MÁS SEGURIDAD

Magazine

Agosto 2026 / No. 164 / Año 18
Internacional / precio $60.00 MXN

GRUPO EDITORIAL • MS GLOBAL

ESS+®
FERIA INTERNACIONAL DE SEGURIDAD

26 AL 28 AGOSTO 2026
›CORFERIAS‹

INTEGRACIÓN DE TECNOLOGÍAS GLOBALES

ESS+ 2026 - La plataforma estratégica para fabricantes de seguridad en América Latina y el Caribe

Exhiba su tecnología donde se toman las decisiones

Acceso directo a proyectos activos en:

- Infraestructura crítica y energía
- Banca y finanzas
- Retail y centros comerciales
- Transporte y logística
- Gobierno y ciudades seguras
- Industria y data centers

ESS+ Hub para expansión comercial de América Latina y el Caribe

Contáctenos

Adriana Patricia Márquez Acosta
Directora Comercial
Correo: amarquez@securityfaircolombia.com
Teléfono: +57 310 334 1669

ORGANIZAN

IFEMA MADRID · PAFYC · corferias

Conozca más información aquí o en securityfaircolombia.com

Para ampliar información, modificaciones/actualizaciones y ver términos y condiciones de la feria consulte securityfaircolombia.com.
Organizado por: PAFYC y Corporación de Ferias y Exposiciones S.A - NIT 860.002.464-3 - Cra. 37 # 24-67 Bogotá

MÁS SEGURIDAD
Magazine

HUMBERTO MEJÍA HERNÁNDEZ
DIRECCIÓN GENERAL
humberto@revistamasseguridad.com.mx

MARÍA ANTONIETA JUÁREZ CARREÑO
DIRECCIÓN COMERCIAL Y RELACIONES PÚBLICAS
marieclaire@revistamasseguridad.com.mx

BEATRIZ CANALES HERNÁNDEZ
COORDINACIÓN EDITORIAL
edicion@revistamasseguridad.com.mx

DG CREATIVE
DISEÑO Y DESARROLLO VISUAL

CLAUDIA IVETTE MARTÍNEZ GUTIÉRREZ
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

SARA LUCÍA MEJÍA CASTRO
DESARROLLO DE NEGOCIOS LATAM
negocios@revistamasseguridad.com.mx

FREY NICACIO DÍAZ GÜIZA
DESARROLLO DE NEGOCIOS COLOMBIA
ventas@revistamasseguridad.com.mx

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@globaldefense.com.mx

OSCAR TENORIO COLÓN
ADMINISTRACIÓN Y CONTABILIDAD
contabilidad@revistamasseguridad.com.mx

JORGE MERCADO ABONCE
SERVICIOS JURÍDICOS INTEGRALES

ANAZALDO-MARTÍNEZ-MERCADO
DIRECCIÓN JURÍDICA
juridico@revistamasseguridad.com.mx

ASISTENCIA A CLIENTES
atencion@revistamasseguridad.com.mx

CONTACTO
Tel/WhatsApp: (+52) 55 1894 7067
asistencia@revistamasseguridad.com.mx
atencion@msglobal.com.mx

SÍGUENOS EN:

Revista Más Seguridad
@revmasseguridad
revistamasseguridad
revmasseguridad
Revista Más Seguridad
Revista Más Seguridad
Más Seguridad Magazine

Revista Más Seguridad Año 18, No 164, Agosto 2026, Publicación mensual de **Grupo Editorial MS Global S. de R.L. de C.V.**, con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 5555272279 / +52 5528732719. Editor responsable: **Humberto Mejía Hernández**. Certificado de Reserva 04-2022-050614181900-102 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No. 11483 y Certificado de Licitud de Título No. 13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: Grupo Mejía Impresores, calle La Poza No. 72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel: +52 5518947067.

¿Fenómeno propio o réplica regional?

la evolución del crimen organizado en LatAm

El crimen organizado se ha transformado en uno de los principales desafíos para la seguridad en América Latina; por ello Chile frente a este fenómeno en constante evolución, a través de SeguridadExpo 2026 realizará el conversatorio “Crimen organizado en Chile y la región: diagnóstico actual, tendencias emergentes y respuestas estratégicas”. En dicho foro se buscará analizar las características que ha adquirido esta amenaza y las capacidades que el país deberá fortalecer para enfrentarla de cara a los próximos años.

Importante resaltar que esta actividad será parte del programa del Congreso de **SeguridadExpo 2026** y se llevará a cabo el miércoles 9 de septiembre, en Metropolitan Santiago. La agenda de la feria también abordará otros temas relevantes para el país, como la seguridad fronteriza, los ecosistemas penitenciarios, la inteligencia artificial y la protección de datos. Sin duda, la feria deja de ser solo un escaparate de tecnología para que expertos toquen estos delicados temas que permean en casi todo el continente.

Rodrigo Bastidas, gerente de SeguridadExpo, dejó ver uno de los propósitos de **SeguridadExpo** es generar conversaciones que contribuyan al desarrollo de la industria y al fortalecimiento de las capacidades del país en materia de seguridad. Reunir a especialistas con experiencia en investigación, inteligencia y políticas públicas permitirá enriquecer el debate sobre un fenómeno que hoy exige respuestas cada vez más coordinadas en materia.

Luis Toledo, abogado, exfiscal del Ministerio Público y actual director del Centro de Estudios en Seguridad y Crimen Organizado (CESCRO), es uno de los expositores confirmados destaca. Durante sus más de dos décadas en la Fiscalía encabezó investigaciones de alta connotación pública, entre ellas el Caso Caval, además de desempeñarse como director de la Unidad Especializada de Crimen Organizado y Drogas de la Fiscalía Nacional, experiencia que hoy lo posiciona como una de las principales voces del país en materias de crimen organizado y persecución penal.

Pablo Zeballos, consultor e investigador especializado en crimen organizado transnacional, economías ilícitas, gobernanza extralegal y terrorismo; Pilar Lizana, asesora de la Unidad de Modernización del Estado del Ministerio de Seguridad Pública; y el general de Carabineros Juan González Albornoz, director de CICPOL (Centro Integrado de Coordinación Policial), participarán en el panel.

Durante el conversatorio se abordarán diversas interrogantes. Por ejemplo, si en Chile se está configurando un modus operandi propio del crimen organizado o si el país continúa replicando dinámicas observadas en otras naciones de la región. Se discutirá si la persecución está enfocada en quienes ejecutan los delitos o en quienes administran y facilitan las redes criminales, además de analizar dónde se ejerce actualmente el control territorial de estas organizaciones.

Se abordarán los desafíos en materia de inteligencia, interoperabilidad entre instituciones, persecución financiera, cooperación internacional, prevención y el rol que puede desempeñar el sector privado frente a un fenómeno cada vez más sofisticado, aportando insumos para la discusión sobre las capacidades que Chile requerirá fortalecer durante los próximos años. Una tarea nada fácil para los gobiernos latinoamericanos.

Los Profesionales de LATAM

Licenciado Gerardo de Lago Acosta, MSc, CPP

México

Químico Farmacéutico Biólogo (QFB) por la Universidad La Salle.
Maestría en Justicia Criminal con énfasis en Seguridad Nacional (Homeland Security) por la Universidad de Phoenix.
En 2025 fue Presidente Ejecutivo de ASIS Internacional, Capítulo Ciudad de México.

Es Director de Consultoría & Miembro del Consejo de Timur Latinoamérica & Galeam Security Services, firmas especializadas en consultoría y servicios de seguridad privada, con base en la Ciudad de México, y operaciones en Latinoamérica.

Posee diversos Certificados de Seguridad, como el CPP y la Certificación de Protección Ejecutiva ambos de ASIS International y el Certificado de Operaciones contra Incendios de la Universidad Texas A&M. Recibió el entrenamiento en Manejo y Negociación de Secuestros impartido por GardaWorld en Londres, Inglaterra, obtuvo el grado de instructor en el proceso A.L.I.V.E. de reacción ante el escenario de Tirador Activo, impartido MPS Security & Protection en California, EE. UU.

En Procter & Gamble, fue Gerente de Relaciones Laborales, Gerente de Producción, Gerente de Administración de Riesgos y Gerente de Security para Latinoamérica Norte con responsabilidad por la seguridad de todas las operaciones en México y Centro América, posicionándose como el experto regional para Latinoamérica de Planeación de Continuidad de Negocios y como Responsable del establecimiento del estándar de Equipo Electrónico de Seguridad.

Fue Director de Seguridad de Laureate Education para Latinoamérica, teniendo a su cargo los temas de Security, Safety, Protección contra Incendios, Protección Civil, Seguridad Técnica, Protección Ejecutiva y Seguridad Ambiental, con responsabilidad por la protección de más de 450,000 alumnos en Campus Universitarios en 9 países.

Sumario

MÁS SEGURIDAD
Magazine

Tour Internacional 2026

EXPO NAVAL 2026
XIV EXHIBICIÓN Y CONGRESO INTERNACIONAL NAVAL Y MARÍTIMO PORTUARIO PARA LATINOAMÉRICA
1-3 DICIEMBRE
ESPACIO RIESCO
AV. EL SALTO 5000, HUECHURABA

ESS+
FERIA INTERNACIONAL DE SEGURIDAD

intersec
BUENOS AIRES

SEGURIDADEXPO
by Fisa | CHILE

EXPO SEGURIDAD TELECOM COSTA RICA

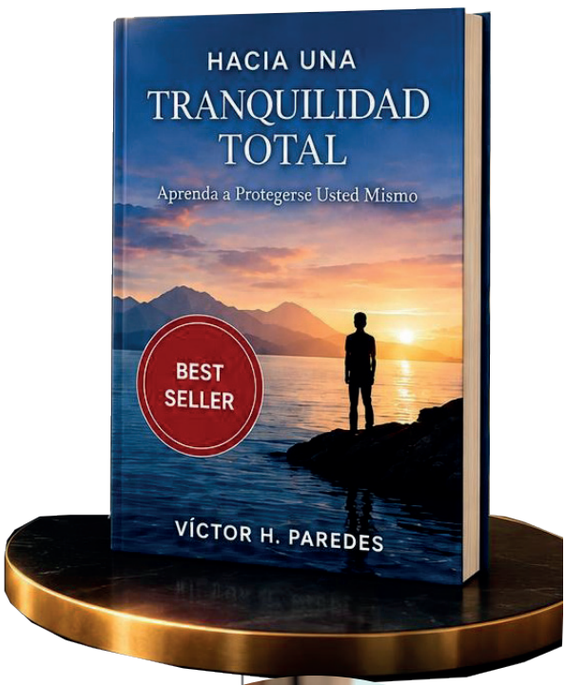
EXPO SEGURIDAD TELECOM PANAMÁ

EXPO SEGURIDAD TELECOM EL SALVADOR

Sigue la cobertura informativa en redes sociales, sitio web y revista

Víctor Paredes Consultor de Seguridad - Colombia

Propone hallar el éxito en la Seguridad desde la paz interior



Bogotá, Colombia.- El autor Víctor H. Paredes, presenta un libro centrado en el desarrollo personal y el bienestar emocional. Su propuesta parte de una idea clara: el verdadero éxito no nace de lo material, sino de la capacidad de construir una mente en calma y una vida con propósito.

La obra reúne herramientas prácticas y reflexiones dirigidas a personas que buscan manejar mejor sus pensamientos, reducir el estrés y fortalecer sus emociones.

El autor señala que muchas veces se persiguen metas externas sin atender primero el equilibrio interno, lo que puede generar ansiedad y desgaste. Uno de los ejes del texto es la paz interior como base para tomar mejores decisiones y avanzar con mayor claridad.

También aborda la construcción de una mentalidad orientada a la abundancia, entendida como una forma de pensar abierta a nuevas oportunidades y cambios positivos. Con un lenguaje sencillo, Paredes invita a revisar creencias limitantes, fortalecer la confianza personal y crear hábitos mentales saludables.

El libro propone acciones aplicables a la rutina diaria, enfocadas en responder con serenidad ante los retos. La frase “La verdadera seguridad no está afuera, está dentro de ti” resume el mensaje central de una publicación que busca acompañar procesos de cambio personal y una vida más consciente.

“La seguridad es la sensación de tranquilidad que experimentamos todos cuando estamos protegidos”.

Bajo esa premisa, el autor ha dedicado 12 años a escribir Hacia una Tranquilidad Total, un libro que hoy pone a disposición de los lectores.

En su contenido se encuentran técnicas sencillas para lograr una seguridad plena y alcanzar la tranquilidad que se busca. Una invitación a adquirirlo y comenzar el camino hacia una vida más segura y en calma.

Víctor Paredes
— Security Consultant —

Adquiera el libro AQUÍ

Compras

Colombia: WhastApp – 3115090619
Internacional: Amazon
https://www.amazon.com/dp/B0GWQ4M82T/

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. Respaldado 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.

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 Hikvision México.

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, 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".

La empresa 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.

introduce software Blaze:

VMS híbrido con búsqueda semántica y por apariencia

Hanwha Vision, líder global en soluciones de videovigilancia y analítica de datos, presentó de manerade manera oficial Blaze, su nuevo software de gestión de video (VMS), un sistema híbrido de gestión de nueva generación diseñado para simplificar el despliegue del sistema, las investigaciones impulsadas por Inteligencia Artificial y la gestión de múltiples ubicaciones en entornos de videovigilancia modernos. Esta plataforma destaca por la incorporación de herramientas avanzadas de búsqueda semántica y por apariencia, diseñadas para optimizar los tiempos

de respuesta ante incidentes y elevar la eficiencia en tareas de análisis forense.

Enrique Cortés, Regional CES Manager de la zona Pacífico, de Hanwha Vision, detalló que Blaze opera bajo un esquema híbrido, lo que permite a las organizaciones mantener una infraestructura local (on-premise) o migrar hacia ecosistemas mixtos basados en la nube, adaptándose a las necesidades de escalabilidad y presupuesto de cada cliente.

Uno de los pilares de Blaze es su capacidad de integración con analíticas de terceros a través de alianzas tecnológicas clave. De acuerdo con Cortés, el software maximiza el procesamiento perimetral (Edge AI) y de servidor mediante la compatibilidad con tecnologías de procesamiento gráfico NVIDIA, integradas de forma nativa en dispositivos como la cámara multisensor de la marca. Para ofrecer soluciones hiperespecializadas por vertical de negocio, Blaze llega al mercado con socios de software como:

- Skyla: Enfocado en el reconocimiento facial y esquemas como la detección temprana de armas de fuego.
- Gapi: Especializado en el sector de la agroindustria, con algoritmos desarrollados para el monitoreo y la detección de anomalías en plantíos.
- Spotvision: Solución orientada al retail optimizando la seguridad en puntos de venta.
- Lumeo: Una plataforma de arquitectura abierta que otorga a los integradores y usuarios finales la flexibilidad para desarrollar e implementar sus propios analíticos.

En cuanto a la infraestructura de cámaras, Cortés aclaró que Blaze alcanza su máximo nivel de integración y rendimiento analítico cuando trabaja con el portafolio de productos de Hanwha Vision, pero gracias a la compatibilidad con el estándar ONVIF, la plataforma puede gestionar e integrar dispositivos de videovigilancia de otros fabricantes, facilitando la actualización tecnológica de sistemas heredados sin necesidad de sustituir por completo el hardware existente.

Con este lanzamiento, Hanwha Vision consolida su transición de un fabricante de componentes de seguridad a un proveedor integral de soluciones de inteligencia visual, apostando por la reducción de la fatiga del operador y la automatización del análisis masivo de datos de video.

Blaze está diseñado para escalar desde implementaciones en una única ubicación hasta entornos distribuidos con múltiples sedes.
Su arquitectura en clúster permite ampliar el sistema a medida que crecen las necesidades operativas, manteniendo el rendimiento y la resiliencia del sistema. Mediante la gestión en la nube, múltiples sistemas pueden conectarse dentro de una misma organización, lo que permite la administración unificada de usuarios y el acceso mediante single sign-on entre diferentes ubicaciones.

Al conectar los sistemas locales de cada sede con BLAZE Cloud, los operadores, administradores y técnicos pueden acceder de forma remota y segura sin necesidad de configuraciones complejas como redirecciones de puertos o VPN.

Enrique Cortés, Regional CES Manager de la zona Pacífico, de Hanwha Vision

Las grandes marcas de la industria de la seguridad ya forman parte de ALAS.

AJAX · ALARM.COM · ALCEA ASSA ABLOY · Altronix · AXIS COMMUNICATIONS · BOLIDE TECHNOLOGY GROUP · CAME · dahua TECHNOLOGY · EXPO SEGURIDAD MÉXICO · GARNET TECHNOLOGY · Genetec · Hanwha Vision · HID · HIKVISION · Honeywell · IKUSI velatia · Johnson Controls · milestone · MOTOROLA SOLUTIONS · Network Optix · NVT PHYBRIDGE · OpenEye · PROSEGUR SECURITY · RBH ACCESS · resideo · SECURITY SIS SERVICIOS INTEGRALES DE SEGURIDAD · SoftGuard · Verkada · wesco | anixter · ZKTeco

Su confianza fortalece una comunidad que conecta a fabricantes, integradores, distribuidores, consultores y empresas de seguridad en toda Latinoamérica y el Caribe.

Ahora es el momento de que tu empresa también sea parte de esta comunidad.

Únete a ALAS

ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

www.alas-la.org

AJAX fortalece presencia en México con Muñoz Solutions

como nuevo subdistribuidor autorizado

Ajax Systems continúa expandiendo su red de distribución en Latinoamérica con la incorporación de Muñoz Solutions como nuevo subdistribuidor autorizado en México. A partir de esta alianza, la empresa distribuirá el portafolio completo de soluciones Ajax, acercando la tecnología de seguridad inteligente a integradores, instaladores y empresas de seguridad en el norte y occidente del país.

Con presencia en los estados de Tamaulipas, Nuevo León, Coahuila, Chihuahua y Jalisco, Muñoz Solutions se ha consolidado como un aliado estratégico para el canal de seguridad electrónica, ofreciendo soluciones tecnológicas que responden a las necesidades actuales del mercado. Su enfoque combina asesoría especializada, diseño de proyectos y soporte postventa, permitiendo a sus socios de negocio desarrollar soluciones más eficientes y competitivas.

La incorporación de Muñoz Solutions fortalecerá la disponibilidad de los productos Ajax en México, mejorando la cobertura logística y facilitando el acceso de los profesionales de la seguridad a capacitación, demostraciones y acompañamiento especializado para el desarrollo de nuevos proyectos.

“México es uno de los mercados estratégicos para Ajax Systems en Latinoamérica y seguimos comprometidos con fortalecer nuestra red de distribución para estar cada vez más cerca de nuestros clientes. La incorporación de Muñoz Solutions como subdistribuidor representa un paso importante en esa estrategia. Su experiencia, conocimiento del mercado y presencia en estados clave nos permitirán ampliar la disponibilidad de nuestras soluciones, impulsar la capacitación de integradores y brindar un mejor acompañamiento a los profesionales de la seguridad. Estamos convencidos de que esta alianza contribuirá al crecimiento de ambas compañías y, sobre todo, a generar más oportunidades para nuestros clientes en la región”, afirmó Alberto Treviño, Sales de Ajax Systems para Latinoamérica.

Para Muñoz Solutions, esta alianza representa una oportunidad para ampliar su propuesta de valor con una de las marcas de seguridad electrónica más innovadoras del mercado y continuar impulsando el crecimiento tecnológico de sus clientes.

“En Muñoz Solutions nos caracterizamos por mantenernos a la vanguardia tecnológica y ofrecer a nuestros clientes soluciones respaldadas por las mejores marcas del mercado. Convertirnos en Subdistribuidor Oficial de Ajax Systems representa una oportunidad para fortalecer esta visión y ampliar nuestro portafolio con soluciones de detección de intrusión, automatización y tecnologías AIoT que ofrecen innovación, confiabilidad y un alto desempeño”, comentó Bryant Muñoz, Gerente de Muñoz Solutions.

Bryant agregó: “Nuestro objetivo es construir una relación comercial de largo plazo con Ajax Systems, impulsando la capacitación continua de nuestro equipo, fortaleciendo nuestra presencia en el mercado y consolidándonos como un referente en la implementación de soluciones de seguridad electrónica de última generación. Además de la distribución de productos, buscamos aportar valor mediante asesoría especializada, diseño de proyectos, soporte postventa y estrategias que contribuyan al crecimiento de la marca en nuestra región.”

A través de esta alianza, ambas compañías trabajarán conjuntamente para desarrollar nuevas oportunidades de negocio, promover la capacitación técnica y comercial del canal, y acercar soluciones de seguridad inteligentes a más proyectos en el mercado mexicano.

Control de acceso sin credenciales físicas:
el nuevo estándar en seguridad corporativa

Victor H. Manzanilla R.
Managing Director ALCEA Mexico.
Victor.manzanilla@assaabloy.com
Venezuela
Articulista Invitado

Durante años, el control de acceso en las organizaciones se ha sustentado en credenciales físicas como tarjetas, teclados numéricos y llaves electrónicas. A pesar de su evolución tecnológica, estos sistemas comparten una debilidad estructural: son estáticos en un entorno donde los riesgos son cada vez más dinámicos.

Hoy, las organizaciones líderes están adoptando un enfoque distinto: modelos de acceso adaptativos y sin credenciales físicas, capaces de responder en tiempo real al contexto, al comportamiento del usuario y al nivel de riesgo.

El modelo tradicional presenta limitaciones claras: credenciales compartidas o robadas, clonación sin detección inmediata, falta de trazabilidad real sobre quién accede y procesos rígidos que no responden a escenarios cambiantes. En consecuencia, muchas empresas operan bajo una falsa sensación de control, particularmente en entornos críticos.

El nuevo paradigma rompe con esta lógica. En lugar de validar el acceso solo en el punto de entrada, introduce un enfoque de validación continua de la identidad. Esto se logra mediante el uso de credenciales digitales dinámicas, autenticación multifactorial (incluyendo biometría, dispositivos móviles, llaves electrónicas dinámicas) y evaluaciones de riesgo en tiempo real basadas en variables como ubicación, horario, revalidaciones y patrones de comportamiento.

Este cambio permite que el nivel de seguridad se ajuste de manera inteligente en cada interacción, sustituyendo reglas fijas por decisiones contextuales.

La eliminación de las credenciales físicas tradicionales no solo reduce vulnerabilidades, sino que transforma la operación. Se elimina el riesgo de pérdida o clonación, se fortalece la trazabilidad, se simplifica la administración de accesos y se mejora de forma significativa la experiencia del usuario. En este modelo, el acceso deja de ser un objeto y se convierte en una extensión de la identidad digital de los colaboradores.

Para las organizaciones, los beneficios son contundentes: mayor seguridad real, reducción de riesgos internos y externos, integración más eficiente con ecosistemas tecnológicos y capacidades avanzadas de auditoría. Más importante aún, permite evolucionar el rol del área de seguridad, pasando de un enfoque operativo a uno estratégico.

El control de acceso ya no puede verse como un sistema aislado. Hoy es un componente central de la arquitectura de seguridad integral. Los modelos adaptativos y sin credenciales físicas no representan una tendencia futura, sino una respuesta necesaria a los desafíos actuales.

Desde mi experiencia acompañando procesos de transformación en seguridad corporativa, este cambio no es únicamente tecnológico, sino cultural. Adoptar estos nuevos modelos no tradicionales, implica replantear cómo entendemos la confianza, el riesgo y la identidad dentro de la organización.

Las empresas que realmente están avanzando en este camino son aquellas que dejan de ver el control de acceso como un punto de control aislado, y comienzan a integrarlo como parte de una estrategia digital más amplia, donde la seguridad habilita el negocio en lugar de limitarlo.

En mi opinión, el reto no está en la tecnología —que ya existe—, sino en la capacidad de las organizaciones para evolucionar sus procesos, su gobierno y su mentalidad. Quienes lo logren, no solo estarán mejor protegidos, sino que tendrán una ventaja competitiva clara en un entorno cada vez más exigente.

SALTO WECOSYSTEM facilita control de accesos mediante enrolamiento autónomo

INSPIRED ACCESS

En el mercado actual de la seguridad electrónica, la tendencia apunta hacia la eliminación de fricciones en la gestión de identidades y la reducción de costos en infraestructura local. Por ello es que Salto Systems presentó sus nuevas soluciones de acceso biométrico basadas en una arquitectura Cloud, Salto Space.

En entrevista durante la pasada edición de Expo Seguridad, Jorge Olmedillo, gerente regional de ventas en Salto México, destacó que el elemento diferenciador de esta propuesta radica en la descentralización del proceso de registro, trasladando el poder de gestión al teléfono del usuario. A través de Salto Space, se ha diseñado un ecosistema de enrolamiento remoto intuitivo.

Olmedillo dijo que el proceso es sencillo, consiste en enviar una invitación al usuario mediante correo electrónico; se le asignan los privilegios de acceso para ciertas puertas. El usuario recibe un correo electrónico en su smartphone y, a través de su propio teléfono, realiza su enrolamiento biométrico.

Para los integradores y directores de seguridad que buscan optimizar recursos, una de las mayores ventajas técnicas de esta solución es su topología de red. La plataforma biométrica opera mediante un servidor en la nube totalmente independiente, el cual se comunica de forma directa y transparente con el software local o híbrido de Space.

“Hay muchas soluciones de reconocimiento facial de muchos países. El gran diferenciador de Salto es que el enrolamiento lo haces a través de tu teléfono, a través de nuestra potente plataforma Space tú invitas a un usuario, le das acceso a ciertas puertas, el usuario recibe un correo y a través de su correo se enrola, va a dar de alta su cara en el sistema y eso es único de Salto, es lo que nos hace muy diferentes, no tienes qué ir en cada cámara enrolando tu cara, lo haces a través del teléfono, se sube a la nube y ya puedes acceder a cualquier puerta: ya sea una cerradura, un locker, entonces, ese es el gran diferenciador, el enrolamiento a través del teléfono”, señaló Olmedillo.

Por su versatilidad y facilidad de implementación, Salto opera a nivel global y Salto México apunta a un abanico de verticales clave en el país, que incluyen corporativos y oficinas, Para flujos dinámicos de empleados y visitantes, hotelería, optimizando la experiencia del huésped desde su llegada, manufactura e infraestructura crítica, asegurando perímetros de alta sensibilidad sin retrasar la operación y educación, simplificando el acceso masivo a campus universitarios.

Salto: controles de acceso con sentido común

Olmedillo afirmó que la marca busca democratizar el acceso biométrico de alta gama en México. Al combinar una solución fácil de implementar, un soporte normativo de primer nivel y un precio competitivo, Salto busca liderar la migración de las empresas hacia entornos de seguridad sin llaves y gestionados desde la nube. “Es una solución bastante económica, somos una empresa española, todo se fabrica, se desarrolla en España bajo las normativas que hay en Europa y aún así tiene un precio competitivo”.

Jorge Olmedillo, gerente regional de ventas en Salto México

salto

INSPIRED ACCESS

SALTO WECOSYSTEM

Impulsando un acceso más inteligente

SALTO lidera la transformación digital en la gestión de accesos e identidades, combinando tecnologías innovadoras con soluciones pensadas para cada necesidad.

Desarrollamos tecnología de vanguardia en control de accesos, gestión de identidades y cerraduras electrónicas, para ofrecer experiencias seguras, confiables y sin fricciones en todo tipo de espacios.

saltosystems.com

Datos de contacto
marketing.cala@saltosystems.com

Más allá del uniforme

Las marcas invisibles del operador de seguridad

Bruno Vidal
Bombero de Aeródromo Rescatista, especialista en Gestión de Seguridad y Safety & Security. Graduado en Gestión de Seguridad Privada, con formación de posgrado en Safety en Aviación y Seguridad de Vuelo. Actúa en operaciones críticas, análisis de riesgos y seguridad operacional aplicada.
Brasil
Articulista Invitado

Bahía, Brasil.- No todas las huellas que deja la profesión de seguridad son visibles. Algunos no permanecen en uniforme ni aparecen en los informes operativos. Se asientan en silencio en el cuerpo y la mente, reflejados en sueños fragmentados, hipervigilancia constante, dificultad para relajarse y la sensación de que el cuerpo nunca descansa completamente.

En profesiones relacionadas con la protección de personas, activos y entornos críticos, el estado de preparación ya no es solo un requisito operativo y pasa a formar parte de la forma de funcionamiento del individuo. El operador aprende a observar detalles, anticipar amenazas y reaccionar rápidamente ante estímulos adversos. Sin embargo, el mismo mecanismo responsable de preservar vidas puede, si se mantiene de forma contìnua, convertirse en una fuente de agotamiento físico y emocional.

Entre la preparación y el desgaste

Desde la perspectiva de la fisiología ocupacional, el organismo humano no estaba diseñado para permanecer en alerta constante durante largos periodos. En situaciones críticas, la activación del sistema nervioso desencadena respuestas esenciales de supervivencia, aumentando los niveles de adrenalina y cortisol, acelerando el ritmo cardíaco y preparando el cuerpo para actuar ante el riesgo. Este es un mecanismo indispensable en situaciones de emergencia.

Por tanto, el estrés no debe entenderse necesariamente como un enemigo de la actividad operativa. En ciertas circunstancias, favorece la concentración, la energía, la preparación y la capacidad de respuesta. El punto crítico no está en la presencia de tensión, sino en su permanencia no regulada. Cuando la activación fisiológica no encuentra periodos de recuperación adecuados, el rendimiento previamente apoyado

comienza a deteriorar progresivamente al propio operador. El problema surge cuando este estado deja de ser episódico y se convierte en rutina.

Con el tiempo, muchos profesionales empiezan a operar en un sistema de vigilancia continua. El cuerpo se adapta a la tensión diaria y comienza a reaccionar a estímulos mínimos como si estuviera enfrentándose permanentemente a una amenaza. La consecuencia no se limita a la fatiga física. El desgaste prolongado compromete la calidad del sueño, altera los procesos cognitivos, aumenta los niveles de irritabilidad y reduce la capacidad de recuperación fisiológica.

La mente que no se desarma

En la psicofisiología del trabajo, se entiende que cuerpo y mente funcionan de manera integrada. Cada estímulo emocional produce respuestas orgánicas, así como cada cambio fisiológico influye directamente en el comportamiento y la percepción del individuo. En entornos de alta presión operativa, esta relación se vuelve aún más evidente.

El operador de seguridad a menudo vive con situaciones de tensión, incertidumbre y riesgos potenciales. Poco a poco, el cerebro se adapta a este patrón de funcionamiento. Las estructuras relacionadas con el procesamiento del miedo y la vigilancia permanecen hiperactivadas, mientras que los mecanismos vinculados al control racional y al equilibrio emocional empiezan a funcionar en sobrecarga. El resultado es una mente que encuentra difícil desconectarse del entorno operativo, incluso cuando está fuera de servicio.

La hipervigilancia se convierte en un fenómeno silencioso y a menudo sigue naturalizada dentro de la cultura operativa. El profesional empieza a observar excesivamente el entorno, mantiene altos niveles de atención incluso en lugares seguros y tiene dificultades para relajarse completamente. En muchos casos, el estado continuo de alerta invade momentos de descanso, vida familiar y ocio.

El cuerpo como reflejo del entorno operativo

Además del impacto emocional, existen factores físicos directamente asociados con la rutina operativa. Los turnos prolongados, la privación de sueño, la nutrición inadecuada, la exposición constante al estrés y la ausencia de descansos adecuados comprometen el equilibrio hormonal y la regulación del ciclo circadiano. Progresivamente, el cuerpo pierde eficiencia en los procesos de recuperación física y mental.

Este desgaste no siempre surge de un solo evento extremo. A menudo, se forma por acumulación. Cada turno pesado, cada noche de mal sueño, cada episodio de una carga emocional fuerte y cada periodo sin recuperación adecuada añade una nueva capa de estrés. Poco a poco, el margen de recuperación disminuye y el cuerpo empieza a transportar desechos fisiológicos y emocionales incluso cuando la sucesión ha terminado.

Estas son algunas de las marcas invisibles de la profesión. Marcas que no aparecen en equipos dañados ni en estadísticas institucionales, sino que se acumulan silenciosamente en la mente y el cuerpo de quienes permanecen expuestos a la presión operativa a diario.

Entre el deber y el silencio

Durante mucho tiempo, la cultura de seguridad asoció la resistencia emocional con la ausencia de vulnerabilidad. Expresiones como “esto es parte de ello” o “el operador debe soportar la presión” siguen reflejando una visión obsoleta del rendimiento en entornos críticos. Sin embargo, la psicología aplicada a las operaciones en sí misma demuestra que estabilidad emocional y autocuidado no representan fragilidad, sino factores estratégicos para mantener la capacidad operativa.

Los profesionales emocionalmente agotados tienden a tener mayor dificultad para concentrarse, menor conciencia situacional y mayor susceptibilidad a fallos bajo presión. Por otro lado, los operadores que mantienen el equilibrio psicofisiológico suelen tener respuestas más estables, decisiones más asertivas y mejor adaptación a escenarios complejos.

Otro punto delicado es la dificultad para reconocer los signos de agotamiento antes de que se vuelvan incapacitantes. La fatiga persistente, los trastornos del sueño, la irritabilidad, el cinismo, la pérdida de interés, la sensación de impotencia y la reducción de la disposición a trabajar no deben tratarse como debilidad individual. En muchos casos, son indicadores de que el sistema psicofisiológico del operador ya funciona por encima de su capacidad sostenible.

Preservar al operador no significa reducir la eficiencia operativa. Significa garantizar la longevidad física, la estabilidad cognitiva y la respuesta continua. Preservar a quienes protegen

Desde el punto de vista de la neurociencia y la psicofisiología aplicadas al trabajo, el rendimiento operativo y la salud psicofisiológica no deben tratarse como conceptos opuestos. Al contrario: son complementarios entre sí. El sueño adecuado, la condición física, una dieta equilibrada y el apoyo psicológico no deben considerarse elementos secundarios, sino como parte integral de la

¿Grietas en el software? ¿qué nos dice el OWASP Top 10?

Dr. Gustavo Guzmán Hernández,
Ciudad de México, México LinkedIn: Gustavo Guzmán Hdez.
México

Articulista Invitado

Introducción

Cada aplicación que usamos a diario —la app del banco, la red social, la aplicación del ejercicio, la de la edición de fotos y videos, y otras tantas más— es, en al final del día, una superficie llena de decisiones de diseño que alguien tomó -muchas veces bajo presión de tiempo-. Algunas de esas decisiones pasan desapercibidas, pero algunas se convierten, años después, en la puerta por la que entra un atacante. Desde 2003, el proyecto OWASP (Open Web Application Security Project) se dedica a documentar, con datos, cuáles son esas puertas más comunes. El resultado es el OWASP Top 10, probablemente el documento de referencia más citado en toda la disciplina de seguridad de aplicaciones, usado por igual por desarrolladores junior, arquitectos de software y directores de seguridad de la información. En noviembre de 2025 se publicó su octava edición, y los cambios que trae no son cosméticos: reflejan un giro real en cómo pensamos la seguridad del software, de perseguir síntomas a entender causas. Vale la pena detenerse a mirar qué dice esa lista, cómo se construye y qué implica para cualquier organización que hoy dependa de código para funcionar, que ya es, prácticamente, cualquier organización.

Desarrollo

Lo primero que distingue al OWASP Top 10 es su metodología que combina dos fuentes de evidencia. Por un lado, analiza datos reales de pruebas de seguridad enviados por decenas de organizaciones y proveedores de herramientas, cientos de miles de aplicaciones evaluadas y, en la edición 2025, casi 590 debilidades técnicas catalogadas bajo el estándar Common Weakness Enumeration, frente a las cerca de 400 que se analizaban en 2021 (OWASP Foundation, 2025). Por otro lado, como reconoce el propio equipo del proyecto, los datos históricos siempre miran hacia atrás: para capturar tendencias emergentes que la industria todavía no sabe medir a escala, se complementan ocho categorías basadas en evidencia con dos elegidas por encuesta directa a profesionales en ejercicio. Esta combinación de rigor estadístico y criterio experto es, en sí misma, una lección de buena práctica científica aplicada a un problema de ingeniería.

El primer lugar de la lista 2025 lo conserva, como ya ocurría en 2021, el control de acceso roto: la falla que permite que un usuario vea o haga algo que no debería (OWASP Foundation, 2025). Es una categoría interesante precisamente porque desafía la automatización: una herramienta puede detectar con relativa facilidad una inyección de código, pero determinar si el usuario A debería poder ver el expediente del usuario B depende de la lógica de negocio de cada sistema, algo que ningún escáner entiende por sí solo. Es, en el sentido más literal, un problema humano de diseño disfrazado de problema técnico.

El cambio más revelador de esta edición, sin embargo, es el ascenso de la configuración de seguridad deficiente, que salta del quinto al segundo puesto. No sorprende a quien haya trabajado en entornos de nube moderna: cuantos más servicios, contenedores y capas de infraestructura como código se apilan, más oportunidades hay de dejar un permiso demasiado abierto o una credencial por defecto sin cambiar. A esto se suma una categoría completamente nueva, las fallas de la cadena de suministro de software, que absorbe y expande lo que antes se llamaba “componentes vulnerables y desactualizados”. El cambio de nombre no es casualidad: reconoce que el software moderno es, en esencia, un ensamblaje de código de terceros, y que ataques como el de SolarWinds en 2020, la puerta trasera descubierta en la utilidad xz Utils en 2024, o el hackeo del paquete ua-parser-js, no fueron fallas de una sola empresa, sino fallas de todo un ecosistema de dependencias compartidas. La otra novedad, el manejo inadecuado de condiciones excepcionales, aborda algo tan cotidiano como qué hace un sistema cuando algo sale mal: si un error revela información sensible, si un fallo de validación termina otorgando acceso por accidente, o si el sistema, ante la duda, decide “fallar abierto” en lugar de “fallar seguro”.

Detrás de estos diez puntos hay una idea que la disciplina

de seguridad de software viene defendiendo desde hace más de dos décadas: la seguridad no se puede añadir al final, como una capa de pintura sobre un edificio ya construido. Gary McGraw, uno de los autores más influyentes en este campo y pionero del concepto de "software security" como disciplina propia, lo resumió con una frase que hoy es casi un mantra de la industria: la seguridad debe construirse desde adentro, no atornillarse después (McGraw, 2006). El propio Instituto Nacional de Estándares y Tecnología de Estados Unidos formalizó esta idea en su marco de desarrollo seguro de software, que exige integrar prácticas de seguridad en cada etapa del ciclo de desarrollo, no solo al final en una auditoría de última hora (NIST, 2022). El OWASP Top 10 es, en ese sentido, menos una lista de amenazas externas y más un espejo que le muestra a cada organización sus propios hábitos de construcción.

Y ese espejo importa porque las consecuencias no son abstractas. El informe anual de investigación de brechas de datos de Verizon, uno de los estudios empíricos de mayor escala sobre causas reales de incidentes, ha documentado de forma consistente que la mayoría de las brechas de seguridad analizadas involucran algún tipo de error o debilidad evitable, no un ataque de sofisticación extraordinaria (Verizon, 2024). Dicho de otro modo: la mayoría de las veces -no siempre- que algo sale mal -haciendo referencia a un ataque satisfactorio-, no es porque un atacante haya inventado una técnica nueva y deslumbrante, sino porque alguien dejó una puerta que ya sabíamos que existía sin cerrar del todo. El OWASP Top 10 no es una lista de rarezas; es, casi con crueldad, una lista de lo previsible.

Conclusión

Vale la pena preguntarse, sin ánimo retórico, cuántas de las aplicaciones que hoy sostienen la operación de nuestra empresa, nuestra universidad o nuestro consultorio han sido evaluadas alguna vez contra esta lista. El OWASP Top 10 no es un documento decorativo para presentaciones de comité: es una herramienta de trabajo, gratuita y de acceso público, que cualquier equipo de desarrollo puede usar mañana mismo para auditar su propio código. La invitación es concreta y no requiere presupuesto extraordinario: que cada organización que desarrolla o contrata software pregunte explícitamente, en su próxima revisión de seguridad, si el equipo conoce esta lista y si la está usando como referencia desde el diseño y no solo como checklist de última hora. La seguridad de la información dejó hace tiempo de ser un tema exclusivo del departamento de sistemas; es, cada vez más, una responsabilidad compartida entre quien escribe el código, quien lo aprueba y quien decide qué tan rápido se publica. Ignorar el mapa que ya tenemos trazado no nos hace más ágiles, solo nos hace más vulnerables por elección.

Referencia

- McGraw, G. (2006). Software security: Building security in. Addison-Wesley.
- National Institute of Standards and Technology. (2022). Secure Software Development Framework (SSDF) Version 1.1 (NIST Special Publication 800-218). U.S. Department of Commerce.
- OWASP Foundation. (2025). OWASP Top 10:2025.
- Verizon. (2024). 2024 Data Breach Investigations Report.

Centro Global para la Seguridad Corporativa:

¿Existe una necesidad? ¿Qué criterios?

Antonio Celso Ribeiro Brasiliano
PhD, Doctor en Filosofía de las Ciencias de la Seguridad Internacional, Universidad de Cambridge, Inglaterra. Presidente de Brasiliano INTERISK. abrasiliano@brasiliano.com.br
Brasil
Articulista Invitado

São Paulo, Brasil.- Para los líderes de seguridad corporativa, el valor de un Centro Global de Operaciones de Seguridad (CGOS) debe medirse por la calidad de las decisiones que la operación ayuda a apoyar.

Un CGOS puede centralizar la monitorización de CCTV, la actividad de control de acceso, las alarmas y la notificación de incidentes. Pero para organizaciones con áreas físicas complejas en múltiples ubicaciones, viajes de negocios más frecuentes, la monitorización aislada rara vez es suficiente.

Un CGOS maduro reúne personas, tecnología, inteligencia, protocolos de comunicación y marcos de escalada para ayudar a los equipos de seguridad empresarial a evaluar lo que está ocurriendo y apoyar una respuesta estructurada.

La mejor pregunta es si el GSOC se alinea con el perfil de riesgo, la complejidad y las prioridades empresariales de la organización.

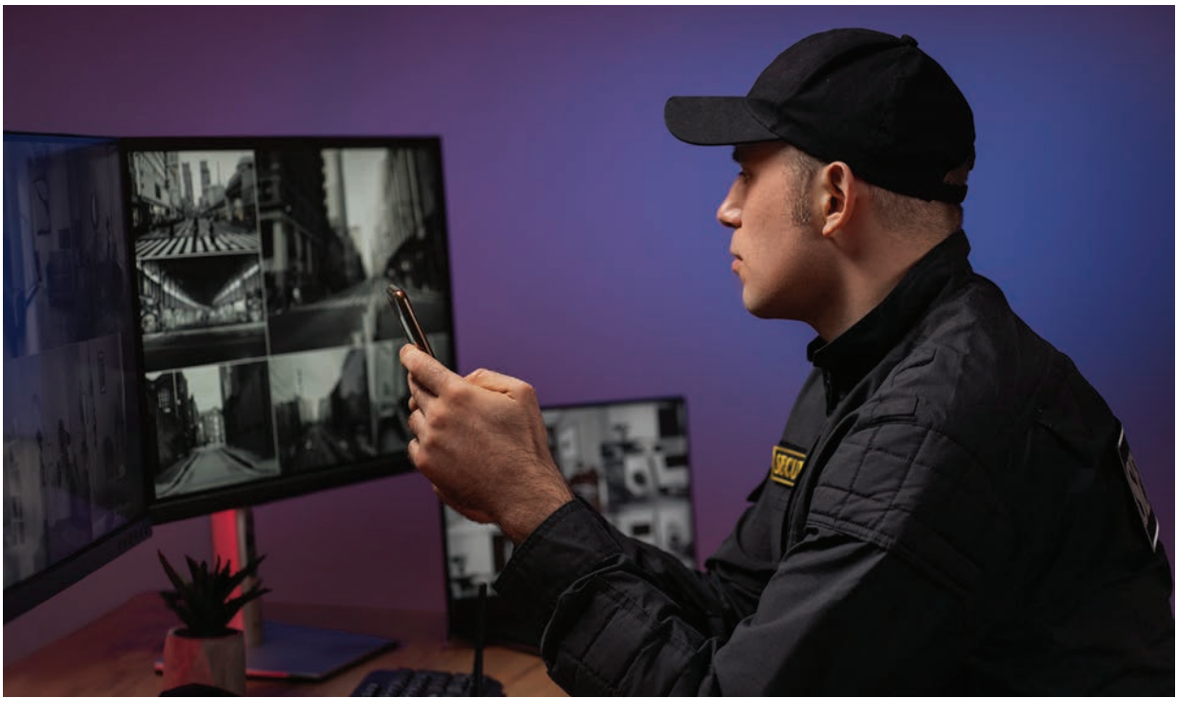
¿Qué soporta un CGOS?

Un CGOS apoya las operaciones de los centros de seguridad: vigilancia por CCTV, control de acceso, monitorización de alarmas, solicitudes de visitantes o acreditaciones, documentación de incidentes y notificaciones a las partes interesadas. Este modelo funciona para organizaciones más pequeñas con una complejidad limitada.

El reto surge cuando un equipo CGOS tiene que lidiar con escenarios más complejos que requieren que el personal evalúe el contexto, el impacto empresarial y las necesidades de escalabilidad más allá de lo que cubre un procedimiento estándar. Esta transición desde la finalización de tareas hasta la evaluación y respuesta a incidentes es donde surgen las necesidades de madurez del equipo CGOS.

¿Cuándo necesita una organización un CGOS más maduro?

Cuando su perfil de riesgo y complejidad operativa han superado las capacidades del modelo actual.



Los indicadores comunes incluyen:
Área amplia: Un área mayor suele generar una mayor variedad de actividades para monitorizar en distintas áreas de seguridad.

Operaciones 24/7: Un entendimiento más avanzado de los procesos de escalada y la toma de decisiones independiente de la noche a la mañana.

Viajes frecuentes de empleados: Viajar aporta exposición más allá del entorno laboral y puede requerir conciencia en tiempo real, responsabilidad e información para la toma de decisiones.

Alta visibilidad pública: Una marca visible, un perfil ejecutivo o una misión de cara al público pueden aumentar el escrutinio, la atención no deseada y la exposición reputacional.

Infraestructura crítica: Los centros de datos, laboratorios, centros de operaciones y otros entornos especializados pueden tener mayores implicaciones para la continuidad del negocio.

Brechas de escalada: Caminos complejos de notificación, estándares de documentación o umbrales de decisión pueden requerir personal más avanzado.

Preocupaciones sobre la continuidad del negocio: Las condiciones meteorológicas adversas, disturbios civiles, preocupaciones por violencia laboral, fallos en infraestructuras o interrupciones locales pueden afectar a personas, instalaciones, desplazamientos y operaciones al mismo tiempo.

Estos factores deben evaluarse de forma holística. Por ejemplo, una gran empresa global puede tener un CGOS inferior al esperado si el tiempo del personal se centra en el tráfico de radio local y en las actividades diarias del sitio.

Por otro lado, una organización pequeña puede necesitar un CGOS más avanzado al supervisar viajes ejecutivos complejos u operaciones sensibles. Las decisiones deben basarse en una evaluación exhaustiva del perfil de riesgo global de la organización y sus objetivos de seguridad.

¿Por qué los profesionales de seguridad son fundamentales para el rendimiento de CGOS?
La tecnología avanzada, junto con IA, ayuda a parametrizar sistemas en actividades críticas de tipo ejecutivo de seguridad y, especialmente, riesgos operativos de intrusión e intrusiones con el Estado Final Deseado de sabotaje y ataques terroristas.

Los profesionales de la seguridad necesitan juicio operativo, disciplina en la comunicación, familiaridad con la plataforma, habilidades de reporteo y comprensión del negocio. Necesitan saber cuándo escalar, monitorizar, documentar o buscar más contexto. Este juicio ayuda a mantener agilidad y reducir impactos, aumentando la resiliencia.

Programas sólidos de CGOS construyen consistencia mediante simulaciones para que los equipos tengan resiliencia en todas las dimensiones, asegurando marcos de escalada de calidad y documentados, especialmente cuando los servicios de seguridad empresarial apoyan legal, cumplimiento, riesgos, instalaciones, recursos humanos y partes ejecutivas.

Resultado
Un CGOS estándar supervisa las actividades a tiempo completo, las 24 horas del día, durante 7 días. Un CGOS maduro ayuda a interpretar actividades, evaluar el impacto y apoyar mejores decisiones.

Para los líderes de seguridad, riesgo, legal, instalaciones y ejecutivos, la cuestión es si el CGSOC está posicionado para soportar la complejidad de la organización a la que sirve.

Los programas sólidos combinan profesionales de seguridad formados, tecnología de última generación, inteligencia empresarial estructurada y documentación clara para realizar la escalada. Así es como un CGOS se convierte en un activo estratégico en la gestión de la complejidad del riesgo, resistiendo presiones sistémicas, integrándose con capacidades de resiliencia, apoyando la continuidad del negocio y fortaleciendo la imagen y credibilidad de la seguridad corporativa.

El riesgo no avisa REC SAFE® SÍ

Convierte la incertidumbre en control

Con 30 Años de experiencia y presencia en México, Argentina, Colombia y Estados Unidos, REC SAFE Integra tecnología, inteligencia y reacción para proteger la cadena de suministro de origen a destino.

Tecnología • Inteligencia • Reacción

En la cadena de suministro, los acontecimientos decisivos rara vez piden permiso. Un desvío no programado, una detención fuera de contexto, una pérdida de señal, un exceso de velocidad o una comunicación que no llega a tiempo pueden modificar en minutos el destino de una carga, la continuidad de una operación y la confianza de un cliente. Por eso, hoy la seguridad ya no puede limitarse a observar un punto en el mapa. Debe entender lo que ocurre, anticipar escenarios y activar una respuesta coordinada. Esa convicción resume una de las ideas que definen a REC SAFE: **“El riesgo no avisa. REC SAFE sí”**

Durante tres décadas, REC SAFE ha acompañado la evolución de la seguridad y la trazabilidad en México y Latinoamérica. Su trayectoria comenzó cuando el GPS era todavía una herramienta emergente para la operación empresarial y se consolidó con soluciones para flotas, activos críticos, centros de comando y proyectos de seguridad de alta complejidad, incluidos desarrollos vinculados con entornos C4 y C5. Entre sus hitos se encuentra el Proyecto Orion en Puebla, reconocido con el Premio COLADCA en el marco de ESS+ Bogotá 2024. Hoy, con más de 50,000 equipos GPS

Seguridad que comienza antes de la alerta

activos a nivel global, esa experiencia histórica, sumada a tecnología propia y acompañamiento permanente, permite comprender algo esencial: una alerta aislada informa; un ecosistema de seguridad bien diseñado protege.

De la visibilidad a la capacidad de decisión

El reto actual no es obtener más datos, sino convertirlos en decisiones oportunas. REC SAFE articula diagnóstico, dispositivos, conectividad, plataformas, inteligencia artificial, protocolos y especialistas para dar continuidad a cada operación crítica. La propuesta puede resumirse en una segunda declaración de marca: "CONVIERTE LA INCERTIDUMBRE EN CONTROL". Esto significa saber dónde está una unidad, pero también reconocer si se apartó de la ruta autorizada, conocer su velocidad, pero además advertir y escalar una conducta de riesgo; recibir una alerta, pero sobre todo asegurar que alguien la atienda, documente y cierre.

La diferencia está en conectar toda la información relevante: ruta, vehículo, operador, mercancía, horarios, zonas de riesgo, evidencias y protocolos. Con esta visión unificada, las áreas de seguridad, logística y dirección obtienen una base común para actuar. Se reducen puntos ciegos, se fortalece la trazabilidad, se estandariza la reacción y se genera una bitácora útil para auditorías, investigaciones, reclamaciones y mejora continua.

REC GUARDIAN: la nueva generación de custodia inteligente

CONVIERTE LA INCERTIDUMBRE EN CONTROL

Entre las novedades más relevantes se encuentra REC GUARDIAN, una solución que lleva el monitoreo convencional a una nueva categoría: custodiar la operación completa. El ecosistema combina una aplicación móvil para el operador, una capa autónoma de inteligencia artificial y una Torre de Control con intervención experta. Su misión es detectar, comprender, actuar, recuperar y escalar, según el nivel de riesgo y el protocolo definido por cada organización.

En el portal web, los servicios se visualizan en tiempo real y se priorizan por gravedad. Los eventos críticos —como pánico, desvío, detención, ingreso a zona de riesgo o pérdida de GPS— suben automáticamente en la bandeja de atención. El monitorista puede comparar la ruta autorizada con la ruta real, consultar la ficha completa del viaje, medir tiempos de respuesta y dejar evidencia de cada acción. Si una alerta no se atiende dentro del plazo previsto, el sistema puede escalarla de acuerdo con reglas preconfiguradas.

Para el conductor, REC GUARDIAN añade una capa de seguridad manos libres. Incluye botón de pánico, solicitud de asistencia, validación de identidad, PIN de confirmación y PIN de coacción, comandos por voz, navegación, avisos de desvío, alertas de velocidad, geocercas y registro del recorrido aun cuando se pierde temporalmente la cobertura. La comunicación con la central integra texto, voz, indicaciones con confirmación de lectura y protocolos paso a paso. La inteligencia artificial puede conversar con el operador, analizar el contexto del viaje y escalar a una persona cuando la situación lo exige.

El beneficio es concreto: la organización deja de depender exclusivamente de la atención individual y obtiene una respuesta repetible, medible y documentada. Esto acorta el tiempo entre la detección y la acción, mejora la coordinación y permite aprender de cada incidente para elevar el nivel de prevención.

ANTICIPACIÓN	REACCIÓN	EVIDENCIA	CONTINUIDAD
Detección temprana de anomalías y puntos ciegos.	Protocolos, escalamiento y coordinación 24/7.	Bitácoras, tiempos de atención y trazabilidad.	Decisiones más rápidas para mantener la operación.

Un portafolio para proteger cada punto crítico

REC SAFE no ofrece una solución única para riesgos distintos. Su portafolio se adapta a la madurez, el tipo de carga, la red logística y los objetivos de cada cliente. El Diagnóstico SCS ayuda a identificar brechas y prioridades con referencia a marcos como OEA, C-TPAT, ISO 28000 y BASC. Esta evaluación transforma la seguridad en una hoja de ruta: qué controlar primero, dónde invertir y cómo medir el avance.

FleetControl PRO centraliza la administración y la visibilidad de flotas mediante GPS, conectividad y alertas operativas. El onboarding de seguridad para cadena de suministro integra GPS, sensores IoT, videotelemática y protocolos, de modo que la tecnología se incorpore al proceso y no se convierta en un elemento aislado. Las soluciones de control de velocidad ayudan a reducir exposición, promover hábitos de conducción más seguros y proteger la continuidad del servicio.

Para activos que requieren discreción y flexibilidad, la trazabilidad IoT amplía la visibilidad con etiquetas delgadas Bluetooth para escenarios estáticos o en movimiento. Estas herramientas pueden apoyar la localización y recuperación de equipos, mercancías y objetos de valor sin depender de la misma arquitectura que un rastreador vehicular tradicional. A ello se suman soluciones con inteligencia artificial y RFID, videotelemática, sensores y esquemas de trazabilidad multinivel para operaciones de mayor complejidad.

La Torre de Control y el monitoreo 24/7 completan el modelo. La tecnología detecta y ordena, los especialistas interpretan, coordinan y documentan. Esta integración permite que las empresas mantengan una capacidad de respuesta permanente sin tener que construir desde cero toda la infraestructura, el personal, los procesos y la supervisión necesarios para operar una central propia.

REC SAFE®

GPS + IA + IoT + VIDEOTELEMÁTICA + PROTOCOLOS + MONITOREO 24/7

Beneficios que impactan la operación y el negocio

Elegir REC SAFE significa avanzar de una seguridad reactiva a una gestión preventiva basada en información. La visibilidad en tiempo real permite detectar desviaciones antes de que se conviertan en pérdidas mayores. Los protocolos automatizados reducen la improvisación. La medición de tiempos de atención genera responsabilidad operativa. La evidencia digital facilita el análisis posterior y la defensa ante reclamaciones. La integración de datos ayuda a encontrar patrones, corregir rutas, fortalecer hábitos de conducción y enfocar recursos donde el riesgo es realmente mayor.

También existe un beneficio estratégico: una cadena de suministro protegida mejora la confianza de clientes, aseguradoras, socios y autoridades. La organización puede demostrar que cuenta con controles, seguimiento y procesos de reacción, elevar su preparación frente a estándares internacionales, reducir tiempos de investigación; y tomar decisiones con evidencia en lugar de suposiciones. En mercados donde el cumplimiento y la continuidad son ventajas competitivas, la seguridad deja de ser solo un costo y se convierte en un habilitador del crecimiento.

Presencia regional, entendimiento local

La expansión de REC SAFE responde a la realidad de cadenas que cruzan fronteras y requieren continuidad entre países. Actualmente, la empresa tiene presencia en México, Argentina, Colombia y Estados Unidos. Esta cobertura permite acompañar operaciones regionales con una visión común, sin perder la sensibilidad frente a las particularidades de cada mercado, cada ruta y cada entorno operativo.

La experiencia acumulada incluye proyectos para empresas de transporte y logística, manufactura, distribución, comercio exterior, sector farmacéutico, organizaciones empresariales y entidades gubernamentales. Por confidencialidad, el valor no se expresa en una lista de nombres, sino en la capacidad demostrada para integrar trazabilidad, prevención, centros de comando y respuesta en operaciones que no pueden detenerse.

La mejor elección es la que mantiene el control

REC SAFE combina 30 años de aprendizaje operativo con plataformas propias, integración tecnológica, monitoreo permanente y una evolución constante hacia la inteligencia artificial. No se limita a vender equipos: diseña una arquitectura de protección alrededor de los riesgos reales de cada organización. Diagnostica, conecta, monitorea, automatiza y acompaña.

En un entorno donde la amenaza puede aparecer en cualquier punto del trayecto, la mejor decisión es anticiparse. “El Riesgo No Avisa. Rec Safe Sí”. Y cuando cada alerta, cada dato y cada acción forman parte de una estrategia integral, la promesa se vuelve operativa: “CONVIERTE LA INCERTIDUMBRE EN CONTROL”.

EL RIESGO NO AVISA. REC SAFE SÍ.

SOLICITE UNA CONVERSACIÓN ESTRATÉGICA

Diagnóstico SCS:
diagnostico.recsafe.tech |
contacto@recconsultores.com |
+52 55 8650 9325

Presencia en
México • Argentina • Colombia • Estados Unidos

HELP
RANSOMWARE

Desencriptación y recuperación total de datos tras ataques ransomware

Escanea
Evalúa y fortalece tu defensa digital

La defensa ya no es solo física. También es digital

Prevención de trata de personas en eventos masivos

Violeta E. Arellano Ocaña
Gerente Seguridad Corporativa
Corporación Interamericana de Entretenimiento
México
Articulista Invitado

La trata de personas —definida en el Protocolo de Palermo como la captación, transporte o recepción de personas mediante engaño, coerción o abuso de poder con fines de explotación— es uno de los delitos más lucrativos del crimen organizado transnacional. Su intersección con los eventos masivos no es casual: los mismos factores que convierten a un concierto, un torneo deportivo o una exposición internacional en un imán económico, también crean las condiciones que los tratantes explotan.

El Informe Mundial sobre Trata de Personas 2024 de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), que cubre 156 países y analiza casos detectados entre 2019 y 2023, registra una tendencia al alza:

Indicador	Dato
Víctimas detectadas mundialmente (2020–2023)	Más de 200,000 — y se estima que son solo la punta del iceberg (ONU)
Incremento global 2019–2022	+25% en víctimas detectadas (UNODC, 2024)
Personas en situación de trata o explotación (estimado total)	50 millones — OIT / Walk Free / OIM (2023)
Generación de ingresos ilícitos	USD 172,600 millones anuales (ILO Global Estimates, 2023)
Perfil de víctimas por género	61% mujeres y niñas; 38% del total son menores de edad
Trabajo forzoso: incremento 2019–2022	+47% en víctimas detectadas
Trata con fines de criminalidad forzada	Pasó del 1% (2016) al 8% (2022) del total de víctimas
Trata doméstica	58% de las víctimas son explotadas en su propio país (UNODC, 2024)

Estas cifras representan exclusivamente los casos detectados. La naturaleza oculta del delito implica que la magnitud real es sustancialmente mayor: por cada víctima identificada, se estima que existen varias más que permanecen invisibles para las autoridades.

América Latina y el Caribe: un mapa de vulnerabilidades

La región concentra patrones propios que los profesionales de seguridad deben conocer:

- En América del Sur, las mujeres representan el 45% de víctimas detectadas y las niñas el 15% adicional. En Centroamérica y el Caribe, las niñas constituyen la mayoría —52%— de las víctimas identificadas (UNODC).
- En Centroamérica y el Caribe, el 89% de las víctimas son mujeres y niñas, explotadas principalmente en bares, clubes nocturnos y espacios digitales.
- La trata es predominantemente intrarregional y doméstica: la mayoría de los tratantes son nacionales del país donde operan. Alrededor del 25% de las víctimas en 2020 provenían de otros países, incluyendo regiones distantes.
- En México hasta el 96% de los casos de trata no se reportan, y el 80% de las víctimas son trasladadas vía aérea (estimación UNODC México).
- El proyecto Track4Tip de UNODC —activo en ocho países latinoamericanos— ha generado más de 90 investigaciones penales e identificado más de 600 víctimas de trata desde su creación.

Cómo operan las redes en contextos de eventos masivos

No existe evidencia estadística que demuestre que los eventos masivos por sí solos incrementen la trata de personas. Sin embargo, los factores estructurales que acompañan a estos eventos sí facilitan la operación de redes criminales que ya existen.

Las estafas de captación siguen patrones documentados que combinan elementos presenciales y digitales:

- Ofertas de empleo falso: puestos de hostelería, entretenimiento o servicios asociados al evento, con promesas de altos ingresos y alojamiento incluido.
- Lovefraud o “novio trampa”: relación romántica acelerada que deriva en traslado, aislamiento y control.
- Captación digital previa: más del 45% de las víctimas

atendidas por el Consejo Ciudadano de la CDMX entre 2022 y 2024 fueron contactadas inicialmente a través de Facebook, Instagram, WhatsApp, Telegram o plataformas como Litmatch.
- Promesas de agencias de modelaje o casting: dirigidas especialmente a menores y jóvenes en zonas cercanas a los recintos.
- Explotación laboral encubierta: menores utilizados como vendedores ambulantes, repartidores o cocineros en economías informales que rodean los eventos.

La captación casi nunca ocurre durante el evento mismo. Los tratantes identifican y trabajan a sus víctimas semanas o meses antes, usando el evento como pretexto para la oferta o el traslado. La prevención efectiva debe comenzar mucho antes de la apertura de recintos.

Marco de prevención para organizadores y responsables de seguridad

La prevención efectiva opera en tres capas: antes del evento, durante la operación y en la cadena de proveedores.

Antes del evento — Planeación y habilitación
- Integrar la detección de trata en el Plan de Seguridad del evento como amenaza específica, con protocolos de actuación diferenciados.
- Capacitar a todo el personal de seguridad, atención al cliente, transporte y hospitalidad en identificación de indicadores
- Establecer acuerdo formal con autoridades (policía, Ministerio Público, fiscalías especializadas) para definir el protocolo de reporte y transferencia de casos.
- Publicar y difundir la línea de denuncia en toda la comunicación del evento. En México: 800 55 33 000 (Consejo Ciudadano) o 01 800 5533 000 (FEVIMTRA-FGR).
- Revisar contratos con proveedores de servicios de hospitalidad, catering y seguridad, entre otros, para incluir cláusulas de cumplimiento en materia de trata.

Durante el evento — Vigilancia operativa
- Implementar puntos de atención visible para víctimas, distintos de los puestos de seguridad, para reducir la barrera de acercamiento.
- Realizar monitoreo activo en zonas de alta rotación: estacionamientos, accesos a transporte público.
- Aplicar protocolos diferenciados para menores no acompañados: registro, verificación de acompañante y canalización inmediata si existen indicios de control externo.
- Coordinar con plataformas de transporte (aplicaciones de movilidad) para que sus conductores tengan visible la línea de reporte.

Cadena de valor — Responsabilidad extendida
- Hoteleros y arrendadores temporales deben reportar huéspedes con múltiples acompañantes rotativos o comportamientos de control sobre terceros.
- Plataformas digitales deben colaborar en el monitoreo de ofertas de empleo fraudulentas asociadas al evento, publicadas semanas antes del mismo.

Identificación de víctimas: indicadores operativos

Regla práctica para personal de seguridad:
Si al interactuar con una persona observa tres o más de estos indicadores de forma simultánea, active el protocolo previamente establecido por el organizador y autoridades o línea especializada.

No intente “rescatar” por cuenta propia: esto puede poner en riesgo a la víctima y comprometer una investigación en curso.

Conclusión: la seguridad tiene un rol clave

La trata de personas no es un problema ajeno a la industria del entretenimiento y los eventos. Las redes criminales se adaptan a aeropuertos, hoteles, recintos, zonas turísticas, economías informales de alta rotación. La diferencia entre un evento que amplifica el delito y uno que lo inhibe está, en buena parte, en la capacidad de detección dentro de su ecosistema de seguridad.

Los responsables de seguridad tienen una posición privilegiada: acceso a cámaras, información operativa, coordinación con autoridades y capacidad de formar a cientos de personas que tienen contacto directo con el público. Ese activo, bien gestionado, convierte a la seguridad privada en un eslabón real de la red de protección.

Profesionalizar esta función —con protocolos, capacitación y coordinación institucional— no es solo un imperativo ético. Es también una condición de sostenibilidad reputacional para cualquier organización que opere eventos masivos en un entorno global cada vez más exigente en materia de derechos humanos corporativos.

Categoría	Indicadores de alerta
Comportamiento	Parece asustada, evita el contacto visual, responde con monosílabos o repite frases memorizadas.
Control externo	Alguien más responde por ella, la acompaña en todo momento y no la deja hablar a solas.
Documentos	No porta identificación o alguien más “guarda” sus documentos.
Físico	Presenta signos de desnutrición, cansancio extremo, lesiones o ropa inapropiada para el contexto.
Orientación	No sabe en qué ciudad se encuentra, desconoce la dirección de donde se hospeda.
Laboral	Trabaja en condiciones de servidumbre, sin pago ni libertad de movimiento.
Digital	Fue contactada previamente por redes sociales con oferta de empleo, hospedaje o pareja romántica.

Envía tus comentarios, dudas, experiencias o sugerencias de temas a: varellano@cie.com.mx

HTT – SECURITY GROUP – apuesta por un modelo integral para anticipar los nuevos riesgos corporativos

La transformación de los riesgos empresariales modificó ya la forma en que las organizaciones entienden la seguridad. Hoy, proteger un negocio implica muchos más aspectos que sólo resguardar instalaciones o controlar accesos. También exige garantizar la continuidad de las operaciones, fortalecer la cultura ética, responder a crisis, prevenir incidentes y preservar la confianza de clientes, colaboradores e inversionistas.

Con esa visión, HTT Security Group presentó una nueva estructura corporativa integrada por empresas especializadas para responder a las necesidades actuales de organizaciones nacionales e internacionales mediante soluciones coordinadas de gestión de riesgos.

Después de 15 años de crecimiento en servicios de seguridad privada, la organización inicia una nueva etapa con un modelo que integra consultoría

- *Presenta una estructura empresarial que integra consultoría, continuidad de negocio, protección ejecutiva, compliance y seguridad especializada.*
- *Su ecosistema reúne firmas con experiencia en riesgos corporativos, ética empresarial, protección escolar y operaciones regionales en América Latina.*
- *La organización busca convertirse en un aliado estratégico para empresas que requieren proteger personas, operaciones, información y reputación.*

Gerardo de Lago, Socio Fundador y Director de Consultoría

José Antonio Mollevi, Director Jurídico y Compliance

Francisco de Lago, Presidente de Consejo

estratégica, protección ejecutiva, continuidad de negocio, inteligencia corporativa, compliance, protección civil, certificación de instituciones educativas y capacitación especializada.

Lo que representa es la solidez de tener un grupo profesional muy fuerte, donde cuando el cliente tiene un problema, más que sólo ofrecer un acompañamiento simple, es realmente aportar soluciones de largo plazo, explicó Gerardo de Lago, socio fundador y director de Consultoría de HTT Security Group.

"Esta evolución responde a un cambio profundo en la demanda del mercado, ya que cada vez más empresas requieren proveedores capaces de integrar distintas disciplinas bajo una misma estrategia, lo que permite reducción de tiempos de respuesta y facilita la toma de decisiones frente a escenarios de incertidumbre. Esa profesionalización logró que hoy tengamos marcas específicas con identidad propia, con un nivel de experiencia que explota esos 30 años de historia, pero lo hace palpable y profesional en el día a día con los clientes", afirmó el directivo.

Como parte de esta reorganización, el grupo incorpora firmas especializadas como Timur Latinoamérica, enfocada en consultoría de riesgos, continuidad de negocio, protección civil, manejo de crisis y compliance; Ética Integral, dedicada a fortalecer programas de integridad corporativa, canales de denuncia y cumplimiento normativo; y Safe Schools Certification, iniciativa mexicana que promueve estándares de seguridad para instituciones educativas en América Latina.

Experiencia como propuesta de valor

Asimismo, el crecimiento se sustenta en la experiencia de su equipo directivo liderado por Gerardo de Lago, quien acumula más de tres décadas en posiciones de liderazgo dentro de corporativos internacionales y cuenta con certificaciones como CPP de ASIS International, además de formación especializada en continuidad de negocio, protección ejecutiva, negociación de secuestros, respuesta a incidentes críticos y seguridad institucional. A lo largo de su trayectoria dirigió programas de seguridad para operaciones multinacionales en América Latina, experiencia que hoy forma parte de la propuesta de valor del grupo.

Entre los servicios desarrollados por HTT Security Group destacan la evaluación integral de riesgos, investigaciones corporativas, programas de continuidad operativa, protección de ejecutivos, entrenamiento basado en escenarios reales, análisis de responsabilidades, cumplimiento normativo, gestión ética y plataformas tecnológicas para la recepción confidencial de denuncias. El propósito consiste en acompañar a las organizaciones antes, durante y después de un incidente, fortaleciendo su capacidad de respuesta y recuperación.

Uno de los principales objetivos del grupo consiste en simplificar la gestión de la seguridad mediante un esquema de atención integral: "Lo que queremos es que cuando el cliente piense en seguridad, piense que ofrecemos un servicio de 360 grados, que no tenga que buscar siete proveedores para desarrollar un programa integral", señaló de Lago.

Clientes y personal al centro

La organización mantiene operaciones en México y una red de especialistas en Guatemala, Honduras, Costa Rica, Colombia, Perú y Venezuela, lo que le permite atender proyectos regionales bajo metodologías homogéneas. Entre las organizaciones mencionadas durante la presentación figura Amazon como uno de los primeros clientes internacionales atendidos por el grupo.

Finalmente, la dimensión humana continúa siendo uno de los pilares del proyecto: "De esta empresa comemos 700 familias y eso lo tomamos muy en serio. Queremos ser una empresa responsable para los clientes, para nuestros colaboradores y contribuir a un México más tranquilo", concluyó el directivo.

El cumplimiento regulatorio y la continuidad operativa ocupan hoy en día un lugar prioritario en las agendas corporativas, y la firma HTT Security Group ha decidido apostar por una estrategia basada en especialización, experiencia internacional y soluciones integradas que acompañan la evolución de las empresas frente a los desafíos de un entorno mucho más difícil y complejo.

Seguridad privada en México
bajo presión regulatoria, laboral y operativa:

AMESP
Asociación Mexicana de Empresas de Seguridad Privada A.C.

La seguridad privada en México ha adquirido un papel central dentro de la operación de múltiples sectores, pues hoy cubre funciones críticas en instalaciones estratégicas, centros comerciales, aeropuertos, hospitales y corporativos, entre otros.

El crecimiento del sector responde a una realidad muy concreta: la capacidad del Estado para cubrir la totalidad del territorio y de los servicios es limitada, lo que ha abierto espacio a una industria que ya supera los 600 mil elementos operativos en el país y que agrupa a más de 8 mil empresas, muchas de ellas sin regulación formal.

En este contexto, la Asociación Mexicana de Empresas de Seguridad Privada -AMESP-, es un eje de orden y profesionalización en un mercado fragmentado. Además de representar intereses empresariales, su papel también intenta establecer estándares mínimos de operación en una industria donde la heterogeneidad es la regla.

Desde la presidencia de la AMESP, Daniel Espinosa Ávila, describe el momento que atraviesa el sector como una etapa de transformación profunda: “La seguridad privada está cambiando… debemos volvernos mucho más profesionales, tenemos que entregar personal muy bien capacitado”, señala.

El diagnóstico apunta a un problema de tipo estructural donde el crecimiento del sector no ha ido acompañado de una homologación en calidad, capacitación ni cumplimiento normativo.

Uno de los puntos más críticos es la competencia desleal. Las llamadas “empresas patito” operan sin registro, sin controles y sin responsabilidad legal sobre su personal. El directivo advierte que el problema no es únicamente en lo económico: “No solamente es un precio, es un riesgo muy grande para la seguridad”. La ausencia de controles tiene implicaciones operativas graves. En caso de incidentes, la trazabilidad se pierde: “No sabemos quién es, no hay ni cómo empezar una investigación”, afirma.

El problema se agrava por una limitación institucional. De acuerdo con el titular de la AMESP, la autoridad tiene capacidad para supervisar a empresas registradas, pero no necesariamente para identificar y sancionar a las que operan fuera del sistema: “La autoridad solamente tiene dientes… para atender a las empresas que están registradas”, explica. Esto genera un incentivo perverso: quien cumple con la ley asume mayores costos, mientras que quien opera en la informalidad reduce precios sin asumir responsabilidades.

El resultado es que su impacto se traslada directamente al mercado. Las empresas formales enfrentan una presión constante sobre sus tarifas. Al respecto, Espinosa Ávila utiliza una analogía: contratar servicios irregulares “es como comprar mercancía pirata”, puede funcionar en el corto plazo, pero no garantiza continuidad ni seguridad. Además, la afectación no se limita a las empresas; alcanza a los trabajadores, que en muchos casos quedan fuera de esquemas de seguridad social y capacitación.

A esta presión estructural se suma un cambio regulatorio que podría redefinir la operación del sector: la reducción de la jornada laboral de 48 a 40 horas. Aunque la medida responde a una lógica de derechos laborales, su implementación en seguridad privada presenta desafíos específicos. La industria opera bajo esquemas de turnos extendidos —12x12 o 24x24— que no se ajustan fácilmente a una jornada estándar.

Daniel Espinosa lo plantea sin matices: trasladar ese ajuste a la operación tiene un impacto directo en costos: “Imposible… tenemos que trasladarlo al cliente”, reconoce. La consecuencia es inmediata: servicios más caros o reducción en cobertura.

Cuando hay un entorno de competencia desleal, el riesgo es que las empresas formales pierdan mercado frente a esquemas informales que no cumplen con la regulación.

La reforma laboral también suma un riesgo adicional: el crecimiento de la informalidad, por lo que se advierte que algunos sectores ya están sustituyendo empresas formales por esquemas alternativos: “Empiezan a contratar gente… que le pusieron otro nombre pero que hacen esas labores”, explica.

Frente a este escenario, la AMESP ha optado por fortalecer mecanismos internos de control. El proceso de afiliación incluye verificación de cumplimiento legal, capacitación continua y actualización en temas fiscales, regulatorios y operativos. “Cuando ingresa una nueva empresa verificamos que efectivamente cumpla con la ley… y además les damos capacitación”, señala. La estrategia apunta a elevar el estándar de sus asociados por encima del mínimo legal.

La asociación ha impulsado diplomados y programas dirigidos a niveles administrativos y directivos, incorporando temas fiscales, legales y de gestión de riesgos. El objetivo es cerrar brechas de conocimiento que afectan la operación completa de las empresas. La expansión del sector es evidente, pero su consolidación depende de resolver problemas estructurales que van más allá de la oferta de servicios.

Daniel Espinosa Ávila, presidente de la AMESP

GRUPO ALEM

Seguridad Privada Integral S.A. de C.V.

¡Garantizamos su tranquilidad!

Guardias intramuros: Capacitados en diferentes modalidades (condominios, plazas comerciales, fábricas, etc)

Escoltas: Entrenados constantemente y especializados de acuerdo a la actividad del protegido

Custodias: Para todo tipo de transporte de mercancías en tránsito

Rastreo satelital: Vehículos particulares, carga o flotillas

Videovigilancia: Fija, móvil y remota

Análisis de riesgos y vulnerabilidades: Desarrollado por expertos en seguridad física y patrimonial

www.grupoalem.mx

edgar.seguridad.integral@gmail.com

+52 564705 2246

Calidad vs cantidad,

objetivo del sector de geolocalización:

AMESIS[MR]

- Muchas compañías están debidamente registradas, pero muy pocas son confiables y seguras.
- Es necesario prestar atención sobre todo cuando se trata de intangibles que tienen que ver seguridad y están involucrados unidades, mercancías y vidas humanas.

Apesar de que no existe un padrón real sobre el universo de compañías de localización satelital que atienden al transporte de carga, pasaje y particular, se estima que existen alrededor de 300, incluso muchas están registradas ante las secretarías de Seguridad y Protección Ciudadana (SSPC) y estatales, pero no significa que cuenten con estándares de calidad en el servicio y confiabilidad de las plataformas y procedimientos que ofrecen al mercado.

De acuerdo con datos de la SSPC, en la actualidad están registradas a nivel federal más de 3 mil empresas de seguridad privada y cientos de estas compañías ofrecen el servicio de rastreo satelital.

Raymundo Mancera Sandoval, presidente de la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital (AMESIS), alertó que otro fenómeno adicional de la competencia desleal con las compañías “irregulares”, es aquel donde muchas firmas legales de la geolocalización poseen los permisos oficiales pertinentes, pero carecen de certificados en cuanto a calidad del producto y servicio al usuario final.

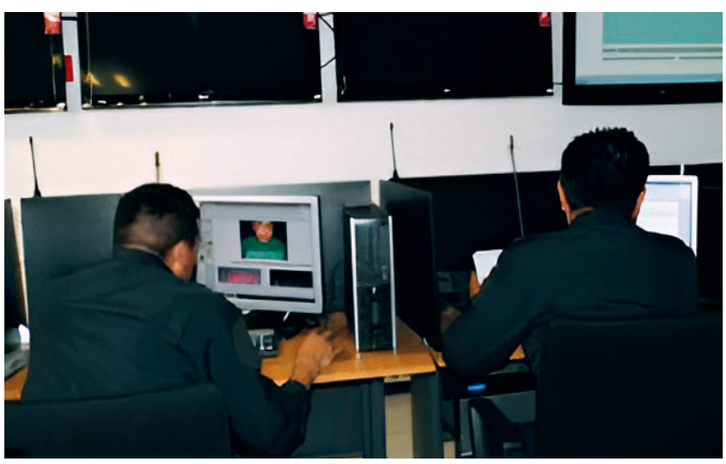
“Como empresas formales y profesionales, instamos a nuestros clientes a que investiguen y clasifiquen a los proveedores confiables, ya que, aunque muchos de ellos estén autorizados por las SSP, esto no garantiza su profesionalismo ni la calidad de sus servicios”. Señaló que es vital tener cuidado, especialmente cuando se trata de intangibles relacionados con un asunto tan sensible como la seguridad y que involucra a vidas humanas, unidades y mercancías.

A juicio de la AMESIS, organización con 18 años de existencia y permanencia en los sectores del transporte de carga y seguridad, muy pocas firmas llevan a cabo evaluaciones de satisfacción al cliente, de la infraestructura, experiencia, durabilidad, calidad y eficiencia de las soluciones de localización.

“Es importante señalar que, para aquellos de nosotros que nos ocupamos de proteger vehículos y mercancías en tránsito, proporcionar resultados satisfactorios es una prioridad. Es necesario que los protocolos se apliquen en segundos, que la reacción no tarde más de 20 minutos y que la resolución ocurra lo más pronto posible, ya que de esto depende si un delito se frustra”, añadió el directivo.

El GPS y sus servicios ofrecidos debe ser confiable y sobre todo proteger las cuantiosas inversiones de prácticamente todos los sectores económicos, contando con el respaldo de técnicos monitoristas capacitados, centros de monitoreo para emergencias (no garajes o automonitoreo por internet) y asesores de seguridad especializados en el tema de rastreo satelital.

La inseguridad en México es considerada por la asociación como el detonante principal de la proliferación de centenares de empresas ilegales que ofrecen servicios de rastreo satelital y seguridad sin ningún tipo de regulación. Por esta razón, se considera prioritario mantener una relación con las autoridades gubernamentales en los tres niveles para cooperar eficazmente en beneficio de los usuarios finales.



Recomendaciones vs empresas irregulares

AMESIS recomienda que, para cerrarle el paso a las empresas irregulares de rastreo y localización satelital, el cliente puede contribuir si al momento de contratar el servicio exige:

- Que cuente con la autorización vigente expedida por la autoridad federal o estatal.
- Verificar si posee alguna certificación de calidad (ISO o similar).
- Asegurar el servicio mediante un contrato avalado por la PROFECO.
- Exigir una factura oficial de los trabajos contratados.
- Exigir la garantía por escrito del producto y servicio contratado.
- Preferir empresas que se manejen sobre Estándares de Competencia Laboral del CONOCER.
- Verificar si cuenta con reconocimientos vigentes de asociaciones relacionadas al sector.
- Solicitar la documentación que avale la experiencia de la empresa.
- Solicitar al menos cinco referencias comerciales para validar su servicio.

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 ingenio en tiempos de guerra

el blindado polaco FT-B con plataforma del Ford modelo T

Ricardo Guzmán
Director de operaciones en vinculo estrategas comerciales. Amplia experiencia en el ámbito del blindaje automotriz y colaborador comecial a nivel gerencial y directivo en las más importantes blindadoras de México
rguzman@vinculoec.com.mx
México
Articulista Invitado

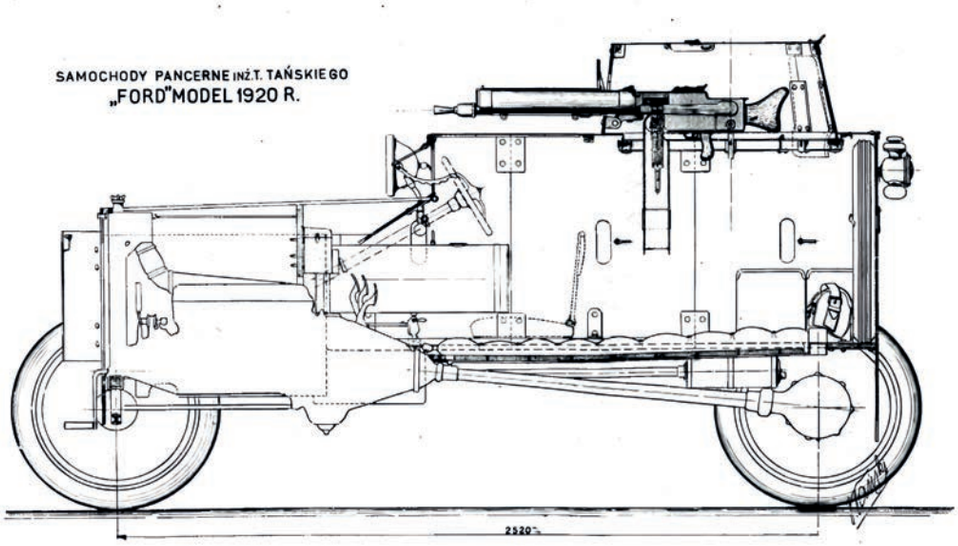
En 1920 Polonia estaba en guerra con la Unión Soviética, los rusos habían llegado a través de Ucrania y estaban a las puestas de Varsovia. Polonia tenía la cuarta división blindada más grande del mundo en ese momento. Sin embargo, los tanques Renault FT-17 eran vehículos lentos e inadecuados para el tipo de maniobras rápidas que los polacos necesitaban para contrarrestar a los soviéticos. Esto hacia la urgente necesidad de hacerse de una flotilla de acorazados y en parte lo lograban capturando algunos vehículos de combate de otros países, pero presentando los mismos problemas de movilidad con las orugas. El pueblo polaco había utilizado el ingenio para improvisar vehículos blindados en el pasado reciente, sobre todo con el camión blindado conocido como “Tank Pilsudskiego” de 1918. Diseñado en 1920 por Tadeusz Tanski, el Ford FT-B se basaba en el chasis clásico del Ford Modelo T, ligeramente modificado.

Motor Ford de 22,5 CV, 2900 cc, a gasolina, 4 cilindros en línea, 4 tiempos, refrigerado por agua, arranque con manivela.

Contaba con un bastidor rectangular de acero y suspensión con ballestas transversales semielípticas. El eje trasero se reforzó adicionalmente con largueros. La posición del depósito de combustible se cambió de transversal debajo del asiento del conductor a longitudinal, junto al conductor. Las ruedas eran de madera y las dimensiones de los neumáticos eran de 30 x 3.5 pulgadas. Tanski utilizó planchas hechas con placas de acero de trincheras alemanas, material recuperado de los campos de batalla polacos tras la primera guerra mundial y rellenó los neumáticos con pulpa de madera para protegerlos hasta cierto punto contra las balas de fusil y ametralladora. El resultado fue un pequeño vehículo blindado, con una tripulación de dos personas, armado con una ametralladora en una torreta giratoria.

El blindaje tenía un espesor de 8 mm. En algunas publicaciones se indica que las placas superiores tenían un blindaje de 3 mm. sin embargo, según el informe de la comisión de abril de 1921, las placas superiores no estaban blindadas, sino que eran de chapa de acero común de 2 mm. La parte inferior no estaba blindada, sino hecha de tablones de madera. Se podía utilizar una cubierta blindada sobre el radiador de agua de la ametralladora con un pequeño escudo.

También había una escotilla de dos partes sobre el conductor que facilitaba la conducción en condiciones no de combate. El radiador estaba protegido con puertas blindadas. Una rueda de repuesto se transportaba en el interior a lo largo de una plancha trasera del casco. Los coches podían diferir en los detalles del blindaje, inicialmente no tenían faros, posteriormente se les instaló un único faro delante de la plancha frontal del conductor. La torreta tenía forma pentagonal, estrechándose hacia adelante, con una pequeña escotilla en una plancha superior. El blindaje protegía contra balas perforantes de fusil a 300 m y contra balas de fusil convencionales a cualquier distancia. El peso de la armadura era de aproximadamente 590 kg.



El cuerpo blindado podía desmontarse de una sola pieza y estaba sostenido por una estructura de ocho puntos.

El diseño fue aprobado de inmediato por las autoridades el 12 de junio de 1920 y el prototipo se completó en dos semanas a finales de junio. Las pruebas resultaron satisfactorias

y se encargó una serie. Los Ford blindados se construyeron bajo la supervisión de Tański en la fábrica de herramientas

Gerlach & Pulst en Varsovia, que ya había fabricado vagones para trenes blindados. El Ford FT-B fue el primer vehículo blindado polaco fabricado en serie produciéndose entre 16 y 17 unidades según algunas fuentes.

El coche tenía puntos débiles como las tablas del piso de madera sin protección y los mismos radios de madera en las ruedas. Sin embargo, en parte debido a que era un vehículo considerado rápido en la época, el enemigo nunca pudo aprovechar esas debilidades. Cada coche estaba tripulado por dos hombres armados con una sola metralleta alemana Maxim 05/15 de 7.92 mm. con 1250 balas, así como 25 granadas de mano. Debido a la naturaleza simple del motor Ford, los vehículos rara vez se averiaban y cuando lo hicieron, los equipos hicieron reparaciones en el campo, incluso a veces bajo el fuego mismo incluso si se requería una reparación más profunda, toda la parte blindada del coche podía levantarse del bastidor en una sola pieza. Un aspecto curioso es que el FT-B podía funcionar con combustible y aceite de mala calidad, una ventaja indispensable en condiciones de escasez de suministros en tiempos de guerra.

El Ford FT-B se desempeñó bien durante la guerra polacobolchevique de 1920, sobresaliendo en el combate de alta movilidad que caracterizó ese conflicto, tan diferente de la guerra de trincheras estática de la Primera Guerra Mundial. El Ford se distinguió particularmente en “La incursión en Kovel” y salvó a muchos soldados polacos durante la retirada de Ucrania hacia Varsovia. Luego apoyó el contraataque hacia el este, después de la exitosa defensa de Varsovia, conocida como el “Milagro del Vístula”, donde Sikorski derrotó a los rusos haciéndolos huir en el proceso y enviando ellos retrocediendo por la frontera ucraniana y más allá. Bastantes Ford FT-B sobrevivieron hasta la década de 1920, en 1930 solo tres todavía estaban en condiciones de uso y fueron retirados en 1931, aunque algunos indicios sugieren que al menos uno sobrevivió hasta 1939.

Arquitectura de la paz

Dra. Mercedes Escudero Carmona

Presidenta de CPTED México ICA Chapter. Analista especialista, comentarista, conferencista y ponente internacional en temas de seguridad humana, seguridad, prevención del delito y violencia en diferentes ciudades y países.

México

Articulista Invitado

EL DATO

26 %

Reducción de incidentes violentos entre internos expuestos a imágenes de naturaleza (proyecto NIPP, Snake River Correctional Institution).

Parte 2 de 2

Cancún, México.- En la primera parte de este artículo, mencionaba que durante siglos pensamos la seguridad de una prisión como una cuestión de muros: cuanto más altos, mejor. Pero los muros solo detienen cuerpos. Lo que ocurre dentro —si un centro fabrica reincidentes o los desactiva— se juega en un territorio mucho más sutil: la forma del espacio que las personas habitan cada día.

La prueba noruega:

Si todo esto suena a teoría, hay un experimento a escala real. Los países nórdicos adoptaron el **principio de normalidad:** la vida dentro debe parecerse a la de fuera tanto como la seguridad permita, porque la privación de libertad es el castigo y no hace falta añadir sufrimiento ambiental. Habitaciones individuales, madera, colores neutros, verde y agua. El resultado no es sentimental, es estadístico: tasas de reincidencia en torno al 20 %, frente al 45 % de sistemas estrictamente punitivos.

> "El diseño no es indulgencia: es una inversión en seguridad pública futura."

La evidencia se acumula en la misma dirección. El proyecto Nature Imagery in Prisons Project (NIPP), en Oregón, de 2012 a 2017, midió una caída del 26 % en la violencia de internos que veían vídeos de naturaleza. Otros estudios muestran que fragmentar los grandes pabellones en unidades pequeñas reduce el aislamiento y la ansiedad. El diseño ambiental, visto así, no es un gasto blando: es una infraestructura de prevención con retorno medible en víctimas evitadas y reingresos que no ocurren.

Cinco fases para que el diseño rinda cuentas:

Lo que separa a este enfoque de una buena intención es el método. El sistema despliega el diseño en cinco fases encadenadas, cada una anclada a normas concretas. Gobernanza, donde se fijan políticas, responsables y respeto a los derechos humanos. Evaluación, donde se identifican amenazas y se documenta el riesgo antes de trazar una línea. Diseño y protección, el corazón técnico, donde convergen las seis estrategias físicas y las cuatro sociales con la arquitectura de seguridad protectora de la ISO 22341:2021 y 22341-2:2025. Capacidades operativas, que garantizan que el centro resista emergencias sin perder su blindaje. Y mejora continua, que audita los incidentes contra la configuración del espacio y realimenta todo el ciclo.

El efecto de esta cadena es que ninguna decisión de diseño queda a merced del gusto o la improvisación: todas son verificables, defendibles y mejorables. Es, en el fondo, aplicar a los muros la misma exigencia de calidad que cualquier sistema crítico.

El ojo que aprende:

La última frontera es digital. La analítica de vídeo con inteligencia artificial permite detectar anomalías de movimiento —un corrillo que se forma donde no debería, un patrón que anticipa una riña— sin alterar la naturaleza del espacio ni convertir el centro en un panóptico. La cámara deja de ser un ojo pasivo y se vuelve un sensor del sistema de riesgo, sujeto además a su propio marco de control y de auditoría de sesgos. Tecnología al servicio del entorno, no al revés.

Gobernar, pacificar, reinsertar:

La conclusión atraviesa todo el recorrido. La sofisticación de una prisión del siglo XXI no está en elegir entre dureza y humanidad, sino en equilibrarlas con precisión científica. La ecuación de vulnerabilidad lo formaliza; la hoja de ruta del Sistema de Gestión de Riesgos Socio Urbano CPTED lo hace trazable; la evidencia lo confirma; los indicadores lo hacen auditable. Un centro concebido de este modo no se limita a contener. Gobierna, pacifica y reinserta. Y al hacerlo protege algo que empieza dentro de sus muros pero se juega fuera de ellos: la seguridad de todos.

Autoría. Dra. Mercedes Escudero Carmona

FUENTES DE CONSULTA BÁSICA:

Marco normativo. ISO 22341:2021 (CPTED) · ISO 22341-2:2025 (entornos residenciales/resguardo) · ISO 22340:2024 (arquitectura de seguridad protectora) · ISO 31000/IEC 31010 (gestión del riesgo) · ISO 19011 (auditoría) · ISO/IEC 42001 (IA).

Evidencia citada. Nature Imagery in Prisons Project (~26 % de violencia); principio de normalidad nórdico (~20 % vs ~45 % de reincidencia); literatura sobre diseño salutogénico y trauma-informado en instituciones juveniles.

¡Únetenos!

CON SEGURIDAD
Magazine Latam

Síguenos en

Telegram e Instagram

@conseguridadmagazine

La atención como activo organizacional

Milagros Céspedes Alvarez
Directora de CES Latam. Especialista en Neuroseguridad y Neuroliderazgo en la Seguridad Corporativa
Perú

Articulista Invitado

La primera línea de defensa no siempre es un procedimiento. A veces es una mente verdaderamente presente.

Parte 2 de 2

Lima, Perú.- En la primera parte de esta entrega, comenté que durante más de 30 años que llevo en el rubro y como muchos profesionales de seguridad, aprendí a evaluar amenazas, vulnerabilidades y fallas en los controles. Sin embargo, hace semanas vengo observando algo que aparentemente podría ser insignificante pero que me llevó a una pregunta de reflexión. Hace ya varios meses que conduciendo de noche noto que varios vehículos circulan sin las luces delanteras encendidas.

Nicholas Carr, en The Shallows, plantea que Internet no necesariamente reduce nuestra inteligencia, pero sí modifica la forma en que prestamos atención, favoreciendo un procesamiento superficial sobre uno profundo.

Por otra parte, Gloria Mark ha demostrado que el tiempo que permanecemos concentrados antes de cambiar de estímulo se ha reducido de manera significativa y que cada interrupción tiene un costo cognitivo que rara vez percibimos.

No se trata de demonizar la tecnología, en absoluto. La tecnología seguirá potenciando nuestras capacidades y transformando la forma de trabajar.

El desafío consiste en **comprender cómo influye sobre el comportamiento humano para gestionar mejor sus riesgos**. Y eso tiene una razón potente, un cerebro saturado detecta menos anomalías, comete más errores, es más vulnerable a la ingeniería social, prioriza peor, responde con mayor dificultad durante una crisis y disminuye su capacidad para tomar decisiones de calidad.

Eso deja de ser únicamente un asunto de bienestar o de recursos humanos para convertirse en un asunto de gobernanza, resiliencia y seguridad corporativa.

Quizá por eso empiezo a pensar que, así como hoy evaluamos la madurez de una organización respecto a sus procesos, tecnologías o controles, en un futuro también evaluaremos su **capacidad para gestionar la carga cognitiva, la fatiga digital y la calidad de la atención de sus equipos**.

No porque la atención sea una moda. Sino porque cada vez será más evidente que constituye un recurso estratégico.

Durante años hablamos de la gestión del conocimiento, quizás la siguiente evolución sea la **gestión de la atención, no para producir más, sino para pensar mejor.**

Y aquí aparece una idea que considero importante para quienes lideramos personas.

No basta con desarrollar competencias, debemos desarrollar presencia.

No me refiero a presencia como una práctica de moda, como un estado físico, hablo de la capacidad de estar completamente disponible para la realidad que tenemos delante.

Cuando un gerente está presente detecta señales débiles, un investigador presente realiza mejores entrevistas, un operador presente evita accidentes, un líder presente escucha aquello que nadie dijo, un comité presente toma mejores decisiones. Todo comienza allí.

Después de más de tres décadas en seguridad, hoy tengo la impresión de que la atención podría ser el primer control de seguridad de cualquier organización, antes que una cámara, un procedimiento o un algoritmo.

Porque finalmente todos esos controles dependen de un ser **humano capaz de observar, interpretar y actuar.**

Quizá la pregunta que deberíamos empezar a hacernos ya no es cuánto conocimiento posee una organización, sino

¿Cuánta atención es capaz de sostener?

Las crisis rara vez comienzan por falta de conocimiento.
Con frecuencia comienzan porque alguien no vio
no escuchó
no conectó
no preguntó
no estuvo verdaderamente presente.

Porque al final, antes de cualquier decisión existe un instante del que depende todo: el momento en el que prestamos, o dejamos de prestar, atención.

Alianza internacional:

SERCOPP

MÁS SEGURIDAD Magazine

CON SEGURIDAD Magazine Latam

Ya está en México

- Instalaciones
- Vehículos
- Rutas
- Rondas
- Minuta
- Novedades

LA HERRAMIENTA MÁS COMPLETA PARA LA SEGURIDAD PRIVADA

1. Licencia de uso por el termino de un año, con el IVC - imagen visual corporativa de la empresa, colores, logo. Imagen o video de fondo en el front principal o de menú.

2. Usuarios individuales ilimitados mes (3 tipos de perfil: Operador, Analista, Director).

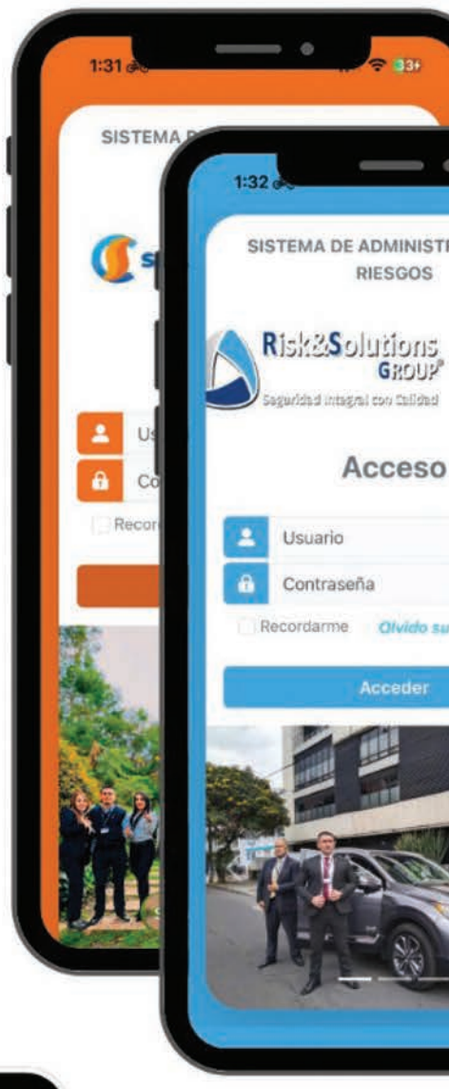
3. Capacitación y entrenamiento al personal operativo actual y nuevo del nivel Supervisores, Analistas, Coordinadores, Jefes y Directores.

4. Servidor o alojamiento dedicado para los Análisis de Riesgos e informes de la empresa, con alta redundancia y disponibilidad.

5. Certificado SSL (Secure Sockets Layer): certificado digital que autentica la identidad de sari.com.

6. Dominio con nombre de la empresa: https://empresa.sari.com.co/index.html

7. Soporte técnico de Lunes a Sábado de 08:00 a 18:00 horas y/o 24 * 7 nivel de critico de la plataforma.



SOLICITA TU DEMO YA!

08:00 A. M. - 06:00 P. M. (57) 3108052421 DG 81I #74C-19 OF. 202 - BOGOTÁ, COLOMBIA

RocketGO Academy educación que potencia conocimientos

conocimientos en capacidades para América Latina

Bogotá, Colombia.- RocketGO nace en Colombia en 2020, en uno de los momentos más desafiantes para la humanidad: la pandemia. Mientras empresas, profesionales y estudiantes enfrentaban nuevas formas de trabajar y aprender, también surgía la necesidad de fortalecer conocimientos, gestionar riesgos y adaptarse a entornos inciertos. En ese contexto, Leonardo Garcés (Colombia) y Rodolfo Cepeda (México), dos empresarios y emprendedores comprometidos con el mejoramiento de las organizaciones y las personas, decidieron crear una plataforma educativa con visión regional.

Desde su origen, RocketGO ha tenido un propósito claro: potenciar conocimientos, habilidades y competencias aplicables a la vida profesional y empresarial. Su propuesta se enfoca en áreas estratégicas como gestión de riesgos, seguridad, mejoramiento de procesos, continuidad de negocio, cumplimiento, ética, seguridad de la información y resiliencia organizacional.

Su mayor fortaleza en el sector de la seguridad es la educación, entendida no solamente como transmisión de información, sino como una herramienta para prevenir, anticipar escenarios, tomar mejores decisiones y construir organizaciones más confiables.

La presencia de RocketGO en Colombia, México y Estados Unidos impulsa su expansión en América Latina. La compañía proyecta ampliar su oferta académica mediante un modelo integral, accesible, innovador y económicamente competitivo, respaldado por altos estándares de calidad. El objetivo es democratizar el acceso a conocimientos especializados que, con frecuencia, se concentran en programas costosos, extensos o dirigidos únicamente a expertos.

Uno de sus principales diferenciadores es su metodología de aprendizaje. RocketGO reconoce que las personas aprenden de maneras distintas y, por ello, combina videos, clases breves, casos prácticos, evaluaciones, infografías, documentos técnicos, podcasts y ejercicios aplicados. Esta diversidad permite avanzar desde un nivel básico hasta uno avanzado, mediante rutas flexibles para estudiantes,

profesionales, emprendedores, empleados, directivos y cualquier persona interesada en fortalecer sus capacidades.

La plataforma también fue concebida como una comunidad de conocimiento. RocketGO busca integrar expertos, instituciones técnicas, organismos sectoriales, empresas y universidades, bajo la convicción de que nadie posee una verdad absoluta, pero todos pueden aportar experiencias y aprendizajes que enriquezcan a los demás. Esta visión permitirá desarrollar alianzas regionales y programas adaptados a las necesidades de distintos sectores.

En materia de certificación, RocketGO quiere ir más allá del diploma tradicional. Su modelo contempla certificados de habilidades e insignias digitales que permiten evidenciar las competencias fortalecidas por cada estudiante. Así, la formación se convierte en un activo útil para la empleabilidad, el crecimiento profesional y el desarrollo del talento dentro de las organizaciones.

Los resultados ya respaldan esta visión. Más de 2.000 estudiantes en América Latina han participado en sus procesos de formación. Además, diferentes empresas han confiado en RocketGO para fortalecer las competencias de sus equipos y convertir el aprendizaje en buenas prácticas, mejoras de procesos y decisiones más seguras.

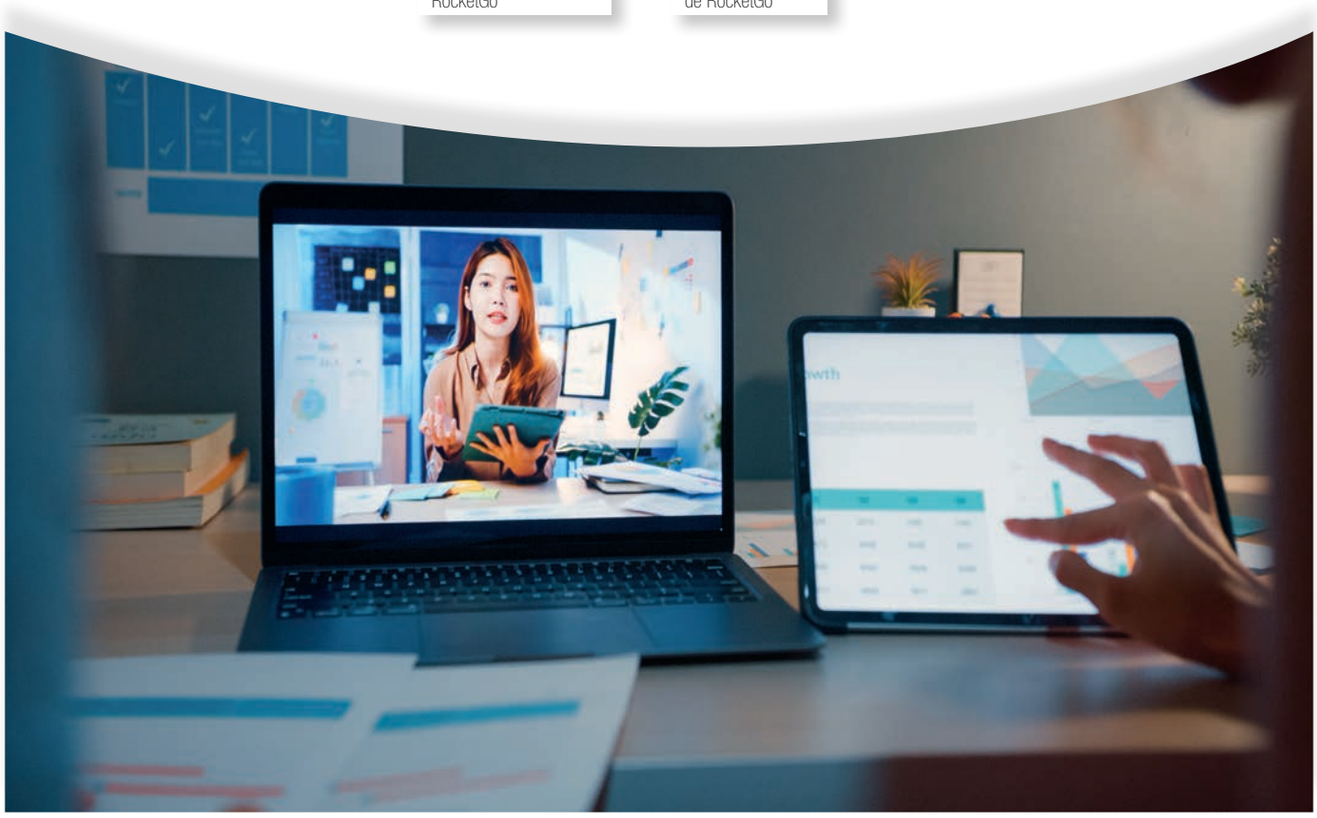
RocketGO no es solamente una plataforma de cursos. Es un ecosistema educativo diseñado para transformar conocimiento en acción, conectar personas con oportunidades y preparar a las organizaciones para los desafíos del presente y del futuro.

Su apuesta es ambiciosa: convertirse en un referente latinoamericano de educación aplicada en gestión, riesgos, seguridad y resiliencia. Porque aprender es importante, pero aplicar lo aprendido es lo que realmente transforma.

Potencia Tus Conocimientos!

Leonardo Garcés (Colombia), directivo de RocketGo

Rodolfo Cepeda (México), directivo de RocketGo



Cuando la inteligencia artificial mejora el discurso

pero no la capacidad de proteger

Edison Cadena Ayala
MSC, CPO, CPOI, CSSM
CEO
SEINNATIONAL CIA. LTDA.
Ecuador
Articulista Invitado

> El riesgo de confundir sofisticación narrativa con madurez operacional
> «El verdadero problema no es si las máquinas piensan, sino si los seres humanos lo hacen».
> *— B. F. Skinner*

Quito, Ecuador.- Debo comenzar este artículo con transparencia, indicando que yo también utilizo inteligencia artificial. El uso que le doy está enfocado en contrastar ideas, ordenar información, identificar vacíos y comunicar con mayor claridad. Sería incoherente descalificar una herramienta de cuyo potencial me beneficio.

Precisamente por utilizarla, reconozco su límite y en ese contexto estoy seguro que puede mejorar la forma de un análisis antes de que el autor haya consolidado el conocimiento que aparenta representar.

Y eso en seguridad, es una diferencia que importa mucho. Hoy es posible producir en minutos informes, matrices, procedimientos e indicadores con lenguaje técnico convincente. Sin embargo, una recomendación no es pertinente porque esté bien redactada; un procedimiento no es aplicable porque parezca completo; ni un indicador demuestra eficacia por aparecer en un tablero.

La expansión es innegable. El AI Index 2026 de Stanford señala que la adopción organizacional de IA llegó al 88 % entre las entidades encuestadas. Los incidentes documentados relacionados con IA aumentaron de 233 en 2024 a 362 en 2025: 55,4 %. Esto no prueba causalidad, pero advierte que la capacidad tecnológica crece más rápido que su gobernanza responsable.

El Global Cybersecurity Outlook 2026 refuerza esa lectura: 77 % de las organizaciones consultadas ya utiliza IA en ciberseguridad, mientras 54 % identifica falta de conocimientos o competencias, 41 % reconoce la necesidad de supervisión humana y 39 % mantiene incertidumbre sobre los riesgos. La brecha, por tanto, no está entre seres humanos y máquinas, sino entre velocidad de adopción y capacidad de juicio.

IA EN LAS ORGANIZACIONES: Adopción, incidentes y brechas de supervisión

Indicador	Resultado
Adopción organizacional de IA	88 %
Incidentes documentados relacionados con IA, 2024–2025	233 → 362 (+55,4 %)
Organizaciones que utilizan IA en ciberseguridad	77 %
Falta de conocimientos o competencias	54 %
Necesidad de supervisión humana	41 %

Fuente: elaboración propia con datos de Stanford Institute for Human-Centered Artificial Intelligence (2026) y World Economic Forum (2026). La variación del 55,4 % corresponde a cálculo propio basado en el aumento de 233 a 362 incidentes documentados.

La IA puede formular un diagnóstico, pero no verificar por sí sola si comprendimos el contexto. Puede proponer un control, pero no constatar que existan recursos y autoridad para implementarlo. Puede redactar un protocolo impecable, pero no observar la fatiga de un guardia, un ángulo muerto o una reacción humana bajo presión. Tampoco responde por las consecuencias.

NIST y UNESCO coinciden en que no basta invocar la "supervisión humana". Esta debe traducirse en trazabilidad de fuentes, supuestos explícitos, validación contextual, pruebas operacionales, responsables definidos, indicadores pertinentes y revisión posterior. El profesional debe poder explicar qué aportó la IA, qué verificó personalmente y por qué aceptó, corrigió o descartó sus resultados.

El problema comienza cuando la asistencia tecnológica sustituye conocimiento todavía no construido y la elegancia del documento oculta la debilidad del método. Allí surge una peligrosa madurez narrativa: organizaciones que hablan mejor de seguridad, pero no necesariamente protegen mejor.

De ninguna manera propongo renunciar a la inteligencia artificial. Propongo utilizarla con mayor disciplina, puesto que de echo está diseñada para ampliar nuestra capacidad de análisis, pero algo que siempre hago hincapié, no debe reemplazar la experiencia, la observación del terreno, el contraste técnico ni la responsabilidad profesional. En seguridad, proteger no consiste en producir respuestas convincentes, sino en tomar decisiones justificadas, implementar controles verificables y responder por sus resultados. Cuanto más poderosa sea la herramienta, mayor debe ser nuestro criterio para gobernarla.

Bibliografía

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). NIST. https://doi.org/10.6028/NIST.AI.100-1

Skinner, B. F. (1969). Contingencies of reinforcement: A theoretical analysis. Appleton-Century-Crofts.

Stanford Institute for Human-Centered Artificial Intelligence. (2026). Artificial Intelligence Index Report 2026. https://hai.stanford.edu/ai-index/2026-ai-index-report

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence

World Economic Forum. (2026). Global Cybersecurity Outlook 2026. https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

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 líder 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

La seguridad ya no solo se especializa se integra

Jesús M. Chuquillanque Huaman
Ingeniero Industrial CIP, candidato al grado de MBA y Subgerente de Seguridad Integral y Mantenimiento en Oechsle. Certified Protection Officer (CPO) y Certified in Security Supervision and Management (CSSM) por IFPO. Especialista en gestión integral de riesgos, seguridad corporativa, seguridad patrimonial, Seguridad y Salud en el Trabajo (SST)
Perú
Articulista Invitado

El mayor riesgo no siempre está en las amenazas visibles, sino en dirigir los desafíos del presente con el conocimiento del pasado.

Lima, Perú.- Durante décadas, la seguridad organizacional evolucionó bajo un modelo de especialización. La seguridad patrimonial protegía los activos, Seguridad y Salud en el Trabajo velaba por las personas, Mantenimiento aseguraba la continuidad operativa de la infraestructura. Cada disciplina desarrolló metodologías, indicadores y equipos propios que respondían eficazmente a una realidad relativamente estable y predecible. Sin embargo, ese modelo comienza a mostrar sus límites frente a un entorno VUCA (Volátil, Incierto, Complejo y Ambiguo), donde los riesgos evolucionan con mayor rapidez, se interconectan y desafían las estructuras tradicionales de gestión.

En este escenario, el mayor riesgo para la seguridad no siempre es una amenaza visible. Muchas veces es quedarnos con el conocimiento de ayer. Persistir en modelos diseñados para responder a problemas del pasado puede resultar más peligroso que la ausencia de nuevas tecnologías. Cuando los riesgos cambian, también debe cambiar la manera de comprenderlos. La verdadera transformación no consiste únicamente en incorporar herramientas más sofisticadas, sino en revisar los paradigmas sobre los cuales se toman las decisiones.

Basta observar una situación cotidiana para comprenderlo. Un sistema contra incendios fuera de servicio deja de ser un problema exclusivo de mantenimiento para convertirse, simultáneamente, en un riesgo para la seguridad de las personas, una vulnerabilidad patrimonial, un posible incumplimiento normativo y una amenaza para la continuidad del negocio. Del mismo modo, un accidente laboral rara vez tiene una causa aislada, generalmente es el resultado de decisiones relacionadas con infraestructura, mantenimiento, comportamiento humano y gestión del riesgo. En consecuencia, los problemas ya no pertenecen a una sola disciplina y, por lo tanto, las soluciones tampoco deberían hacerlo.

Esta nueva realidad explica por qué cada vez es más frecuente encontrar líderes que integran bajo una misma responsabilidad la Seguridad Patrimonial, la Seguridad y Salud en el Trabajo y el Mantenimiento. Lejos de representar únicamente una ampliación de funciones, esta convergencia refleja una evolución natural del liderazgo en seguridad. El punto de encuentro entre estas disciplinas no es la operación, sino la prevención. Prevenir una pérdida, evitar un accidente o anticipar una falla crítica responde a un mismo principio: identificar riesgos antes de que se materialicen, comprender sus causas y actuar oportunamente para reducir su impacto.

Asimismo, esta integración exige un perfil profesional diferente. El líder de seguridad ya no puede limitar su aporte al dominio técnico de una única especialidad, debe interpretar información proveniente de distintas áreas, comprender cómo interactúan los riesgos, liderar equipos multidisciplinarios y tomar decisiones considerando, de manera simultánea, el impacto sobre las personas, los activos, la infraestructura y la continuidad del negocio. En otras palabras, la multifuncionalidad ha dejado de ser una ventaja competitiva para convertirse en una competencia esencial del liderazgo moderno.

A esta transformación se suma el acelerado avance de la inteligencia artificial, la analítica predictiva, la automatización y los edificios inteligentes, tecnologías que asumirán progresivamente muchas de las tareas operativas que históricamente realizaban las personas. Paradójicamente, cuanto mayor sea la capacidad tecnológica para procesar información, mayor será la necesidad de líderes capaces de integrar conocimientos, cuestionar supuestos y conectar disciplinas que durante años trabajaron de forma independiente. La tecnología podrá anticipar eventos; sin embargo, seguirá siendo el criterio humano el que determine la calidad de las decisiones.

En definitiva, la seguridad del futuro no será liderada por quienes administren más sistemas, más cámaras o más procedimientos, sino por quienes comprendan que la prevención constituye el lenguaje común que integra todas las disciplinas relacionadas con la gestión del riesgo. Las organizaciones que continúen abordando la seguridad desde compartimentos aislados difícilmente podrán responder a un entorno caracterizado por la incertidumbre y la complejidad. Porque, al final, el mayor riesgo nunca fue la aparición de nuevas amenazas; el verdadero riesgo es seguir enfrentando los desafíos del presente con el conocimiento del pasado.

SEGURIDADEXPO®

08 al 10 septiembre | METROPOLITAN SANTIAGO

www.seguridadexpo.cl

info@seguridadexpo.cl

CONOCE TECNOLOGÍAS DE VANGUARDIA, ACTUALIZA TUS CONOCIMIENTOS Y AMPLÍA TU RED DE CONTACTOS

¡NO TE QUEDES FUERA!

Consigue tu ticket y sé parte del evento líder en seguridad

INVITA MOTOROLA SOLUTIONS

AUSPICIA GRUPO SAFETECK

PATROCINA

ORGANIZA Fisa

COORGANIZA

El enfoque real de la Seguridad Ciudadana:

Reto de la

Lima, Perú. – El paradigma global de la seguridad cambia constantemente. Hoy en día, abordar las amenazas a la tranquilidad pública desde una perspectiva ligera o reactiva es una estrategia obsoleta. Para comprender la complejidad del entorno delictivo y los riesgos sociales actuales, se requiere ciencia, experiencia de campo y comprensión del territorio. Bajo esta premisa opera la Asociación Nacional de Consultores de Seguridad Ciudadana e Integral (ANCSCI), organización que se ha consolidado como un referente indispensable en el análisis de riesgos y el diseño de políticas de protección.

Presidida por Carlos Miguel Pérez Chávez desde 2016, la ANCSCI nació a partir de una necesidad crítica en el sector: agrupar y dignificar a los profesionales expertos en seguridad, defensa y atención de emergencias. El origen de la asociación estuvo marcado por el rigor técnico; sus 17 miembros fundadores iniciaron este camino especializándose en un programa de alta exigencia sobre seguridad ciudadana e integral. Hoy, la organización ha crecido considerablemente al contar con más de 60 consultores asociados de primer nivel. Un aspecto a resaltar de su evolución es la inclusión y el rol de las mujeres profesionales en sus filas, ya que 15 expertas lideran áreas importantes como la comunicación, el sector jurídico y la gestión operativa de emergencias, lo que da una visión integral y multidisciplinaria al gremio.

Una solución social para una geografía compleja

En entrevista para Más Seguridad Magazine, Carlos Miguel Pérez Chávez, dijo que el núcleo metodológico de la ANCSCI radica en el análisis avanzado de la gestión de riesgos, abarcando desde entornos sensibles como la seguridad escolar hasta los riesgos cotidianos que enfrenta el ciudadano común. Sin embargo, su principal factor diferenciador es el diagnóstico. Como aseveró Carlos Pérez, el liderazgo, la criminalidad y la vulnerabilidad no se pueden resolver únicamente con el despliegue de fuerzas del orden, se requiere una solución de corte social y sociológico.

Este enfoque se debe a las marcadas diferencias geográficas y demográficas de la región. Las problemáticas de protección varían entre la costa, la sierra y la selva. Incluso dentro de estas grandes áreas, coexisten microrregiones, con operaciones delictivas y necesidades socioeconómicas particulares. La ANCSCI actúa como un puente técnico, señalando que cada territorio posee demandas específicas que el gobierno central, los Ministerios, los gobernadores y los alcaldes deben resolver eficazmente. Para dar respuesta a esta fragmentación, la asociación ha desplegado una red táctica con siete representaciones a nivel nacional, cubriendo regiones clave como Tacna, Cusco, Arequipa, San Martín, La Libertad, Ancash, Lima, Ica y el norte del país.

La inseguridad actual obliga a mirar más allá de las fronteras. La seguridad ciudadana está fuertemente ligada a riesgos transnacionales de gravedad, como el narcotráfico y la minería ilegal. Estos fenómenos criminales no operan de forma aislada. Por ejemplo, mientras que Colombia, Ecuador y Perú comparten el problema de la minería ilegal y el tráfico de drogas, existen otros países en la región que actúan como “almacenes” o centros logísticos de acopio, donde se conglomeran los insumos y productos ilícitos para realizar envíos masivos hacia otros continentes.

Ante esta realidad, la internacionalización y las alianzas estratégicas son fundamentales. A través de la red internacional de ANCSI, la organización mantiene lazos y representantes en Argentina, Brasil, Bolivia, Ecuador, Colombia, Panamá, México, Estados Unidos, España y Alemania. No obstante, Carlos Pérez enfatizó que Perú, Colombia y Ecuador comparten una matriz de seguridad ciudadana muy similar, marcando una clara distancia técnica con los modelos de Chile, Bolivia, Brasil o Argentina, cuyas realidades institucionales y criminológicas corren por carriles distintos.

El mayor valor de la ANCSCI está en el perfil de sus integrantes. El conglomerado está compuesto principalmente por oficiales de la policía, las fuerzas del orden, el Ejército y la Marina. Estos profesionales tienen conocimiento empírico del territorio profundo. Han operado en los puntos cardinales más remotos del país, enfrentando condiciones climáticas y geográficas extremas que condicionan cualquier despliegue operativo.

Carlos Pérez concluyó con un mensaje para el sector de la seguridad: “Si no conoces tu país, las soluciones no serán exactas, siempre habrá errores”. La ANCSCI no trabaja en oficina, sus propuestas nacen de la experiencia en campo combinada con el análisis científico, buscando siempre dar al Estado y a las organizaciones privadas un enfoque real ante problemas reales.

Carlos Miguel Pérez Chávez, presidente de la ANCSCI

EXPO 2026 NAVAL®

XIV EXHIBICIÓN Y CONGRESO INTERNACIONAL NAVAL Y MARÍTIMO PORTUARIO PARA LATINOAMÉRICA

1-3 DICIEMBRE

ESPACIO RIESCO

AV. EL SALTO 5000, HUECHURABA

SOMOS LA FERIA DE NEGOCIOS PARA LA INDUSTRIA NAVAL LATINOAMERICANA

ORGANIZA

Fisa | GL events

PATROCINA

Ministerio de Defensa Nacional Gobierno de Chile

WWW.EXPONAVAL.CL | Exponaval | info@exponaval.cl | +56 9 4481 6922

Cuando la inteligencia artificial mejora el discurso

pero no la capacidad de proteger

Andrea Guidugli
Consultor Miembro Federación Periodistas de la ciudad di Madrid. Periodista y Opinador acreditado por la Federación Internacional de la Prensa de Bruselas
Italia
Articulista Invitado

Anatomía secreta de la nueva vigilancia silenciosa

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 ciber-percepción: 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 multiespectrales 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 soplones. 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-vibracionales, 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.

ASIS INTERNATIONAL™ CAPÍTULO MÉXICO 217

ASISte a una de nuestras **Reuniones Mensuales** y conoce de primera mano el valor que **ASIS** te aporta.

REUNIÓN MENSUAL RM

Hacemos del mundo un lugar *más seguro*

Beneficios de la membresía

Oportunidades de intercambio de conocimiento, recursos valiosos y conexiones entre pares.
Expande tu experiencia y desarrolla tu carrera, sin importar tu nivel profesional (precios afiliación).

Haz crecer tu experiencia uniéndote a nuestras Comunidades.

INCLUIDO EN TU MEMBRESÍA ASIS

¿Eres profesional de seguridad privada y aún no formas parte de **ASIS Capítulo México 217**?

Escanea el código QR, afíliate hoy y empieza a disfrutar del mejor networking de la industria y la mejor oferta de profesionalización del sector.

¡Qué esperas!

ASOSEC®
ASOCIACIÓN COLOMBIANA DE SEGURIDAD

35 ANIVERSARIO

CONGRESO
NACIONAL DE **SEGURIDAD**

Seguridad Privada:
Orgullo, Fortaleza y Transformación

23 24 25 Sept. 2026

DANN CARLTON HOTEL & CONVENTION CENTER ★★★★★ BARRANQUILLA

Inscríbete Aquí

APOYAN

ASIS INTERNATIONAL® Caribe Colombia Chapter | BASC | MÁS SEGURIDAD Magazine | CON SEGURIDAD Magazine Latam | GLOBAL DEFENSE MAGAZINE

Informes:

@asosec.co @asosec @asosec.co asosec asosec

312 686 4435 - 301 539 7542 asosec@asosec.co