vigilante frente a irregularidades o amenazas.

5. Discreción y enfoque. En trabajos donde se requiere mantener confidencialidad o trabajar en entornos silenciosos o sin necesidad de mucha interacción social, algunas personas autistas pueden destacar, especialmente si prefieren entornos con baja estimulación social.

Ejemplos de roles en seguridad donde estas fortalezas pueden ser valiosas: operador de vigilancia (CCTV), analista de ciberseguridad, control de acceso o monitoreo de alarmas, evaluación de riesgos o cumplimiento normativo, técnico en sistemas de seguridad.

Importante: No todas las personas autistas son iguales. Las habilidades y desafíos varían enormemente dentro del espectro. La clave está en adaptar el entorno y los roles para aprovechar al máximo las fortalezas individuales, respetando sus necesidades. 🌐

Aclaremos el panorama. ¿Gestión de riesgos o gestión basada en el riesgo?



Audy Francisco Puyosa

MSc. Profesional con más de 25 años desarrollando funciones en Seguridad y Salud Laboral, en cargos de dirección, consultoría y formación. Autor de libros y ponente internacional.

Articlista invitado



Santo Domingo, República Dominicana. - En una era donde la información parece estar al alcance de los dedos, una consulta rápida nos pone en camino hacia una ingente cantidad de datos, y las decisiones suelen requerir premura; contar con indicadores, esquemas y valoraciones pasa a ser una necesidad para todas las organizaciones.

Entre las muchas variables que resultan ser de interés, el riesgo es, por mucho, uno de los datos más valorados entre las líneas de gerencia. Ahora, este riesgo puede significar diferentes cosas para cada escenario o necesidad.

Partiendo de la premisa de que cada organización afronta diferentes escenarios potencialmente adversos (o beneficiosos), el riesgo pasa a ser una herramienta con base estadística para la toma de decisiones. Nótese que se habla de una herramienta y no de un agente, actor o aspecto tangible dentro de los procesos; por el contrario, es un concepto abstracto al cual algunos autores buscan ponerle un rostro o darle entidad propia.

A diferencia de los eventos no deseados, los escenarios adversos, las causas, consecuencias, vulnerabilidades y amenazas; el riesgo no es un "algo" sino un "cómo". Es una forma que se ha ideado para dar escala y priorizar diferentes aspectos de interés para la toma de decisiones. Mientras todos los aspectos mencionados pueden identificarse en cualquier momento de la historia humana, el riesgo es un concepto relativamente nuevo, que nace recién con el desarrollo del cálculo estadístico.

Haciendo un poco de historia, aunque la aplicación de las primeras valoraciones asociables con las estadísticas puede identificarse durante la realización de los censos (recogida y tratamiento de la información) en tiempos tan remotos como el 3.050 a. C., en Egipto; el término "estadística" recién se acuñó en el siglo XVIII, por el trabajo de autores como Gottfried Achenwall; a pesar de que las herramientas de cálculo estadístico (Teoría de la Probabilidad y la Inferencia Estadística) podemos atribuirla a autores como Fermat o Pascal en el siglo XVII.

Para entender esta perspectiva, hagamos un símil con otra función matemática: la suma. Cuando queremos conocer el total de reunir bajo un mismo marco de referencia una variedad de elementos dispersos o agrupados en conjuntos; todos de las mismas características, naturalmente; aplicamos una abstracción

matemática que permite conocer el total de dichos elementos. Es decir, la suma como tal no es un aspecto material sino un proceso del pensamiento consciente y voluntario. Y más que innato, es aprendido.

De igual manera, el riesgo es un proceso que permite, merced a un análisis (cuantitativo o cualitativo), entender la tendencia o magnitud relativa entre diferentes escenarios de interés; con lo cual podemos establecer un orden o prioridad necesaria para afrontarlos. Por tanto, el riesgo no es el elemento sobre el cual pretendemos ejercer control sino el mecanismo que nos permitirá tomar la decisión.



Una vez que entendemos que el riesgo no es un elemento natural sino un constructo sociológico, empezamos a dar una justa dimensión a todo cuanto se deriva de él. Podemos enfocar nuestra vista en lo realmente importante: el aspecto de interés. El riesgo pasa a ser ese elemento indicador asociado a la toma de decisiones; el mapa u hoja de ruta desde los datos hasta esas decisiones. De ahí que sea un paso más (aunque clave) dentro de la gestión organizacional.

Para ponerlo en términos mucho más gráficos; el riesgo es el dedo que señala hacia donde están los elementos que debemos afrontar. Y si nos quedamos mirando el dedo que apunta, podemos perder de vista el autobús que se dirige hacia nosotros a toda velocidad. 🚌

Impulsa seguridad IAAPA® en parques y atracciones

- El Mes de la Seguridad IAAPA 2025 reunió a expertos globales para reforzar el compromiso de la industria de parques y atracciones con la protección.
- Iniciativa internacional que une educación, colaboración e innovación a través de eventos virtuales y presenciales.

Cada año, más de 332 millones de personas visitan parques de diversiones, temáticos, acuáticos, centros de entretenimiento familiar, zoológicos, acuarios, entre otras atracciones en América Latina y el Caribe, de acuerdo con IAAPA la Asociación Global para la Industria de las Atracciones.

A ese total, México aporta 74.5 millones de visitantes anualmente, esta cifra no solo refleja la popularidad de esta industria, sino también el nivel de confianza que millones de visitantes depositan en ella cada año. Detrás de cada atracción, existe un compromiso inquebrantable con la seguridad mantenido por más 528 mil profesionales en la región, siguiendo estándares y protocolos de seguridad.

Mes de la Seguridad IAAPA

La oficina de IAAPA para América Latina y el Caribe presentó la edición 2025 del Mes de la Seguridad IAAPA, iniciativa internacional que une educación, colaboración e innovación a través de eventos virtuales y presenciales. El objetivo: elevar las prácticas de seguridad en parques, atracciones y centros de entretenimiento familiar, entre otros.

"En IAAPA sabemos que la seguridad es la base de las operaciones en nuestra industria. La capacitación continua es esencial para construir y mantener una fuerte cultura de seguridad que garantice experiencias memorables y seguras" señala Paulina Reyes vicepresidente y directora ejecutiva de IAAPA América Latina, Caribe. "El Mes de la Seguridad IAAPA ofrece una oportunidad única para aprender, conectar e intercambiar ideas con profesionales de la industria en toda la región".

Durante el pasado mes de mayo, profesionales y expertos de la industria se reunieron de manera virtual y presencial para compartir buenas prácticas, explorar estrategias innovadoras y fomentar una cultura proactiva de seguridad y prevención. La oferta en línea de esta iniciativa incluyó una masterclass, un simulacro virtual, así como foros y paneles con una red global de expertos, diseñados para fortalecer las operaciones, proporcionar conocimientos y una cultura de prevención, así como herramientas prácticas para una mayor seguridad en las operaciones. Los interesados en extender la experiencia del Mes de la Seguridad, se registraron

además en un Bootcamp práctico de dos días en el parque de diversiones Mundo Petapa, en Guatemala.



Además de los eventos, los asistentes contaron con acceso a contenidos educativos grabados, materiales de apoyo descargables y herramientas digitales que les permitió implementar de inmediato lo aprendido en sus organizaciones. Para asegurar el acceso global a esta información, IAAPA utiliza tecnologías avanzadas de traducción, asegurando que los recursos educativos estén disponibles en múltiples idiomas y puedan beneficiar a la industria en todo el mundo.

Gracias a sólidos protocolos de seguridad, a la innovación constante y a un personal altamente calificado, la industria de las atracciones sigue ofreciendo experiencias seguras y memorables a millones de familias alrededor del mundo. 🌍

México registra gran atraso en materia de **Protección Civil**

- Se ha avanzado en cuestión de sismos, pero aún tenemos grandes carencias en materia de prevención de incendios.
- En el primer semestre de 2025 se registraron pérdidas por 12 mil millones de pesos, y diariamente se suscitan en territorio nacional 260 incendios.

Guadalajara, Jalisco.- México tiene un gran atraso en materia de protección civil que se debe corregir de inmediato para evitar muertes y daños económicos. Y es que en el primer semestre de 2025 se registraron ya 12 mil millones de pesos en pérdidas por incendios.

Por ello es necesario que juntos, gobierno, industria y sociedad en general actúen y generen políticas públicas para, como en el caso de los sismos, preparar a la población para saber qué hacer en caso de incendios en casas, escuelas, oficinas, comercios y fábricas, pero sobre todo cómo prevenirlos y evitarlos, aseguró Juan José Camacho Gómez, presidente del Consejo Nacional de Protección contra Incendios (CONAPCI).



A su vez, Juan Francisco Guzmán Hernández, presidente de la Asociación Mexicana de Rociadores Automáticos Contra Incendios (AMRACI) informó que en el territorio nacional se registran al año más de 95 mil incendios urbanos y no urbanos, es decir 260 al día, según datos del INEGI.

Ambos especialistas en materia de prevención de incendios participaron en la inauguración de la 8ª Expo Fire & Safety 2025, que se llevó a cabo en la ciudad tapatía de México.

El presidente de AMRACI advirtió que el 31% de los desastres en México son ocasionados por los incendios, que son responsables del 26.1% de la totalidad de la mortalidad por humo y gases tóxicos.

Esto, sin duda es muestra del gran impacto que tienen los incendios, que, a diferencia de los sismos y huracanes, no reciben la misma importancia de las autoridades e incluso de la misma sociedad, a pesar de que provocan mayores daños que estos últimos.

Asimismo se dieron a conocer avances del programa "Aprende a Mantenerte Seguro" para niños de preescolar y primaria que se pretende implementar en todo el país y se llevó a cabo en "Rally de Prevención" el cual estuvo conformado por diversas actividades educativas en las que se enseñó a niños pequeños cómo actuar en casos de incendios.

Durante el mismo evento, AMRACI y CONAPCI concretaron la firma de un convenio de colaboración con la Secretaría de Educación Pública del estado de Jalisco, para aplicar en la entidad dicho programa que consiste en capacitar a los niños en qué hacer previo, durante y posteriormente a un incendio, pero, sobre todo, en cómo provenirlo y evitarlo.

Esta firma de convenio es punta de lanza en el país, al poner en marcha de manera conjunta esta prueba piloto del programa de educación en materia de prevención de incendios en niños de tercer año de educación básica, en planteles ubicados en zonas de alta vulnerabilidad.

Por su parte, Bomberos de Madrid, España donaron equipo y capacitaron a sus homólogos del estado de Jalisco sobre nuevas técnicas para la prevención y combate de incendios urbanos; en especial mostraron nuevas formas de enseñanza a niños y jóvenes para que estén alertas y sepan cómo actuar ante siniestros de este tipo, en sus casas y escuelas.

La inauguración del evento a nombre del gobernador del estado Pablo Lemus Navarro, estuvo a cargo de la Coordinadora General Estratégica de Gestión del Territorio, Karina Hermosillo Ramírez. En el acto, ambos organismos otorgaron un donativo por 100 mil pesos a la fundación Michou & Mau que encabeza su presidenta Virgina Sendel, para la atención de niños quemados.

La Expo Fire & Safety contó con la participación de diversos especialistas en materia de prevención de incendios provenientes de varios estados de la República, así como de Costa Rica, República Dominicana, Perú, Brasil, Colombia, Paraguay, Ecuador y Estados Unidos.



A lo largo de 240 stands se presentaron las últimas tendencias de prevención y protección de riesgos por la llegada de tecnologías emergentes, baterías de litio, almacenamiento, manufactura, edificios altos y centros de datos, privilegiando la seguridad humana y la continuidad de operaciones.

Participaron los proveedores líderes y las soluciones más avanzadas en protección pasiva, detección, alarma y supresión de conflagraciones, así como personalidades varias del sector de la prevención de incendios. 🇪🇺

Nueva serie de paneles INSPIRE de Honeywell

- Con Connected Life Safety Services (CLSS) para simplificar la instalación, el mantenimiento y el cumplimiento de normativas.

La empresa global en tecnologías de protección contra incendios y seguridad para la vida, Honeywell, presenta NOTIFIER INSPIRE, sistema de protección contra incendios todo en uno que ofrece un rendimiento fiable, monitoreo inteligente, mantenimiento simplificado e integración perfecta. El sistema se conecta a la plataforma Connected Life Safety Services (CLSS) de la firma, proporcionando información en tiempo real y aumentando la productividad de los técnicos.

Asimismo, la marca también está lanzando en México el detector de humo Self-Test, que automatiza el diagnóstico para verificar el estado del dispositivo y el cumplimiento de las normas NFPA 72, mejorando la seguridad y reduciendo la necesidad de inspecciones manuales.

Ventajas del producto:

La serie NOTIFIER Self-Test cuenta con los primeros detectores homologados por UL capaces de realizar pruebas totalmente automatizadas. Esta revolucionaria innovación está lista para transformar la forma en que se instalan, prueban y mantienen los sistemas de seguridad contra incendios.

Las pruebas de seguridad tradicionales pueden ser lentas, caras y molestas, especialmente en espacios cerrados, zonas de difícil acceso o edificios con techos altos. Estas dificultades hacen que a menudo no se comprueben los detectores, lo que pone en peligro la seguridad.

Los detectores NOTIFIER Self-Test superan estos obstáculos con una tecnología de autodiagnóstico patentada y aprobada por UL. Cada dispositivo puede generar calor y humo internamente para verificar la funcionalidad de los sensores térmicos y fotoeléctricos, a la vez que garantiza que los puntos de entrada de humo permanezcan despejados y sin obstrucciones.

Gracias a las avanzadas funciones de autodiagnóstico de NOTIFIER, incluso los sistemas en red más grandes pueden comprobarse de forma rápida y eficaz, lo que permite ahorrar tiempo, reducir costos y mejorar la seguridad general contra incendios.

"Con el lanzamiento de INSPIRE, reafirmamos nuestro compromiso de ofrecer soluciones de detección de incendios no sólo tecnológicamente avanzadas y fáciles de usar, sino también adaptadas a las necesidades locales en Latinoamérica. Este sistema además de mejorar la seguridad, garantiza una integración perfecta con la infraestructura existente, reforzando nuestra misión de proteger vidas y activos valiosos", comenta Neove Pipper, director general de Building Automation para Latinoamérica.

Aspectos a destacar:

- Refuerza el compromiso de Honeywell con edificios más seguros e inteligentes.
- Reduce el tiempo de los técnicos in situ con diagnósticos remotos.
- Ofrece soluciones de protección contra incendios escalables y rentables.
- Respalda el cumplimiento de normativas y la eficiencia operativa en todos los mercados de Latinoamérica. 



México se suma al ICC para evitar daños por incendios

- Adoptará para la industria de la construcción nacional códigos y estándares internacionales de actuación.
- En los últimos 4 años se registraron pérdidas por 34 mil millones de pesos a causa de los incendios.

Guadalajara, Jalisco.- Para evitar que los incendios sigan causando graves daños y pérdidas, México, a través de la Asociación Mexicana de Rociadores Automáticos Contra Incendios (AMRACI) y el Consejo Nacional de Protección Contra Incendios (CONAPCI), se sumarán y adoptarán los códigos y estándares de actuación del International Code Council (ICC) para la seguridad y las experiencias exitosas de naciones latinoamericanas.



El foro que cambió la forma de ver a la industria

¡Gracias por acompañarnos en la 8ª edición de **Expo Fire & Safety 2025!**



Para ello, directivos de estos organismos se reunieron en nuestro país para compartir información y firmar los acuerdos de colaboración correspondiente, encabezados por David Morales, vicepresidente de AMRACI; Juan José Camacho, presidente de CONAPCI; José Roig, miembro del Consejo Directivo del ICC y Víctor Espínola, director general de AMRACI y CONAPCI.

A nombre del ICC, José Roig, explicó que este organismo es la principal fuente mundial de códigos y normas modelo, así como de soluciones para la seguridad en la construcción.

Por ello, brindarán colaboración a AMRACI y CONAPCI en cuanto a la evaluación de productos, acreditación, tecnología, capacitación y certificación. Los códigos, normas y soluciones del ICC se utilizan para garantizar comunidades y edificios seguros, asequibles y sostenibles en todo el mundo.

Toda esta experiencia se sumará a los esfuerzos que lleva a cabo AMRACI y CONAPCI para prevenir las conflagraciones urbanas, las cuales han sido de más de 34 mil millones de pesos en pérdidas registradas en los últimos cuatro años, según informe de las principales instituciones de seguros del país.

De ahí la importancia de atender y prevenir ese tipo de accidentes, los cuales son los responsables del 31% de los desastres en territorio nacional y del 26.9% de la mortalidad asociada.

En la reunión, los directivos destacaron que los incendios urbanos en México se han convertido ya en un grave problema de salud pública y, a diferencia de los sismos o huracanes, se presentan con mayor frecuencia de lo que parece. Anualmente se registran más de 95 mil incendios urbanos y no urbanos. 260 al día, según el Instituto Nacional de Estadística y Geografía (INEGI).

De ahí la importancia de la 8ª edición de Expo Fire & Safety, el evento mundial en protección contra incendios en México y Latinoamérica, que se realizó por vez primera en Guadalajara, Jalisco. Este evento abordó la alarmante problemática de incendios que azotan a diversos estados de la República Mexicana impactando todos los sectores económicos y la vida de miles de personas.

Juan Camacho Gómez, presidente de CONAPCI, informó que en México en los últimos 10 años más de 6 mil personas fallecieron por exposición a fuego no controlado. Los grupos más afectados son niños y adultos mayores.

Por su parte David Morales, vicepresidente de AMRACI, comentó que la industria de protección contra incendio es uno de los sectores que tiene un impacto transversal en todas las actividades económicas y sectores industriales, comercio y turismo, y ahora en el nearshoring.

Por tanto, al incidir en prácticamente todos los sectores industriales, podría representar un verdadero riesgo para la salvaguarda de la vida de las personas, continuidad de operaciones y la competitividad de una industria.

AMRACI y CONAPCI representan a más del 70% del sector de protección contra incendios en México. Son la voz de la industria con objeto de impulsar, mejorar, legislar, profesionalizar y promover la cultura de prevención y protección a través del desarrollo de normas, códigos, buenas prácticas de diseño, instalación y mantenimiento con el fin de salvar vidas y proteger propiedades promoviendo una industria ordenada que permita un crecimiento sostenible

Expo Fire & Safety 2025

Por su parte, Víctor Espínola, director de AMRACI y CONAPCI, se refirió a la realización de la Expo Fire & Safety 2025, el cual es un foro único que reunió a las personalidades y proveedores más importantes a nivel global.

Permitió actualizarse con las tendencias de prevención y protección de los riesgos que demandan las distintas industrias con la llegada del nearshoring, en materias como tecnologías emergentes, uso de baterías de litio, almacenamiento, manufactura, edificios altos, centros de datos; privilegiando siempre la seguridad humana y la continuidad de operaciones.

El evento contó con una gran convocatoria nacional e internacional, en ella se dieron cita:

- 4,500 asistentes
- 400 congresistas en las Máster Class
- 25 estados de la República
- 12 países visitantes
- 8,700 metros de exhibición
- 230 stands

Asimismo, se presentó el Museo Itinerante de Prevención de la Fundación Michou & Mau; y se realizó un rally presentación del Programa de Educación Pública "Aprende a Mantenerse Seguro" para niños de primaria con participación de la SEP y DIF Jalisco. 🌐

Análisis comparativo:

Evolución de la protección ejecutiva – De la discreción física a la seguridad integral



Dr. John Tovar Cartaya
CPO, Especialista en Seguridad Integral
Comisario General CICPC Venezuela
Articulista invitado



Introducción

Caracas, Venezuela.- La protección ejecutiva ha experimentado una transformación paradigmática en el último quinquenio, evolucionando desde un servicio de seguridad física reactiva hacia un modelo integral de gestión de riesgos. Este análisis contrasta ambos enfoques, destacando los cambios fundamentales en conceptos, metodologías y tecnologías.

Modelo tradicional (2019): La era de la discreción física

El enfoque preponderante hace cinco años se caracterizaba por su naturaleza esencialmente física y táctica, estructurada alrededor de principios de disuasión visible y contención de amenazas inmediatas.

Características principales:

- Enfoque físico-reactivo: Basado en técnicas de escolta, defensa personal y planificación de rutinas seguras
- Evaluación de riesgos tradicional: Análisis puntuales basados en OSINT básica e informes convencionales
- Tecnología auxiliar: Equipamiento centrado en vehículos blindados, comunicaciones por radio y escáneres portátiles
- Compartimentación operativa: Separación entre seguridad física, logística y ciberseguridad

Limitaciones críticas:

- Vulnerabilidad ante amenazas asimétricas
- Escasa adaptabilidad a entornos dinámicos
- Dependencia excesiva de percepción humana no asistida

Modelo contemporáneo (2025): La seguridad integral

El paradigma actual se define por su carácter multidimensional y proactivo, integrando protección física con capacidades tecnológicas avanzadas.

Componentes Esenciales:

- Fusión de dominios: Integración orgánica entre seguridad física, ciberseguridad personal y gestión de información
- Inteligencia anticipativa: Sistemas de monitoreo predictivo y análisis de patrones de riesgo
- Automatización de procesos: Tecnologías SOAR para gestión integral de incidentes
- Resiliencia operativa: Capacidad de mantener operatividad bajo condiciones adversas

Tecnologías clave:

- Plataformas unificadas de comando y control
- Sistemas de reconocimiento biométrico y facial
- Dispositivos IoT para monitoreo ambiental
- Análisis predictivo mediante machine learning

Análisis comparativo de capacidades

Tecnología 2019 vs. 2025:

- Comunicaciones: Radios UHF/VHF → plataformas unificadas
- Vigilancia: CCTV básico → reconocimiento facial y biométrico
- Análisis: Evaluación manual → machine learning predictivo
- Movilidad: Vehículos blindados → dispositivos IoT y drones

Metodologías operativas:

- Planificación: Experiencias previas → análisis en tiempo real
- Gestión: Comunicación vertical → flujos multidireccionales
- Capacitación: Habilidades físicas → Competencias multidisciplinarias

Innovaciones transformadoras

La fusión de dominios representa el avance más significativo, disolviendo las barreras entre seguridad física y digital. La inteligencia artificial permite ahora analizar sentimiento en redes sociales e identificar patrones de vigilancia hostil, capacidades impensables hace cinco años.

Los dispositivos wearables de emergencia transmiten ubicación exacta, audio ambiental y métricas biométricas en tiempo real, mientras los drones proporcionan capacidades de reconocimiento y respuesta rápida.

Perspectivas futuras

Las tendencias emergentes apuntan hacia:

- Hiper-personalización mediante "gemelos digitales"
- Biometría conductual para autenticación continua
- Protección predictiva basada en análisis de tendencias macro
- Modelos de seguridad como servicio (Security as a Service)

El desafío crítico será equilibrar la hiper-conectividad con la privacidad del ejecutivo y la eficacia operativa.

Conclusiones

La evolución demuestra una maduración significativa de la disciplina, donde:

1. La integración tecnológica transforma la protección en ciencia estratégica
2. El análisis predictivo constituye la ventaja competitiva fundamental
3. La convergencia físico-digital resulta irreversible
4. El perfil profesional requiere evolución constante hacia competencias multidisciplinarias

Esta transformación representa una evolución -no abandono- de los principios fundamentales, hacia un modelo más comprehensivo, inteligente y efectivo. 🌐

Convirtiendo la seguridad física reactiva a proactiva



Juan Carlos Granier

Consultor en Seguridad y Protección Física.
Miembro por República Dominicana al
Consejo Consultivo Latino de IFPO.

Articulista invitado



Santo Domingo, República Dominicana. - En estos últimos años, la Inteligencia Artificial (IA) ha ido evolucionando hasta convertirse en una herramienta utilizada para agregar valor a la seguridad física. Hoy, está presente en torno a nosotros en centros de monitoreo, sistemas de control de acceso, de videovigilancia, incluso en la gestión de riesgos aportando la capacidad de predecir y anticipar lo que antes solo podíamos registrar después de que sucediera.

La seguridad fue en gran medida reactiva durante mucho tiempo actuando después de que ocurre un incidente, un evento, una alerta o una intrusión, generando información sin contexto, evolucionando hacia la necesidad de crear cambios que provocaran una acción más proactiva ante las amenazas que son cada vez más elusivas y dinámicas, y que a la velocidad con la que estas llegan hace que necesitamos de soluciones que aprendan a anticipar, predecir y accionar medidas junto a nosotros más rápidas y eficientes.

Es aquí en este punto donde la IA marca una diferencia predominante. Hoy en día, los sistemas de seguridad basados en IA, logran procesar cientos de imágenes en segundos y detectar comportamientos anómalos en una persona que se encuentre por ejemplo, merodeando de forma sospechosa, sosteniendo un arma, un vehículo estacionado donde no debería estar o un objeto dejado demasiado tiempo en un lugar sensible, además de agregar una capa de comprensión contextual con una percepción casi a nivel humano, con la capacidad de análisis continuo de las transmisiones de video en tiempo real durante 24 horas, aumentando la productividad y eficiencia de los oficiales de seguridad encargados de la protección con la capacidad de generar indicadores que nos ayuden a medir que tan eficiente es nuestra respuesta ante la materialización de las amenazas.

De igual manera esta evolución de la IA ha cambiado la forma en que percibimos el riesgo. Ya no estamos limitados a auditorías constante en análisis forense de la información pudiendo generar y analizar grandes cantidades de datos y encontrar patrones que antes habríamos pasado por alto, como, por ejemplo, decidir en qué lugar o turno es más probable que ocurran incidentes y ajustar los controles sobre esos puntos.

La IA permite la automatización de decisiones operativas. Dentro de un centro de monitoreo, los sistemas también pueden clasificar alertas, ordenarlas según su nivel de emergencia e incluso activar

procedimientos de respaldo sin intervención humana. Esto libera a los operadores para realizar un trabajo más reflexivo como la verificación y coordinación de respuestas.

La tecnología, por supuesto, no es todo. La IA requiere buenos datos, reglas específicas y vigilancia constante. Un sistema inteligente no reemplaza la experiencia del personal de seguridad, si no que facilita y optimiza su trabajo haciéndolo más eficiente, complementándose a través de un modelo convergente donde la IA procesa datos en tiempo real y el equipo encargado de la seguridad decide con juicio y responsabilidad las acciones a tomar.

Es por ello podemos afirmar que nos encontramos en una transición hacia un punto donde la seguridad física y la IA están estrechamente interconectadas. Los sistemas de seguridad ya no actúan por separado cámaras, sensores, ciberseguridad y control de acceso operan todos juntos. En este nuevo entorno convergente, la IA sirve como la red central que los une a todos, facilitando una forma de gestión de riesgos mucho más sinérgica y efectiva.



Al final del día, la IA está redefiniendo cómo cuidamos lo que más valoramos. Nos permite pasar de un enfoque reactivo a predictivo y proactivo, donde la prevención es realmente el poder. Pero independientemente de los algoritmos y plataformas, el ejercicio del juicio humano sigue siendo esencial. La tecnología es velocidad y precisión; nosotros añadimos experiencia y sentido ético. Y cuando ambos lados están en equilibrio, se obtiene una seguridad más segura, inteligente y humana. 🤖

¿Qué APPS utiliza un protector?



Gustavo Merani CPO
Especialista en Protección Ejecutiva
Articulista invitado



Buenos Aires, Argentina.- La protección ejecutiva evolucionó. La tecnología se convirtió en un aliado estratégico para todos los que trabajamos en protección. Las aplicaciones móviles son herramientas digitales que potencian nuestra operación. Con el fin de conocer la relevancia de su empleo, consultamos a distintos colegas de la región para que mencionarán cuáles eran las apps más utilizaban en su móvil.

Hay apps que en ciertos países no están disponibles y que hay operadores que usan iOS como sistema operativo y otros Android, sin mencionar los sistemas operativos cifrados que utilizan equipos de protección de organismos estatales o equipos exclusivos como el Samsung Galaxy S23 Tactical Edition.



Sugerimos evitar el uso de aplicaciones de descarga gratuita, en caso de hacerlo recomendamos leer cuidadosamente la lista de permisos, las valoraciones de otros usuarios y sus opiniones; utilicemos apps pagadas las cuales tienen un soporte mayor.

Debemos tener en cuenta puntos fundamentales para la operación diaria de un equipo de protección corporativo en cuanto al uso de apps:

1. Comunicación segura y en tiempo real.

Las aplicaciones de mensajería encriptada permiten coordinar movimientos, dar instrucciones discretas y mantener al equipo interconectado en entornos de riesgo. La reducción de la vulnerabilidad frente a interceptaciones resulta fundamental.

2. Geolocalización y seguimiento.

Las apps de rastreo permiten conocer en tiempo real la ubicación del protegido, del vehículo y de los miembros de nuestro equipo. Esta función facilita la toma de decisiones en situaciones dinámicas para planificar rutas alternativas, detectar desvíos sospechosos o responder rápidamente ante una contingencia.

3. Gestión de riesgos y alertas.

Existen plataformas que integran información de inteligencia: niveles de amenaza en determinadas zonas, alertas de disturbios, reportes meteorológicos y datos de tránsito.

4. Control de accesos y verificación de identidades.

Hay aplicaciones que permiten administrar credenciales digitales, escanear identificaciones y gestionar accesos a eventos o instalaciones.

5. Riesgos asociados al uso de aplicaciones:

Nos plantea desafíos como el riesgo de

filtración de datos o hackeos, confiar en la herramienta digital y también la geolocalización puede traernos una sorpresa.

¿Cuáles son las apps más utilizadas?

La primera es la de mensajería. WhatsApp seguida por Signal, Telegram, Threema; luego son muy utilizadas Waze, Google Maps y Magic Earth y también LIFE360. Otra muy recomendada What 3 Words; Zello para comunicación similar a un radio y también Notion como un espacio donde todos pueden aportar y crear documentos para centralizar la información. CamScanner para escanear documentos, anuncios y convertirlos a archivos .pdf o .jpeg fue recomendada por usuarios de Android, al igual que la app "Notas" nativa de Iphone.

Para no hacer un listado de apps más descargadas por equipos de protección menciono las "categorías":

- 1) Navegación y tráfico
- 2) Seguimiento de vuelos
- 3) Clima
- 4) Comunicación
- 5) Inteligencia artificial
- 6) Correos electrónicos seguros
- 7) Grabadora de voz y de llamadas
- 8) Primeros socorros
- 9) Borrado de información
- 10) VPN

Debemos agregar a la mochila de nuestros operadores una bolsa Faraday por si necesitamos proteger nuestros equipos o si por algún motivo debemos guardar un teléfono móvil de un tercero y queremos evitar que accedan a él, en forma remota.

¿Y el móvil de nuestro protegido?

A medida que la seguridad dentro de las corporaciones avanza, los ciberdelincuentes atacan cada vez más a individuos en forma personal con acceso a información confidencial de alto valor, comprometiendo sus redes domésticas e infectando dispositivos no protegidos con Malware y Ransomware.

En los últimos años, vimos numerosos ataques contra ejecutivos de corporaciones de primer nivel como Microsoft, Twitter, Amazon y Meta y muchos más ocurren sin ser reportados por los medios, por la sencilla razón de no mostrar que fueron vulnerados y mostrarse débiles. Los ciberdelincuentes exploran una combinación de preocupaciones sobre privacidad, limitaciones legales, restricciones de recursos y exposición de información que impide a los equipos corporativos proteger completamente la vida digital personal de sus ejecutivos. Se han convertido en el camino de menor resistencia para actores de amenazas motivados y un trampolín hacia su objetivo

final. Los atacantes suelen dirigirse a redes domésticas y dispositivos con escasa seguridad, aprovechando contraseñas recurrentes y tácticas avanzadas como suplantaciones con Deepfakes.

Dato:

El 68% de los profesionales de seguridad considera probable que su protegido reutilice una contraseña comprometida de sus cuentas personales dentro de la corporación.

Solo el 43% de los encuestados proporcionan capacitación a los ejecutivos para proteger sus activos digitales personales.

Los ataques más comunes siguen siendo el Malware en dispositivos personales o familiares y la exposición de información personal como la dirección particular, el número de teléfono y el correo electrónico personal.

Los actores de amenazas están explotando rápidamente sus capacidades para extraer datos de objetivos en internet, creando perfiles o comunicaciones realistas que podrían engañar incluso a las personas más cuidadosas. Los ataques Deepfake dirigidos a ejecutivos han aumentado en los últimos dos años, pasando del 34% de encuestados que reportaron un incidente en 2023 al 41% en 2025. La suplantación de contactos de confianza y las demandas urgentes de pagos o información sobre una brecha de seguridad detectada han sido las tácticas más comúnmente empleadas



Deepfake es una imagen o vídeo artificial generado por una forma de inteligencia artificial que parece real, pero es falso. El atacante recopila muestras auténticas de medios de su objetivo para usarlas como material de entrenamiento del modelo de aprendizaje profundo, estas muestras incluyen imágenes fijas, vídeos y clips de audio. Cuanta más información de entrenamiento obtenga el atacante, más auténtico parecerá el deepfake resultante.

Sin dudas una de las consecuencias más graves de un ataque digital a un ejecutivo es que se pueda utilizar su información personal para causarle algún tipo de daño físico. El 50 % de los profesionales encuestados cree que sus ejecutivos serán objetivo de un ataque digital en un futuro cercano.

Para los usuarios de Iphone existe MDM Mobile Device Management una herramienta que las empresas y organizaciones usan para administrar, configurar y asegurar los iPhone proporcionados a sus empleados. Esto permite controlar las aplicaciones, los ajustes, la seguridad y los datos de los dispositivos de forma remota.

Debemos tener presentes marcos de referencia internacionales como NIST CSF, ISO 27001/27035.

Tenemos que adaptarnos a los cambios que nos propone la tecnología aplicada a la industria de la protección.

La protección ejecutiva evolucionó. Bienvenidos. 🌐

Analíticas inteligentes de video: la revolución en la seguridad



Yesid Alexander Méndez Rincón
Consultor y Gerencia Global de Riesgos
Tecnologías para la defensa y la seguridad
Alexander.mendez@outlook.com
Articulista invitado



Introducción

Barranquilla, Colombia.- En cuanto a los retos que requieren de una arquitectura tecnológica, he tenido la inmensa gratitud de hacer parte de cientos de proyectos incorporando innovaciones que aportan a la disminución del impacto de los riesgos en las empresas privadas y en las entidades de gobierno en Colombia; entre ellos, hace varios años fuimos pioneros al incursionar con los primeros sistemas de analíticas de video para la lectura de matrículas en la Policía Nacional para la seguridad (no de multas), generando resultados inmediatos como la recuperación de vehículos hurtados y aportes determinantes para las investigaciones de otros delitos, tecnologías que hoy están presentes en las principales ciudades del país.

La seguridad moderna ha evolucionado gracias a la Inteligencia Artificial aplicada al análisis de video. Hoy, los sistemas no solo graban imágenes, sino que interpretan comportamientos, detectan amenazas y optimizan la labor humana. Es importante comprender que son sistemas que deben ser diseñados con una arquitectura especial para el cumplimiento de los objetivos.

¿Cómo funciona esta tecnología y por qué es tan relevante?

Los puntos de videovigilancia en nuestras organizaciones han crecido a lo largo el tiempo y llega hoy a un número importante de cámaras instaladas. Este valioso inventario pierde su eficacia por la disminución en el control de las herramientas tecnológicas y, de acuerdo a los estudios para la seguridad y salud en el trabajo, debido a la fatiga ocular, también conocida como Astenopia (Vista Sánchez Trancón, 2025), es un síntoma natural en donde cada operador pierde su capacidad de observación minuto a minuto, el enfoque y la concentración de su actividad, convirtiendo nuestros sistemas en una herramienta forense no proactiva (Sánchez, et al., 1996).

Aplicando las analíticas inteligentes de video se reducen los riesgos en la salud, cómo la Astenopia, mencionada anteriormente, al disminuir el esfuerzo visual que genera fatiga ocular, dolor de cabeza, visión borrosa y picazón o ardor en los ojos.

Automatizar los procesos en la seguridad es una decisión muy necesaria al comprender que incluir el análisis inteligente de video y la integración con otros subsistemas de seguridad podemos empezar realmente a prevenir incidentes, generar alertas en tiempo real, controlar eficazmente nuestros recursos tecnológicos y a generar resultados medibles para la toma de decisiones.

Una de las grandes ventajas halladas en nuestras asesorías en varias empresas de diversas verticales de negocios es que, para incorporar rápidamente las analíticas inteligentes de video en nuestros sistemas de videovigilancia existentes, podemos aprovechar en promedio en la mayoría de casos hasta un 75% de estas cámaras junto con los sistemas de administración y de grabación. Esto permite realizar un diseño más acertado basado en la experiencia y las necesidades de nuestra operación.

En esta oportunidad, les comparto algunas de las funciones principales de las analíticas inteligentes de video existentes y una descripción funcional con las cuales podemos ir creando el escenario propicio en los diferentes puntos de video vigilancia existentes y futuros en nuestras organizaciones.



1. Detección de comportamiento y amenazas

Estas funciones están diseñadas para identificar situaciones de riesgo o anormales en tiempo real cómo:

Comportamiento inusual: el sistema aprende los patrones de movimiento normales en una escena y genera alertas ante cualquier desviación, reduciendo la necesidad de que los operadores de CCTV analicen el 95% al 98 % del video. El aprendizaje se basa en el análisis de píxeles y permite que el sistema aprenda cómo se mueven normalmente los objetos dentro de una escena; después de establecer una norma, el sistema generará una alerta sobre cualquier desviación. Esto permite que el sistema reduzca entre un 95 % y un 98 % la cantidad de video que debe analizar un operador de CCTV.

Amenaza inminente: alerta sobre objetivos que se aproximan a zonas críticas.
Advertencia: Objetivo aproximándose a zonas críticas.

Defensa: detectar y rastrear objetos muy pequeños y/o que se mueven muy rápido. Esta es una solución vital, por ejemplo, para detectar objetos lanzados por encima de vallas o muros. Permite eliminar sensores de infrarrojos activos, pasivos o sensores de microondas a lo largo de muros o vallas, pudiendo detectar intrusiones en zonas muy estrechas, incluso de unos pocos centímetros.

Detección Avanzada de Merodeo: herramienta configurable con parámetros específicos (tiempo de espera, tamaño del objeto) y *Deep Learning* para generar alertas en situaciones complejas de merodeo, con parámetros específicos como el tiempo de espera y el tamaño del objeto, junto con *Deep Learning* y el motor de reglas, es posible generar alertas específicas de situaciones de merodeo complejas y exigentes.

2. Clasificación, seguimiento y cumplimiento

Funciones centradas en la identificación, rastreo y el cumplimiento de normativas:

Clasificación y extracción de objetivos: rastrear elementos de interés, ignorando los factores ambientales inherentes a analíticas de CCTV, como condiciones variables de luz, lluvia, nieve, viento e incluso el ruido intrínseco del sensor de la cámara. Se utiliza para detectar objetos o personas en movimiento a distancias desde decenas de metros hasta kilómetros, por ejemplo, en el caso del control de fronteras.

Clasificación de objetos: se pueden clasificar más de 100 objetos, como por ejemplo, personas, vehículos, animales, ordenadores portátiles, entre otros.

Detección de objetos abandonados o removidos: genera una alerta si un objeto permanece estacionario más de un tiempo predefinido (abandonado) o si es retirado de la escena. La detección de objetos abandonados creará una alerta cuando un objeto aparece en la escena y permanezca estacionario por más de un periodo de tiempo predefinido configurable. Además, es posible detectar lo contrario a esta función, es decir, si se retira un objeto de una escena, cuando el sistema también puede generar una alerta.

Salud y Seguridad del Trabajo (EPIs): detección del uso correcto de protección auditiva, cascos, chalecos de alta visibilidad, visores/gafas, etc. Clasificación de la postura, en pie, acostado, caminando, sentando, agachado, cayendo, etc.

Control de flujo y densidad: incluye conteo de objetos (Entrada/Salida), ocupación del área de conteo y monitoreo e informes de densidad, conteo de objetos (Entrada/Salida), ocupación del área de conteo de objetos (cámara), monitoreo e informes de densidad (área), aplica para zonas de calor con fines comerciales o de organización de flujo para personas y vehículos.



3. Detección de intrusiones (alcance)

La detección de intrusiones se clasifica por distancia y precisión:

Corto alcance: alta precisión corto alcance y baja latencia 0-70 metros.

Alcance medio: alta precisión detección de intrusiones alcance medio: alta precisión hasta 250 metros.

Largo alcance: detección de intrusiones con la capacidad de alcanzar varios kilómetros.

4. Funciones avanzadas con vehículos.

Las utilidades de la lectura de matrículas, la clasificación de están enfocadas al control y gestión de tráfico en vías públicas, parqueaderos y control de acceso.

Identificación del tipo de vehículo, sentido, color, lectura de reconocimiento de matrículas, tiempo de estacionado, exceso de velocidad, sentido de tránsito, invasión de zonas, colisiones y conteo entre otras.

5. Funciones especializadas para lectura y reconocimiento facial (FR).

Las utilidades están enfocadas en la detección de rostros y su identificación comparativa dentro de una base de datos que puede utilizarse con múltiples propósitos.

Clínicas y hospitales: FR protege áreas sensibles como las unidades neonatales y las farmacias, gestiona el acceso del personal y mejora

la atención al paciente. Refuerza la seguridad al garantizar que solo el personal autorizado tenga acceso a las áreas restringidas. Agiliza la identificación del paciente, reduciendo los tiempos de espera y los errores administrativos. Facilita una experiencia más personalizada para el enfermo y ayuda a rastrear sus movimientos con fines de seguridad y análisis.

Educación: FR supervisa la seguridad del campus, automatiza el control de asistencia e implementa protocolos de respuesta ante emergencias eficientes. Incrementa la seguridad del campus al identificar rápidamente a personas no autorizadas. Simplifica los procesos administrativos con el registro automatizado de asistencia. Proporciona apoyo crucial durante emergencias al contabilizar rápidamente a estudiantes y personal.

Gobierno y seguridad ciudadana: la tecnología FR mejora la seguridad pública, optimiza la gestión del tráfico y contribuye a la planificación urbana. Mejora la protección ciudadana con vigilancia en tiempo real, lo que facilita la labor policial. Gestiona el control de multitudes y el flujo vehicular durante eventos y horas pico. Ofrece información demográfica que ayuda a una planificación urbana y una asignación de recursos eficaces.

Seguridad de la información: FR mejora la seguridad en edificios gubernamentales, gestiona el acceso a información confidencial y mantiene la integridad del servicio público. Refuerza la protección de información y lugares sensibles. Agiliza la gestión de visitantes sin comprometer los protocolos de seguridad. Apoya la preparación y respuesta ante emergencias con recuentos precisos de personas y verificación de identidad.

Banca, retail e ISP: FR protege las transacciones financieras, gestiona el acceso a las sucursales y mejora la atención al cliente. Protege contra el fraude mediante la autenticación de identidades durante las transacciones y operaciones bancarias. Controla el acceso a áreas restringidas dentro de las instituciones financieras. Ofrece una experiencia bancaria personalizada para clientes premium.

Puertos, aeropuertos, industria, logística, corporaciones e infraestructura crítica: FR refuerza la seguridad en los centros de transporte, agiliza el flujo de pasajeros y optimiza las operaciones logísticas. Incrementa la seguridad mediante alertas de listas de vigilancia. Mejora la eficiencia logística vía seguimiento del movimiento de personal y mercancías.



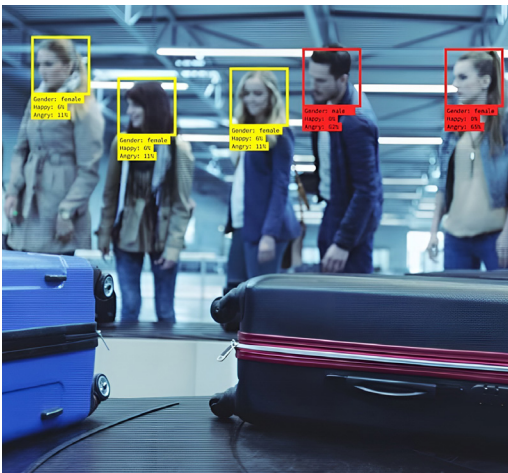
Funciones complementarias

Informes de BI (Business Intelligence): informes de KPI (indicador clave de desempeño) sobre el historial de alertas por cámara, por sitio, por tipo de evento, etc. Y sobre la eficiencia del operador responsable.

Búsqueda forense: permite buscar objetos clasificados dentro de los datos de alerta preexistentes por cámara.

Difuminado facial: difuminado facial para el RGPD Reglamento General de Protección de Datos, normativa de la Unión Europea sobre la privacidad y protección de datos personales que establece reglas para la recopilación, procesamiento y almacenamiento de datos de ciudadanos de la UE, y el anonimato de acuerdo a la legislación en los EE.UU. y otros países.

Análisis de sonido: detección y análisis de audio (estrucendos, disparos por armas de fuego, gritos, sirenas, entre otros).



Para destacar

En este contexto, la correcta aplicación de los procesos de las analíticas inteligentes de video generan beneficios con resultados parametrizables y medibles, siendo aún más importante la posibilidad y la viabilidad ya que estas tecnologías con componentes de Inteligencia Artificial, se implementan sobre los sistemas de videovigilancia ya existentes e instalados en nuestras organizaciones y ciudades. En su mayoría, y sin importar las marcas, ya que las resoluciones básicas y protocolos estándar se ajustan a los modelos existentes.

Sea esta una invitación para avanzar al siguiente nivel y disminuir la brecha que generan los riesgos y las tecnologías que ya no pueden ser gestionados en su totalidad por nuestro factor humano.

Referencias

Raúl Sánchez-Román, F., -, C. P.-L., -, C. J.-R., Mayola Vélez-Zamora, N., & Jiménez- Villarruel, M. (1996). Factores de riesgo para la astenopia en operadores de terminales de computadores. Salud Pública De México, 38(3), 189-196. Recuperado a partir de <https://www.saludpublica.mx/index.php/spm/article/view/5922>

Vista Sánchez Trancón (2025). Ojos cansados: qué es la fatiga ocular o astenopia. Clínica VISTA Sánchez Trancón. [https://vistasancheztrancón.com/ojos-cansados-que-es-la-fatiga-ocular/#:~:text=La%20fatiga%20ocular%20\(tambi%C3%A9n%20llamada,de%20cabeza%2C%20enrojecimiento%20o%20lagrimeo.](https://vistasancheztrancón.com/ojos-cansados-que-es-la-fatiga-ocular/#:~:text=La%20fatiga%20ocular%20(tambi%C3%A9n%20llamada,de%20cabeza%2C%20enrojecimiento%20o%20lagrimeo.)

Lo que no ves también te vigila

Anatomía secreta de la nueva vigilancia silenciosa



Andrea Guidugli

Consultor Miembro Federación Periodistas de la ciudad de Madrid. Periodista y Opinador acreditado por la Federación Internacional de la Prensa de Bruselas

Articlista invitado



La Spezia, Italia. - Una conversación, una voz, una vibración mínima: Todo basta. La vigilancia moderna ya no necesita micrófonos, solo rastros. De las salas seguras a los teléfonos de operativos, de los láseres que leen ventanas a los algoritmos que reconocen una voz entre millones: un viaje por la vigilancia que no se declara, la que no deja huellas físicas, pero sí digitales. Un territorio donde México tampoco es ajeno.

La voz que te delata

Durante años pensé que la seguridad era cuestión de prudencia. Una tarjeta SIM extranjera, un teléfono comprado en un aeropuerto remoto, una llamada hecha desde un pasillo de hotel en un país donde nadie conocía mi nombre. Creía —como tantos— que cambiar de tarjeta equivalía a cambiar de identidad. Era ingenuidad. Elegante, pero ingenua. Aquel día, en un despacho sin ventanas de una empresa del grupo —un lugar donde los técnicos de ciberseguridad hablaban en voz baja incluso estando solos— un colega se echó a reír al escuchar mis “métodos”.

Si alguien te está vigilando, no necesitan tu número. Necesitan tu voz. Una vez que la tienen, te siguen donde vayas. Cambies la SIM, el teléfono o de continente.

Me quedé callado. Él agregó, casi divertido: El error clásico del aficionado es creer que la vigilancia depende del dispositivo. En realidad, depende de ti.

Aquella frase me acompañó durante años y hoy, cuando miro el ecosistema de vigilancia mundial, me doy cuenta de que tenía demasiada razón.

No vivimos en la era de la ciberseguridad. Vivimos en la era de la ciberpercepción: donde las máquinas ya no buscan lo que haces, sino lo que eres.

Y ahí empieza esta historia.

La vigilancia que ya no necesita micrófonos: anatomía de un mundo silencioso

La vigilancia moderna ha cambiado de piel. No se basa en cables escondidos, grabadoras incrustadas en muebles o micrófonos diminutos. Eso es arqueología operativa. Hoy la vigilancia es óptica, vibratoria, algorítmica y, sobre todo, es pasiva.

No emite señales. No interfiere. No deja huellas. Solo observa.

1. Visual Intelligence (VISINT): cuando la luz escucha

El MIT lo demostró en 2014: una bolsa de patatas filmada a miles de fotogramas por segundo podía revelar conversaciones enteras. Pero ese experimento —*The Visual Microphone*— fue solo el prólogo. Desde entonces, varias unidades de inteligencia lo han llevado más lejos:

- NSA, Tailored Access Operations (TAO): integración de VISINT con SIGINT
- Unidad 8200 israelí: fusión de análisis temporal de video con captación de micro vibraciones

- GCHQ británica: análisis de ventanas a 200 metros con láseres de bajo retorno
- DEFENSA y SEMAR mexicana (información pública): uso de sensores ópticos en vigilancia urbana de alto riesgo.

Nada de esto es secreto; solo se comunica poco. Esta nueva generación de herramientas no escucha sonidos: escucha movimientos. Una cortina. Una botella de agua. Una lámpara. Una chapa metálica. Una ventana. Todo vibra cuando hablas y todo lo que vibra puede ser traducido.

2. El método Lamphone: la bombilla que delata secretos Universidad Ben-Gurión, Israel, 2020. Demostración pública: captaron una conversación entera observando únicamente la luz de una bombilla. ¿Por qué funciona? Porque el filamento o el LED vibra y la luz vibrada contiene sonido codificado. Ese estudio está hoy en bases de datos policiales y militares internacionales. No porque sea exótico. Sino porque es operativo.

3. LDV (Laser Doppler Vibrometry): lo que revela un cristal La técnica favorita de varias agencias: leer ventanas, detectar patrones de voz, captar discusiones de salas “seguras” que no lo son tanto. Un láser que apunta al cristal refleja micro oscilaciones que, reconstruidas, devuelven la voz. Ya no necesitas plantar un micrófono. Solo necesitas mirar el reflejo de un vidrio.

De la física a la doctrina: cómo operan los Estados Los países que trabajan con vigilancia pasiva no improvisan. Tienen doctrinas, manuales internos, reglas de despliegue, cadenas de autorización. Aquí menciono las partes públicas, accesibles mediante fuentes abiertas:

1. Estados Unidos – Doctrine for Technical Surveillance Countermeasures (TSCM)

Manual desclasificado parcialmente, protocolo para detectar: vibraciones sospechosas, interferencias ópticas, emisiones secundarias, manipulación de ventanas, presencia de VISINT remota. Cada año se entrenan unidades específicas del FBI y del servicio diplomático.

2. Israel – SIGINT Fusion Doctrine

La Unidad 8200 integra: vibración, imagen, acústica residual, análisis de tráfico digital No buscan pruebas directas. Buscan correlaciones y esas correlaciones valen más que una grabación clásica.

3. Francia – DGSI/DGSE

Usan VISINT en: negociaciones de rehenes, seguimiento antiterrorista, operaciones contra crimen organizado de origen saheliano. Francia fue de las primeras en integrar VISINT en operaciones urbanas en Marsella y Lyon.

4. México – DEFENSA, SEMAR, CN5I

México no se queda atrás. En 2022 y 2023, varios documentos públicos mencionan uso de sensores ópticos de largo alcance, estaciones móviles de vigilancia vibratoria, integración con plataformas de reconocimiento urbano. México tiene una ventaja: su “experiencia de frontera” con Estados Unidos ha permitido cooperación técnica constante.

El error humano: somos rastros antes que personas
Aquí entra mi anécdota personal, que ahora adquiere un peso distinto. Aquello que me dijo mi colega “necesitan tu voz, no tu teléfono” es una doctrina real. Se llama: Speaker Identity Tracking (S.I.T.).

No importa qué número uses. Da igual en qué país estés. Si una agencia tiene tu firma vocal, puede detectarte cuando: llamas por VoIP, envías un mensaje de voz, hablas cerca de un dispositivo conectado, apareces en el audio de un video, incluso cuando hablas dentro de un automóvil moderno. La voz es más fuerte que tu pasaporte y más traidora que tu SIM.

Los casos reales que nunca se cuentan
Aquí es donde la historia deja de ser técnica y se vuelve humana. La vigilancia pasiva es tan poderosa como discreta. Sus éxitos no suelen aparecer en comunicados oficiales, y cuando lo hacen, se atribuyen a “trabajo de inteligencia”, una expresión que sirve para ocultar tecnologías que no conviene mencionar. Aquí van versiones ampliadas, basadas en información pública, documentos judiciales y reconstrucciones de fuentes abiertas, que permiten entrever cómo estas técnicas operan realmente.

1.- Beirut, 2019 – El eco de un vidrio
(Información cruzada de prensa libanesa, Haaretz e informes de la ONU)

Un edificio aparentemente anodino, en un barrio donde ninguna agencia occidental podía plantar un micrófono y sin embargo, una reunión de comandantes de un grupo armado fue detectada. ¿Cómo? Una cámara térmica situada a más de 300 metros captó oscilaciones irregulares en el vidrio del piso superior. No era suficiente para oír palabras, pero sí para detectar *ritmo conversacional*, intensidad, número de voces y momentos de tensión. Ese “perfil vibracional” permitió confirmar que la cúpula estaba reunida. El ataque selectivo llegó horas después. Nunca se mencionó VISINT. Solo se habló de “información precisa y oportuna”.



2.- Sonora, 2021 – Un dron contra el silencio
Arresto de un operador del CJNG tras análisis de vibración en techos refrigerados.
México, 2022 — Drones con telemetría térmica vibracional.

No fue una llamada interceptada ni un informante infiltrado. El inicio de la operación provino de un dato anómalo: la vibración térmica irregular en un techo industrial ubicado en el corredor entre Caborca y San Luis Río Colorado, Sonora, una región donde células del Cártel Jalisco Nueva Generación (CJNG) mantenían laboratorios de procesamiento y bodegas refrigeradas para el almacenamiento de droga sintética.

Los agentes federales no buscaban exactamente ese edificio. La vigilancia aérea formaba parte de un reconocimiento rutinario, usando drones multispectrales con sensores de telemetría térmica vibracional, tecnología que combina tres matrices:

- Radiometría infrarroja (cambios de temperatura, incluso bajo cubiertas opacas)
- Patrones de vibración estructural (micro oscilaciones por voz, maquinaria o movimiento humano)
- Análisis de coherencia acústica residual (traducción matemática en patrones rítmicos)

Lo que llamó la atención no fue el calor — muy común en instalaciones clandestinas — sino una frecuencia vibratoria rítmica, comparable a la cadencia del habla humana. El techo del contenedor refrigerado vibraba a entre 82 y 134 Hz durante lapsos irregulares. Esa banda de frecuencia es consistente con conversaciones masculinas en voz baja. El dron no captó palabras. Tampoco necesitaba hacerlo. Los especialistas del Centro Nacional de Fusión de Inteligencia (CN5I) detectaron algo más interesante: las vibraciones indicaban dos patrones vocales distintos, uno dominante y otro subordinado. Era, estadísticamente, una conversación de mando.

Aquello transformó el vuelo de rutina en un objetivo prioritario.

La segunda confirmación: los compresores

El análisis térmico detectó que los compresores de refrigeración se apagaban durante lapsos de 4 a 7 minutos, siempre después de las vibraciones. Los peritos concluyeron que el silencio mecánico se usaba para conversaciones sensibles, reduciendo ruido ambiental y facilitando la comunicación interna. Eso es doctrina. Doctrina criminal, pero doctrina al fin.

La fase terrestre

En menos de cuatro horas, un equipo mixto Sedena-FGR ejecutó una incursión silenciosa.

Dentro del contenedor encontraron:

- 14 kg de metanfetamina en etapa cristalina
- 1 prensa hidráulica contaminada con fentanilo
- 2 radios Kenwood modificados con cifrado casero
- 1 cuaderno con rutas en Arizona y contactos en Mexicali
- y, sobre todo, al objetivo esperado:

Eduardo “N”, alias *El Ganso*, operador logístico del CJNG, con órdenes de aprehensión por tráfico transfronterizo. En ningún boletín oficial se mencionó la tecnología utilizada.

Se emitió la versión estándar: trabajo de inteligencia, seguimiento y coordinación interinstitucional.

Pero la realidad —según dos funcionarios consultados bajo reserva— es otra: “No hubo llamadas interceptadas. No hubo soplonés. Lo que habló fue el techo”.

Por qué este caso cambió protocolos internos

Tras la operación, la FGR y DEFENSA ajustaron criterios de vigilancia para bodegas refrigeradas, creando una matriz de riesgo vibracional, ahora usada en varios estados:

1.- París, 2022 – La botella que habló

(Información judicial francesa)

En un apartamento vigilado por la policía francesa, no era posible introducir micrófonos: el sospechoso desmontaba el mobiliario tras cada visita. La solución fue inesperada: una cámara térmica registró la vibración mínima de una botella de vidrio sobre la mesa. El software reconstruyó patrones térmico-vibratoriales, suficientes para confirmar órdenes, tiempos y la implicación del sospechoso. La prensa habló de “seguimiento técnico”. Nunca explicaron la botella.

2.- Kandahar, 2018 – La motocicleta delató al mensajero

(Fuentes abiertas afganas y estadounidenses)

Un reclutador talibán evitaba teléfonos, radios y reuniones en interiores. El error: hablar mientras conducía. Su motocicleta vibraba más cuando hablaba que cuando circulaba en silencio. Un dron analizó micro fluctuaciones del chasis. La vibración reveló su identidad vocal. Lo siguieron tres semanas. Arrestado sin haber pronunciado una sola palabra en un teléfono.

3. Madrid, 2020 – La impresora que los delató

(Datos de sentencia judicial)

Hubo casos europeos —como la operación en Madrid contra una red de trata, en la que la vibración térmica de una botella dejó al descubierto una reunión clandestina—, pero aquellos episodios son hoy casi prehistoria. La doctrina operativa real está naciendo en Beirut, en los túneles de Siria y en los galpones refrigerados del norte de México.

En una célula yihadista, nadie usaba móviles. Se comunicaban escribiendo mensajes y destruyéndolos. Pero una impresora vieja vibraba de forma distinta cuando había varias personas hablando alrededor. Esas vibraciones, cruzadas con cámaras de tráfico del barrio, permitieron deducir asistencia, turnos y jerarquías internas.

Estos casos no aparecen a menudo en manuales abiertos. Pero son los casos que explican por qué la vigilancia moderna ya no busca sonido. Busca patrones.

La frontera mexicana: un laboratorio silencioso
Pocos países han visto su territorio convertirse, sin anunciarlo, en un laboratorio de vigilancia pasiva. México es uno de ellos. No por un plan maestro, sino porque su geografía, su criminalidad organizada y su cooperación con Estados Unidos han creado un ecosistema operativo único.

1. Las "casas mudas" de los cárteles
En estados fronterizos, los cárteles adaptaron habitaciones enteras con materiales acústicos comprados en EE. UU. Creían haber logrado silencio total. Error: las paredes insonorizan sonido, pero no frenan vibración estructural. En 2023, una operación en Tamaulipas detectó actividad en una casa "muda" gracias a la vibración de una tubería exterior expuesta al viento. El análisis reveló movimientos internos equivalentes a conversaciones. Los agentes entraron sin haber escuchado un solo sonido.



2. Vehículos "insonorizados" que no lo son
Varios grupos criminales usan camionetas modificadas con paneles acústicos. Pero la vibración de los espejos retrovisores — captada por cámaras de tráfico mexicanas integradas a software estadounidense — permite deducir si dentro se está hablando, cuántas voces hay y si la conversación es tensa o relajada. Esto ya se usa en Nuevo León y Baja California.

3. Drones híbridos de vigilancia vibracional
Sedena y Marina han adquirido, según documentos públicos de compra, drones equipados con:

- cámaras de 120-240 fps
- sensores IR para vibración térmica
- algoritmos de correlación VISINT

Los despliegues están concentrados en Tijuana, Mexicali, Matamoros y Ciudad Juárez.

4. Intercambio técnico México-EE.UU.
En centros binacionales (como el de El Paso), agentes mexicanos reciben formación en análisis vibracional. México, a su vez, entrega datos operativos reales, imposibles de obtener en territorio estadounidense. Es cooperación pragmática: ellos tienen la tecnología; México tiene el escenario operativo.

5. Intercambio El "Efecto Migratorio"
La biometría no solo controla quién entra. Desde 2021, varios sistemas fronterizos detectan:

- nivel de estrés en la voz
- micro tensiones faciales
- vibración involuntaria del tórax

No es psicología. Es física más machine learning. Ese cruce de señales alimenta bases de riesgo que, oficialmente, no existen. La frontera mexicana es hoy un aula donde las agencias aprenden cómo vibra el crimen y cómo vibra quien intenta no dejar rastro.

El núcleo del asunto: ya no importa qué dices, sino cómo vibras
En vigilancia moderna, toda identidad es física antes que digital. No importa la contraseña, el número de teléfono o el dispositivo: la vibración es el nuevo ADN operativo.

La voz, convertida en arma de rastreo
La técnica S.I.T. (Speaker Identity Tracking) permite identificar a un individuo incluso cuando:

- usa un modulador de voz
- habla detrás de un vidrio
- está a más de 20 metros del micrófono accidental
- aparece en un video ambient noise

La firma vocal es más estable que una huella digital.

El cuerpo vibra, aunque guardes silencio
Incluso sin hablar, un individuo genera:

- vibración torácica
- micro flujos de aire
- resonancias de pasos
- presión rítmica en superficies

Un láser bien ajustado puede detectar la respiración acelerada de alguien que está nervioso detrás de una pared.

Los objetos a tu alrededor son tus enemigos
Todo delata:

- una taza de café (excelente resonador)
- una laptop (la tapa vibra con la voz del usuario)
- una mesa metálica
- un parabrisas
- una persiana barata

Cada objeto es un micrófono involuntario.

La luz también escucha
Cámaras de tráfico en ciudades como Tokio, Londres, París y CDMX pueden detectar micro variaciones lumínicas en ventanas o fachadas. No "escuchan": reconstruyen movimiento y el movimiento es conversación.

El enemigo verdadero: la correlación
No hace falta oír tu voz. Basta correlacionar:

- vibración de objetos
- ubicación GPS
- horarios
- temperatura ambiente
- redes Wi-Fi visibles

Cada variable aislada es inocente. Juntas, construyen tu presencia.

El silencio ya no existe
Quien crea que la vigilancia moderna funciona como en las series, micrófonos, pinchazos, hackers tecleando frenéticamente, está viendo una película antigua. Hoy la inteligencia no te busca, te percibe. No entra en tus dispositivos, entra en tus vibraciones. No quiere tu contraseña, quiere tu patrón. Y eso, si se usa bien, puede salvar vidas. Si se usa mal, puede destruir libertades. Esa es la paradoja del siglo XXI. 🇺🇸

Bandas criminales en Latinoamérica

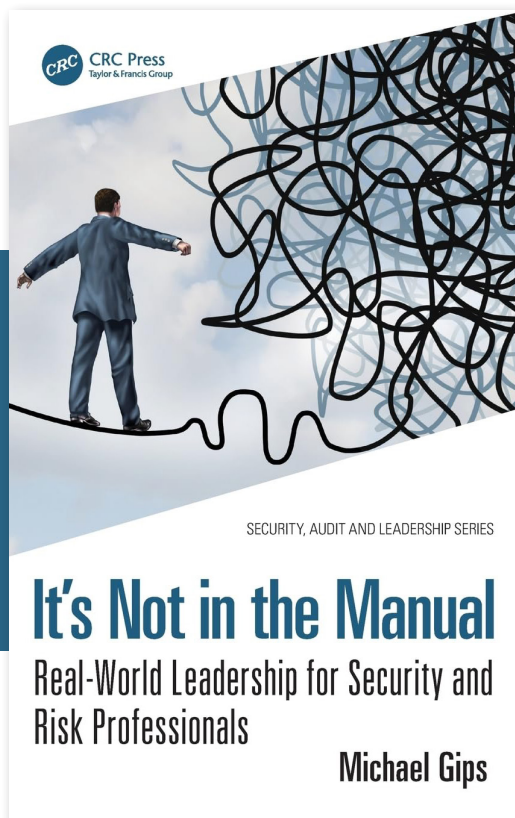
Tomo I. Fernando Vaccotti. (2025)

En este primer tomo, Fernando Vaccotti traza un mapa riguroso del crimen organizado en América Latina. Desde los carteles mexicanos hasta el PCC brasileño, desde las mafias que gobiernan desde la cárcel hasta las redes narco que cruzan fronteras y corrompen gobiernos, este libro revela como las bandas criminales se han convertido en actores clave del poder real que comprenden una amenaza estructural que redefine las democracias latinoamericanas.

BANDAS CRIMINALES EN LATINOAMÉRICA

PODER, VIOLENCIA
Y REDES TRANSNACIONALES
EN EL SIGLO XXI
TOMO I

FERNANDO VACCOTTI



¿Qué define a un gran líder. No está en el manual en seguridad y gestión de riesgos?

El consultor de seguridad Michael Gips, autor de "No está en el manual", desafía la idea de que liderar eficazmente en temas de protección, riesgo y resiliencia depende solo de títulos, certificaciones o reglas estrictas. Ante desafíos como ciberamenazas, riesgos internos, problemas de reputación y caos global, este libro aporta algo aún más importante: lecciones aprendidas con experiencia, apertura humana y un humor irónico.

El libro combina perspectivas probadas con ingenio agudo, basándose en fuentes tan diversas como Sócrates y Snoopy, Bill Gates y Bill Bryson, la física cuántica y las peleas en el patio de recreo. Si busca un libro sobre liderazgo sencillo, siga buscando. Este libro es liderazgo con ligereza, franqueza y conciencia.

El tomo, basado en numerosas entrevistas con expertos y ejecutivos, combina tácticas prácticas con reflexiones filosóficas.

Desde la gestión de la complejidad y la policrisis hasta el fomento del bienestar y el pensamiento adaptativo, It's Not in the Manual llega donde las guías convencionales no llegan. No solo te enseña a liderar. Te muestra por qué es importante, cuándo falla y qué se necesita para liderar con integridad en la incertidumbre. 



15^{VA} FERIA INTERNACIONAL DE SEGURIDAD

MAYO
27 - 29
2026
LIMA-PERÚ



FÍSICA & ELECTRÓNICA ✓
PERSONAL (EPP) ✓
DEFENSA PERSONAL ✓
INCENDIO Y RESCATE ✓
VIGILANCIA & PROTECCIÓN ✓
POLICÍA Y SERENAZGO ✓
VIAL ✓
CIBERNÉTICA ✓
COMUNICACIONES ✓
PROTECCIÓN OCUPACIONAL ✓

¡RESERVE SU STAND HOY!

www.seguritec.thaiscorp.com

Sede



Oficialización



PERÚ

Ministerio de Comercio
Exterior y Turismo



Prensa Asociada

MÁS SEGURIDAD
Magazine



CON SEGURIDAD
Magazine Latam

Organiza: Thais Corporation S.A.C. - thais@thaiscorp.com - [+51 989-177-352](https://www.whatsapp.com/+51989177352)



CIRO GÓMEZ
LEYVA

REGÍSTRATE CON EL CÓDIGO

CONSEGURIDAD

CN SEGURIDAD
Magazine Latam

antes del 20 de febrero y obtén un **10%**
de descuento en tu registro en **FASE 2**



TEODORO
SERRALDE,
CPP



DAVID
LEE



VÍCTOR
SANTIAGO
FLORES



ERICK
JHONATHAN
SALDAÑA



DAVID
ESTEBAN
SAUCEDO



MARTÍN
GRANILLO



JORELVY
CALIXTO



JOSÉ LUIS
CALDERÓN



MATTHEW
A. CRAIG



RICHIE
DELMONT



JORDI
MARTELL



EDUARDO
VÁZQUEZ



JORGE
MEDINA



OMAR LARA



ALFREDO
GONZÁLEZ



DANIEL
PORTUGAL

+18

EXPERTOS QUE HABLARÁN
SOBRE DIVERSOS TEMAS
DE BLINDAJE

+700

M2 DE EXHIBICIÓN PARA
LAS MARCAS LÍDERES EN
EL MERCADO

+170

TOMADORES DE DECISIÓN
EN TEMAS DE BLINDAJE

**ESPACIO ÚNICO
DE NETWORKING
EN BLINDAJE**



www.congresonacionaldelblindaje.com.mx