MÁS SEGURIDAD

Magazine

ESS+ FERIA INTERNACIONAL DE SEGURIDAD

ASOSEC ASOCIACIÓN COLOMBIANA DE SEGURIDAD

Colombia: referente en protección privada

Julio 2026/ No. 163 / Año 18

Internacional / precio $60.00 MXN

EXPO SEGURIDAD
VIGILANCIA • SEGURIDAD PRIVADA • TECNOLOGÍA

GRUPO EDITORIAL MS GLOBAL

Organiza

Grupo Empresarial íntegra
Soluciones en Propiedad Horizontal

EXPO SEGURIDAD

VIGILANCIA • SEGURIDAD PRIVADA • TECNOLOGÍA

El punto de encuentro de la industria de la SEGURIDAD

¡VINCÚLATE YA!

Julio 28 y 29 | 2026

ÚLTIMOS CUPOS PARA EXPOSITORES

NEOMUNDO

Informes
(+57) 318 623 5411

BUCARAMANGA | COLOMBIA

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 163, Julio 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.

Colombia:
fortaleza en seguridad privada

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

Según cifras de la Superintendencia de Vigilancia y Seguridad Privada (en 2025), cerca de 390 mil personas trabajan de manera directa en esta industria, entre guardias, escoltas, técnicos e ingenieros. El aporte económico del sector ronda el 1.2% del Producto Interno Bruto (PIB), con una participación aproximada de 10.5 billones de pesos colombianos (en 2022). El 95% de la actividad aún corresponde a vigilancia presencial, mientras que el componente electrónico representa solo el 5% en línea con una transición gradual hacia modelos tecnológicos.

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

En Colombia, existe un importante número de organizaciones gremiales que a nivel internacional se han distinguido por sus aportes a la industria latinoamericana, en beneficio de sus agremiados, impulsando en primera instancia el profesionalismo y capacitación en diversas disciplinas.

Destacan entre estos gremios, la Asociación Colombiana de Seguridad (ASOSEC), conformada por más de 30 empresas y cerca de 30 mil empleados a nivel nacional. Este organismo promueve el desarrollo del sector mediante eventos como el **Congreso Nacional de Seguridad** —donde se reconocen los méritos de los guardas y se impulsan alianzas con entidades como la Superintendencia y la Policía Nacional— y campañas de liderazgo, inclusión y profesionalización.

Para potenciar a la industria, en Colombia se desarrollan anualmente diversos foros y eventos donde convergen la protección intramuros y electrónica. Muestra de ello es la Feria de Seguridad y Eficiencia **ESS+**, evento que por más de tres décadas ha demostrado por que se le considera “la madre de las expos de seguridad” en la región, al incrementar cada año el número de expositores y visitantes nacionales e internacionales de diversas partes del mundo.

En este rubro de las exposiciones llega un nuevo jugador que promete llevar los avances tecnológicos al oriente colombiano: **Expo Seguridad Bucaramanga**¸ evento para profesionales de la industria, donde se presentarán tendencias en vigilancia inteligente, ciberseguridad, domótica, robótica y tecnología aplicada.

Hoy las ferias y eventos han evolucionado y son verdaderas opciones para comparar precios, calidad y soporte postventa. Sin duda este tipo foros están diseñados para conectar a empresas y líderes del gremio. La feria incluye muestra comercial y B2B con stands y demostraciones en vivo, simulacros de productos y networking para alianzas estratégicas, actualización académica con talleres prácticos y conferencias magistrales enfocadas en el futuro de la seguridad privada y el sector tecnológico de la región.

Con apenas una “pincelada de información”, se vislumbra un panorama general de la industrial, lo cual permite comprender la magnitud, diversidad y responsabilidad que implica el sector de la seguridad privada en Colombia. Anualmente, miles de personas se suman a la actividad laboral del sector con estándares altos de conocimientos que a nivel internacional son muy apreciados. Sin duda, el segundo semestre del año trae nuevas oportunidades para el gremio, tomando en cuenta que Colombia estrenará gobierno nacional.

Los Profesionales de LATAM

MBA. Rodolfo Cepeda Rico
México

Licenciado en Mercadotecnia. Maestría en Administración con especialidad en Negocios Internacionales por el ITESM.
Certificación de PECB Canadá en ISO 31000, ISO 28000, ISO 37001, ISO 27001, ISO 900-2015 e ISO 18788.
Maestría de Seguridad Integral en la EPFAC (Escuela de Postgrado de la Fuerza Aérea Colombiana) 2021.
Empresario, asesor y consultor internacional con 30 años de experiencia en la implementación de estrategias de Seguridad Integral a nivel empresarial.
Actualmente implementa estrategias de Seguridad Integral en las industrias farmacéutica, automotriz y consumo, entre otras.
Es presidente de COLADCA Capítulo México.

Sumario

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

Colombia como eje rector de la seguridad privada

Seguridad privada para muchos engloba las distintas verticales de protección pagada para personas, bienes y servicios, pero además relacionar a Colombia con esta industria, es sin duda el mejor y más completo referente en la materia. El presente trimestre será una vez más el escenario internacional para que los empresarios de este gremio y los usuarios finales converjan en tres importantes foros de este país sudamericano: **Expo Seguridad Bucaramanga, ESS+** y el **Congreso Nacional de Seguridad.**

La novel **Expo Seguridad Bucaramanga** se llevará a cabo el 28 y 29 de julio en el Gran Salón de Neomundo. A decir de su organizador, Mauricio, Espinoza, este es el evento y cumbre más importante del oriente colombiano para profesionales, donde se presentarán tendencias en vigilancia inteligente, ciberseguridad, domótica, robótica y tecnología aplicada. El evento está diseñado para conectar a empresas y líderes del gremio.

La feria incluye muestra comercial y B2B con stands y demostraciones en vivo, simulacros de productos y networking para alianzas estratégicas, actualización académica con talleres prácticos (hands-on) y conferencias magistrales enfocadas en el futuro de la seguridad privada y el sector tecnológico. La innovación es exposición directa de equipos, drones operativos y plataformas de gestión avanzadas…

Del 26 al 28 de agosto será el escenario para el desarrollo de la 33 edición de la feria **ESS+**, donde Inteligencia Artificial (IA) y ciberseguridad ocuparán la titularidad de la muestra, la cual ya es considerada como el principal punto de encuentro para la industria de safety and security en la región sudamericana. Una vez más Bogotá será el epicentro para las novedades tecnológicas que más de 19 mil personas podrán conocer.

Bajo la dirección de Patricia Acosta, la ESS+ abordará temas como la integración de tecnología, IA, analítica de datos, ciberseguridad, tecnologías para infraestructuras críticas y ciudades seguras. La feria proyecta un crecimiento del 20% tanto en espacio de exhibición como en asistencia, impulsado por un panorama político regional que demanda una inversión sin precedentes en infraestructura de seguridad.

Este año, además, ESS+ expande su alcance global con la incorporación de delegaciones comerciales de Turquía e India, que se suman a los 23 países que ya participan, como México, Suecia, Argentina, Francia, Italia, Brasil, Perú, Estados Unidos, Corea del Sur y China. La apuesta es a las ciudades capitales, a los alcaldes y Ministros de seguridad estatales y metrópolis intermedias, no solo de Colombia, sino de la región andina y el Caribe…

Para cerrar trimestre, del 23 al 25 de septiembre, se desarrollará el **Congreso Nacional de Seguridad**, organizado por la Asociación Colombiana de Seguridad (ASOSEC), que preside Gabriel Berrío. Este evento que por varios años se ha llevado a cabo en la ciudad de Barranquilla, se ha convertido en un punto de encuentro para líderes gremiales, representantes de entidades gubernamentales y especialistas internacionales.

En este espacio se abordarán temas como el cumplimiento normativo, gestión del riesgo y nuevas tendencias tecnológicas, todo desde una perspectiva de formación, análisis y networking.

A lo anterior se suman diplomados, talleres técnicos, foros temáticos, asesorías personalizadas y sesiones que ASOSEC realiza de forma sostenida: Los beneficios para los afiliados son concretos: acompañamiento permanente, actualización normativa, capacitación constante y representación ante los entes rectores, asegura Gabriel Berrío.

Por supuesto, **Más Seguridad Magazine** participará de forma directa. Es cuanto…

Gracias y nos leemos pronto, pero ¡Fuera de Grabación!

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.

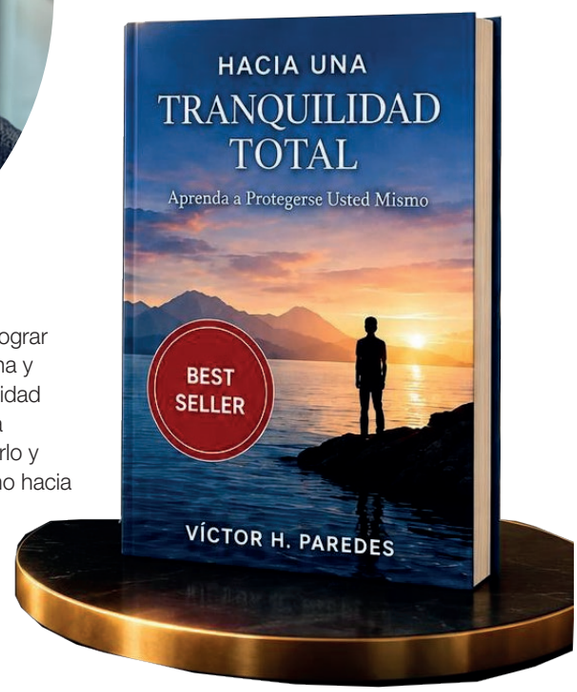
También aborda la construcción de una mentalidad orientada a la abundancia, entendida como una forma de pensar abierta a nuevas oportunidades y cambios positivos. Con un lenguaje sencillo, Paredes invita a revisar creencias limitantes, fortalecer la confianza personal y crear hábitos mentales saludables.

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/

HIKVISION®

Historias de tecnología que fortalecen la seguridad en México a través de HikTech Star Show 2026

Después de dos años reconociendo el talento de integradores y especialistas en seguridad, Hikvision anunció el inicio de HikTech Star Show 2026, su concurso global de video que busca destacar proyectos, experiencias y casos de éxito desarrollados con tecnología de la marca. Como parte de esta convocatoria, cuatro integradores mexicanos tendrán la oportunidad de ganar un viaje todo incluido a Hangzhou, China, donde conocerán las oficinas centrales de Hikvision y participarán en la ceremonia internacional de premiación junto con representantes de otros países.

Para esta nueva edición, el concurso incorpora cuatro categorías de participación y permitirá que algunos ganadores de años anteriores regresen para compartir sus experiencias con los nuevos participantes. Además, los contenidos más destacados podrán obtener uno de los 10 Super Pass que se entregarán a nivel mundial, lo que les garantizará automáticamente un lugar en el HikTech Star.

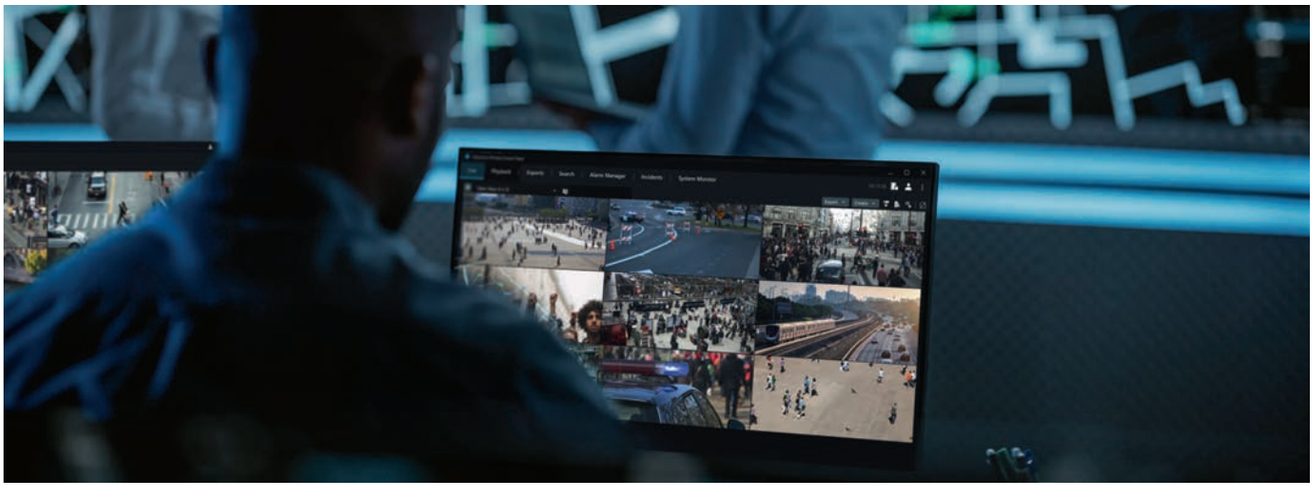
"La evolución de HikTech Star refleja lo que estamos viendo todos los días en la industria. Cada vez hay más integradores y creadores de contenido que utilizan redes sociales y plataformas digitales para mostrar su trabajo, compartir proyectos y contar cómo la tecnología les ayuda a resolver necesidades reales en negocios, hogares y otros espacios. Por eso, en esta edición queremos conocer esas historias de primera mano. Nos interesa saber qué retos han enfrentado, cómo los han resuelto, qué resultados han obtenido y cómo han ido creciendo profesionalmente con el uso de nuestras tecnologías. También queremos ver ejemplos reales de cómo la Inteligencia Artificial y las analíticas están ayudando a hacer más eficiente la seguridad. Lo más valioso será conocer, a través de la experiencia de los propios integradores, cómo estas herramientas han ayudado a sus clientes, qué problemas han solucionado y qué diferencia han hecho en sus proyectos», comenta Fran Sánchez, marcom director en Hikvision México.

Paulina Lordméndez, Brand Communications & Content Lead de Hikvision México, indica que, para esta tercera entrega, los participantes podrán inscribirse en las siguientes categorías diseñadas para reconocer distintos perfiles y formas de aplicar la tecnología:

1.- Explora más está dirigida a quienes cuentan con conocimientos técnicos avanzados y desean demostrar su dominio de los productos y soluciones de Hikvision.
2.- Piensa sin límites busca premiar la creatividad, destacando proyectos que utilicen la tecnología de maneras originales o poco convencionales.
3.- Crea con ingenio está enfocada en soluciones prácticas para PyMEs y en proyectos que integren diferentes tecnologías para resolver necesidades específicas.
4.- Comparte valor reconocerá historias que muestren cómo la tecnología ha generado un impacto positivo en las personas, las empresas o las comunidades.

Los videos podrán enviarse del 22 de junio al 23 de agosto de 2026. Únicamente se tomarán en cuenta las publicaciones y las interacciones generadas dentro de ese periodo, por lo que las visualizaciones, «me gusta», comentarios y demás métricas obtenidas antes o después de esas fechas no serán consideradas. El viaje a China se realizará en octubre de 2026, en las fechas que determine Hikvision.

Para participar, los interesados deberán seguir las cuentas oficiales de Hikvision México en Instagram, YouTube y TikTok (@hikvisionmx), así como en Facebook (@hikvisionmex), y compartir un video original en el que demuestren sus habilidades tecnológicas o conocimientos aplicados sobre los productos de la marca. Cada video participante deberá publicarse acompañado del hashtag oficial #HikTechStar2026Mx y del hashtag asignado a la categoría seleccionada.



milestone revoluciona videovigilancia mediante IA aplicada a la gestión operativa y anonimización forense

Durante la pasada edición de Expo Seguridad México, Milestone Systems, proveedor mundial en tecnología de video de plataforma abierta, además de presentar su portafolio XProtect, BriefCam y Arcules, mostró su proyecto Hafnia con dos soluciones: Inteligencia Artificial y anonimización forense de datos en un mercado regional que demanda cada vez mayor eficiencia y adaptabilidad.

1. Resumen de video optimizado a través de prompts. A través de modelos de lenguaje visual (VLM), Milestone System introdujo el resumen de video, una herramienta con la que las personas dedicadas al monitoreo de video podrán interactuar con el sistema a través de instrucciones de texto (prompts) para identificar con exactitud qué ocurrió un día y hora determinados. Con esta innovación, se elimina la necesidad de realizar búsquedas manuales.
2. Anonimización de video para privacidad garantizada. Con esta solución, se ejecuta un difuminado automático (blur) de los rostros y cuerpos de las personas en escena, garantizando su privacidad. Sin embargo, el sistema mantiene un diseño flexible para que en caso de que haya una investigación forense, el proceso de anonimización pueda revertirse.

Johanaana Arias, directora de Vventas para Milestone System en América Latina, afirmó que el fabricante adapta su ecosistema tecnológico a las necesidades puntuales de cada infraestructura corporativa o gubernamental. Su versatilidad permite atender a sectores como cCiudades inteligentesSeguras, centros comerciales, infraestructura crítica, corporativos y manufacturacorporativos, manufactura, educación, y salud,; banca, entre otros.

Los valores agregados de Milestone: iInnovación y un robusto ecosistema abierto

Arias aseguró que el éxito de Milestone en México y en el mundo, se sustenta en una serie de ventajas competitivas como:

- Ecosistema abierto e integración total: fFiel a su filosofía fundacional, Milestone cuenta con una plataforma abierta que permite la integración con prácticamente cualquier tecnología. Esto se potencia gracias a una red de más de 500 socios tecnológicos globales, lo que garantiza que los clientes no queden cautivos con una sola marca de hardware o software.
- Innovación en I+D 100% nueva: El compromiso de la compañía con la vanguardia tecnológica se refleja en su área de Investigación y Desarrollo (I+D), donde los nuevos lanzamientos e innovaciones se diseñan y desarrollan desde cero (100% nueva), asegurando soluciones nativas más eficientes y preparadas para el futuro.
- Tecnología e Inteligencia Artificial Ética: eEn un panorama donde el uso de los datos personales es sensible, Milestone se destaca por su estricta alineación con el uso ético de la tecnología y la IA. La compañía promueve activamente que el análisis de video se utilice para proteger a las personas y optimizar negocios, sin comprometer los derechos humanos ni la privacidad ciudadana.

Con esta sólida propuesta, Milestone Systems no solo simplifica las operaciones diarias de los profesionales de la seguridad en México y América Latina, sino que redefine los estándares de cómo la tecnología puede hacer que los entornos urbanos, industriales y corporativos sean más eficientes, productivos y seguros.

Johanaana Arias, directora de Vventas para Milestone System

Hanwha Vision introduce software Blaze:

VMS híbrido con búsqueda semántica y por apariencia

En el marco de la edición 2026 de Expo Seguridad México, 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.

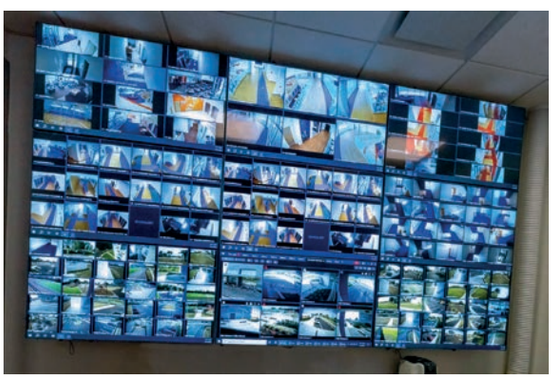
Enrique Cortés, Regional CES Manager de la zona Pacífico, de Hanwha Vision

rediseña el mundo del monitoreo con Avigilon y Operator

La seguridad electrónica se encuentra en el umbral de su transformación más disruptiva: la transición de los sistemas reactivos a los ecosistemas predictivos y asistidos por inteligencia artificial generativa. Motorola Solutions, a través de su división de video y control de accesos, presentó Avigilon Cloud, que ahorra a los clientes la compra de infraestructura y permite la flexibilidad de movimiento, pues elimina para los usuarios finales la necesidad de invertir en infraestructuras locales de servidores.

En entrevista durante Expo Seguridad 2026, Ernesto Sodi, director comercial para México de la división de Video y Control de Accesos de Motorola Solutions, desglosó el impacto de su ecosistema en la nube y afirmó que la plataforma se despliega principalmente en dos vertientes: la videoseguridad inteligente (core business de la firma) y la viabilidad financiera del negocio.

Actualmente, Avigilon Cloud tiene principalmente dos verticales: “En retail puedes tener



muchas tiendas de retail montado en la nube y el sector Healthcare. Healthcare internamente deben tener mucha analítica para poder determinar tanto las filas de espera, videovigilancia en perímetros y que te permite la flexibilidad de tener todo montado en la nube”, indicó el directivo.

El debut de Operator: el copiloto táctico en situaciones de crisis

Ernesto Sodi también habló sobre el próximo lanzamiento al mercado de Operator, una solución que integra IA generativa directamente en las consolas de supervisión. Cuando ocurre una eventualidad o siniestro, el sistema genera de forma automática una alerta crítica en la interfaz del supervisor. “Estamos indagando en la parte de Inteligencia Artificial Generativa y esto nos permite tener una nueva solución”.

Se trata de un operador virtual montado en la nube, en caso de emergencia, automáticamente emitirá una alerta, se desplegarán varias estrategias a seguir y el operador escogerá la que considere más viable. Una vez que el operador selecciona la estrategia, el sistema desglosará una serie de instrucciones secuenciales y detalladas sobre los protocolos exactos que se deben ejecutar, como dar aviso a autoridades locales, activar sistemas de voceo masivo o cerrar accesos perimetrales.

“Esto permite que un operador aunque no tenga la experiencia necesaria tomará una acción y el sistema dará una serie de instrucciones sobre las acciones que se deberán llevar a cabo”, detalló Sodi. De esta manera, Operator podría resolver problemas como la alta rotación y la curva de aprendizaje del personal de seguridad corporativa.

Cabe destacar que actualmente Operator se monta sobre el VMS de Unity, una solución On-premise, pero la idea es que pueda montarse en la nube, Motorola Solutions ya trabaja en ello. Lo que la compañía ya tiene establecido en México y otros países donde lidera es el lenguaje natural, que se refiere a las herramientas impulsadas por Inteligencia Artificial Generativa. Estas herramientas permiten a operadores y centros de mando interactuar con los sistemas de seguridad, radio y video mediante comandos de voz cotidianos.

Ernesto Sodi, director comercial para México de la división de Video y Control de Accesos de Motorola Solutions

doinGlobal™

El verdadero juego táctico:

Cuando el soccer depende del SOC

De la vieja escuela reactiva a la inteligencia artificial predictiva: cómo la evolución de los Centros de Operaciones de Seguridad (SOC) en México está transformando la gestión de eventos masivos y por qué la profesionalización es el verdadero boleto a la final.

Cuatro años esperando y preparándose para vivir la mayor fiesta del fútbol. Millones de personas siguen desde sus pantallas el evento más masivo que pueda existir. Y cuanto mayor es la escala del evento, mayores son también los desafíos para garantizar su seguridad. En este escenario, el riesgo es altísimo: se puede sufrir una gran derrota mucho antes de disputar la final. Un paso en falso en la logística, un cuello de botella en los accesos o una falla en las comunicaciones, y el éxito de toda la operación se puede comprometer gravemente en cuestión de minutos, transformando un hito histórico en una crisis de reputación e infraestructura de consecuencias incalculables.

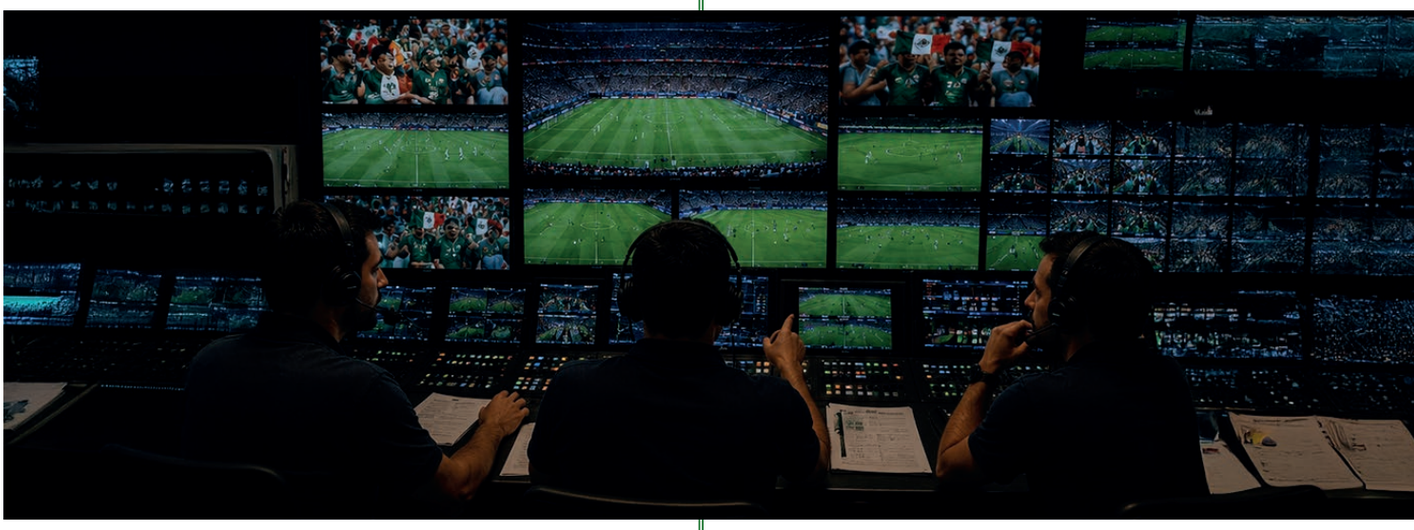
La experiencia del aficionado no comienza cuando el árbitro da el silbatazo inicial y la Trionda empieza a rodar. Arranca desde que pisa el aeropuerto, toma el transporte hacia el estadio, cruza los filtros perimetrales y, finalmente, encuentra su butaca. Todo debe fluir en una armonía perfecta y sin contratiempos. Pero para que esa aparente calma sea posible, con una presencia que acompaña cada paso del camino opera una maquinaria milimétrica.

La seguridad moderna ya no se mide por la cantidad de guardias o policías desplegados en las puertas, sino por la inteligencia capaz de predecir el siguiente movimiento de miles de personas en tiempo real. Hoy, México es un auténtico laboratorio de seguridad masiva. Este mundial en marcha no es solo una vitrina deportiva; es el escenario real que está cambiando las reglas para siempre en la gestión de los grandes eventos.

¿Qué cambió en México respecto a 1986? La revolución tecnológica

La última vez que México albergó una Copa del Mundo, en 1986, la seguridad en los estadios dependía casi por completo del ojo humano, la intuición de los oficiales y redes de radiocomunicación propensas a saturarse. En aquel mundial, la gestión era meramente reactiva: el éxito consistía en contener el problema una vez que este ya había iniciado. Cuarenta años después, la tecnología ha revolucionado por completo estos sistemas, transformando la gestión de la seguridad en una disciplina predictiva.

La introducción de los Centros de Operaciones de Seguridad (SOC) modernos permite que lo que antes requería horas de recopilación de reportes dispersos, hoy se traduzca en datos unificados en una sola pantalla y en tiempo real. México sabe hoy que la masividad no se controla con fuerza, sino con información estratégica, interoperabilidad y anticipación.



El punto de dolor en la gestión de seguridad: la herencia de la «vieja escuela»

A pesar de este avance, la gestión de la seguridad en muchos lugares continuó durante décadas con una visión que hoy resulta obsoleta: entender el SOC como una simple «sala de cámaras». En la vieja escuela, este espacio era ese cuarto oscuro lleno de monitores donde el personal se limitaba a observar de forma reactiva. Básicamente, se usaba para ver cómo ocurría un incidente o, peor aún, para revisar la grabación después de que el daño ya estaba hecho.

Esta percepción reduccionista es el principal punto de dolor del sector. Tratar la seguridad como tecnologías aisladas (un proveedor para el circuito cerrado, otro para el control de accesos y uno más para las alarmas) genera vacíos de información críticos.

¿Qué es un SOC moderno? El centro neurálgico

Un SOC de estándar internacional, como los exigidos por la FIFA, dista mucho de ser un almacén de pantallas. Es un sistema integral de toma de decisiones a partir de la interoperabilidad. Su arquitectura funcional conecta el conteo electrónico de espectadores en los sistemas de control de accesos, los sistemas de megafonía externa e interna, los paneles de detección de incendios y las redes de radiocomunicación redundantes que no se saturan cuando el inmueble ruge.

El verdadero salto cualitativo de la industria actual está en pasar del monitoreo reactivo a la anticipación pura. Hoy, gracias a la Inteligencia Artificial (IA), los operadores del SOC pueden analizar el modelado de flujos de personas, detectar anomalías en el comportamiento de las multitudes e integrar alertas previas provenientes de plataformas digitales. El objetivo es predecir el riesgo y disolverlo antes de que se manifieste.

¿Qué sigue después del Mundial?

La gran pregunta para los gestores en México es: ¿qué pasará cuando el torneo termine? Los estándares internacionales de este mundial dejarán un marco metodológico completamente escalable. No se necesita el presupuesto de un gigante de la FIFA para aplicar estos principios en estadios de la Liga MX, conciertos, festivales masivos o centros comerciales. Las tecnologías de integración ya son accesibles para el mercado medio; lo que falta es el cambio de chip cultural y estratégico.

La seguridad contemporánea ya cambió y la improvisación es el desafío a superar. Por esta razón, la formación profesional y la especialización continua se han convertido en la única estrategia real para liderar el sector. Para responder a esta exigencia en la región, doinGlobal ofrece programas avanzados de formación permanente en alianza con la reconocida Universidad de Salamanca (España). Estos programas destacan por particularidades clave:

- Especialización en la frontera tecnológica: Cuentan con planes de estudio innovadores diseñados específicamente para dominar las herramientas de analítica predictiva de las que dependen los SOC modernos.
- Enfoque de dirección y toma de decisiones: Son formaciones que no se quedan en el plano técnico operativo, sino que desarrollan competencias de liderazgo estratégico para coordinar nodos complejos bajo situaciones de alta presión.

El Mundial nos pone bajo la lupa del mundo entero. Asegurar que cada aficionado viva una experiencia inolvidable y segura, desde que llega a la ciudad hasta que festeja un gol, es un reto que solo aquellos profesionales debidamente preparados y actualizados sabrán liderar con éxito. ¿Estás listo para asumir los desafíos de la seguridad contemporánea?

Conoce cómo prepararte: https://short.do/iX4UYm

HID Amico

nuevo lector de reconocimiento facial biométrico

HID, empresa especializada en soluciones de identidad confiable, reafirmó su autoridad en el mercado con el lanzamiento de HID Amico, lector biométrico de reconocimiento facial diseñado para entornos de alta exigencia.

Rogerio Coradini, director Comercial de PACS para América Latina en HID, en el marco de Expo Seguridad 2026, detalló los alcances de esta tecnología y señaló que el valor diferencial de HID Amico radica en su compatibilidad absoluta, tanto con el portafolio de tarjetas físicas tradicionales de HID como con sus credenciales virtuales (identidades móviles), permitiendo a las organizaciones una transición tecnológica sin fricciones.

"Es un producto nuevo, tardó un poco en salir al mercado, justo para evaluar bien las demandas, las necesidades de la industria. Es un producto 100% novedoso dentro del portafolio de HID", aseguró Coradini y agregó que es una solución premium con un precio competitivo.

Como diferenciador de otras compañías, HID Amico ofrece como ventaja la integración con el algoritmo de Paravision, una compañía de inteligencia artificial y visión computacional reconocidas a nivel mundial. "Utilizamos la tecnología de IA de Paravision, un algoritmo muy robusto, muy probado, que trae un nivel de seguridad muy alto. También tenemos la compatibilidad de todas las tarjetas HID tanto físicas como virtuales; se puede utilizar QR, PIN y otros factores de autenticación que pueden trabajar de forma combinada llevando el nivel de seguridad a una gama más alta", puntualizó Coradini.

El directivo destacó que entre las principales verticales de adopción de la plataforma HID Amico destacan el sector bancario y financiero, donde se resguardan centros de datos y áreas corporativas restringidas. Otra vertical es el sector educativo, particularmente universidades, para gestionar el flujo masivo de estudiantes y personal docente en campus distribuidos. Por último, el sector de infraestructura crítica, donde puertos y aeropuertos de la región adoptaron la plataforma para mitigar riesgos en puntos de acceso de alta sensibilidad perimetral.

Paralelamente a este lanzamiento, Coradini enfatizó que HID continúa manteniéndose como el líder absoluto en el mercado de identidades móviles. En el caso específico de México, subrayó un incremento acelerado en la adopción de tarjetas virtuales, impulsado por la digitalización de los espacios de trabajo y la demanda de soluciones contactless basadas en teléfonos inteligentes. "Más del 70% del mercado de tarjetas virtuales lo maneja HID. Hacemos las cosas para liderar y HID Amico es un ejemplo de esto".

Pilares tecnológicos que definen a HID Amico

Reconocimiento rápido y preciso: impulsado por la tecnología de IA líder de Paravision, que minimiza retrasos y falsos rechazos para una entrada fluida y segura, evitando cuellos de botella.

Múltiples métodos de autenticación: Admite cinco métodos de autenticación para satisfacer las necesidades de seguridad (reconocimiento de rostro, credencial, HID Mobile Access, código QR y PIN). Las opciones se pueden combinar para la autenticación multifactor, lo que proporciona mayor seguridad.

Seguridad y privacidad desde el diseño: cumple con los controles de privacidad y seguridad aplicables, en línea con las mejores prácticas de la industria y los requisitos normativos. Además, HID Amico ofrece una plantilla opcional en la tarjeta, donde los datos biométricos se almacenan de forma segura en la credencial del usuario (tarjeta o móvil) en lugar de en una base de datos centralizada.

Integración perfecta: soporte listo para usar para OSDP y Wiegand para integrarse sin esfuerzo con los sistemas de control de acceso existentes a través de la API. La alimentación a través de Ethernet (PoE) simplifica la instalación, lo que reduce el tiempo y el costo.

Rogerio Coradini, director Comercial de PACS para América Latina en HID

Gabinetes inteligentes

traka
ASSA ABLOY

transforman la gestión de accesos en entornos corporativos

El uso de llaves posee un gran impacto en las operaciones empresariales. Y es que si se extravían afectan la productividad, pero sobre todo la seguridad en una empresa. En la era de la transformación digital, la protección corporativa ha encontrado un nuevo aliado. Traka (parte de ASSA ABLOY) empresa líder en sistemas inteligentes para la gestión de llaves y equipos, presentó en Expo Seguridad México 2026, su línea Traka STouch Pro y Traka MTouch Pro, caracterizadas por su versatilidad, integración, robustez y estética.

Diego Cota, gerente Regional de Ventas para América Latina y el Caribe de Traka, mencionó que la propuesta consiste en transformar la operación manual de la gestión de llaves mediante un gabinete electrónico que opera mediante autenticación por biometría, tarjeta de proximidad o código PIN. El gabinete solo desbloqueará la ranura específica de la llave que ese usuario tiene autorizada utilizar; el resto permanecerán bloqueadas. El software registrará quién toma la llave, por cuánto tiempo, si hubo un problema con la llave o con el equipo que se intentó abrir.

La seguridad corporativa es la vertical nativa de Traka. Y es que, en el pasado, el control de llaves en las organizaciones dependía de registros manuales en libretas, un método altamente vulnerable al error humano. La propuesta de Traka da un giro de 180 grados a esta situación al integrar tecnología de punta para que cada llave se convierta en un activo inteligente e identificable

Integración con los sistemas de seguridad

"Más allá de los gabinetes inteligentes, el verdadero valor de esta tecnología radica en su capacidad de integración, automatización y generación de información estratégica para las operaciones", explica Diego Cota.

Todas las soluciones inteligentes de gestión de acceso de Traka son administradas a través del software Traka Web, una plataforma diseñada para centralizar el control de llaves y activos desde un único equipo o a través de múltiples servidores conectados en red. La solución ofrece funciones avanzadas de monitoreo, administración y generación de reportes en tiempo real, permitiendo a las organizaciones optimizar procesos y fortalecer la trazabilidad de sus operaciones.

"La gestión de llaves ya no debe verse únicamente como un mecanismo de control o restricción. Hoy una llave puede convertirse en una fuente de información estratégica para las operaciones, ayudando a mejorar la eficiencia, la trazabilidad y la seguridad en toda la organización", concluyó Cota.

Gracias al respaldo de ASSA ABLOY, las soluciones de Traka también cuentan con la capacidad de integrarse con plataformas de control de acceso, sistemas de gestión de asistencia y servicios de directorio de otros fabricantes, facilitando la creación de ecosistemas de seguridad más conectados y eficientes.

Traka presenta gabinete de resguardo inteligente de armas

Fabricados con estructura de acero y equipados con puertas de policarbonato, Traka presentó sus gabinetes de resguardo de armas de fuego, que operan mediante un software de gestión centralizado. El usuario puede interactuar con asistema para seleccionar qué tipo de armamento requiere extraer, ya que en el gabinete se pueden almacenar armas largas o cortas.

Para reforzar las medidas de seguridad de dichos gabinetes en el resguardo de armas largas, Traka integra tecnología de identificación por radiofrecuencia, a cada una de las piezas de armamento se les agrega un tag electrónico. Así, el casillero incorpora una antena que sensa las señales de los dispositivos y determina si el arma se encuentra dentro o fuera del lgabinete, registrando automáticamente la hora, fecha y la identidad del operador que realizó el movimiento.

En el caso de armas cortas, se les implementan micro tags, el gabinete cuenta con un sistema de sensores de posición que detecta si se encuentra el arma dentro del gabinete y si está bien colocada.

Diego Cota, gerente Regional de Ventas para América Latina y el Caribe de Traka

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

LAR redefine estrategia de impulso a fabricantes en América Latina

La industria de la seguridad electrónica en América Latina atraviesa una etapa de transformación impulsada por la inteligencia artificial, la integración de sistemas y una creciente demanda de soluciones especializadas. En este contexto, LAR Group inicia una nueva etapa corporativa con un objetivo claro: consolidar el legado construido durante más de dos décadas y acelerar el crecimiento de sus fabricantes representados en la región.

José Pablo Mora, presidente de LAR, explicó que la reciente adquisición del 100% de las acciones de la compañía representa una transición que busca preservar la esencia de la organización. La operación, concretada en enero de 2026, marca el inicio de una nueva administración, aunque, enfatizó, sin modificar ni el legado ni la identidad que ha distinguido a la empresa durante 23 años.

"Somos afortunados de construir sobre la base que desarrolló Glenn Patrizio durante más de dos décadas", afirma Mora al referirse al fundador de la compañía, quien continúa colaborando como consultor estratégico y mentor. Su permanencia, señaló, garantiza la continuidad del conocimiento, las relaciones comerciales y la visión que posicionaron a LAR como uno de los principales representantes de fabricantes de tecnología de seguridad en América Latina.

Lejos de plantear una ruptura, la nueva dirección busca fortalecer el modelo de negocio que ha permitido a la empresa convertirse en un puente entre fabricantes internacionales y los mercados latinoamericanos. Para Mora, el principal activo de LAR es precisamente el prestigio construido a lo largo de los años, razón por la cual descartó cualquier modificación de la marca.

"Sería un error estratégico cambiar el nombre de una empresa que ha construido una reputación tan sólida en la región. Nuestro compromiso es mantener ese legado y crecer sobre él", aseguró.

Uno de los ejes de esta nueva etapa será la incorporación de tecnologías basadas en inteligencia artificial. La firma trabaja en el fortalecimiento de las capacidades analíticas de los fabricantes que representa, impulsando nuevas herramientas para videovigilancia, automatización e integración de sistemas, además de consolidar alianzas tecnológicas con actores estratégicos como Intel.

Estas colaboraciones buscan que los fabricantes cuenten con plataformas más robustas y con mayores capacidades de procesamiento para responder a las nuevas exigencias del mercado, donde la analítica avanzada y la toma de decisiones en tiempo real adquieren cada vez mayor relevancia.

Actualmente, LAR representa a 11 fabricantes, mientras que NUVA —empresa del mismo grupo— integra otras seis marcas. La estrategia contempla ampliar este portafolio de manera selectiva, privilegiando aquellas soluciones que complementen la oferta tecnológica y aporten valor tanto a fabricantes como a integradores.

Mora explicó que el modelo de negocio de LAR consiste en operar como una extensión de los fabricantes. La empresa proporciona servicios especializados de ventas, mercadotecnia e ingeniería para aquellas compañías que buscan desarrollar mercados en América Latina sin establecer una estructura propia en cada país.

"Somos un outsourcing de la fuerza comercial, de marketing y de ingeniería de los fabricantes que deciden confiar en nosotros para desarrollar la región", afirmó.

Este esquema, todavía poco común en América Latina, permite reducir costos y riesgos para los fabricantes, al tiempo que ofrece un conocimiento profundo de los mercados locales y de las necesidades específicas de cada país.

Con un equipo de 20 especialistas y presencia en países como México, Guatemala, Venezuela, Colombia, Perú, Chile y Argentina, LAR mantiene cobertura en algunas de las principales capitales latinoamericanas. La compañía considera que esta infraestructura le permitirá fortalecer la integración regional y ampliar el alcance de las tecnologías de seguridad que representa.

Para Mora, el futuro de la industria dependerá cada vez más de la capacidad para integrar soluciones complejas, desarrollar proyectos de alta especialización y aprovechar herramientas de inteligencia artificial que incrementen la eficiencia operativa.

En esa dirección, la empresa proyecta una etapa de consolidación orientada a fortalecer la participación de sus fabricantes en el mercado, ampliar su presencia regional y continuar impulsando tecnologías que contribuyan a elevar los estándares de seguridad en América Latina, apoyándose en una combinación de experiencia, innovación y relaciones de largo plazo con fabricantes, distribuidores e integradores.

José Pablo Mora, presidente de LAR

Key® Business Process Solutions apuesta por la gestión inteligente con “KeyVisitor”

Jörg Altenheimer, managing director de Key Business Process Solutions (BPS) en México, presentó el robusto portafolio de software propio desarrollado en el país, diseñado bajo una arquitectura de alta interoperabilidad para transformar radicalmente la automatización de accesos y la gestión de contingencias. Particularmente exhibió una plataforma enfocada en la seguridad y eficiencia en los procesos de ingreso a edificios corporativos, industrias, conjuntos residenciales e incluso instalaciones gubernamentales.

La solución llamada KeyVisitor, tiene como característica la integración con diversas plataformas de seguridad, lo que permite centralizar la gestión de accesos en un solo sistema. “Ya somos un fabricante de software hecho en México”, destacó Jörg Altenheimer y dijo que la plataforma se integra con sistemas de control de acceso como LenelS2, cámaras Mobotix y herramientas de comunicación como correo electrónico y WhatsApp.

Entre sus funciones destaca el envío de credenciales digitales mediante códigos QR que permiten abrir torniquetes o puertas autorizadas. Además, el sistema puede validar la identidad del visitante mediante el escaneo de identificaciones oficiales, como la credencial para votar o el pasaporte.

Uno de los diferenciadores de la plataforma es la integración con Apple Wallet y Google Wallet, lo que permite que los visitantes almacenen su pase digital directamente en su celular sin necesidad de buscar correos electrónicos o mensajes para acceder a sus credenciales.

La plataforma fortalece la seguridad de las instalaciones, pues a diferencia de los tradicionales registros en papel, el sistema mantiene un control en tiempo real de las personas que se encuentran dentro de un edificio. Esta información puede ser especialmente útil durante una evacuación por incendio, sismo u otra emergencia. “Sabemos cuántos visitantes se encuentran en el edificio y eso permite ser más proactivos en la búsqueda de personas durante un incidente”, comentó.

La solución está dirigida principalmente a empresas, complejos industriales, desarrollos residenciales y dependencias gubernamentales que reciben un alto flujo de visitantes.

Digital Signage que salva vidas

Para complementar la arquitectura de seguridad, la compañía presentó Digital Signage, que amplía las capacidades de comunicación y monitoreo dentro de las organizaciones.

La aplicación, disponible para Apple TV a través del App Store, permite integrar en una misma pantalla información del sistema de visitantes, videovigilancia, control de acceso, anuncios corporativos y alertas de emergencia. En resumen, la solución se vincula directamente con la nube (vía Dropbox) y con el sistema Visitante para desplegar en

pantallas tableros informativos sobre quién está dentro de las instalaciones o por llegar.

Más allá del ámbito corporativo o comercial, esta herramienta se transforma en un activo de protección civil. Al estar interconectada con los sistemas de control de acceso y circuito cerrado de televisión, la plataforma cuenta con la posibilidad de modificar de manera dinámica las rutas de evacuación durante una contingencia. Si una salida de emergencia queda bloqueada por fuego o representa un riesgo, el sistema puede redirigir automáticamente a las personas hacia rutas seguras mediante las pantallas instaladas en el inmueble.

Lanzada al mercado hace año y medio, la solución ya registra aproximadamente 500 descargas y, al igual que el sistema Visitante, fue utilizada primero de manera interna antes de su comercialización. Con este tipo de desarrollos, Key BPS simplifica la implementación técnica para los integradores del sector, además introduce soluciones de alta tecnología y bajo costo que redefinen la gestión de riesgos en corporativos, gobierno y desarrollos residenciales.

La integración entre KeyVisitor y KeyDigitalSignage permite que la información capturada durante el proceso de registro se convierta inmediatamente en comunicación operativa. De esta forma, las organizaciones pueden conocer quién se encuentra dentro de las instalaciones y utilizar esa información para fortalecer la seguridad, agilizar la operación y mejorar la respuesta ante incidentes.

Jörg Altenheimer, managing director de Key Business Process Solutions (BPS) en México

Expo Seguridad México 2026

el principal foro de innovación y negocios para la industria

Expo Seguridad México, fue el punto de convergencia de la industria en el país y Latinoamérica para celebrar su 23ª edición, que se llevará a cabo del 2 al 4 de junio del presente año. En el marco de inauguración, Luiz Bellini Luiz Bellini, director de RX México, expuso que, en un contexto marcado por la incertidumbre económica, los cambios tecnológicos y los desafíos globales, la seguridad se ha convertido en un factor estratégico para la continuidad y competitividad de las organizaciones. “Hoy, más que una exposición, reunimos un ecosistema de innovación, conocimiento y negocios que permite a las empresas prepararse mejor para enfrentar riesgos cada vez más complejos y conectados”, aseveró.

“Las amenazas ya no existen de forma aislada, convergen en los ámbitos físico, industrial y digital. Por ello, Expo Seguridad México, Expo Seguridad Industrial e Infosecurity México conforman el ecosistema de seguridad más relevante de América Latina, un espacio donde la colaboración, la tecnología y el intercambio de conocimiento impulsan la resiliencia, la confianza y nuevas oportunidades de negocio para toda la industria”, indicó Bellini.

Por su parte, Paola Buenrostro, Show Manager en RX México para Expo Seguridad México, Expo Seguridad Industrial e Infosecurity México, destacó que esta edición fue sido diseñada para generar valor más allá de la exhibición tecnológica. Con demostraciones en vivo, espacios especializados, más de 90 activaciones y programas que facilitaron encuentros estratégicos entre compradores y proveedores.

“La seguridad se fortalece cuando existe colaboración. La presencia de asociaciones, expositores, aliados estratégicos y visitantes confirma que este sector continúa evolucionando a través del intercambio de conocimiento, la generación de alianzas y la construcción conjunta de soluciones que respondan a los desafíos actuales de la seguridad en todas sus dimensiones”, expresó Buenrostro.

Importante destacar que Expo Seguridad México, Expo Seguridad Industrial e Infosecurity México 2026 concluyeron con éxito al reunir a más de 20,000 profesionales de la industria y 400 empresas expositoras en un piso de exhibición superior a 25,000 m². Durante tres días, el piso de exhibición se convirtió en el principal punto de encuentro para fabricantes, distribuidores, integradores, usuarios finales, autoridades y especialistas que buscaron fortalecer la protección de personas, instalaciones, operaciones y activos digitales en un entorno cada vez más complejo y desafiante.

Rumbo a 2027

Uno de los principales hitos de esta edición fue la integración de los tres eventos, que permitió ofrecer a los asistentes una visión integral de los desafíos que enfrentan las organizaciones y de las tecnologías necesarias para fortalecer su resiliencia frente a riesgos cada vez más interconectados.

Desde la protección de infraestructuras críticas y la prevención de accidentes laborales hasta la defensa contra amenazas digitales, los asistentes tuvieron acceso a tecnologías, servicios y estrategias diseñadas para fortalecer la continuidad operativa y la capacidad de respuesta de organizaciones públicas y privadas.

Expositores nacionales e internacionales presentaron más de 420 soluciones orientadas a la protección de organizaciones públicas y privadas, entre las que destacaron plataformas de videovigilancia inteligente impulsadas por inteligencia artificial; sistemas avanzados de control de acceso y biometría, drones para monitoreo y respuesta operativa, herramientas de análisis predictivo, tecnologías para la prevención de riesgos laborales, sistemas contra incendio, automatización industrial; así como soluciones de ciberseguridad.

unifica la seguridad electrónica en una sola interfaz

En el mercado de la seguridad electrónica, la integración es una necesidad operativa crítica tanto para integradores como para usuarios finales. Actualmente, la tendencia global exige simplicidad, robustez y convergencia. Por ello, Ajax Systems propone un ecosistema de soluciones integrales que protege desde un hogar residencial hasta corporativos de gran escala.

Ana Laura Hernández, gerente comercial para México, de Ajax Systems, en el marco de Expo Seguridad 2026, puntualizó que la marca estructuró su portafolio de forma que todas sus líneas de productos coexistan y se comuniquen de forma nativa. Esto significa que las soluciones de intrusión, detección de incendios y automatización son totalmente compatibles entre sí. Así, se eliminan las barreras técnicas tradicionales y permite a los profesionales del sector personalizar sus servicios para cada cliente.

La propuesta de Ajax Systems consiste en centralizar la gestión de todo su ecosistema en una única interfaz intuitiva. A través de esta plataforma unificada, un monitorista o el propio usuario pueden verificar una alerta de intrusión, revisar el flujo de video en tiempo real para descartar falsas alarmas y activar un protocolo de automatización. La experiencia de usuario se simplifica, lo que eleva la eficiencia operativa y reduce los tiempos de capacitación para el personal de seguridad.

En Noruega, la compañía cuenta con varios casos de éxito en museos y sitios de alto valor patrimonial. Uno de los más destacados en la protección de una iglesia, donde se implementó el sistema de detección de incendios EN54 de Ajax Systems. Al ser una solución completamente inalámbrica, permite proteger edificaciones históricas sin realizar modificaciones estructurales que pueden afectar su arquitectura o valor patrimonial.

Para reforzar su calidad, la compañía cuenta con la normativa EN54, un estándar europeo de referencia para el diseño, fabricación, instalación, certificación y mantenimiento de sistemas automáticos de detección y alarma de incendios. Su aplicación resulta imprescindible tanto en edificios públicos como privados. Su objetivo es garantizar la máxima fiabilidad, resistencia y compatibilidad de todos los equipos, desde los detectores de humo y centrales de control, hasta los altavoces de evacuación.

“La firma tiene varias verticales: en la vertical industrial cubre hospitales, escuelas, corporativos y hotelería, por mencionar algunos. Se espera que la solución contra incendio EN54 esté disponible en el mercado mexicano a partir de agosto”, acotó Ana Laura Hernández.

Y para refrendar su compromiso tanto con distribuidores como con socios, la compañía anunció un ciclo de talleres con distribuidores, así como ofertas de certificaciones en línea, eventos presenciales y en línea, cursos en video y demostraciones en línea que ayudan a los socios y distribuidores a trabajar con los productos Ajax de forma más eficaz, ofrecer mejores soluciones a los clientes y aprovechar más oportunidades de negocio.

Los productos de Ajax han sido diseñados bajo los más estrictos controles de calidad, cumpliendo con las normas locales e internacionales. Este factor es clave para los integradores de la región, ya que les permite participar en licitaciones y proyectos donde la certificación del hardware es un requisito obligatorio de cumplimiento. Gracias a este respaldo normativo, los sistemas son plenamente aptos para proteger instalaciones de cualquier tipo y escala: hospitales, escuelas, corporativos

El enfoque de Ajax Systems demuestra que el futuro de la seguridad no radica en la acumulación de dispositivos aislados, sino en la capacidad de estos para trabajar como un solo organismo inteligente. Al derribar los muros entre la detección de intrusos, la prevención de incendios, el análisis de video y la automatización, y al respaldarlo con certificaciones globales, la marca ofrece una solución integral, escalable y fácil de gestionar.

Ana Laura Hernández, gerente comercial para México, de Ajax Systems

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 preparación operativa de los profesionales continuamente expuestos al riesgo.

Las instituciones que comprenden esta realidad tienden a construir entornos más estables, reducir las tasas de absentismo y fortalecer la capacidad de respuesta de sus equipos. Al fin y al cabo, preservar a quienes protegen también es preservar el propio sistema de seguridad.

Preservar a quienes protegen también es preservar el propio sistema de seguridad. Detrás de cada uniforme hay un ser humano sometido a demandas físicas, cognitivas y emocionales que a menudo son invisibles para el ojo externo. Reconocer los impactos silenciosos de esta rutina no es solo una cuestión de salud laboral, sino también de responsabilidad institucional y madurez operativa.

Porque la seguridad que se ofrece a otros inevitablemente comienza con la preservación de quienes permanecen diariamente en primera línea.

México registra más de 435 mil accidentes laborales al año

Cada día, cerca de mil trabajadores en México sufren un accidente laboral. No es una estimación: es la realidad documentada por el Instituto Mexicano del Seguro Social (IMSS) en su Memoria Estadística 2024, que registró un promedio de 527,802 riesgos de trabajo anuales,equivalentes a aproximadamente 1,446 accidentes de trabajo por día en el territorio nacional.

Los accidentes laborales generaron pérdidas superiores a 76 mil millones de pesos en 2025, con un costo promedio de 21,500 pesos por trabajador lesionado. El impacto indirecto por pérdida de productividad supera los 35 mil millones de pesos adicionales. A esto se suma la dimensión humana: hasta el tercer trimestre de 2025, se reportaron 796 muertes en accidentes laborales, lo que representó un aumento del 10% en comparación con el año anterior.

Las cifras también muestran una tendencia al alza y solo el año pasado los accidentes crecieron un 15%, de acuerdo con datos del IMSS. Ante esta realidad, la Organización Internacional del Trabajo (OIT) estima que el costo económico de los accidentes laborales puede representar hasta el 4% del PIB.

Una nueva versión de la norma que llega 16 años después

En respuesta directa a este escenario, el 28 de marzo de 2025 se publicó en el Diario Oficial de la Federación la nueva versión de la Norma Oficial Mexicana NOM-017-STPS-2024, “Equipo de protección personal – Selección, uso y manejo en los centros de trabajo”, que entró en vigor el 28 de septiembre de 2025, sustituyendo la NOM-017-STPS-2008, que estuvo vigente durante 16 años.

La actualización no es menor. La versión 2025 introduce una clasificación de cuatro niveles de protección y eleva de forma sustancial las exigencias técnicas para fabricantes, importadores y empleadores. Entre los cambios más relevantes se encuentran:

- La exigencia de un análisis de riesgos más detallado del entorno laboral, considerando riesgos físicos, químicos, biológicos, ergonómicos y psicosociales para determinar el EPP necesario por puesto y área.
- La obligación de que el EPP cuente con normas o estándares técnicos avalados por laboratorios autorizados. Si no existe una norma específica, se aceptarán datos del fabricante validados por laboratorios independientes.
- La ampliación del deber de protección a visitantes, terceros y prestadores de servicios que ingresen a áreas con exposición ocupacional.
- El establecimiento de registros detallados sobre entrega, mantenimiento, reposición, limpieza y disposición final del EPP. Las multas por incumplimiento pueden alcanzar hasta $542,350 pesos.

El mercado migra hacia la validación técnica

El cambio regulatorio refleja una tendencia global: en operaciones industriales con exposición simultánea a partículas, líquidos químicos y contaminantes biológicos, la comprobación del desempeño real de los EPP dejó de ser una ventaja competitiva para convertirse en una obligación legal y ética.

En este contexto, las empresas que ya operaban con procesos estructurados de certificación y pruebas de laboratorio tienen ventaja. DuPont, por ejemplo, realiza evaluaciones técnicas rigurosas en sus líneas de prendas de protección (como ProShield®, Tyvek® y Tychem®), utilizadas en aplicaciones industriales, de laboratorio y en operaciones con riesgo químico.

“Los nuevos requisitos refuerzan un movimiento importante del mercado hacia la validación técnica de los equipos de protección. Hoy, no basta con declarar un nivel de protección: las empresas deben demostrar, mediante pruebas y certificaciones, que los materiales realmente ofrecen el desempeño esperado en condiciones reales de uso”, afirma Karen Ranocchia, gerente de marketing para América Latina en DuPont Personal Protection.

Según Ranocchia, la nueva norma también eleva el estándar de seguridad en toda la región. “DuPont trabaja desde hace muchos años con procesos de pruebas de laboratorio, evaluaciones de permeación química y cumplimiento de normas internacionales en sus prendas de protección. Este enfoque ayuda a las empresas a tener mayor confianza en la elección de sus EPP y fortalece la cultura de prevención dentro de las operaciones”, concluye. Implicaciones para los empleadores.

Con la NOM-017-STPS-2024 ya en vigor, las empresas deben revisar sus programas de seguridad en tres frentes simultáneos: la selección técnica de los equipos de protección con respaldo documental y de laboratorio; la capacitación continua y la trazabilidad de los EPP entregados a cada trabajador; y la extensión de las obligaciones de protección a todos quienes ingresen a áreas de riesgo, incluyendo contratistas y visitantes.

Los sectores con mayor urgencia de adaptación son la construcción, la manufactura y el transporte, que históricamente concentran la mayor incidencia y gravedad de accidentes laborales en México.

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

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

APOYAN

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

Informes:

1 312 686 4435 - 301 539 7542 asosec@asosec.co

Neurociencia, Inteligencia Artificial y ciberseguridad

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

Articulista Invitado

Introducción

Durante años pensamos en la ciberseguridad como una carrera entre candados y ganzúas: firewalls contra exploits, antivirus contra malware. Esa imagen ya no alcanza. Los sistemas de inteligencia artificial que hoy amenazan (y defienden) nuestras redes no funcionan como cajas fuertes ni como cerraduras; funcionan, cada vez más, como cerebros. Aprenden de la experiencia, se adaptan al entorno, reconocen patrones y explotan los mismos atajos mentales que usamos los humanos para tomar decisiones rápidas. Por eso, entender cómo opera el cerebro ya no es un tema exclusivo de neurólogos y psicólogos: se ha convertido en una pieza clave para entender —y frenar— los ciberataques del futuro. En las siguientes líneas exploraremos la intersección poco intuitiva entre neurociencia, inteligencia artificial y ciberseguridad, y por qué ignorarla puede dejarnos en desventaja frente a adversarios que ya la están explotando.

Desarrollo

¿Qué es la neurociencia?

La neurociencia es el campo que estudia el sistema nervioso y, en particular, cómo el cerebro procesa información, aprende, recuerda y toma decisiones. No es una disciplina única, sino un cruce de biología, psicología, computación y medicina, interesado en preguntas muy concretas: ¿cómo se forman las conexiones entre neuronas cuando aprendemos algo nuevo? ¿Por qué el cerebro prioriza cierta información sobre otra? ¿Qué mecanismos nos hacen vulnerables a la manipulación o el engaño? Dos conceptos son centrales para lo que sigue: la neuroplasticidad, es decir, la capacidad del cerebro de reorganizar sus conexiones para adaptarse a nuevas circunstancias, y el sesgo cognitivo, esos atajos mentales que nos permiten decidir rápido pero que también pueden llevarnos a errores sistemáticos y predecibles.

¿Cómo se relaciona la neurociencia con la IA y la ciberseguridad?

El puente entre ambos mundos no es casual: buena parte del diseño de la inteligencia artificial moderna se inspiró explícitamente en cómo funciona el cerebro. Las redes neuronales artificiales imitan, de forma simplificada, la manera en que las neuronas se conectan y refuerzan sus vínculos con la experiencia. La computación neuromórfica va un paso más allá al intentar replicar en hardware físico el procesamiento paralelo del cerebro humano, en contraste con el procesamiento secuencial de las computadoras tradicionales. El resultado es una IA cada vez más capaz de aprender de forma autónoma, adaptarse en tiempo real y anticipar comportamientos, exactamente las cualidades que la vuelven tan útil para automatizar procesos y, al mismo tiempo, tan peligrosa en manos equivocadas.

Esta conexión se vuelve todavía más inquietante cuando la IA no solo imita al cerebro, sino que aprende a leerlo. Los sistemas de biometría conductual analizan el ritmo de tecleo, el movimiento del mouse o la forma de deslizar el dedo en una pantalla, rasgos determinados por nuestra neurología y tan únicos como una huella digital. Un atacante que logre modelar esos patrones con suficiente precisión puede suplantar a un usuario sin necesidad de robar una contraseña. Y hay un segundo frente, quizás más cercano al día a día de cualquier persona: el de los sesgos cognitivos. El sesgo de confirmación, el sesgo de autoridad, el efecto de recencia y el exceso de confianza son mecanismos bien documentados por la neurociencia, y son también la materia prima de la ingeniería social. Lo que antes hacía un estafador por intuición, hoy lo hace un modelo de lenguaje analizando miles de interacciones para identificar exactamente qué mensaje, con qué tono y en qué momento, tiene más probabilidades de manipular a una persona específica.

Riesgos, retos y perspectivas

Entre los riesgos más evidentes están el phishing automatizado que imita con precisión el lenguaje de un colega o jefe, los ataques de deepfake capaces de clonar voces para autorizar transferencias fraudulentas, el malware que aprende a esconderse observando el comportamiento del software de seguridad, y las botnets que estudian el tráfico normal de una red antes de lanzar

un ataque de denegación de servicio. El reto de fondo es que las defensas basadas en firmas estáticas y patrones conocidos ya no bastan frente a adversarios que se adaptan más rápido de lo que cualquier equipo humano puede reaccionar.

Pero la misma neurociencia que inspira el ataque puede inspirar la defensa. Sistemas de detección basados en comportamiento, capaces de identificar desviaciones de la actividad normal igual que el cerebro detecta una alteración en su entorno, son una aplicación directa del principio de neuroplasticidad. Los mecanismos de respuesta automática que ajustan reglas de firewall en tiempo real recuerdan a cómo el cuerpo reacciona ante una amenaza sin esperar una orden consciente. El aprendizaje iterativo tras cada incidente, la vigilancia proactiva inspirada en el sistema inmune, e incluso la arquitectura distribuida de la defensa, que evita que un solo punto de falla comprometa todo el sistema, son ideas tomadas prestadas directamente de cómo el cerebro y el cuerpo se protegen a sí mismos. A esto se suma la capacitación de usuarios basada en el conocimiento de los sesgos cognitivos: entrenar a las personas para reconocer sus propios atajos mentales, mediante simulacros de phishing, retroalimentación de comportamiento y técnicas de memoria, convierte el eslabón más débil de cualquier organización en una línea de defensa activa.

La perspectiva hacia adelante es de una carrera continua y probablemente permanente. Si la computación neuromórfica madura, veremos sistemas de IA capaces de monitorear tráfico, detectar debilidades y atacar antes de que cualquier medida de seguridad tradicional lo note, lo que exigirá defensas igual de veloces y adaptativas. El futuro de la ciberseguridad no dependerá únicamente de mejores algoritmos, sino de qué tan bien logremos traducir el conocimiento sobre cómo aprende, decide y falla la mente humana en arquitecturas de defensa igual de flexibles.

Conclusión

La frontera entre la mente humana y la máquina se está volviendo cada vez más difusa, y la ciberseguridad no puede darse el lujo de ignorarlo. Entender la neurociencia ya no es un ejercicio académico distante: es una herramienta práctica para anticipar cómo piensan, aprenden y engañan los sistemas de IA, y también para diseñar defensas que se adapten con la misma velocidad que las amenazas. La pregunta que vale la pena hacerse no es si la inteligencia artificial seguirá acercándose al funcionamiento del cerebro, sino qué tan preparados estamos, como organizaciones y como individuos, para reconocer cuándo nuestra propia mente está siendo el objetivo del ataque.

Vale la pena, entonces, invitar a la reflexión: ¿cuántas de las decisiones digitales que tomamos cada día son realmente nuestras, y cuántas están siendo anticipadas por un algoritmo que conoce nuestros sesgos mejor que nosotros mismos? La invitación es concreta: revisemos hoy mismo los protocolos de capacitación en nuestras organizaciones, incorporemos el conocimiento de los sesgos cognitivos en los programas de concientización, y exijamos que los equipos de seguridad dialoguen con especialistas en ciencias cognitivas antes de que sea el atacante quien lo haga primero.

Referencia

Kritika. (2025). A neuroscience perspective on AI and cybersecurity. ISACA Journal, 1, 44-49. https://www.isaca.org/resources/isaca-journal

De la gestión de riesgos a la gestión de la complejidad: una evolución necesaria para el siglo XXI

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.- Durante décadas, la gestión de riesgos ha evolucionado significativamente. Las organizaciones públicas y privadas comenzaron a estructurar metodologías, matrices, indicadores y procesos destinados a identificar, analizar y tratar riesgos. Se han desarrollado estándares internacionales, consolidado modelos corporativos y han surgido nuevas disciplinas para apoyar la toma de decisiones.

Sin embargo, a pesar de este avance metodológico, sigue existiendo un fenómeno intrigante. Las organizaciones siguen sorprendidas. Crisis financieras, pandemias, ciberataques, interrupciones logísticas, conflictos geopolíticos, desastres reputacionales, fallos regulatorios y colapsos operativos continúan ocurriendo incluso en instituciones consideradas maduras en gestión de riesgos.

La pregunta se vuelve inevitable: ¿Por qué las organizaciones que tienen procesos estructurados de gestión de riesgos siguen sorprendiéndose por eventos que amenazan su supervivencia?

La respuesta puede no estar en ausencia de metodologías. Puede que esté en la forma en que vemos la realidad. Durante gran parte de los siglos XIX y XX, predominó una visión mecanicista del mundo. Esta visión, profundamente influenciada por el pensamiento cartesiano y la ciencia clásica, asumía que los sistemas podían entenderse mediante la descomposición de sus partes.

Divídete y entiende. Aparte para analizar. Fragmento al control. Esta lógica ha producido avances extraordinarios para la ciencia, la ingeniería y la gestión. Sin embargo, también ha producido una consecuencia menos percibida: la fragmentación de la comprensión de la realidad.

El problema no está en analizar las piezas. El problema surge cuando las piezas empiezan a reemplazar el conjunto. Es precisamente en este punto cuando surge la contribución de Edgar Morin.

Morin sostiene que los grandes desafíos contemporáneos no pueden entenderse mediante enfoques lineales, aislados y fragmentados. El mundo moderno se caracteriza por relaciones, interdependencias, retroalimentaciones, incertidumbres y fenómenos emergentes que escapan a los modelos tradicionales de análisis.

Según Morin, la simplificación excesiva produce lo que él llama “inteligencia ciega”. Una inteligencia capaz de analizar elementos aislados, pero incapaz de entender sus conexiones.

Esta crítica resulta especialmente relevante para la gestión de riesgos. En muchos casos, los riesgos se identifican individualmente, se evalúan y se tratan individualmente. Pero los hechos reales no se comportan así.

Los riesgos interactúan. Se distribuyen. Se amplifican entre sí. Los riesgos transforman otros riesgos.

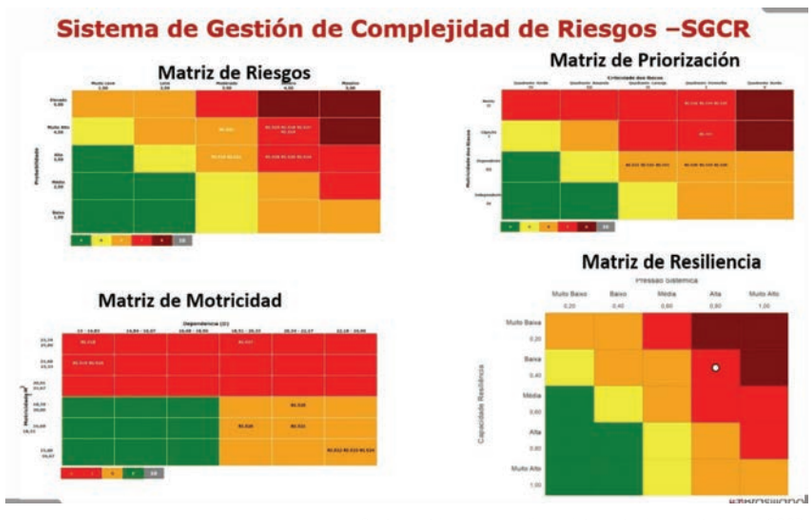
En entornos complejos, el problema a menudo no reside en el riesgo aislado, sino en las relaciones entre ellos. Es precisamente este cambio de perspectiva lo que requiere una evolución de la gestión tradicional de riesgos a un enfoque basado en la complejidad.

Un punto esencial: complejidad no significa confusión, desorden ni complicaciones excesivas. Un fenómeno complicado puede ser difícil, pero aún así descomponible en partes relativamente estables. Un motor de avión es complicado; una organización humana en crisis es compleja. El complicado puede desmontarse y volver a montarse con alta previsibilidad. El complejo cambia cuando interactúa, aprende, reacciona y se reorganiza.

Para Morin, la complejidad requiere pensar que apoye simultáneamente orden y desorden, estabilidad y ruptura, autonomía y dependencia, individuo y sistémico, certeza operativa e incertidumbre estratégica.

En otras palabras, ya no debemos implementar un Sistema de Gestión de Riesgos, sino un Sistema de Gestión de Complejidad de Riesgos – SGCR, con el objetivo de tener una visión sistémica y, además, trabajar con más herramientas de análisis e interpretación.

Hoy, en Brasiliano INTERISK ya hemos operacionalizado un SGCR con herramientas de IA e integración de resultados. Con esto, la visión que tenemos ahora es mucho más completa y sistémica.



Cuatro matrices para analizar e interpretar los resultados del SGCR

REC SAFE®

MÉXICO · COLOMBIA · ARGENTINA · USA

TU OPERACIÓN LOGÍSTICA SIEMPRE PROTEGIDA

GPS & RASTREO
Flota · Activos · Carga

VIDEO TELEMÁTICA
IA embarcada · Eventos

DIAGNÓSTICO SCS
OEA · C-TPAT · BASC

ANGEL GUARDIAN
Control IA/RFID

FLEETCONTROL PRO
Gestión de flota

PREVENCIÓN DE PÉRDIDAS
Robo · Fraude · Merma

OEA | **C-TPAT** | **ISO 28000** | **BASC**

+ 30 AÑOS	+ 50,000 EQUIPOS GPS	4 PAÍSES	24/7/365
De experiencia	Activos	Méx · Col · EUA · Arg	Sin interrupciones

contacto@recconsultores.com

+52 55 8650 9325

www.recsafe.tech

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:

- 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.

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

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

REC SAFE®

Seguridad Preventiva Integral en la era de la IA

Tres décadas de innovación han dado paso a un ecosistema tecnológico sin precedentes: FleetControl PRO, Ángel Guardian, drones con IA y presencia en cuatro países.

Gestión de flotas y trazabilidad en tiempo real: el núcleo de FleetControl PRO.

30 años construyendo el estándar de seguridad logística en América Latina

Fundada hace tres décadas, REC SAFE® revolucionó el mercado mexicano al introducir los primeros equipos de localización satelital orientados a la seguridad de mercancías y personas en tránsito. Lo que comenzó como una visión pionera en la comercialización de tecnología GPS, se ha transformado en la plataforma de seguridad preventiva integral más completa del continente americano.

En 2026, REC SAFE® opera con presencia activa en México, Estados Unidos, Colombia y Argentina, atendiendo a gobiernos, corporativos multinacionales, operadores logísticos globales e instituciones financieras con una cartera de soluciones que integra Inteligencia Artificial, videotelemática, reconocimiento biométrico, drones de ala fija, sistemas RFID y diagnóstico de cadena de suministro bajo los más exigentes estándares internacionales: OEA, C-TPAT, ISO 28000 y BASC.

> "Nuestro crecimiento no es casualidad: es el resultado de entender las necesidades reales de seguridad de cada cliente y entregar soluciones que generan resultados medibles desde el primer día".
> *— Rodolfo Cepeda Rico, Presidente — REC SAFE®*

El portafolio que redefine la seguridad: innovaciones 2025-2026

La evolución tecnológica de REC SAFE® en el último año representa el salto cualitativo más significativo en su historia. La empresa ha integrado capacidades que hasta hace poco eran exclusivas de agencias de inteligencia y fuerzas del orden de primer nivel, poniéndolas al alcance de empresas, industrias y gobiernos con modelos de servicio flexibles, escalables y orientados a resultados.

Solución / Servicio	escripción y Ben
FleetControl PRO	Plataforma avanzada de administración de flotas con telemetría en tiempo real, alertas inteligentes, geofencing dinámico y reportería ejecutiva. Integra SIMs Telcel para cobertura nacional e internacional.
Ángel Guardian (IA/RFID)	Sistema de identificación y control de acceso que combina Inteligencia Artificial con tecnología RFID. Detecta anomalías, identifica personas y genera alertas automáticas en entornos críticos.
Diagnóstico SCS	Plataforma digital de evaluación de seguridad en cadena de suministro bajo estándares OEA, C-TPAT, ISO 28000 y BASC. Disponible en: diagnostico.recsafe.tech — genera un mapa de vulnerabilidades y un plan de mejora priorizado.
Videotelemática Avanzada	Cámaras de video con análisis de comportamiento a bordo de unidades: detección de distracción al volante, somnolencia, uso de teléfono y eventos de riesgo. Evidencia digital para aseguradoras y procesos legales.
Portafolio de Drones con IA	Drones de ala fija y multirrotores con hangares fijos, centros de comando móviles (C2), reconocimiento de armas de fuego con IA, identificación facial y cobertura de grandes extensiones urbanas y periurbanas.
Central de Monitoreo 24/7	Servicio de monitoreo activo de embarques con operadores certificados, protocolos de respuesta inmediata, coordinación con autoridades y central de gestión de incidentes. Capacidad para 500+ embarques/mes bajo esquema de cuentas espejo.
Control de Velocidad Inteligente	Solución de gestión de velocidad con alertas al operador y al gestor de flota, integrada a FleetControl PRO. Reduce siniestralidad y optimiza consumo de combustible en flotas corporativas.
Portafolio Gubernamental	GPS y dashcams para patrullas, video analítica para aplicación de la ley, seguimiento de reos y control de inventario de armas de fuego. Proyectos llave en mano para municipios y estados.
C4/C5 — Centros de Atención a Emergencias	Diseño, construcción y equipamiento integral bajo especificaciones PEAR 6. Incluye videowalls, infraestructura de voz/datos, software de despacho, capacitación internacional y transferencia de tecnología.
Trazabilidad Multinivel para Cadena de Suministro	Solución de seguimiento de mercancía con evidencias documentales, protocolos personalizados, plataformas de gobernanza digital y capacitación especializada para operadores logísticos globales.

Por qué REC SAFE® es la decisión correcta para su empresa

En un entorno donde las amenazas evolucionan a la velocidad de la tecnología, elegir al socio estratégico correcto puede ser la diferencia entre la continuidad operativa y una crisis irreversible. REC SAFE® no vende equipos: construye ecosistemas de seguridad que funcionan.

- 30 años de experiencia comprobada: Pionero en GPS en México con historial verificable de proyectos exitosos en gobierno y sector privado. No somos un experimento — somos el estándar de la industria.
- Metodología de Análisis de Riesgos (ISO 31000): Cada proyecto inicia con un diagnóstico riguroso bajo metodologías internacionales. Entendemos su mapa de vulnerabilidades antes de proponer cualquier solución.

> "Nuestro crecimiento internacional no es solo expansión geográfica; es la validación de que el modelo de seguridad preventiva integral que desarrollamos en México funciona en cualquier mercado, con cualquier cliente, bajo cualquier exigencia."
> *— Rodolfo Cepeda Rico, Presidente — REC SAFE®*

Pais de Operacion	Alcance y Proyectos Destacados
México	Sede central de operaciones. Proyectos activos con gobiernos municipales y estatales, operadores logísticos globales y sector financiero. Caso de éxito emblemático: Proyecto Orion — Secretaría de Seguridad Ciudadana de Puebla, reconocido internacionalmente por COLADCA en ESS+ Bogotá.
Estados Unidos	Operaciones iniciadas con enfoque en seguridad corporativa, gestión de flotas y soluciones para empresas con operaciones transfronterizas. Mercado estratégico por su alta demanda de tecnología de seguridad certificada bajo estándares C-TPAT.
Colombia	Presencia activa en múltiples distritos con soluciones de seguridad preventiva para empresas, industrias y gobiernos. La alianza con expertos locales para capacitación policial y municipal ha consolidado la reputación de REC SAFE® en el país.
Argentina	Nuevo mercado en expansión con alto potencial para soluciones de trazabilidad en cadena de suministro, videotelemática y diagnóstico bajo estándares internacionales. Presencia en el corredor del Mercosur para atención a corporativos regionales.

- Soluciones llave en mano: Nos hacemos cargo de todo como iseño, instalación, configuración, capacitación y soporte continuo. Usted no gestiona proveedores, obtiene resultados.
- ROI medible y comprobable: Nuestros clientes en el sector logístico reportan reducciones de hasta 40% en costos operativos de monitoreo al migrar a Central de Monitoreo REC SAFE® vs. operación interna.
- Certificaciones internacionales: Operamos bajo los estándares más exigentes: OEA, C-TPAT, ISO 28000 y BASC. Su cadena de suministro queda blindada ante auditorías de clientes nacionales e internacionales.
- Alianza con fabricantes tecnológicos: Sinergias que nos permite operar con infraestructura tecnológica de primer nivel en todo el continente americano.
- Presencia en 4 países: México, Estados Unidos, Colombia y Argentina. Nuestros clientes multinacionales operan con un solo proveedor de seguridad en toda su geografía de negocios.
- Innovación continua con IA: Somos el único proveedor de la región que combina drones, reconocimiento de armas, identificación facial, videotelemática y RFID en una sola plataforma integrada y gestionada.

De México al mundo: expansión en el corazón de América

El crecimiento sostenido de REC SAFE® ha traspasado las fronteras nacionales con solidez y estrategia. Lo que comenzó como el proyecto de seguridad más ambicioso de México se ha convertido en un modelo replicable que hoy transforma la seguridad logística y gubernamental en cuatro mercados clave.

Con más de 30 años liderando la industria de seguridad tecnológica en México y América Latina, Rodolfo Cepeda Rico es Presidente de REC SAFE® y miembro del Comité de Tecnología del Consejo Nacional de Seguridad Privada (CNSP). Su visión estratégica ha llevado a la empresa a convertirse en referente internacional, con proyectos icónicos como "Orion" en Puebla, galardonado en la Feria Internacional de Seguridad ESS+ en Bogotá, Colombia.
Bajo su liderazgo, REC SAFE® ha expandido operaciones a cuatro países y desarrollado un portafolio tecnológico que abarca desde drones con Inteligencia Artificial hasta plataformas de diagnóstico de seguridad en cadena de suministro certificadas internacionalmente

Contacto ejecutivo:
presidencia@recconsultores.com
Tel. 5586509325 Ext. 111

Contacto comercial:
contacto@recconsultores.com
www.recsafe.tech

Tres décadas de protección con

En auge el crimen organizado, se destaca en la feria

Lima, Perú.- En un contexto global donde la evolución de las amenazas exige respuestas tecnológicas cada vez más sofisticadas, se dio la bienvenida a la 30ª edición de la Feria Internacional de Seguridad - Securitec Perú. Desde su fundación en 1996, este encuentro se ha consolidado como el epicentro del debate, la innovación y el análisis estratégico de la seguridad, reuniendo a expertos, distribuidores y público interesado en el tema de la protección privada.

Para comprender el impacto y la longevidad de Securitec Perú, es importante mirar atrás. El terrorismo que sufrió la nación entre 1980 y 2000 fue el móvil fundamental para organizar la feria a mediados de los años noventa. En aquella época, el país requería con urgencia un espacio especializado que ofreciera las herramientas para proteger las infraestructuras críticas, a las empresas y a la ciudadanía en general, recordó Guillermo Thais, director de Seguritec Perú.

Mencionó que en sus primeras ediciones, en la feria se exhibía todo lo necesario para combatir a la delincuencia y sus modus operandi: Era común ver armas de alto calibre para fuerzas del orden y seguridad privada, chalecos antibalas con los más altos estándares de resistencia balística, así como robots de última generación diseñados para la desactivación de artefactos explosivos.

Sin embargo, las dinámicas de seguridad nacional obligaron a un cambio de rumbo. Debido al terrorismo que iba en crecimiento y a la necesidad de pacificar el territorio, el gobierno del Perú prohibió a los civiles utilizar armas de fuego. Como consecuencia directa de esta política pública, en Securitec se dejaron de exhibir armas de fuego (cortas y de alto poder), reenfocando el perfil del evento hacia la seguridad electrónica, la prevención, la protección perimetral e ciberseguridad

El nuevo enemigo: El crimen organizado y la extorsión

A pesar de los esfuerzos históricos, el panorama actual presenta desafíos alarmantes. Los organizadores del evento aprovecharon la plataforma para emitir un llamado de atención sobre la realidad que azota a las calles peruanas, destacando que el crimen organizado lastimosamente está más fuerte que nunca.

"Todos los días vemos por televisión cómo los terroristas dejan explosivos en bodegas, bazares y restaurantes sin que se adopte una estrategia integral para luchar contra esta lacra, que es tierra fértil para que el terrorismo renazca. Si seguimos indiferentes, pronto nos sentiremos secuestrados en nuestro país y será difícil recuperar la libertad de vivir en un país libre", advirtió Guillermo Thais.

Ante la falta de una respuesta estatal contundente, la feria se colocó como un bastión para la resiliencia comercial y residencial. "Una de las maneras de protegernos del crimen organizado es asegurar nuestras viviendas y negocios, por lo que en esta feria hemos convocado a los principales distribuidores, a los que agradezco por la confianza depositada en nuestra empresa para dar a conocer los productos más avanzados del mercado", señaló el directivo.

Innovación y acción en el terreno

Fiel a su tradición, Securitec Perú combinó la teoría con la práctica. Paralelamente a la exhibición comercial, se llevó a cabo un robusto Congreso Tecnológico donde se desarrollaron temas cruciales relacionados

con la ciberseguridad, la videovigilancia con Inteligencia Artificial, la gestión de crisis y la protección ciudadana en entornos urbanos de alto riesgo.

El dinamismo del evento alcanzó su punto álgido durante la última jornada, destinada a las simulaciones operativas en vivo: La trigésima edición de Securitec Perú no solo ha sido un escaparate de tecnología, sino un foro de demanda política. La organización convocó de manera abierta y firme al gobierno a realizar su trabajo, dando una respuesta inmediata y eficiente a la ciudadanía en lo que respecta al combate frontal al terrorismo y crimen organizado.

Alianza internacional:

SERCOPP

MÁS SEGURIDAD Magazine

CON SEGURIDAD Magazine Latam

Ya está en México

SARI

- 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

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

Por qué el diseño de una cárcel decide, en silencio, quién vuelve a delinquir

Parte 1 de 2

Cancún, México.- 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.

Esa es la premisa de una disciplina que lleva medio siglo madurando y que hoy tiene, por fin, norma internacional. Se llama CPTED —Prevención del Delito a través del Diseño Ambiental— y sostiene algo tan simple como incómodo: la configuración física de un lugar influye, de forma medible, sobre la probabilidad y el miedo al delito. En 2021, la Organización Internacional de Normalización la elevó a estándar con la ISO 22341; en 2025 la especializó para entornos residenciales y de resguardo con la ISO 22341-2. El diseño dejó de ser decoración para convertirse en un control de seguridad auditable.

El fin del muro como única respuesta:

El paradigma tradicional es reactivo: rejas, cámaras y una fuerza que se activa cuando el incidente ya ocurrió. Funciona, pero llega tarde. Trata el síntoma —la fuga, el motín, la agresión— y desatiende su causa ambiental. La seguridad contemporánea propone lo contrario: intervenir la relación entre el entorno y la conducta antes de que el conflicto estalle. No se trata de vigilar más, sino de diseñar mejor.

Bajo esa lógica, el diseño se integra en una cadena de gestión del riesgo que va del gobierno de la institución, Enterprise Security Risk Management (ESRM) de ASIS International, a la evaluación de amenazas, de ahí al diseño y la protección, y termina en un ciclo de mejora continua que audita si el espacio realmente reduce los incidentes. Cada decisión queda trazada sobre normas ISO. Es seguridad que puede rendir cuentas.

> El contenedor detiene el cuerpo; el entorno modela la conducta.

Una ecuación incómoda:

Los especialistas lo resumen en una fórmula que parece técnica y es, en realidad, una advertencia. La vulnerabilidad de un centro crece con su exposición al riesgo y decrece con la eficacia de dos tipos de estrategia: las físicas (vigilancia natural, control de accesos, iluminación, territorio) y las sociales (cohesión, cultura, vínculo familiar, densidad habitable). La clave está en que ambas no se suman: se multiplican.

La consecuencia es contundente. Si una de las dos se acerca a cero, la seguridad se desploma aunque la otra sea máxima. Un perímetro impenetrable sobre un clima social degradado no produce orden: produce una olla a presión. Hacinamiento, subcultura carcelaria, violencia latente. Por eso invertir solo en acero es, literalmente, media solución.

> "Un perímetro impenetrable con un clima social degradado no produce seguridad: produce una olla a presión."

Imagen diseñada con Gemini IA

No es lo mismo un adulto que un cerebro en construcción:

Aquí aparece la distinción más delicada del oficio: una cárcel de adultos y un centro de menores no se diseñan igual. Y la diferencia no es de tamaño, sino de naturaleza. En el adulto, el entorno gestiona una conducta ya consolidada y prioriza la contención. En el menor, moldea trayectorias todavía abiertas.

La neurociencia lo respalda. El cerebro adolescente está en plena maduración de las áreas que gobiernan el impulso, el juicio y la emoción. Los entornos punitivos —gritos, aislamiento, ausencia de autonomía— activan respuestas de trauma y agravan el daño. Pero esa misma plasticidad que lo hace vulnerable lo hace también extraordinariamente receptivo: un espacio que estabiliza, regula y acompaña deja huella duradera. De ahí que el diseño para menores deba ser, por defecto, trauma-informado: luz natural, materiales cálidos, módulos pequeños, umbrales de confianza en lugar de esclusas, biofilia en lugar de neutralidad estéril.

En el centro de adultos, la gramática es otra: zonificación segregada, esclusas, contención geométrica, neutralidad cromática para impedir que pandillas marquen territorio, y una vigilancia tecnológica que cubra los puntos ciegos. Mismo objetivo último —la paz—, caminos arquitectónicos opuestos.

Continuará...

Liderazgo inclusivo:

Plan estratégico de Laura Alcas en ALAS Perú

Lima, Perú.- En un momento crucial para el sector de la seguridad en Perú, la Asociación Latinoamericana de Seguridad (ALAS) marca un diferenciador con la gestión de Laura Alcas, la primera mujer en asumir la presidencia del Comité de Perú en la historia de la organización. Cuenta con 17 años de trayectoria en la industria, es miembro de ASIS Internacional y aliada honoraria de la Asociación Nacional de Consultores en Seguridad Ciudadana Integral (ANCSCI). Propone un liderazgo fundamentado en la cooperación público-privada y un enfoque de gestión de riesgos integral que trasciende las fronteras tradicionales de la protección patrimonial.

Un comité integral y de "metro cuadrado"

En entrevista con **Más Seguridad Magazine**, Laura Alcas, destacó que ALAS es un "Comité de metro cuadrado", pues hay un carácter multidisciplinario y multinacional en su equipo de trabajo. Este Comité cuenta con la participación activa de especialistas chilenos y locales en vicepresidencias clave como transporte, infraestructura crítica, gobierno, capacitación y membresías. Esta diversidad busca consolidar una red de soporte técnico y comercial robusta para hacer frente a los desafíos del mercado peruano.

"La seguridad dentro del mercado corporativo viene a ser la continuidad operativa del negocio, es la promesa de atención al negocio, en el gobierno, es la promesa de crecimiento de una nación. La promesa es que sin seguridad no podemos crecer", afirmó la directiva, subrayando el papel que juega la asociación como puente entre la inversión privada y el desarrollo nacional.

Alcas anunció Mesa Estratégica Internacional

Como antesala al Encuentro Tecnológico programado para el mes de septiembre, ALAS Perú afinó los detalles de su próxima Mesa Estratégica. Este evento será de carácter abierto e internacional conectará a dos países en un entorno de aprendizaje mutuo, donde se expondrán casos de éxito y estrategias de profesionales que han revolucionado la gestión de la seguridad en América Latina. La convocatoria está extendida a socios actuales, antiguos miembros, profesionales independientes y participantes de otras asociaciones del sector.

El objetivo central de estas actividades es inspirar un impacto real tanto en las empresas privadas como en las entidades gubernamentales y las futuras autoridades que conducirán el país. Alcas enfatizó que la gestión de su comité no solo busca la representación de género, sino el fortalecimiento de la industria mediante capacidades intrínsecas de convocatoria y el sentido de protección natural de las mujeres, proyectado hacia el ámbito corporativo y técnico.

Alianzas transversales y metas de crecimiento

Con una base actual de más de 120 socios —que incluye a clientes finales, integradores y fabricantes corporativos con voz y voto en el país—, el Comité se ha fijado la ambiciosa meta de crecer un 100% durante este año. Para lograrlo, la estrategia se centrará en la inserción de profesionales y empresas de las distintas provincias de Perú, llevando la capacitación y el entrenamiento técnico fuera de Lima.

"Quiero conocer a mis socios, escucharlos y orientar la visión colectiva que tenemos de llevar conocimiento y entrenamiento fuera de Lima, de poder ser un puente de comunicación entre las soluciones tecnológicas y los usuarios finales que tanto necesitan la información y el respaldo al momento de impulsar una inversión que significa mucho para las compañías", aseveró Laura Alcas.

Para robustecer esta visión global, ALAS Perú busca sinergias con organizaciones complementarias. Un ejemplo de ello es el acercamiento con SINKY, entidad especializada en la prevención y mitigación de ataques con armamento químico o contaminación de efluentes, lo que añade una capa de especialización técnica indispensable para los planes de contingencia actuales.

Finalmente, con el propósito de democratizar el acceso a la red de networking, la asociación anunció un registro libre de costo para usuarios finales y una tarifa accesible de 280 dólares anuales para nuevos miembros, la cual contará con un descuento exclusivo del 10% al presentar la tarjeta de invitación del Comité. La visión es clara: escuchar la voz de cada socio, entender sus necesidades y consolidar un ecosistema de seguridad interconectado y con impacto social y económico en todo el territorio nacional.

Laura Alcas, Presidenta de ALAS Perú

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 1 de 2

Lima, Perú.- 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. Al principio pensé que era una casualidad. Pero en semanas ocurrió una vez y otra, y otra más. No se trataba de una sola persona. Era un patrón.

Lo más curioso era que los conductores no parecían distraídos en el sentido tradicional. No iban mirando el teléfono ni realizando maniobras peligrosas. Simplemente habían omitido una acción tan básica como encender las luces.

Entonces recordé que los vehículos modernos automatizan cada vez más funciones. Al mismo tiempo pensé en el propio cerebro humano, cuya naturaleza es ahorrar energía. Cuando una acción deja de requerir atención consciente y el entorno parece predecible, tendemos a delegarla en el piloto automático. Es eficiente, hasta que deja de serlo.

Y ahí aparece la pregunta que me viene dando vueltas hace varios días.

¿Estamos frente a simples descuidos o estamos observando una transformación más profunda en nuestra capacidad de atención?

De esa experiencia y de esa pregunta, nace este artículo.

Hasta ahora las organizaciones gestionan activos físicos, financieros, digitales, de información y humanos. Pero habrá alguna que gestione el activo que determina cómo se utilizan todos los anteriores? la atención. No me refiero a la atención entendida como concepto psicológico. Me refiero a la atención como un recurso estratégico.

Porque de ella depende la percepción del riesgo, la calidad del análisis, la capacidad para detectar anomalías, la comunicación, la creatividad, el liderazgo, la innovación y, sobre todo, la toma de decisiones.

En otras palabras, una organización funciona al nivel de atención de las personas que la integran. Y esa capacidad está siendo sometida a una presión sin precedentes.

Vivimos rodeados de notificaciones, interrupciones permanentes, múltiples pantallas, hiperconectividad, automatización creciente, exceso de información, jornadas prolongadas, fatiga y una constante sensación de urgencia. Nuestro cerebro cambia de estímulo una y otra vez hasta acostumbrarse a procesar información de manera superficial. Lo preocupante es que ese mismo cerebro debe, al día siguiente, conducir un vehículo, supervisar una planta industrial, investigar un fraude, monitorear un centro de control o dirigir un comité de crisis.

Y desde la seguridad corporativa, esto cambia completamente la conversación.

Durante décadas hablamos de error humano, negligencia o incumplimiento. Pero pienso que quizá estamos entrando en una nueva etapa. La del déficit de atención sostenida como riesgo organizacional.

No es solamente un conductor que olvidó encender las luces. Es un operador que omite un bloqueo crítico. Un vigilante que no detecta un comportamiento previo al delito. Un analista que pasa por alto una alerta importante. Un investigador que deja escapar una inconsistencia durante una entrevista. Un gerente que toma una decisión impulsiva después de 10 horas respondiendo mensajes.

Aunque los escenarios son distintos, el origen puede ser el mismo: Una atención fragmentada.

La ciencia lleva algunos años advirtiéndolo.

Continuará...

IA y Ciberseguridad:

Ejes de innovación que marcarán la ESS+ FERIA INTERNACIONAL DE SEGURIDAD

Bogotá, Colombia.- Con una trayectoria de 33 años consolidada como el principal punto de encuentro para la industria de safety and security en la región, la Feria Internacional de Seguridad ESS+, se prepara para su edición 2026, la cual se llevará a cabo del 26 al 28 de agosto en la capital colombiana. Bajo la dirección de Patricia Acosta, el encuentro abordará temas como la integración de tecnología, Inteligencia Artificial, analítica de datos, ciberseguridad, trabajo de tecnologías para infraestructuras críticas y para ciudades seguras.

La feria proyecta un crecimiento del 20% tanto en espacio de exhibición como en asistencia, impulsado por un panorama político regional que demanda una inversión sin precedentes en infraestructura de seguridad. La relevancia del evento y del sector es tal que se espera sea Carlos Fernando Galán, alcalde de Bogotá quien inaugure oficialmente el evento. “Se espera tener al alcalde de Bogotá, porque el sector es prioritario para los alcaldes y gobernadores. De manera que vamos a tener una feria muy movida, donde vamos a mostrar todas las soluciones de primera mano con pantallas interactivas, que van ubicar las soluciones en los sitios y las aplicaciones adecuadas. Es una feria muy tecnológica, muy visitada de América Latina”, señaló Patricia Acosta.

Indicó que se está apostando a las ciudades capitales, a los alcaldes y Ministros de seguridad de las ciudades capitales, de las metrópolis intermedias, no solo de Colombia, sino de la región andina y el Caribe. “Tenemos mucha gente de gobierno porque se vienen cambios importantes, políticos en todos los países, entonces eso genera inversión y desarrollo tecnológico”.

A la feria acudirán expositores que han participado desde hace 32 años, y para la edición 2026 se sumarán más, incrementando la cifra de participación en 20%. Este año además, ESS+ expande su alcance global con la incorporación de delegaciones comerciales de Turquía e India, que se suman a los 23 países que ya participan, como México, Suecia, Argentina, Francia, Italia, Brasil, Perú, Estados Unidos, Corea del Sur y China.

Se prevé la asistencia de más de 19 mil personas, lo que representaría un 20% más vs 2025. Con respecto a la infraestructura, la feria contará con 250 stands y debido a que hay marcas que integran su tecnología con otras (alianza y co-exhibición), se espera la presencia de hasta 400 marcas.

De acuerdo con el comité organizador, las novedades para esta edición girarán en torno a la integración de tecnologías, analítica de datos, ciberseguridad avanzada, trabajo de tecnologías para infraestructuras críticas, ciudades seguras e Inteligencia Artificial.

La feria contará con un gran número de eventos académicos donde se abordarán cuestiones relacionadas con la IA, el Foro Central de la Feria de Pensamiento Estratégico o el de Seguridad y Riesgos, entre otros. “Es el momento de conocer de primera mano todos estos cambios que nos ha traído la Inteligencia Artificial, vamos a tener un tema muy fuerte en este rubro, entonces hay qué ir, conocer, preguntar, hay qué escucharnos, hay qué hablar, son tres días intensos”.

La jornada formativa y de negocios estará a cargo de las asociaciones de mayor peso en el continente como ALAS, ASIS, COLADCA, pues más allá de la muestra comercial, ESS+ 2026 se ratifica como el espacio donde los gremios de la región se reúnen para dialogar sobre aciertos y retos comunes.

Por último, Patricia Acosta indicó que el registro ya está abierto y se puede hacer a través de la página www.securityfaircolombia.com

Patricia Acosta, directora de ESS+

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.

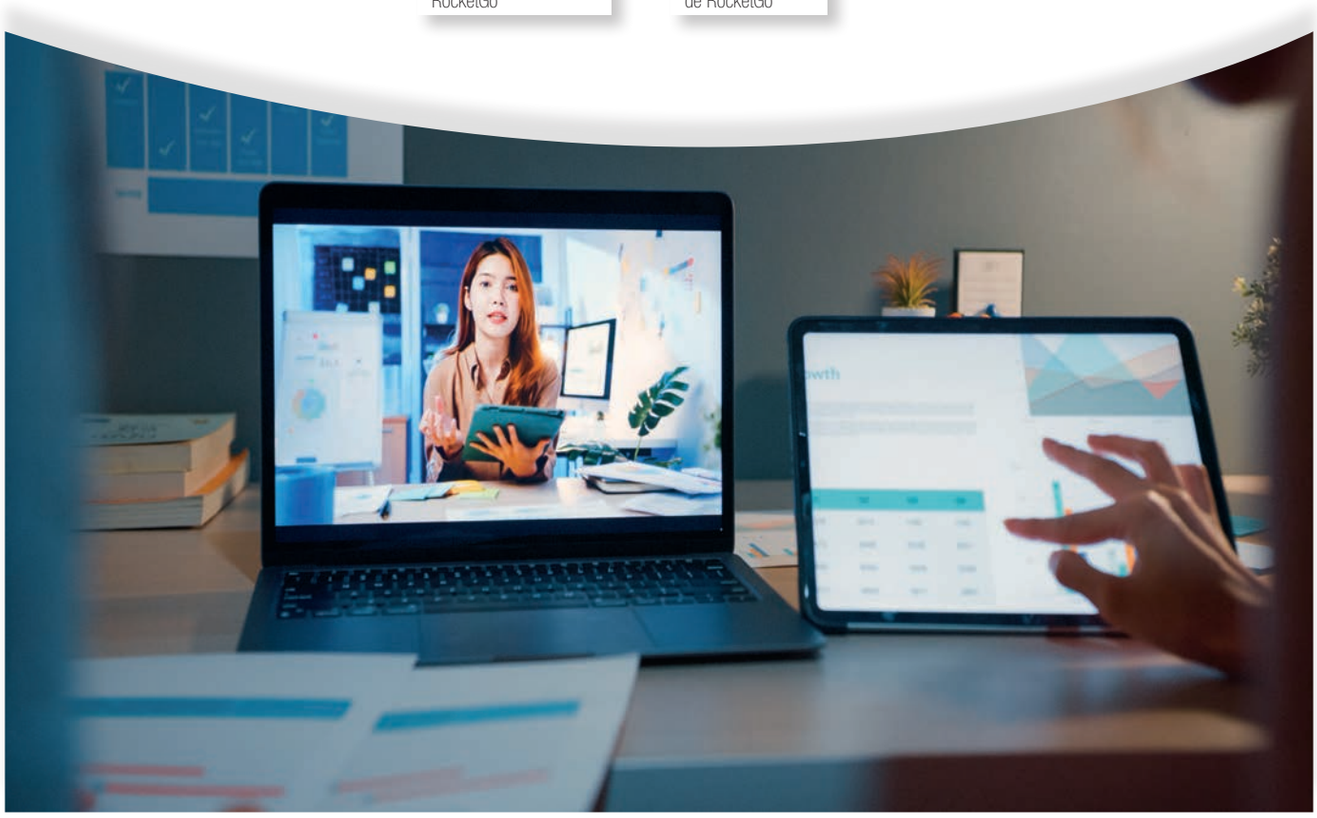
RocketGO no es solamente una plataforma de cursos. Es un ecosistema educativo diseñado para transformar conocimiento en acción, conectar personas con oportunidades y preparar a las organizaciones para los desafíos del presente y del futuro.

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



Extorsión empresarial en América Latina

cuando pagar para trabajar se convierte en normalidad

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

"La injusticia en cualquier parte es una amenaza a la justicia en todas partes"
Martin Luther King Jr.

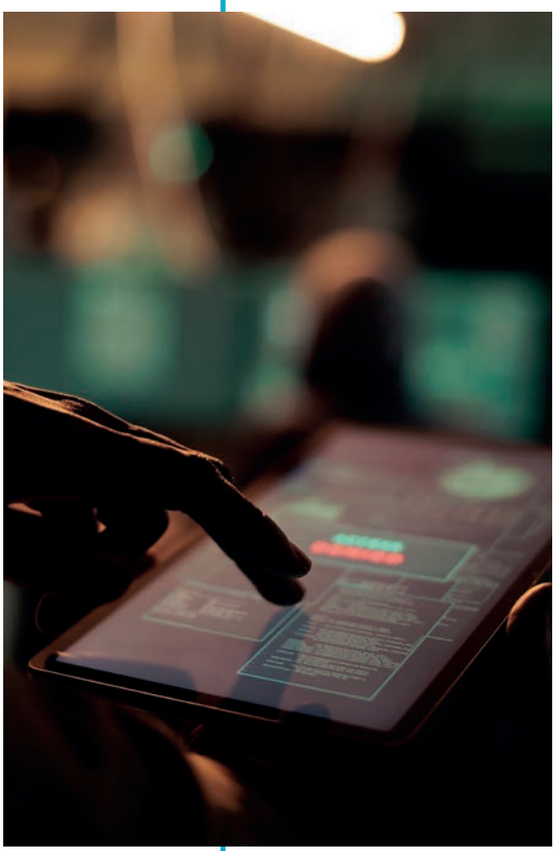
Quito, Ecuador.- En América Latina, miles de pequeños comerciantes, transportistas, emprendedores, distribuidores, agricultores, operadores logísticos y empresarios medianos han empezado a tomar decisiones que no nacen del mercado, sino del miedo. No deciden solamente cuánto vender, a qué precio competir o qué ruta utilizar. Muchas veces deciden si abren o no el negocio, si pagan para seguir operando, si denuncian o callan, si cambian de ciudad o si aceptan que una estructura criminal se convierta en un costo más de funcionamiento.

Ese es el punto más grave de la extorsión empresarial: cuando deja de ser un hecho aislado y comienza a normalizarse como parte del entorno económico.

La extorsión no es nueva en la región ha mutado cambiando en su profundidad, su frecuencia y su capacidad de adaptación. En algunos territorios se presenta como "protección"; en otros, como "vacuna", "cuota", "colaboración", "permiso para trabajar" o "peaje informal". Cambia el nombre, pero no la esencia: una persona o una empresa paga bajo amenaza para evitar daño contra su vida, su familia, su local, sus trabajadores, su transporte, su mercadería o su reputación.

La UNODC describe la extorsión organizada como una dinámica en la cual víctimas pagan a grupos criminales para evitar daños continuados o supuestas amenazas de terceros. En términos simples, el delincuente ya no solo roba: administra el miedo, regula la actividad económica y convierte la amenaza en renta permanente.

El problema, entonces, ya no puede analizarse únicamente como delito patrimonial, se ha convertido en un mecanismo de control territorial, presión social, captura económica y gobernanza criminal. El negocio no solo pierde dinero; pierde autonomía. El propietario no solo enfrenta una amenaza; empieza a tomar decisiones condicionado por actores que no aparecen en la escritura de la empresa, pero que influyen en su operación diaria.



La región ofrece señales suficientes para entender la magnitud del fenómeno. El Banco Interamericano de Desarrollo estimó que los costos directos del crimen y la violencia en América Latina y el Caribe alcanzaron el 3,44% del PIB regional en 2022. Ese costo incluye pérdida de capital humano, gasto público en prevención y justicia, y gasto de mitigación asumido por empresas; de hecho, el BID señala que el gasto privado de las empresas representó el 47% del costo total del crimen en la región.

Este dato debería preocupar al mundo empresarial. No se trata solo de inseguridad en la calle. Se trata de una transferencia constante de recursos desde la productividad hacia la defensa, desde la inversión hacia la supervivencia, desde la innovación hacia la autoprotección. Cada dólar destinado a resistir amenazas es un dólar que deja de invertirse en empleo, tecnología, expansión, capacitación o formalización.

La Global Initiative Against Transnational Organized Crime advierte que los actores privados cumplen un papel cada vez más relevante en las economías ilícitas, especialmente como facilitadores en logística, finanzas y tecnología. Esa observación es clave porque permite entender que el crimen organizado contemporáneo no vive únicamente en la marginalidad; también busca conectarse con sectores formales, cadenas comerciales, proveedores, transporte, financiamiento, bienes raíces y servicios profesionales.

Ahí aparece una frontera peligrosa. El empresario honesto compite con reglas, tributos, obligaciones laborales, permisos y controles. Pero puede terminar compartiendo mercado con negocios financiados

por dinero ilícito, estructuras de fachada, proveedores impuestos o capitales que no buscan rentabilidad normal, sino blanqueamiento, influencia o dominio territorial. No es que la economía ilegal se vuelva legal por sí sola; lo grave es que puede adquirir apariencia de legalidad cuando los controles son débiles, la informalidad es alta, la corrupción abre puertas y el miedo reduce la denuncia.

La extorsión empresarial también tiene una dimensión humana que no siempre se mide. Detrás de cada denuncia hay una familia que duerme mal, un administrador que mira dos veces antes de abrir la puerta, un transportista que cambia rutas, un cajero que teme ser identificado, un trabajador que evita quedarse hasta tarde y un emprendedor que empieza a preguntarse si vale la pena seguir.

Cuando una empresa paga bajo amenaza, el daño no termina en el flujo de caja, altera la cultura organizacional. Se debilita la confianza. Se deteriora la relación con la comunidad. Se instala la idea de que operar depende menos de la ley y más de la tolerancia del grupo que controla la zona.

El crimen organizado en América Latina tampoco actúa de manera aislada. La UNODC ha señalado que el estudio global de homicidios incluye un análisis específico sobre cómo el crimen organizado incide en las dinámicas homicidas de América Latina y el Caribe. Esa relación entre violencia letal, control territorial y economías ilícitas explica por qué la extorsión no puede ser tratada como una simple llamada amenazante o una denuncia individual. Forma parte de ecosistemas criminales más amplios.

Por eso, la respuesta empresarial debe evolucionar. No basta con colocar cámaras, contratar vigilancia o cerrar más temprano. Esas medidas son insuficientes si no se integran con inteligencia corporativa, análisis territorial, debida diligencia, protección de personas clave, gestión de crisis, continuidad operacional, canales seguros de denuncia y coordinación institucional.

Una empresa que opera en zonas de riesgo necesita saber quién controla el territorio, cómo se mueven las amenazas, qué rutas son vulnerables, qué proveedores presentan señales de alerta, qué empleados están más expuestos, qué información sensible se está filtrando y qué decisiones pueden aumentar o reducir la exposición. La seguridad deja de ser un asunto periférico y se convierte en parte de la gobernanza del negocio.

También es necesario decirlo con claridad: pagar puede parecer una solución inmediata, pero muchas veces inaugura una relación de dependencia. La primera cuota puede comprar tiempo; difícilmente compra libertad. Una vez que el grupo criminal confirma que la empresa puede pagar, el negocio deja de ser una víctima ocasional y se convierte en una fuente recurrente de renta.

El desafío actual es impedir que la extorsión se convierta en una forma aceptada de relación económica. Cuando se empieza a decir “así se trabaja aquí”, la amenaza ya dejó de estar afuera: entró en la cultura.

La región necesita liderazgos empresariales capaces de comprender que la seguridad no es un gasto ornamental, sino una condición para competir, invertir y sostener empleo. La extorsión empresarial en América Latina no solo ataca negocios. Ataca la libertad de producir, transportar, contratar, vender y crecer sin permiso criminal.

Y cuando una sociedad acepta que para trabajar hay que pagarle al miedo, no solo pierde seguridad. Pierde futuro.

Referencia

Banco Interamericano de Desarrollo. (2024). High crime costs burden Latin America and the Caribbean. Banco Interamericano de Desarrollo.

Global Initiative Against Transnational Organized Crime. (2025). The Global Organized Crime Index 2025. GI-TOC.

United Nations Office on Drugs and Crime. (s. f.). Extortion racketeering. Education for Justice.

United Nations Office on Drugs and Crime. (2023). Global Study on Homicide 2023. UNODC.

Pedro Oré
Miembro del Consejo Consultivo Latino de IFPO por Perú.
Máster of Business Administration.
Máster en Gestión y Dirección de Equipos.
Licenciado en Administración de Negocios Internacionales.
Certified Protection Officer COP©. Certified Investigations Officer CIO©.
Oficial de Mar de la Marina de Guerra del Perú en retiro.
Coach Ontológico.
Perú
Articulista Invitado

La anatomía de la resistencia

Lima, Perú.- Toda norma de seguridad muere dos veces. La primera vez muere cuando se escribe, porque en el momento exacto en que una idea se convierte en artículo numerado y pierde el pulso de lo que la originó. La segunda vez muere cuando se cumple sin haber convencido a nadie, que es la muerte más recurrente de las dos, porque hacia afuera parece vida y hacia adentro es absolutamente inerte.

Esa segunda muerte es el verdadero objeto de este texto, la presentación de la resistencia, esa fuerza que no aparece en ningún tablero de indicadores porque no se opone a la norma, se opone al gesto de habérsela impuesto sin preguntar, y como no deja rastro medible, la tratamos como ausencia de cultura, cuando en realidad es la cultura más antigua de todas funcionando exactamente como fue entrenada, en la desconfianza de quien dice cuidar mientras controla.

Ningún colaborador nace resistente a una norma de seguridad, se vuelve resistente, y se vuelve resistente porque en algún punto de su historia laboral, no necesariamente en esta empresa, quizás en ninguna que pueda nombrar, aprendió que “por tu bien” y “para que yo no tenga un problema” suenan exactamente igual, aunque signifiquen cosas opuestas. Una vez que el oído aprendió a no distinguir esas dos frases, cualquier norma nueva llega ya sospechada, sin que el mensaje haya tenido oportunidad de defenderse.

Aquí es donde el sector completo comete el mismo error de cálculo, mide su éxito en cumplimiento, cuando el cumplimiento es la cáscara, no la fruta. El compliance perfecto convive, sin ninguna contradicción interna, con una cultura completamente hueca. Ese es el hallazgo que nadie quiere poner en un informe, se puede ganar el indicador y perder por completo a la persona. Esto se vuelve todavía más filoso cuando la conversación gira hacia la transformación digital de la prevención de riesgos, todo empujando deliberadamente lejos del modelo antiguo. La resistencia que aparece ahí casi nunca es técnica, es la sospecha legítima de que toda esta modernización disfrazada de progreso en realidad busca reemplazar la confianza por la vigilancia con mejor marketing.

Existe una versión de la prevención de riesgos que puede mostrar, con total honestidad estadística, una reducción sostenida de la accidentabilidad, y estar hablando de dos fenómenos completamente distintos según qué la haya producido. Una reducción lograda a fuerza de sanción y vigilancia es un número real que describe una cultura frágil, basta con que baje la presión o se relaje el control para que el indicador se revierta, porque nunca hubo nada sostenido más abajo de la superficie.

La gestión del talento y la gestión del riesgo, que durante décadas se enseñaron como disciplinas paralelas con áreas distintas, resultan ser, mirado de cerca, exactamente la misma disciplina disfrazada, un colaborador que se siente escuchado en su desarrollo profesional es, casi sin excepción medible, el mismo colaborador que va a reportar un riesgo antes de que se convierta en accidente.

La resistencia, entonces, nunca fue el enemigo, es el diagnóstico más honesto que una organización puede recibir sobre todo lo que todavía no aprendió a traducir.

SEGURIDADEXPO®

08 al 10 de septiembre | METROPOLITAN SANTIAGO

Estamos buscando a las marcas que lideran la seguridad en Latinoamérica

¿ES TU EMPRESA UNA DE ELLAS?

¡Únete a los **líderes del sector** que ya confirmaron su participación!

- Oportunidades de **networking y alianzas estratégicas** en un entorno propicio para el crecimiento.
- **Visibilidad internacional:** Participa en la feria líder en seguridad en Chile, con proyección en toda Latinoamérica.
- **+8.800** tomadores de decisión y profesionales calificados en la versión 2025.
- **35% más espacios** para que puedas mostrar tus soluciones en un **evento internacional consolidado.**

www.seguridadexpo.cl

INVITA MOTOROLA SOLUTIONS

AUSPICIA GRUPO SAFETECK

PATROCINA

ORGANIZA Fisa

COORGANIZA

La nueva geografía del riesgo
en América Latina

Edgardo C. Glavinich
Es Director Ejecutivo de la Fundación Sherman Kent. Consultor en inteligencia estratégica, riesgos complejos y análisis prospectivo para los sectores público y privado. Linkedin.com/in/edgardoglavinich
Argentina
Articulista Invitado

Por qué operar en la región ya es, sobre todo, un problema de inteligencia.
El crimen organizado dejó de ser un asunto de seguridad para convertirse en una variable estructural del negocio. En el año del súper-ciclo electoral, la empresa que opera en varios países ya no compite contra la incertidumbre, compite contra quien la anticipa mejor.

Buenos Aires, Argentina.- Hay un cambio en América Latina que los balances todavía no terminan de registrar, pero que ya define resultados. El riesgo que más condiciona la operación de una empresa en la región dejó de ser macroeconómico (inflación, tipo de cambio, tasa) y pasó a ser de otra naturaleza; la expansión de economías criminales con capacidad de intervenir mercados, capturar instituciones y reescribir, de un año al otro, el mapa de seguridad de un país entero. No es un problema de orden público que ocurre en paralelo al negocio. Es una variable que entra directamente en la ecuación de continuidad, costos y reputación de cualquier compañía con activos en el territorio.

El informe de Riesgo Político 2026 del Centro de Estudios Internacionales de la Universidad Católica de Chile lo formula sin matices: “el crimen organizado y la captura del Estado encabezan la lista de riesgos de la región, por encima de cualquier variable económica tradicional”. Y lo hacen en un año particularmente sensible en cuatro países, Costa Rica, Colombia, Perú y Brasil, donde se celebrarán elecciones generales, en un clima de volatilidad institucional y violencia política creciente. Para quien dirige una operación regional, la pregunta ya no es si el entorno se va a complicar, sino dónde, cuándo y con qué velocidad.

Un riesgo que cambió de naturaleza

Conviene precisar por qué esto es distinto de lo que la región conoció durante décadas. La economía criminal latinoamericana dejó de ser un fenómeno marginal y externo a los mercados legales para integrarse en ellos. Ya no se limita al narcotráfico, abarcando la minería ilegal, el contrabando, la extorsión sistémica, el lavado de activos y los procesos de corrupción que enlaza puertos, logística y financiamiento. El dato que mejor sintetiza el giro proviene de Perú, donde las ganancias del oro ilegal superan hoy a las del narcotráfico; en Ecuador y Venezuela la minería aurífera ilícita financia estructuras armadas, y los puertos de la región se consolidaron como nodos de exportación de cocaína convertida, vía documentación falsa, en commodities aparentemente legales.

La magnitud humana del fenómeno enmarca la económica. Según el Estudio Global sobre Homicidios de la UNODC, América Latina concentra cerca de un tercio de los homicidios del planeta con apenas alrededor del 8 % de la población mundial, y en el continente americano la mitad de esos homicidios está vinculada al crimen organizado, frente a un promedio global del 24%. Donde la violencia alcanza esa densidad, no existe operación empresarial que quede aislada de ella, afecta cadenas de suministro, costos de seguridad, decisiones de localización, contratación y permanencia del talento.

La economía criminal dejó de correr en paralelo a los mercados legales para integrarse en ellos.

La geografía se volvió heterogénea y veloz

El rasgo más exigente para el análisis es que el riesgo dejó de ser homogéneo y estable. Hoy es heterogéneo entre países y, sobre todo, veloz dentro de cada uno. El caso de Ecuador es la advertencia más clara de la década. De un país considerado de los más seguros de la región hasta hace pocos años cerró 2025 como el más violento de su historia, con mas de 9.000 homicidios, un promedio de 25 por día, y una tasa cercana a 50,9 por cada 100 mil habitantes, la más alta de América Latina según ACLED. La provincia de Guayas, con Guayaquil como epicentro económico y portuario, concentró el grueso de esa violencia. Ninguna planificación de seguridad estática habría anticipado esa curva; solo un seguimiento prospectivo de la disputa territorial entre organizaciones criminales podía hacerlo.

A ese cuadro se suman dinámicas divergentes que conviven en el mismo entorno regional. La consolidación de estructuras criminales con control penitenciario y corredores logísticos en Brasil, la incertidumbre electoral en Colombia y Perú, la presión de la extorsión sobre el tejido empresarial en México y Centroamérica. Para una compañía que opera en seis o siete jurisdicciones, esto significa que no enfrenta un riesgo, sino una cartera de riesgos distintos, que se mueven a velocidades distintas y que la gestión país por país, reactiva y desconectada, no alcanza a leer a tiempo.

Por qué la seguridad tradicional no captura este riesgo

La función de seguridad corporativa fue diseñada para proteger activos como instalaciones, personas, perímetros, o incorporando ciberseguridad. Es necesaria, pero opera sobre lo que ya ocurre o está por ocurrir en un lugar determinado. El riesgo que define hoy la continuidad de un negocio regional vive en otro plano; en el entorno político,

en la evolución de las economías ilícitas, en la captura institucional, en la cadena de proveedores, en el calendario electoral. Ese riesgo no se neutraliza con más dispositivos; se gestiona con conocimiento anticipado. Y producir ese conocimiento de manera rigurosa es, técnicamente, una función de inteligencia, no de vigilancia.

Vale despejar el equívoco que suele frenar la conversación. En el ámbito privado, "inteligencia" todavía evoca, para muchos directivos, espionaje o métodos opacos. Es una confusión costosa. La inteligencia estratégica corporativa o inteligencia competitiva trabaja sobre fuentes abiertas y legalmente disponibles (registros públicos, expedientes, prensa especializada, datos comerciales, redes profesionales, etc.), que concentran la mayor parte de la información estratégicamente relevante. Su valor no está en acceder a lo secreto, sino en una disciplina analítica de transformar información dispersa en juicios útiles y, sobre todo, separar de manera explícita lo que se sabe, de lo que se infiere y de lo que se supone. Esa distinción, que la tradición analítica heredó de Sherman Kent, es lo que permite a un directorio saber con qué grado de certeza está decidiendo.

Qué hace un sistema de inteligencia regional

Llevado a la práctica, un sistema de inteligencia estratégica al servicio de una operación regional entrega cuatro cosas que la seguridad tradicional no produce. Primero, un mapa de riesgo vivo y comparable entre jurisdicciones, que no se actualiza cuando estalla la crisis, sino de manera continua. Segundo, análisis prospectivo anclado en los puntos de inflexión conocidos, el calendario electoral, las disputas territoriales en curso, los cambios regulatorios en gestación, de modo que la organización razone en escenarios y no en reacciones. Tercero, alerta temprana sobre los desplazamientos de la gobernanza criminal y la captura de eslabones de la cadena de valor, que son los que con más frecuencia sorprenden a las empresas. Y cuarto, una lectura del entorno depurada de sesgos, que distingue el hecho verificado, de la versión interesada, en una región donde la desinformación también es una herramienta de presión competitiva.

La asimetría que esto genera es real y medible en resultados. Las multinacionales que ya operan con células de inteligencia regional toman decisiones de inversión, localización y relación institucional con un margen de anticipación del que carecen las compañías que siguen gestionando el riesgo país por país, a partir de noticias y de la experiencia del gerente local. En igualdad de condiciones operativas, gana el que ve antes. Y en un entorno que se mueve a la velocidad del ecuatoriano, ver antes puede ser la diferencia entre ajustar a tiempo o asumir una pérdida que ya no tiene cobertura.

Una compañía regional no enfrenta un riesgo, sino una cartera de riesgos que se mueven a velocidades distintas.

El año que viene, leído hoy

El súper-ciclo electoral 2026-2027 ofrece una experiencia sobre por qué la anticipación dejó de ser un lujo. Las elecciones generales en Brasil, Colombia, Perú y Costa Rica no son solo eventos políticos, son momentos de redistribución del poder en los que la violencia asociada a los comicios, la incertidumbre regulatoria y la disputa por rentas legales e ilegales se intensifican simultáneamente. Una empresa que recién ajuste su postura cuando se conozcan los resultados llegará tarde; otra que haya modelado los escenarios con 12 meses de margen podrá decidir con criterio dónde acelerar, dónde esperar y dónde protegerse. La diferencia no la marcará el tamaño del presupuesto de seguridad, sino la calidad del análisis disponible cuando había que decidir.

Una conclusión de gestión

La transformación del riesgo en América Latina no admite ya una respuesta puramente defensiva. El crimen organizado se profesionalizó, leyó los mercados y aprendió a operar dentro de la economía legal; las instituciones, en muchos casos, quedaron por detrás. En ese contexto, la ventaja competitiva sostenible para quien invierte en la región no será tener el perímetro mejor protegido, sino el mejor entendimiento del terreno antes de pisarlo y a medida que cambia. La inteligencia estratégica dejó de ser una capacidad reservada a los Estados para volverse un instrumento de dirección empresarial. Las compañías que lo incorporen a tiempo no solo reducirán su exposición, estarán mejor posicionadas para capturar las oportunidades que toda incertidumbre, invariablemente, abre para quien la entiende antes que los demás. Esa, y no otra, es la decisión estratégica que la región le está planteando hoy a quien la quiera entender.

IBEROSEC:

certificación que busca elevar el estándar profesional de la seguridad y las emergencias en Iberoamérica

Francisco Javier González Fuentes

Presidente de FIBSEM – Foro Iberoamericano de Seguridad y Emergencias

España

Articulista Invitado

Madrid, España.- La seguridad y las emergencias atraviesan una etapa de profunda transformación. Las organizaciones enfrentan riesgos cada vez más complejos: amenazas híbridas, ciberataques, delincuencia organizada, crisis reputacionales, protección de infraestructuras críticas, continuidad de negocio y fenómenos naturales que obligan a reforzar las capacidades de respuesta.

En este escenario, el factor humano continúa siendo el elemento más importante. La tecnología es una herramienta imprescindible, pero son las personas quienes toman decisiones, gestionan crisis, coordinan recursos y protegen activos estratégicos. Por ello, la profesionalización de quienes trabajan en seguridad y emergencias se ha convertido en una necesidad prioritaria para empresas, instituciones y gobiernos.

Con esta visión nace IBEROSEC Certificación, una iniciativa impulsada por el Foro Iberoamericano de Seguridad y Emergencias (FIBSEM) y avalada por Bureau Veritas Certification, cuyo objetivo es establecer un estándar común de reconocimiento profesional para los especialistas del sector en Iberoamérica.

La necesidad de acreditar competencias reales

Uno de los principales desafíos del sector es la diversidad de perfiles profesionales existentes. En muchos casos encontramos especialistas con amplia experiencia operativa, formación técnica de alto nivel y responsabilidades estratégicas, pero sin mecanismos homogéneos que permitan acreditar objetivamente sus competencias.

La certificación profesional surge precisamente para responder a esta necesidad. Ya no basta con disponer de un currículo o acreditar años de experiencia, las organizaciones demandan profesionales capaces de demostrar conocimientos, habilidades y capacidades alineadas con los nuevos escenarios de riesgo.

IBEROSEC apuesta por un modelo que integra experiencia, formación y evaluación, permitiendo que el profesional pueda acreditar de forma objetiva su nivel de competencia en áreas específicas de la seguridad y las emergencias.

Un estándar pensado para Iberoamérica

La región iberoamericana comparte numerosos desafíos en materia de seguridad. Desde México hasta Argentina, pasando por Centroamérica, el Caribe, España y Portugal, existen problemáticas comunes relacionadas con la protección de personas, infraestructuras, información y continuidad de las operaciones.

Sin embargo, también existe una realidad particular: modelos normativos diferentes, estructuras organizativas diversas y necesidades operativas específicas que requieren una visión adaptada al contexto regional.

IBEROSEC nace precisamente con esa vocación. No pretende sustituir estándares internacionales, sino complementarlos mediante un modelo que reconozca la realidad profesional iberoamericana y facilite el desarrollo de una comunidad de especialistas con criterios comunes de excelencia.

México: un referente estratégico para la seguridad regional

El país ocupa una posición especialmente relevante dentro de este proyecto. Cuenta con uno de los ecosistemas profesionales más desarrollados de América Latina en materia de seguridad corporativa, protección ejecutiva, gestión de riesgos, inteligencia corporativa, ciberseguridad y protección civil.

Además, la creciente participación de empresas mexicanas en mercados internacionales ha incrementado la necesidad de disponer de profesionales certificados y capaces de operar bajo estándares reconocidos.

La certificación profesional se convierte así en una herramienta que aporta valor tanto al especialista como a las organizaciones que requieren talento altamente cualificado para gestionar riesgos cada vez más complejos.

Áreas estratégicas de certificación

IBEROSEC estructura su modelo en torno a las disciplinas que actualmente marcan la evolución del sector:

- Seguridad Corporativa.
- Seguridad Integral.
- Inteligencia Corporativa.
- Prevención de Riesgos.
- Protección Contra Incendios.
- Gestión de Emergencias.
- Ciberseguridad.

Estas áreas reflejan una realidad evidente: la seguridad moderna exige una visión multidisciplinaria. Las amenazas ya no pueden abordarse desde compartimentos estancos. La protección física, la inteligencia, la continuidad de negocio y la seguridad digital forman parte de una misma estrategia de resiliencia organizacional.

El valor de la confianza

Uno de los elementos diferenciales del modelo es el respaldo de Bureau Veritas Certificación, organización internacionalmente reconocida por sus procesos de certificación y evaluación.

Este aval aporta confianza, transparencia y rigor al proceso, permitiendo que la acreditación profesional tenga un reconocimiento sustentado en criterios verificables y metodologías de evaluación contrastadas.

Para los profesionales supone una oportunidad de fortalecer su posicionamiento en el mercado. Para las organizaciones, representa una referencia objetiva a la hora de identificar talento especializado.

Hacia una cultura de excelencia profesional

La evolución de los riesgos obliga a evolucionar también a los profesionales encargados de gestionarlos. La formación continua, la actualización permanente y la acreditación de competencias serán cada vez más importantes para garantizar la capacidad de respuesta de organizaciones e instituciones.

IBEROSEC representa una apuesta por esa cultura de excelencia profesional. Un modelo concebido para reconocer el conocimiento, valorar la experiencia y contribuir a la construcción de una comunidad iberoamericana de especialistas comprometidos con la mejora continua.

En un entorno donde la confianza se ha convertido en un activo estratégico, certificar competencias ya no es una opción diferencial. Es una herramienta necesaria para afrontar con garantías los desafíos de la seguridad y las emergencias del siglo XXI.

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

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

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

www.alas-la.org

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!

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