

Aeropuertos: tecnología y operación



Edición 6 / Año 1
Agosto-septiembre 2026



Precio \$3.00 USD





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



Conozca más información aquí
o en securityfaircolombia.com



Para ampliar información, modificaciones/actualizaciones y ver términos y condiciones de la feria consulte securityfaircolombia.com.

Organizado por: PAFYC y Corporación de Ferias y Exposiciones S.A - NIT 860.002.464-3 - Cra. 37 # 24-67 Bogotá

Aeropuertos bajo presión en seguridad, tecnología y operación

El sistema aeroportuario mundial está cambiando rápidamente de ser una infraestructura estratégica y estable para considerar una variable que lo empuja: volumen. En 2024, el tráfico aéreo global superó los 9.5 mil millones de pasajeros, de acuerdo con el Airports Council International. América Latina crece a un ritmo similar, aunque con una base tecnológica y operativa que no siempre acompaña esa expansión. Ese desbalance coloca a la seguridad como el centro estratégico como condición que permite que el sistema funcione. Es decir, si falla, no hay operación.

América Latina enfrenta ese reto en un momento particularmente exigente y complejo. El aumento del tráfico, la presión logística y la expectativa de eventos internacionales, como el reciente Mundial de 2026, obligaron a replantear cómo se protegen infraestructuras que concentran miles de personas por hora, cientos de operaciones simultáneas y riesgos que evolucionan con rapidez.

Durante años, la seguridad aeroportuaria operó con sistemas independientes: cámaras, controles de acceso, filtros de inspección y monitoreo perimetral funcionaban de forma paralela. Hoy se habla de plataformas integrales que cubren desde el lado aire hasta el lado tierra. Se conjugan controles de acceso y perimetrales, videovigilancia y seguridad física, entre otros.



El cambio tecnológico implica que los sistemas, además de registrar eventos, ahora los conectan. Lo que ocurre en una terminal puede vincularse con movimientos en pista, accesos, equipaje o transporte interno. Esa trazabilidad permite reconstruir situaciones completas, no solo fragmentos.

La evolución de la inspección aeroportuaria también ha redefinido la relación entre operador y sistema. La decisión ya no ocurre únicamente en el punto físico de revisión, sino que existe una segunda validación remota que reduce errores humanos, genera evidencia y fortalece procesos de

auditoría interna. Para aeropuertos con alta afluencia, esta duplicidad de control comienza a operar como estándar y no como algo excepcional.

La seguridad aeroportuaria tiene un punto crítico: los filtros de inspección. Ahí convergen dos exigencias que con dificultad suelen alinearse con facilidad: velocidad y control. Y es que el acceso a tecnologías avanzadas ha cambiado el estándar, o sea, equipos de rayos X con Inteligencia Artificial, escáneres corporales por ondas milimétricas y sistemas de detección no intrusiva, permiten inspeccionar sin contacto físico, reducir tiempos y mejorar la precisión.

En el plano operativo, la seguridad aeroportuaria enfrenta un dilema más allá de lo solamente técnico, y se refiere a lo organizacional. Con ello, el responsable de la seguridad en el aeropuerto marca un límite operativo que, en la práctica, tiene implicaciones económicas. Cada refuerzo en inspección implica retrasos, cada incremento en controles afecta la experiencia del pasajero. La decisión de priorizar seguridad sobre flujo no es neutra, antes bien impacta tiempos, costos y percepción del servicio. Por eso, en escenarios de alta amenaza, ese equilibrio pasa de ser de tipo técnico y se convierte en una decisión estratégica. 🌐

DIRECCIÓN GENERAL

HUMBERTO MEJÍA, DSE, CPSI, CIEIE
Norteamérica / España
hmejia@conseguridad.com

ALFREDO YUNCOZA, CSSM, CPOI, CPO
Centro/Sudamérica
ayuncoza@conseguridad.com

DIRECCIÓN COMERCIAL

MARÍA ANTONIETA JUÁREZ CARREÑO
marieclaire@conseguridad.com

COORDINACIÓN EDITORIAL

BEATRIZ CANALES HERNÁNDEZ
edicion@conseguridad.com

COORDINACIÓN DISEÑO

DG CREATIVE
dgcreative@gmail.com

MARKETING LATAM

SARA LUCÍA MEJÍA CASTRO
negocios@conseguridad.com

CORRESPONSAL ESPAÑA

CARMEN CHAMORRO
corresponsal@conseguridad.com

ADMINISTRACIÓN Y CONTABILIDAD

Virginia Herrera Montiel
contabilidad@conseguridad.com

CONTACTO

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

Con Seguridad Año 1, No 6, agosto - septiembre 2026, Publicación Bimestral 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 5518447067. Editor responsable: **Humberto Mejía Hernández**. Certificado de Reserva 04-2022-050614181900102 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,

Contenido

- 7 Tres pasos para llevar el control de acceso físico al nivel de la era digital
- 10 Ajax Systems fortalece presencia en México con Muñoz Solutions como nuevo subdistribuidor autorizado
- 12 Milestone Systems revoluciona videovigilancia mediante IA aplicada

14 Aeropuertos bajo presión en seguridad, tecnología y operación

- 22 Lumu lanza Threat Observatory
- 32 Hardtech Solutions impulsa la transición a Smart Cities en Perú
- 34 El enfoque real de la Seguridad Ciudadana: Reto de ANCSCI

36 RocketGo educación que potencia conocimientos



+ +

¡Únetenos!

.
.

CON SEGURIDAD
Magazine Latam

Síguenos en
Telegram e Instagram

@conseguridadmagazine

+ +

Profesional del mes

KEVIN PALACIOS
Ecuador



Profesional de seguridad corporativa, protección ejecutiva y gestión de riesgos con una trayectoria internacional centrada en la profesionalización de la industria, formación especializada y aplicación de estándares globales a contextos operativos reales.

Actualmente se desempeña como CEO de HELPS Latam, organización especializada en servicios de protección ejecutiva, transporte seguro, inteligencia protectiva, investigaciones privadas, gestión de riesgos y apoyo en crisis para la región latinoamericana.

Con más de 25 años de experiencia ha desarrollado una carrera orientada a elevar la práctica profesional más allá del enfoque tradicional operativo, promoviendo modelos basados en riesgo, toma de decisiones con datos, cumplimiento de estándares y alineación con sistemas de gestión.

Uno de sus principales aportes intelectuales y metodológicos es el desarrollo del marco Executive Protection Risk Management —EPRM—, concebido para estructurar la identificación, evaluación y mitigación de riesgos en operaciones de protección ejecutiva.

Su perfil combina práctica operativa, pensamiento estratégico y liderazgo institucional. Es miembro del directorio global y directivo para Latinoamérica de IFPO, director en el ASIS Professional Standards Board —PSB—, past chair de la ASIS International Executive Protection Community, fundador del Security Certification Council —SCC— y autor del marco EPRM. Estas funciones evidencian una participación sostenida en iniciativas de estandarización, certificación, educación profesional y fortalecimiento de capacidades en el sector de seguridad. 

Profesional del mes

GUSTAVO MERANI
Argentina



Con más de 25 años de trayectoria en la protección de personas de alto patrimonio neto en América Latina, es uno de los referentes de la Protección Ejecutiva Corporativa en la región.

Certified Protection Officer (CPO) por IFPO y miembro activo de ASIS International, integra las dos organizaciones más importantes del mundo en la industria de la seguridad. Es miembro fundador del Consejo Consultivo Latino de IFPO y Líder de la Comunidad de Protección Ejecutiva del Capítulo 215 de ASIS International en Buenos Aires, Argentina.

Fue miembro del Comité Directivo Global de Protección Ejecutiva de ASIS International y participó en el desarrollo del Estándar de Protección Ejecutiva de ASIS.

Egresado de la Maestría en Inteligencia Estratégica Nacional de la Universidad Nacional de La Plata, cursó además programas ejecutivos en seguridad en la Universidad Católica Argentina, USAL y UCES, y formaciones especializadas en el BID, el EPI Executive Protection Institute y ASIS International, entre otras instituciones.

Es convocado regularmente para dictar charlas, conferencias y capacitaciones sobre Protección Ejecutiva en ámbitos corporativos para equipos de PE de empresas, en ámbitos universitarios y colabora activamente con revistas y medios digitales aportando artículos específicos.

Director de GSGM Security Consulting, donde brinda servicios de PE en Argentina. 

CON SEGURIDAD
Magazine Latam

Tour Internacional 2026



ESS+[®]

intersec
BUENOS AIRES



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

AJAX

DOMINA TU ESPACIO

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



FireProtect 2

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



Dónde comprar

www.ajax.systems

Salas de Control y Monitoreo 4.0: La IA transformando la gestión y respuesta operativa

A lo largo de mi trayectoria en el sector de la seguridad, he visto cómo las salas de control y monitoreo dejaron de ser simples espacios de observación para convertirse en centros críticos de decisión. Hace tres décadas, el trabajo dependía en gran medida de operadores atentos frente a monitores, radios de comunicación y alarmas puntuales. Hoy el escenario es distinto, y es que las organizaciones generan información de manera permanente y el verdadero reto ya no es ver más, sino interpretar mejor.

Una instalación moderna puede producir miles de eventos diarios provenientes de cámaras de video, controles de acceso, sensores de alarma, sistemas de gestión de edificios (BMS), gestión de tráfico (ITS), dispositivos IoT y plataformas de ciberseguridad, entre otros. En ese volumen de datos, el riesgo no está únicamente en que ocurra un incidente, sino en que una señal importante quede perdida entre muchas alertas de bajo valor.

En proyectos de infraestructura crítica, por ejemplo, he observado un patrón común, y es que los operadores a pesar de estar capacitados están expuestos a una carga operativa que supera la capacidad humana de análisis en tiempo real. Es ahí donde la Inteligencia Artificial comienza a aportar valor concreto. No para sustituir el criterio del operador, sino para ayudarlo a priorizar, correlacionar información y

enfocar su atención en lo que realmente requiere acción.

La visión computacional por ejemplo ya permite detectar intrusiones, accesos no autorizados, permanencias indebidas, objetos abandonados, comportamientos inusuales o situaciones de riesgo sin depender exclusivamente de la observación continua y el análisis contextual. Esto cambia la dinámica de la sala de control y el operador deja de ser un espectador pasivo de múltiples pantallas y pasa a gestionar eventos con mayor contexto.

Las plataformas PSIM, (Gestión de Información de Seguridad Física), también cumplen un papel clave. Durante años, la fragmentación tecnológica fue uno de los principales obstáculos en los centros de monitoreo. Cada sistema tenía su propia interfaz y sus propios criterios de alarma. Integrar video, control de acceso, alarmas, BMS, sensores y ciberseguridad en una sola visión operacional permite mejorar la conciencia situacional y reducir tiempos de respuesta.

La IA generativa abre otra posibilidad interesante. Su aplicación en centros de monitoreo y control puede facilitar la elaboración de reportes en la gestión de incidentes, la consulta de procedimientos operativos y el apoyo al operador durante una contingencia. Bien implementada, puede reducir carga operativa y acelerar la toma de decisiones.

La analítica predictiva, por su



Articlista invitado

Juan Carlos Granier, CPO©

Consultor de Seguridad y Protección Integral
juancarlos@venecoconsult.com



parte, permite avanzar hacia modelos preventivos. Analizar patrones históricos, horarios, comportamientos, recurrencias y condiciones del entorno ayuda a anticipar riesgos antes de que se materialicen. A esto se suma el potencial de los digital twins o gemelos digitales, como representación virtual de un activo físico, instalación, proceso o sistema, permitiendo simular escenarios, evaluar impactos y planificar respuestas en instalaciones críticas antes de actuar sobre el entorno físico.

Mi percepción es que las organizaciones más preparadas no serán necesariamente las que adquieran más tecnología, sino las que logren integrar personas, procesos, datos e Inteligencia Artificial dentro de una estrategia coherente de gestión del riesgo.

Las Salas de Control y Monitoreo 4.0 ya no son una promesa futura. Son parte de una transformación en marcha. La Inteligencia Artificial no reemplaza la experiencia humana; la amplifica. Y en un entorno donde cada minuto cuenta, esa diferencia puede ser determinante para proteger personas, operaciones, activos y reputación institucional.



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

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

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

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

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

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

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

Para las organizaciones, los beneficios son contundentes: mayor seguridad real, reducción de riesgos internos y externos, integración más eficiente con ecosistemas tecnológicos

y capacidades avanzadas de auditoría. Más importante aún, permite evolucionar el rol del área de seguridad, pasando de un enfoque operativo a uno estratégico.

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

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

Las empresas que realmente están avanzando en este camino son aquellas



Articlista Invitado

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



que dejan de ver el control de acceso como un punto de control aislado, y comienzan a integrarlo como parte de una estrategia digital más amplia, donde la seguridad habilita el negocio en lugar de limitarlo.

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



Tres pasos para llevar el control de acceso físico al nivel de la era digital



La transformación digital ha cambiado la manera en que las organizaciones gestionan sus operaciones, sus datos y la experiencia de sus usuarios, sin embargo, la modernización de los sistemas de control de acceso físico parece avanzar de una manera más lenta en América Latina.

Mientras los colaboradores realizan pagos desde sus teléfonos, gestionan trámites en línea y trabajan desde plataformas digitales, muchas organizaciones de la región aún continúan dependiendo de procesos manuales para administrar credenciales, accesos y permisos. La consecuencia es una brecha cada vez más evidente entre la experiencia digital que los usuarios esperan y la que reciben al interactuar con los sistemas de acceso.

En este contexto, la integración entre las tecnologías de identidad de HID y la plataforma de experiencia laboral desarrollada por Sharry muestra cómo el control de acceso puede convertirse en una herramienta estratégica para acelerar la transformación digital.

La combinación de ambas soluciones permite abordar tres de los principales desafíos que enfrentan actualmente las organizaciones: mejorar la experiencia de los usuarios, simplificar la administración del acceso físico e integrar el control de acceso con otros sistemas empresariales.

1. Mejorar la experiencia del usuario

Los dispositivos móviles se han convertido en el centro de la vida cotidiana. Por ello, cada vez más organizaciones buscan replicar esa misma experiencia digital dentro de sus edificios y espacios de trabajo.

Las credenciales móviles permiten que los usuarios accedan a oficinas, estacionamientos, salas de reuniones o áreas restringidas utilizando únicamente su teléfono inteligente o dispositivo wearable. Esto elimina la necesidad de portar tarjetas físicas y simplifica considerablemente la experiencia de acceso.

Además de la comodidad, uno de los principales beneficios es la velocidad de incorporación de nuevos colaboradores. En lugar de esperar la impresión, personalización y entrega de una credencial física, los permisos pueden enviarse digitalmente y activarse en cuestión de minutos y de forma remota, desde cualquier parte del mundo.

En América Latina ya comienzan a verse proyectos que reflejan esta transformación. Un ejemplo es la implementación realizada por Buró Property en tres de sus complejos corporativos de Ciudad de México: Puerta Polanco, DEK Polanco e In Situ Santa Fe, donde miles de usuarios pueden acceder a torniquetes, elevadores y estacionamientos utilizando únicamente credenciales digitales almacenadas en Apple Wallet o Google Wallet. La solución eliminó gran parte de los procesos manuales asociados a la emisión y administración de tarjetas físicas, al tiempo que simplificó la experiencia de acceso para usuarios, visitantes e inquilinos.

La evolución del acceso móvil también responde a la necesidad por sistemas de control de acceso que no se limiten solo a abrir puertas. Hoy forman parte de ecosistemas más amplios que incluyen reservas de espacios de trabajo, acceso a estacionamientos, control de ascensores, autenticación de dispositivos y servicios corporativos conectados.

En consecuencia, las organizaciones necesitan soluciones capaces de ofrecer una experiencia fluida y consistente en todos los puntos de interacción.

2. Simplificar la administración del acceso físico

La administración de credenciales representa uno de los mayores desafíos operativos para empresas, propietarios de edificios y administradores de instalaciones.

Los procesos tradicionales implican impresión de tarjetas, personalización, distribución física, reposición por pérdida y múltiples tareas administrativas que consumen tiempo y recursos.

Las credenciales móviles permiten reducir significativamente esta carga operativa. Gracias a modelos de aprovisionamiento basados en la nube, los administradores pueden emitir, modificar o revocar permisos de acceso de forma remota y prácticamente instantánea.

Los beneficios son especialmente visibles en edificios corporativos de múltiples arrendatarios o en organizaciones con grandes volúmenes de personal. La distribución masiva de credenciales puede realizarse mediante correo electrónico o aplicaciones móviles, eliminando los tiempos de espera asociados a la producción y entrega física de tarjetas.

Un ejemplo de estos beneficios puede verse nuevamente en Buró Property. Antes de la implementación, la administración de accesos dependía de tarjetas plásticas y procesos manuales para emitir, reemplazar o desactivar credenciales. Hoy, gracias a la integración entre la credencial digital de HID y la plataforma Sharry, la gestión se realiza de forma digital, permitiendo que miles de usuarios utilicen sus credenciales directamente desde sus billeteras digitales. Además de reducir la carga administrativa, el proyecto preparó la infraestructura para una transición gradual hacia un modelo híbrido, donde las credenciales físicas y móviles conviven sin afectar la operación de los edificios.

La gestión digital también fortalece la seguridad. La pérdida de una credencial física puede pasar desapercibida durante horas o incluso días. En contraste, los usuarios suelen detectar rápidamente la pérdida de su teléfono móvil, permitiendo actuar de forma inmediata.

Además, las plataformas modernas permiten bloquear, actualizar o reemplazar credenciales remotamente, minimizando riesgos operativos y mejorando el control sobre los accesos.

Incluso en organizaciones que aún utilizan tarjetas físicas, las aplicaciones móviles pueden funcionar como una extensión digital de la credencial tradicional, facilitando su administración y fortaleciendo la seguridad.

3. Integrar el control de acceso con otros sistemas empresariales

Quizás el cambio más importante en la industria del control de acceso sea su evolución desde sistemas aislados hacia plataformas integradas de gestión y experiencia laboral.

Durante años, los sistemas de acceso operaron como soluciones independientes. Hoy, las organizaciones buscan consolidar servicios y simplificar la interacción de los usuarios mediante ecosistemas conectados.

La tendencia apunta a que actividades como reservar una sala de reuniones, gestionar un espacio de estacionamiento, solicitar servicios internos o acceder a diferentes áreas del edificio puedan realizarse desde una única plataforma.

Esta integración no solo mejora la experiencia de los usuarios. También genera información valiosa para optimizar operaciones, gestionar recursos y tomar decisiones más informadas.

En organizaciones con modelos de trabajo híbrido, por ejemplo, los sistemas de acceso pueden proporcionar información sobre ocupación de espacios, patrones de uso y flujo de personas, permitiendo una administración más eficiente de oficinas y recursos corporativos.

Para lograrlo, las plataformas abiertas y basadas en interfaces de programación (API) desempeñan un papel fundamental. Estas arquitecturas permiten conectar

sistemas de acceso con soluciones de recursos humanos, plataformas de gestión de edificios, herramientas de reserva de espacios y otras aplicaciones empresariales.

La interoperabilidad también protege las inversiones tecnológicas. En lugar de reemplazar completamente la infraestructura existente, las organizaciones pueden integrar nuevos servicios y funcionalidades de manera progresiva, manteniendo la flexibilidad necesaria para incorporar futuras innovaciones.

Más allá del acceso

La transformación digital del control de acceso no consiste únicamente en sustituir tarjetas físicas por credenciales móviles. El verdadero cambio radica en convertir la identidad digital en un elemento central de la experiencia laboral, la seguridad y la operación empresarial.

Cada organización avanza a un ritmo diferente, condicionado por sus objetivos, infraestructura y recursos. Algunas mantendrán modelos híbridos durante varios años; otras acelerarán la adopción de credenciales móviles y servicios digitales.

Lo importante es contar con una plataforma capaz de evolucionar junto con las necesidades del negocio.

En un entorno donde la experiencia del usuario, la eficiencia operativa y la integración tecnológica se han convertido en prioridades estratégicas, el control de acceso ya no puede entenderse únicamente como un sistema de seguridad. Cada vez más, se consolida como una herramienta clave para impulsar la transformación digital de las organizaciones y generar valor más allá de la protección física de personas y activos.

Alejandro Espinosa, director Comercial de Soluciones de Control de Acceso Físico de HID en México.





fortalece presencia en México con Muñoz Solutions como nuevo subdistribuidor autorizado

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

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

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

"México es uno de los mercados estratégicos para Ajax Systems en Latinoamérica y seguimos comprometidos con fortalecer nuestra red de distribución para estar cada vez más cerca de nuestros clientes. La incorporación de Muñoz Solutions como subdistribuidor representa un paso importante en esa estrategia. Su experiencia, conocimiento del mercado y presencia en estados clave nos

permitirán ampliar la disponibilidad de nuestras soluciones, impulsar la capacitación de integradores y brindar un mejor acompañamiento a los profesionales de la seguridad. Estamos convencidos de que esta alianza contribuirá al crecimiento de ambas compañías y, sobre todo, a generar

más oportunidades para nuestros clientes en la región", afirmó Alberto Treviño, Sales de Ajax Systems para Latinoamérica.

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

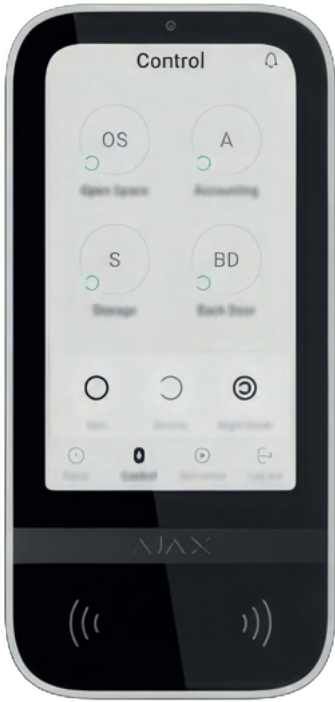
"En Muñoz Solutions nos caracterizamos por mantenernos a la vanguardia tecnológica y ofrecer a nuestros clientes soluciones respaldadas por las mejores marcas del mercado. Convertirnos en Subdistribuidor Oficial de Ajax Systems representa una oportunidad para fortalecer esta visión y ampliar nuestro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

Bryant agregó: "Nuestro objetivo es construir una relación comercial de largo plazo con Ajax Systems, impulsando la capacitación continua de nuestro equipo, fortaleciendo nuestra presencia en el mercado y consolidándonos como un referente en la implementación de soluciones de seguridad electrónica de última generación. Además de la

distribución de productos, buscamos aportar valor mediante asesoría especializada,

diseño de proyectos, soporte postventa y estrategias que contribuyan al crecimiento de la marca en nuestra región."

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



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

AJAX

ALARM.COM

ALCEA
ASSA ABLOY

Altronix

AXIS
COMMUNICATIONS

BOLIDE
TECHNOLOGY GROUP

CAME

dahua
TECHNOLOGY

EXP
SEGURIDAD
MÉXICO

GARNET
TECHNOLOGY

Genetec

Hanwha Vision

HID

HIKVISION

Honeywell

IKUSI
velatia

Johnson Controls

milestone

MOTOROLA SOLUTIONS

Network Optix

NVT PHYBRIDGE

OpenEye

PROSEGUR
SECURITY

RBH
ACCESS

resideo

SECURITY SIS
SERVICIOS INTEGRALES DE SEGURIDAD

SoftGuard

Verkada

wesco | anixter

ZKTeco

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

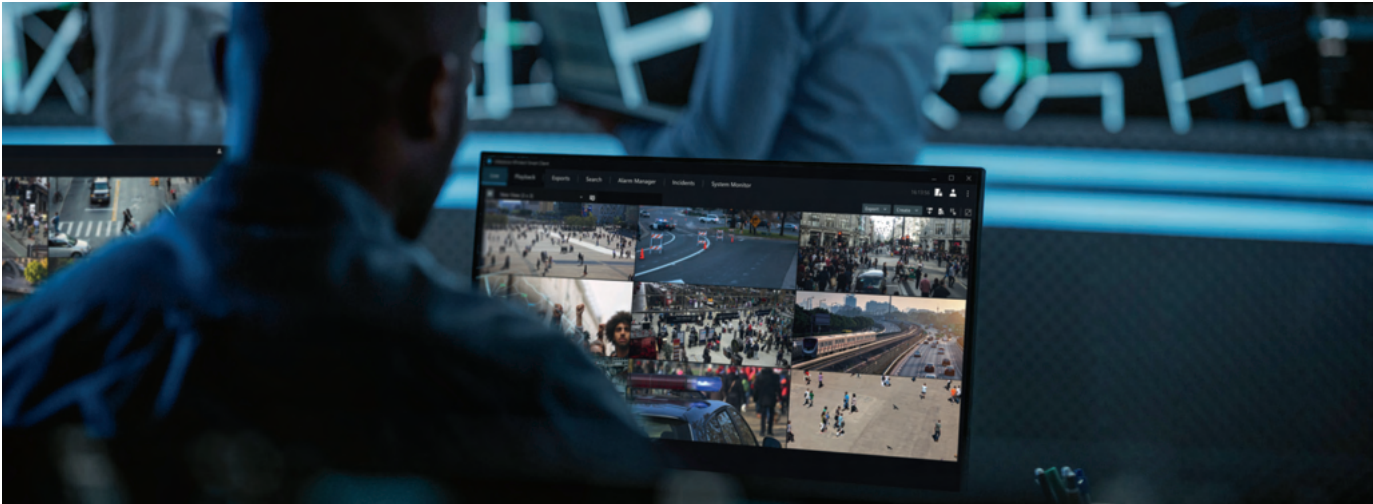
Ahora es el momento de que tu empresa también sea parte de esta comunidad.

Únete a ALAS



ASOCIACIÓN
LATINOAMERICANA
DE SEGURIDAD

www.alas-la.org



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

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: innovación 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. 



Fundamentos para una doctrina de Political Security Risk Management en Latinoamérica

Montevideo, Uruguay- La violencia política continúa siendo una amenaza real para la estabilidad democrática regional. El asesinato del candidato Fernando Villavicencio, el de Miguel Uribe Turbay en y el del alcalde Carlos Manzo en México, demuestran entornos políticos caracterizados por altos niveles de riesgo e incertidumbre. La convergencia entre crimen organizado, violencia política, extremismo, conflictividad social y tecnologías disruptivas está generando un nuevo escenario operativo que obliga a replantear la forma en que se concibe la seguridad electoral. En este contexto, la seguridad privada posee capacidades

legitimidad institucional, la reputación pública, la continuidad operativa de la campaña y la integridad del proceso electoral.

Riesgos y amenazas. La primera tarea del PSRM es identificar los activos que requieren protección: candidatos, dirigentes, familiares, equipos de campaña, información estratégica, infraestructura física, plataformas digitales e imagen institucional. Las amenazas incluyen: atentados físicos, secuestros, espionaje, filtración de información, sabotaje, campañas de desinformación, hostigamiento digital y acciones promovidas por organizaciones criminales interesadas en influir sobre



profesionales que pueden complementar la responsabilidad primaria de los organismos públicos, contribuyendo a proteger personas, instalaciones, información y procesos críticos para el funcionamiento democrático.

Del ESRM al PSRM.

La Gestión Integral de Riesgos de Seguridad (ESRM) demuestra ser una metodología eficaz para proteger organizaciones complejas. Sin embargo, las campañas electorales presentan características particulares que justifican una adaptación específica.

PSRM no pretende sustituir al ESRM. Busca extender sus principios al entorno político-electoral, incorporando variables propias de la violencia política, la gobernanza democrática, la reputación pública y la continuidad operativa de las campañas. Bajo esta perspectiva, los activos críticos dejan de ser exclusivamente físicos y pasan a incluir elementos estratégicos como la

procesos políticos. La seguridad moderna exige comprender que muchas amenazas se desarrollan simultáneamente en los dominios físico, digital y reputacional.

Infraestructura y protección.

Las sedes partidarias, centros de comando y cuarteles generales constituyen nodos críticos dentro de la campaña electoral. La aplicación de criterios CPTED permite reducir vulnerabilidades mediante control de accesos, vigilancia natural, iluminación estratégica, delimitación territorial, monitoreo tecnológico y planes de evacuación. La protección de candidatos y dirigentes requiere además inteligencia preventiva, reconocimientos previos, avanzadas de seguridad, análisis de rutas, evaluación permanente de amenazas, planificación médica y coordinación interinstitucional.

Comando y control.

Toda estrategia PSRM requiere una



Articlista Invitado

Fernando Vaccotti

PhD. CPQ.
Miembro por Uruguay del Consejo Consultivo Latino de IFPD.



estructura de Comando y Control (C2) capaz de integrar información, monitorear riesgos y coordinar recursos en tiempo real. Este centro de coordinación debe actuar como un nodo permanente de análisis, planificación y gestión, conectando a los equipos de protección, logística, comunicaciones, salud, tecnología y conducción política. Su función principal consiste en transformar información dispersa en decisiones oportunas que permitan anticipar amenazas, gestionar crisis y mantener la continuidad operativa de la campaña.

La seguridad deja entonces de ser un conjunto de medidas aisladas para ser un sistema integrado de gestión del riesgo.

Una doctrina de seguridad electoral.

La creciente violencia política en la región requiere desde soluciones tácticas aisladas hacia la construcción de una verdadera doctrina de seguridad electoral para Latinoamérica. El concepto de (PSRM) pretende contribuir a ese debate, ofreciendo un marco conceptual para integrar gestión del riesgo, protección de personas, seguridad física, continuidad operativa y resiliencia institucional dentro de las organizaciones políticas. La seguridad privada puede convertirse en actor estratégico para proteger procesos democráticos. Su contribución no debe limitarse a custodiar personas o instalaciones. Debe fortalecer resiliencia institucional y proteger la integridad de sistemas políticos frente a amenazas cada vez más complejas. Pero proteger la integridad del proceso democrático es una responsabilidad aún mayor.

PSRM no pretende sustituir al ESRM. Busca extender sus principios al entorno político-electoral, incorporando variables propias de la violencia política, la gobernanza democrática, la reputación pública y la continuidad operativa de las campañas.

La seguridad electoral del siglo XXI no necesita más improvisación. Necesita doctrina. 🇺🇷

Aeropuertos bajo presión en seguridad, tecnología y operación



Beatriz Canales Hernández

El sistema aeroportuario está cambiando rápidamente de ser una infraestructura estable para considerar una variable que lo empuja: volumen. En 2024, el tráfico aéreo global superó los 9.5 mil millones de pasajeros, de acuerdo con el Airports Council International. América Latina crece a un ritmo similar, aunque con una base tecnológica y operativa que no siempre acompaña esa expansión.

Ese desbalance coloca a la seguridad como el centro estratégico como condición que permite que el sistema funcione. Es decir, si falla, no hay operación.

México enfrenta ese reto en un momento particularmente exigente y complejo. El aumento del tráfico, la presión logística y la expectativa de eventos internacionales, como el reciente Mundial de 2026, obligan a replantear cómo se protegen infraestructuras que concentran miles de personas por hora, cientos de operaciones simultáneas y riesgos que evolucionan con rapidez.

Integración redefine la seguridad

Durante años, la seguridad aeroportuaria operó con sistemas independientes:

- El tráfico aéreo global superó los 9.5 mil millones de pasajeros en 2024, elevando la presión sobre los sistemas de seguridad.
- América Latina crece por encima del promedio mundial en movilidad aérea, con infraestructura aún en transición tecnológica.
- La seguridad aeroportuaria migra de esquemas reactivos a modelos predictivos, con Inteligencia Artificial y analítica avanzada.

cámaras, controles de acceso, filtros de inspección y monitoreo perimetral funcionaban de forma paralela. Es decir, había que impulsar integración por encima de tecnología. Al respecto, Rodrigo Escamilla Santiago, director de Desarrollo de Negocios en Dahua Technology México, describe el punto de inflexión: “Hoy hablamos de plataformas integrales que cubren desde el lado aire hasta el lado tierra”.



Rodrigo Escamilla Santiago, director de Desarrollo de Negocios en Dahua Technology México

El cambio implica que los sistemas, además de registrar eventos, ahora los conectan. Lo que ocurre en una terminal puede vincularse con movimientos en pista, accesos, equipaje o transporte interno. Esa trazabilidad permite reconstruir situaciones completas, no



solo fragmentos. En ese entorno, la función del operador cambia de manera radical: “El operador se vuelve un gestor de incidentes”.

Así, la vigilancia pasiva deja de ser suficiente, pues la operación exige interpretación, correlación de datos y capacidad de respuesta en tiempo real.

La evolución de la inspección aeroportuaria también ha redefinido la relación entre operador y sistema. Escamilla introduce un elemento que suele quedar fuera de la discusión pública: la supervisión en doble capa: “Esto ayuda a quitar la discrecionalidad... no nada más el operador en los filtros, sino desde el centro de monitoreo puedan verlo”.

La decisión ya no ocurre únicamente en el punto físico de revisión, sino que existe una segunda validación remota que reduce errores humanos, genera evidencia y fortalece procesos de auditoría interna. Para aeropuertos con alta afluencia, esta duplicidad de control comienza a operar como estándar y no como algo excepcional.



¿Dónde se concentra la tensión operativa?

La seguridad aeroportuaria tiene un punto crítico: los filtros de inspección. Ahí convergen dos exigencias que con dificultad suelen alinearse con facilidad: velocidad y control. Ricardo Hernández, Sales Account Manager HikRayin en Hikvision México, explica cómo ha evolucionado ese espacio: “La seguridad de alto perfil ya no es exclusiva de los grandes centros aeroportuarios; hoy es asequible para una mayor diversidad de recintos”.



Ricardo Hernández, Sales Account Manager HikRayin en Hikvision México

Y es que el acceso a tecnologías avanzadas ha cambiado el estándar, o sea, equipos de rayos X con Inteligencia Artificial, escáneres corporales por ondas milimétricas y sistemas de detección no intrusiva, permiten inspeccionar sin contacto físico, reducir tiempos y mejorar la precisión. El impacto es doble, por un lado, se agiliza el paso del pasajero, por otro, el sistema incrementa su capacidad de observación.

La dimensión económica de la seguridad aeroportuaria también ha cambiado. Para Hernández, apunta a un fenómeno que explica la expansión tecnológica: “Los costos... han mostrado una tendencia decreciente sostenida durante la última década”. Este descenso no se da solo por competencia comercial, sino que incluye tres factores técnicos: maduración de componentes electrónicos, estandarización de sensores y entrada de nuevos fabricantes.

El resultado es tangible en aeropuertos regionales que antes operaban con detección básica, que ahora incorporan Inteligencia Artificial, biometría y analítica avanzada. Esto



eleva el estándar general, pero también reduce el margen de error, porque amplía la superficie tecnológica que debe mantenerse operativa.

Concluye al explicar que la automatización no elimina el proceso; lo hace más profundo. Los equipos actuales pueden identificar múltiples categorías de objetos prohibidos y reducir la tasa de error en la detección. Sin embargo, esa eficiencia no elimina el reto principal: mantener el flujo constante sin generar cuellos de botella.

Identidad y acceso como el nuevo eje de control

Actualmente, el control de identidad ya no depende de documentos físicos. La tendencia apunta a sistemas biométricos que operan sin contacto. Omar Velasco Miguel, representante de ZKTeco Latam a nivel nacional, (senior sales manager en control de accesos y asistencia) describe esta transición: “Hoy ya usamos reconocimiento de palma, venas y tarjetas digitales”.



Omar Velasco Miguel,
representante de ZKTeco
Latam a nivel nacional

El cambio responde a necesidades operativas porque la identificación debe ser rápida, precisa y difícil de transferir. Los sistemas biométricos cumplen con esas condiciones y permiten gestionar grandes volúmenes de personas sin detener el flujo.

Por otro lado, también importante, está el componente económico que también ha sido determinante: “Estamos compitiendo aproximadamente entre un 10 y un 15% más rentable”. La reducción de costos ha facilitado la adopción en aeropuertos que antes no podían acceder a estas tecnologías. Esto amplía la cobertura, pero también introduce nuevos desafíos: la integración de sistemas existentes y la gestión de bases de datos cada vez más grandes.

La presión sobre los sistemas



también se traslada a la gestión de datos, como lo explica Velasco, quien lo describe desde la operación tecnológica: “La cantidad de bases de datos es lo más importante que pueda soportar un software”. El crecimiento en el número de pasajeros implica un aumento proporcional en registros biométricos, accesos y trazabilidad. Este volumen exige plataformas escalables, capaces de operar en la nube y procesar información en tiempo real sin comprometer seguridad.

La infraestructura digital se convierte de esta manera en un componente crítico del sistema aeroportuario. Si falla, no solo se detiene el acceso; se pierde la capacidad de verificar identidades y reconstruir eventos.



Perímetros extensos, vulnerabilidades persistentes

Mientras los filtros concentran la atención, los perímetros representan uno de los puntos más críticos de la seguridad aeroportuaria. René Cuenca, gerente de Ventas para la región de México y Centroamérica de Optex, plantea una diferencia que trata de definir el problema: “Detectar todos lo hacen; identificar y clasificar es la diferencia”.



René Cuenca, gerente de Ventas para la región de México y Centroamérica de Optex

La detección sin contexto genera ruido, por ejemplo, alarmas constantes que obligan a movilizar recursos sin distinguir la naturaleza del evento. La capacidad de clasificar amenazas —persona, vehículo, dron o animal— permite priorizar la respuesta.

En México, el caso del Aeropuerto Internacional Felipe Ángeles es un reto evidente. El perímetro alcanza 37 kilómetros, con monitoreo extendido a 44 kilómetros mediante sensores. Proteger esa extensión exige tecnologías de largo alcance, como sistemas de fibra óptica

capaces de cubrir grandes distancias o radares que detectan movimientos a cientos de metros.

Y la experiencia reciente muestra que las fallas existen: intrusiones en pistas, accesos no detectados y vulneraciones perimetrales, que han expuesto debilidades que obligan a replantear el enfoque. Cuenca lo resume con una idea que busca sintetizar la tendencia: “Hoy hablamos de seguridad predictiva”.

El objetivo es anticipar eventos antes de que ocurran. Reducir tiempos de respuesta no es suficiente si el sistema no puede prever amenazas.

El papel del factor humano

El avance tecnológico ha alimentado la idea de una seguridad completamente automatizada. La operación diaria



muestra otra realidad. Eduardo Reyes López, gerente de Seguridad Patrimonial en Schneider Electric, explica: “En seguridad de la aviación civil existe una triada: personal, procedimientos y tecnología”. Los tres elementos son interdependientes. La ausencia de uno compromete la eficacia del sistema.



Eduardo Reyes López, gerente de Seguridad Patrimonial en Schneider Electric

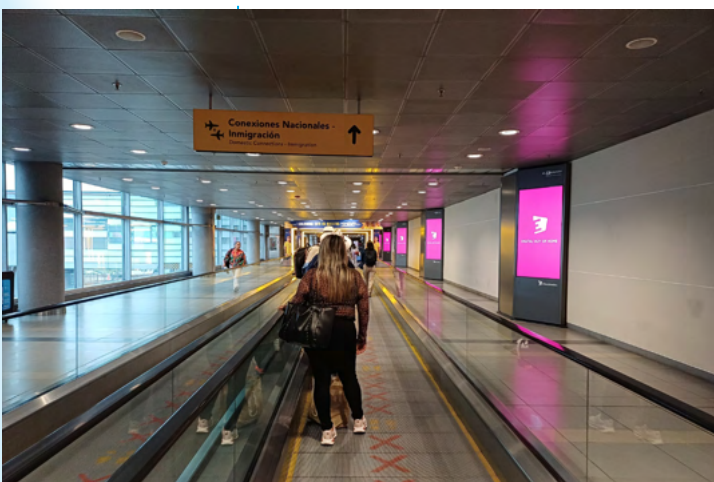
En el plano operativo, la seguridad aeroportuaria enfrenta un dilema más allá de lo solamente técnico, y se refiere a lo organizacional. Reyes lo plantea al referirse al equilibrio entre seguridad y flujo: “Si en determinado momento existe un conflicto... deberá prevalecer la seguridad”.

Con ello, el responsable marca un límite operativo que, en la práctica, tiene implicaciones económicas. Cada refuerzo en inspección implica retrasos, cada incremento en controles afecta la experiencia del pasajero. La decisión de priorizar seguridad sobre flujo no es neutra, antes bien impacta tiempos, costos y percepción del servicio. Por eso, en escenarios de alta amenaza, ese equilibrio pasa de ser de tipo técnico y se convierte en una decisión estratégica.

Y hay una capa adicional en todo esto, y se refiere a la gestión de amenazas internas, por lo que Reyes advierte que “hoy es una de las principales amenazas de la aviación civil”. El concepto de insider —personal con acceso autorizado que puede vulnerar procesos— introduce un riesgo distinto al terrorismo o la intrusión externa.

Este tipo de amenaza no se resuelve con más cámaras o sensores, el experto enfatiza que, con procesos de selección, controles de confianza y monitoreo continuo del personal. La seguridad aeroportuaria no solamente deja de centrarse en el pasajero para incluir a todos los actores que interactúan con la operación: empleados, proveedores, servicios logísticos y personal externo.





Daniel Espinosa Ávila, director general de Grupo COSEPROS, lo aterriza en la práctica y señala: “Cada pasajero que sube a un avión tendrá que ser revisado”. La revisión no es un trámite, más bien es una medida directa sobre la seguridad de las personas: “La tecnología no está peleada con el personal”.

Un sistema puede detectar anomalías, pero la interpretación sigue dependiendo del operador. La diferencia entre una amenaza real y un falso positivo requiere criterio. Otro ejemplo ilustra esa dinámica: un escáner puede identificar un objeto con forma de arma. Solo la verificación humana determina si se trata de un riesgo o de un objeto inofensivo.

Capacidad operativa y el sistema en números

Para los especialistas, la eficiencia del sistema aeroportuario depende de su capacidad de procesamiento. Equipos de rayos X pueden revisar hasta 1,800 equipajes por hora. Sistemas de inspección permiten procesar cientos de pasajeros en el mismo lapso. Estas cifras definen la viabilidad del flujo.

Cuando uno de estos puntos se

satura, el impacto se extiende a toda la operación. Retrasos, acumulación de pasajeros y presión sobre el personal son consecuencias inmediatas, sumemos a esto un elemento menos visible: la información. Eduardo Reyes advierte una limitación de tipo estructural: “La información de amenazas... muchas veces es confidencial”.

La falta de intercambio entre agencias limita la capacidad de anticipación y, sin inteligencia compartida, la seguridad mantiene

la gran mayoría de los visitantes utilizarán estos medios de transporte”. El sistema debe escalar su capacidad sin perder control. Esto implica inversión, integración tecnológica y formación de personal especializado.

El desarrollo más relevante en el horizonte es la integración total de datos. Rodrigo Escamilla describe el objetivo: “La idea es entender qué está pasando detrás de los sensores”. Los llamados gemelos digitales representan ese paso: modelos virtuales que replican el



Daniel Espinosa Ávila, director general de Grupo COSEPROS

un componente reactivo, incluso con tecnología avanzada.

Modernización con presión creciente

En México, la inversión en tecnología aeroportuaria avanza de forma más o menos desigual. Aeropuertos como los de Ciudad de México, Guadalajara, Monterrey y Cancún han incorporado sistemas biométricos, escaneo avanzado y análisis automatizado. Sin embargo, el crecimiento del tráfico y la expectativa de eventos internacionales incrementan la presión sobre la infraestructura.

Daniel Espinosa lo plantea en términos operativos: “Los aeropuertos jugarán una parte muy importante...

aeropuerto en tiempo real, integrando información de cámaras, sensores y sistemas operativos.

Y es que la utilidad va más allá de la observación porque permite simular escenarios, prever comportamientos y tomar decisiones anticipadas. La operación ya no es reactiva nada más, ahora se ha convertido en un proceso basado en análisis continuo.

Un sistema que no admite errores

No es posible evaluar la seguridad aeroportuaria por la ausencia de incidentes visibles. Su eficacia real debe considerar la capacidad de anticipar riesgos, absorber presión operativa y



sostener la continuidad del sistema sin interrupciones.

“El gran reto de la seguridad de la aviación civil es ser predictiva y preventiva más que reactiva” y ello implica modificar la forma en que se diseñan los procesos, se comparten los datos y se toman decisiones en tiempo real. Sin inteligencia anticipada, dice el responsable de Schneider Electric, incluso los sistemas más sofisticados operan en desventaja frente a amenazas que evolucionan más rápido que los protocolos.

Ricardo Hernández, de Hikvision,

concluye por su parte que la evolución tecnológica ha permitido reducir costos y ampliar capacidades, pero ese avance introduce la exigencia adicional de mantener interoperabilidad y control sobre sistemas cada vez más complejos. Y se suma Rodrigo Escamilla, de Dahua Technology, quien advierte que el valor real no está en acumular dispositivos, sino en integrarlos para generar trazabilidad y contexto.

Daniel Espinosa, de Grupo COSEPROS, lo resume: “la tecnología no está peleada con el personal”. La automatización ha desplazado tareas

mecánicas, pero ha elevado el nivel de exigencia sobre quienes operan los sistemas. La verificación final, la interpretación de escenarios ambiguos y la toma de decisiones en condiciones de incertidumbre siguen dependiendo de personas capacitadas.

México y América Latina avanzan hacia esquemas más complejos, pero con diferencias marcadas en inversión, infraestructura y madurez operativa. Aeropuertos con altos niveles de modernización conviven con terminales que aún operan con esquemas básicos, lo que genera asimetrías en la capacidad de respuesta ante incidentes.

El escenario incrementa el riesgo sistémico al observarse que la seguridad de la red depende del eslabón más débil. La presión derivada del crecimiento del tráfico aéreo y de eventos internacionales amplifica estas brechas, obligando a acelerar procesos de actualización tecnológica y profesionalización del personal.

Un evento de seguridad afecta la percepción internacional, impacta el flujo turístico y puede alterar cadenas logísticas completas. La conectividad aérea es un componente clave, la seguridad se convierte en un factor de estabilidad económica, y la capacidad de un aeropuerto para operar sin interrupciones se traduce en confianza para inversionistas, aerolíneas y pasajeros. 



Centro Global para la Seguridad Corporativa: ¿Existe una necesidad? ¿Qué criterios?



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

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

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

La mejor pregunta es si el

GSOC se alinea con el perfil de riesgo, la complejidad y las prioridades empresariales de la organización.

¿Qué soporta un CGOS?

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

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

es donde surgen las necesidades de madurez del equipo CGOS.

¿Cuándo necesita una organización un CGOS más maduro?

Cuando su perfil de riesgo y complejidad operativa han superado las capacidades del modelo actual. Los indicadores comunes incluyen:

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

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

Viajes frecuentes de empleados:

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



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

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

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

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

Estos factores deben evaluarse de forma holística. Por ejemplo, una gran empresa global puede tener un CGOS inferior al esperado si el tiempo del personal se centra en el tráfico de radio local y en las actividades diarias del sitio. Por otro lado, una organización pequeña puede necesitar un CGOS más avanzado al supervisar viajes ejecutivos complejos u operaciones sensibles. Las decisiones deben basarse en una evaluación exhaustiva del perfil de riesgo global de la organización y sus objetivos de seguridad.

¿Por qué los profesionales de seguridad son fundamentales para el rendimiento de CGOS?

La tecnología avanzada, junto con IA, ayuda a parametrizar sistemas en actividades críticas de tipo ejecutivo de seguridad y, especialmente, riesgos operativos de intrusión e intrusiones con el Estado Final Deseado de sabotaje y ataques terroristas. Los profesionales de la seguridad necesitan juicio operativo, disciplina en la comunicación, familiaridad con la plataforma, habilidades de reporte y comprensión del negocio. Necesitan saber cuándo escalar, monitorizar, documentar o buscar más contexto. Este juicio ayuda a mantener agilidad y reducir impactos, aumentando la resiliencia.

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

Resultado

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

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

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



GENERAR
SEGURIDAD
PARA SALVAR
VIDAS

Desarrollamos soluciones de protección balística con los más altos estándares de calidad, confianza e innovación para seguridad privada, corporativa y gubernamental.



SEGURIDAD
PRIVADA

Protegemos a quienes cuidan lo más importante.



POLICÍA
MUNICIPAL

Equipamiento confiable para quienes protegen a nuestra sociedad.



SEGURIDAD
CORPORATIVA
Y EJECUTIVA

Soluciones discretas y efectivas para la protección ejecutiva.



CHALECO
INTERIOR
III-A



CHALECO
EXTERIOR
III-A



PLACAS
BALÍSTICAS
NIVEL III Y IV



UNIFORMES
DE ALTO
DESEMPEÑO



CASCOS
BALÍSTICOS



NUESTRA MISIÓN ES
GENERAR SEGURIDAD
PARA SALVAR VIDAS.

Cada solución que fabricamos está diseñada para superar los estándares más exigentes y proteger lo más valioso.



CALIDAD
CERTIFICADA



FABRICACIÓN
100% MEXICANA



TECNOLOGÍA Y
MATERIALES DE
ALTO NIVEL



DISEÑOS
ERGONÓMICOS
Y DISCRETOS



COMPROMISO
TOTAL

PROTEGEMOS A QUIENES PROTEGEN

Lumu lanza Threat Observatory que ofrece inteligencia de amenazas personalizada y en tiempo real

Las Vegas, EE.UU.- Lumu, creadores del modelo de seguridad Continuous Compromise Assessment®, anunció el lanzamiento de Lumu Threat Observatory™ como parte de Maltiverse, su solución de inteligencia de amenazas. Lumu Threat Observatory es una experiencia de inteligencia de amenazas en vivo y personalizada, que proporciona a las organizaciones una visión completa y en tiempo real de las amenazas activas dirigidas a un sector específico, ayudándolas a identificar actores maliciosos de forma temprana, priorizar vulnerabilidades y bloquearlas automáticamente.

Si bien la inteligencia de amenazas es hoy una pieza fundamental de la estrategia de seguridad de cualquier organización, la mayoría de los equipos de TI y seguridad tienen visibilidad limitada sobre los actores específicos

seguridad existente. En lugar de saturar a las organizaciones con un catálogo genérico de amenazas globales, Lumu Threat Observatory ofrece inteligencia hiperlocalizada y específica por industria, que detalla exactamente qué las está atacando en este momento y cómo detenerlo.

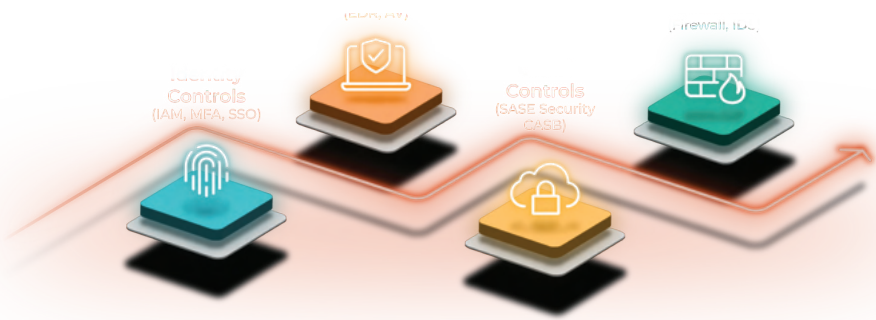
“Los equipos de seguridad actuales no enfrentan una escasez de inteligencia de amenazas, sino una escasez de contexto. Aunque la información sobre amenazas se ha vuelto un componente estándar dentro de las operaciones de seguridad, sigue siendo demasiado genérica para responder preguntas críticas sobre qué actores están atacando activamente a una industria o región específica. Sin esa visibilidad segmentada, los equipos de seguridad terminan defendiendo todo y nada al mismo tiempo, incrementando la fatiga

Threat Observatory agrupa automáticamente las amenazas en vivo en un feed de amenazas focalizado y lo despliega directamente en el Firewall, SIEM (Gestión de Información y Eventos de Seguridad) o EDR (detección y respuesta en endpoints) del usuario en segundos.

- Priorización de vulnerabilidades: identifica con precisión las CVE que están siendo explotadas activamente contra organizaciones similares, garantizando que se implementen los parches que realmente importan.
- Telemetría en vivo e IoCs verificados: cada indicador de compromiso (IoC) es validado mediante telemetría de ataques en vivo, para evitar que datos obsoletos desperdicien la capacidad del firewall y del EDR.

También, en Def Con en Las Vegas, Mario Lobo Romero, investigador de inteligencia de amenazas cibernéticas en Lumu, presentará su investigación sobre Almaru C2 en La Villa Hacker y en Red Team Village. Almaru C2 es un framework de Red Team impulsado por IA que automatiza tácticas Living off the Land al subvertir el Model Context Protocol de Anthropic tunelizar tráfico de comando y control (C2) a través de comunicaciones legítimas con APIs de modelos de lenguaje (LLMs). Su investigación demuestra cómo esta plataforma permite a los operadores ejecutar acciones complejas de PowerShell y evadir defensas usando prompts de lenguaje natural de alto nivel, en lugar de sintaxis de explotación manual.

Disponible desde ahora, Lumu Threat Observatory ofrece inteligencia de amenazas en tiempo real y personalizada, que brinda un briefing a la medida de cada cliente. 



que atacan su industria o región exacta. En lugar de claridad accionable, se ven inundados en un mar de fuentes de datos genéricas y ruidosas que oscurecen el riesgo real.

El nuevo Lumu Threat Observatory cierra esa brecha. Impulsada por el repositorio global de inteligencia de amenazas de Maltiverse, la solución funciona como un observatorio vivo de amenazas y una plataforma abierta de investigación conectada. Su capacidad permite monitorear de manera continua el comportamiento de actores maliciosos, identificar grupos de amenazas activos, rastrear familias de malware, analizar las técnicas utilizadas según el marco MITRE ATT&CK y detectar las vulnerabilidades (CVEs) que están siendo explotadas activamente.

Lumu detalla toda la historia detrás de los atacantes identificados, permitiendo a los equipos de seguridad consultar al instante los adversarios que atacan a organizaciones como la suya y agrupar automáticamente las amenazas en vivo en feeds de inteligencia personalizados para desplegarlos directamente en su stack de

por alertas, manteniendo puntos ciegos y tomando decisiones complejas sobre qué vulnerabilidades priorizar. Creamos Lumu Threat Observatory para eliminar esa incertidumbre y entregar la inteligencia precisa que las organizaciones necesitan para protegerse de las amenazas que realmente importan”, afirmó Ricardo Villadiego, fundador y CEO de Lumu.

Lumu Threat Observatory incluye:

- Visibilidad de amenazas a la medida: Lumu Threat Observatory permite a los usuarios ver exactamente qué actores de amenazas y malware están atacando activamente a organizaciones dentro de su vertical y región específicas, en tiempo real.
- Investigación conectada de amenazas: los usuarios pueden consultar al instante familias de malware o actores de amenazas para ver su historial, patrones de comportamiento y CVE (Common Vulnerabilities and Exposures) explotadas, para actuar de forma rápida y precisa.
- Feeds personalizados: Lumu



Ricardo Villadiego, fundador y CEO de Lumu Technologies



SEGURIDADEXPO®

08 al 10 septiembre | METROPOLITAN SANTIAGO

www.seguridadexpo.cl

info@seguridadexpo.cl

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



¡NO TE QUEDES FUERA!

Consigue tu ticket y sé parte del evento líder en seguridad



MOTOROLA SOLUTIONS

AUSPICIA
**GRUPO
SAFETECK**



La Inteligencia Corporativa
en la Aviación Civil, el
complemento de AVSEC ante
los riesgos
híbridos-convergentes.



Herschel Schultz Chávez, CPP-DES

Gerente de Inteligencia y Protección Corporativa
Grupo AEROMEXICO



Articulista Invitado

En el complejo tablero de la seguridad global, la aviación civil y el sistema aeroportuario ha dejado de ser un simple nodo de transporte para convertirse en un sensor crítico del estado de derecho y la estabilidad de una nación. En países con ecosistemas de seguridad volátiles, como México y Latinoamérica ante el crimen organizado, Norteamérica, Europa y Asia, ante una escalada de conflictos bélicos y guerras no convencionales, la aviación civil enfrenta una metamorfosis en sus amenazas: de la delincuencia y guerra convencional a los riesgos híbridos-convergentes.

Para las aerolíneas y grupos aeroportuarios, el contar con áreas especializadas en Inteligencia Corporativa con experiencia en Seguridad Nacional Multidimensional, les permite identificar

y analizar información de amenazas potenciales antes de que ocurran. Esto permite que las empresas tomen decisiones informadas HOY para neutralizar los riesgos de MAÑANA.

En México y el mundo, las aerolíneas ya no solo enfrentan riesgos operativos (clima, fallas técnicas, pasajeros disruptivos, intervenciones ilícitas, etc.; ahora enfrentan riesgos híbridos -convergentes. Estos combinan amenazas convencionales con métodos no convencionales:

- Desinformación y Reputación: Ataques en redes sociales que pueden generar pánico o boicots con afectación a confianza de inversionistas y la cotización en bolsa de valores.
- Ciberseguridad: Ataques a los sistemas de despacho o reserva, emisión de





- volteos, control aéreo, etc.
- Entornos Político-Legal: Cambios súbitos en la regulación o militarización de funciones civiles, controles migratorios violentos, ataque a aeronaves o infraestructura aeroportuaria para evitar la detención y traslado de objetivos prioritarios convirtiéndose en centros de fricción táctica, cambios súbitos de poder de grupos políticos, etc.
- Violencia Territorial: El control de rutas terrestres hacia el aeropuerto por parte de actores no estatales-gubernamentales y movimientos sociales que afecten la seguridad y movilidad de tripulaciones entre los aeropuertos y hoteles de pernocta.

Ahora bien, los ecosistemas aeroportuarios no son entidades aisladas; es un reflejo dinámico del entorno sociopolítico y económico de la región. Cuando una ciudad sufre una crisis, el aeropuerto es el primer lugar donde se manifiesta.

La inteligencia no es un fin en sí mismo, sino una herramienta para la Gestión de Riesgos Corporativos (ERM) que es un complemento sustantivo y cada vez más necesario con AVSEC. Sus objetivos son proteger tres pilares:

- Personas (safety & security): Integridad física de empleados (tripulaciones y personal en tierra) y clientes, las aeronaves en tierra y aire e infraestructuras críticas como los

- aeropuertos.
- Operación: Mantener la conectividad aérea y los flujos logísticos sin interrupciones costosas.
- Reputación y Branding: Evitar que la marca se vea asociada con incidentes de seguridad o falta de control y gestión en situaciones de crisis.

La delincuencia en México y el mundo ha evolucionado. Ya no solo hablamos de robos, terrorismo convencional, etc.; hablamos de riesgos híbridos que combinan la violencia física con uso de tecnologías disruptivas como drones, desinformación y el sabotaje digital, así como la actividad de actores político-sociales y organizaciones internacionales emergentes. Esta realidad ha obligado a las aerolíneas a abandonar los esquemas de seguridad reactiva y adoptar áreas de inteligencia corporativa robustas.

La inteligencia no predice el futuro, pero al traer los posibles riesgos futuros al presente, con el análisis de escenarios y gestión de riesgos de forma integral con otros ecosistemas, reduce la incertidumbre para que el CEO y el Board puedan decidir si un avión despegue o se queda en tierra ante una crisis inminente. 🌐

Gestión humana en la era de la IA: el valor insustituible de lo humano

Durante años, las organizaciones han protegido a las personas mediante normas, procesos y controles. Más recientemente comprendimos la importancia del blindaje emocional para enfrentar entornos cada vez más complejos. Hoy surge un nuevo desafío para Gestión Humana: cómo preservar el criterio humano en una época donde la Inteligencia Artificial (IA) comienza a participar en muchas de nuestras decisiones.

La conversación ya no gira en torno a si la IA reemplazará a las personas. La pregunta realmente importante es otra: ¿cómo utilizamos esta tecnología para

La IA puede identificar patrones, procesar datos y generar recomendaciones en segundos. Lo que aún no puede hacer es comprender el contexto humano, construir relaciones de confianza, interpretar emociones, ejercer criterio ético o inspirar a un equipo. Es precisamente allí donde Gestión Humana adquiere una relevancia aún mayor.

Los profesionales del área ya no son únicamente administradores de procesos. Se convierten en diseñadores de culturas donde personas y tecnología colaboran para generar mejores resultados. Su desafío no consiste solo



Articlista Invitado

Geraldina Guede
Coach de liderazgo y bienestar.
Consultora organizacional
Creadora formadora de formadores



nos hacen profundamente humanos. El liderazgo también cambia. El líder de la era de la IA se convierte en un orquestador: su responsabilidad no es competir con la tecnología, sino integrar sus capacidades con el talento de los equipos. Ya no se espera que tenga todas las respuestas; su principal desafío es formular mejores preguntas, interpretar

la información con criterio y equilibrar eficiencia con empatía, automatización con propósito, datos con juicio humano. Naturalmente, esta evolución trae consigo desafíos. La privacidad de los datos, los sesgos algorítmicos, la transparencia y el uso ético de la IA no son únicamente asuntos tecnológicos; son decisiones de liderazgo y cultura organizacional. La confianza seguirá siendo uno de los activos más valiosos de cualquier organización, y continuará

construyéndose desde las personas. La inteligencia artificial representa una oportunidad extraordinaria para ampliar nuestras capacidades. Puede ayudarnos a ser más ágiles, productivos e informados, pero el propósito, el sentido y la responsabilidad seguirán siendo profundamente humanos. La ventaja competitiva del futuro no pertenecerá a las organizaciones que simplemente adopten más inteligencia artificial, sino a aquellas que desarrollen una mayor inteligencia humana para trabajar junto a ella. Al final, la tecnología no sustituye el talento: lo amplifica.



potenciar el talento humano y construir organizaciones más inteligentes, éticas y humanas? La inteligencia artificial ya forma parte del mundo laboral. Apoya procesos de reclutamiento y selección, personaliza experiencias de aprendizaje, automatiza tareas administrativas y facilita el análisis de grandes volúmenes de información. Su incorporación avanza con rapidez y continuará transformando la forma en que trabajamos. Sin embargo, el verdadero cambio no está ocurriendo en la tecnología, sino en el papel de las personas.

en incorporar nuevas herramientas, sino en garantizar que su uso fortalezca el aprendizaje, el bienestar, la inclusión y la confianza. Esta transformación también redefine las competencias que las organizaciones necesitan desarrollar. El pensamiento crítico, la creatividad, la inteligencia emocional, la adaptabilidad y el aprendizaje continuo dejan de ser habilidades deseables para convertirse en capacidades estratégicas. Paradójicamente, mientras más inteligente se vuelve la tecnología, más valiosas resultan aquellas cualidades que

APOSEC[®]
ASOCIACIÓN COLOMBIANA DE SEGURIDAD



CONGRESO

NACIONAL DE **SEGURIDAD**

Seguridad Privada:
**Orgullo, Fortaleza y
Transformación**

23 24 25
Sept.
2026



**DANN
CARLTON
HOTEL
&
CONVENTION CENTER

BARRANQUILLA**



Inscríbete Aquí

Informes:

1



312 686 4435 - 301 539 7542



asosec@asosec.co

ASIS
INTERNATIONAL
Caribe
Colombia
Chapter



MÁS SEGURIDAD
Magazine



CON SEGURIDAD
Magazine Latam



APOYAN



@asosec.co



@asosec



@asosec.co



asosec asosec

Liderazgo en seguridad



Santiago, Chile- Definiciones de liderazgo encontramos por doquier. Desde el inicio de la historia de la humanidad, las personas que viven y trabajan en comunidad han necesitado de una dirección, un modelo a seguir, una motivación que guíe sus acciones. Lo que distingue a un líder de quien simplemente ocupa un cargo es su capacidad de influir, entusiasmar y generar cambios efectivos —ideas que se repiten en autores como Maxwell, Kotter, Keith Davis y Powell, y que siguen siendo el núcleo de cualquier definición válida de liderazgo.

En el ámbito de la seguridad corporativa, este concepto adquiere una dimensión particular. La gestión de la seguridad es, en ocasiones, percibida como una intrusión o un exceso de control; sin embargo, detrás del éxito organizacional hay siempre una gestión de seguridad proactiva y reactiva que resulta determinante. El líder de seguridad debe ser, por esa razón, omnidireccional: interactúa hacia arriba con la alta dirección, de forma horizontal con pares de otras áreas y hacia abajo con su propio equipo.

En 2026, ese radio se ha complejizado aún más: ciberseguridad, amenazas híbridas y riesgo reputacional obligan a dialogar también con tecnología, áreas legales y comunicaciones estratégicas. El líder que no puede moverse con comodidad en esos espacios tiene un déficit que ninguna experiencia operacional compensa.

La seguridad corporativa ha dejado de ser un campo exclusivo del personal militar o policial. Hoy convergen en ella profesionales de las más diversas disciplinas: derecho, ingeniería, psicología, administración, tecnología. Esa diversidad es una fortaleza, y el liderazgo en seguridad se nutre precisamente de esa pluralidad de miradas. Dicho esto, la formación castrense sigue entregando una base que pocas trayectorias logran replicar: toma de decisiones bajo presión con



información incompleta, planificación con recursos limitados, cultura de rendición de cuentas y el principio que lo sintetiza todo —el ejemplo es la autoridad moral en el ejercicio del mando. Ese principio es tan válido en una sala de directorio como en el campo de operaciones, y quien lo ha internalizado en contextos de alta exigencia llega al mundo corporativo con una ventaja real. La clave está en la adaptación: en la empresa la autoridad no se impone por el rango sino que se construye a través de la influencia y la demostración sostenida de valor. El profesional que comprende eso convierte su formación en un activo irreproducible; el que no lo comprende, en un obstáculo para sí mismo y para su equipo.

Sin embargo, más allá de la experiencia operacional, el profesional de seguridad proveniente de las Fuerzas Armadas debe aprender el lenguaje empresarial —indicadores de gestión, retorno sobre inversión en seguridad, presentación a comités de riesgo— y dominar herramientas que no existen en el mundo militar: plataformas de gestión de incidentes, análisis de fuentes abiertas, comunicación de crisis ante cámaras y directorios. La experiencia en operaciones multinacionales es en este sentido un diferenciador genuino: aporta perspectiva global y

tolerancia a la ambigüedad, atributos que las organizaciones con presencia internacional valoran con claridad creciente.

Pero el liderazgo en seguridad no se agota en la relación con la organización: incluye también la responsabilidad sobre las personas del propio equipo. El personal de seguridad opera en condiciones sin equivalente en otras áreas —turnos nocturnos, jornadas extendidas, exposición sostenida a situaciones de alta tensión— y el burnout es un riesgo real que el líder tiene la obligación de gestionar.

Cuidar al equipo no es una concesión: es la condición del alto desempeño sostenido. El líder que conoce a su gente, anticipa el agotamiento y construye ambientes psicológicamente seguros, construye también la confianza que hace posible todo lo demás. Y en el centro de todo ello está la ética: en un entorno marcado por la desinformación viral y la modernidad líquida, la autoridad moral del líder —su coherencia entre discurso y conducta— se ha convertido en un activo estratégico, no solo en una virtud personal. Mostrar más que demostrar, hacer más que predicar: en 2026 como siempre, el ejemplo sigue siendo la herramienta más poderosa del liderazgo en seguridad.

Más allá de la protección, creamos tranquilidad.

PROTEX
SEGURIDAD 2019, C.A.

¡SOMOS EL ESCUDO
QUE TE PROTEGE!

PROTEX
SEGURIDAD 2013, C.A.



13 años



Nacional



+ 500

¿QUIENES SOMOS?

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

VENECONSULT
GRUPO CONSULTOR INTEGRAL



SERVICIOS QUE OFRECEMOS A NUESTROS CLIENTES EN EL AREA DE CONSULTORÍA

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

@ Veneconsultsr | @Veneconsult

+1 (809) 519 4092

Juancarlos@veneconsult.com

Inteligencia situacional y análisis del entorno político-social para operaciones minero-petroleras.

Las operaciones minero-petroleras se desarrollan en entornos donde la estabilidad del negocio depende tanto de variables geológicas y técnicas como de factores políticos, sociales y territoriales. En ese contexto, la inteligencia situacional no es un recurso accesorio, sino una capacidad estratégica para anticipar riesgos, sostener la continuidad operativa y proteger a diversos activos como las personas, las maquinarias, los inmuebles y la reputación corporativa, entre otros.

La inteligencia situacional como capacidad crítica

La inteligencia situacional consiste en la lectura sistemática, dinámica y contextualizada del entorno para comprender qué ocurre, por qué ocurre y qué podría suceder después. En operaciones extractivas, esta función integra información de comunidades, autoridades, sindicatos, grupos de interés, dinámicas criminales, conflictividad local, marcos regulatorios, percepción pública y señales tempranas de escalamiento social.

Su valor no radica solo en “saber más”, sino en decidir mejor. Una compañía que observa el entorno con rigor puede identificar patrones de tensión antes de que se traduzcan en bloqueos, sabotajes, protestas, ocupaciones, extorsión, interrupciones logísticas o crisis reputacionales. En sectores de alta

exposición territorial, la inteligencia situacional reduce incertidumbre y permite pasar de la reacción improvisada a la gestión anticipada.

Entorno político-social y exposición operativa

El análisis político-social debe partir de una premisa básica: una mina o un campo petrolero no operan en aislamiento. Se insertan en un ecosistema donde convergen intereses económicos, expectativas comunitarias, disputas por recursos, debilidad institucional y, en ocasiones, presencia de actores ilegales o economías informales.

Entre las variables más relevantes destacan:

- Gobernabilidad local y nacional, incluyendo cambios normativos, ciclos electorales y capacidad real de control estatal.
- Relación empresa-comunidad, marcada por confianza, legitimidad,



Alfredo Yuncoza
Presidente de Smart Management C.A.
Presidente del Consejo Consultivo Latino de IFPD.



Articlista Invitado

- memoria de conflictos previos y cumplimiento de compromisos.
- Presencia de actores no estatales, como grupos armados, redes de minería ilegal, estructuras de extorsión o intermediarios coercitivos.
- Fragilidad socioeconómica del área de influencia, donde el empleo, los servicios y la movilidad social influyen en la percepción del proyecto.
- Narrativas públicas y mediáticas, que pueden amplificar incidentes menores y convertirlos en crisis de legitimidad.

Cuando estas variables se combinan, el riesgo deja de ser meramente operativo y adquiere una dimensión estratégica. Un conflicto por agua o





electricidad, por ejemplo, puede escalar desde una queja local hasta una paralización de transporte, una acción judicial, un pronunciamiento político y una campaña digital hostil.

Metodología de análisis

Un sistema sólido de inteligencia situacional para el sector extractivo debe apoyarse en un ciclo continuo de observación, validación, interpretación y difusión. No basta con recolectar datos; es necesario convertirlos en juicio analítico útil y oportuno para la toma de decisiones.

1. Definición del territorio de interés

Se debe delimitar el área operativa real, no solo la geográfica. Esto incluye rutas de acceso, puertos, campamentos, zonas de influencia indirecta, corredores logísticos, asentamientos cercanos y espacios simbólicos de alta sensibilidad social. El entorno de riesgo suele extenderse mucho más allá del perímetro físico del proyecto.

2. Mapeo de actores

La empresa necesita identificar actores, intereses, capacidades de presión, nivel de legitimidad y posibles alianzas. No todos los grupos con presencia territorial tienen el mismo poder de incidencia. Algunos influyen por capacidad de movilización; otros, por cercanía política, control social o acceso a recursos coercitivos.

3. Indicadores de alerta temprana

La vigilancia debe centrarse en señales débiles, tales como incremento de rumores, discursos hostiles en asambleas, cambios bruscos en la relación con líderes locales, aparición de demandas repetitivas, variaciones en

el discurso de autoridades o circulación de convocatorias en redes sociales. La inteligencia útil es la que detecta el patrón antes del incidente.

4. Evaluación de escenarios

El análisis prospectivo permite construir escenarios de corto y mediano plazo: continuidad estable, tensión administrable, escalamiento de conflicto o ruptura operativa. Cada escenario debe asociarse con impactos probables sobre seguridad física, productividad, cadena de suministro, licenciamiento social y protección reputacional.

Riesgos específicos del sector

En operaciones minero-petroleras, los riesgos político-sociales suelen materializarse en formas recurrentes:

La clave está en entender que estos eventos no siempre emergen como amenazas de seguridad convencional. Muchas veces comienzan como reclamos sociales legítimos y evolucionan por fallas de diálogo, respuestas tardías o ausencia de interlocución confiable.

Gestión estratégica del riesgo

La inteligencia situacional debe integrarse al sistema corporativo de gestión de riesgos y no operar como función aislada. Su utilidad aumenta cuando alimenta decisiones de operaciones, relaciones comunitarias, asuntos públicos, legal,

seguridad física, continuidad de negocio y crisis management.

Una práctica madura incluye:

- Protocolos de monitoreo diario y análisis semanal.
- Matrices de riesgo territorial actualizadas.
- Canales formales de enlace con comunidades e instituciones.
- Procedimientos de respuesta escalonada según severidad.
- Simulaciones de crisis política o social.
- Revisión permanente de supuestos estratégicos.

En este marco, la seguridad deja de ser un componente reactivo y se convierte en un habilitador de sostenibilidad operacional.

Conclusión

La inteligencia situacional aplicada al sector minero-petrolero es, en esencia, una disciplina de lectura del contexto para proteger la viabilidad del negocio en territorios complejos. Su verdadero aporte no está en acumular información, sino en transformar señales dispersas en comprensión operativa, anticipación y decisiones más humanas, oportunas y responsables.

En entornos políticamente inestables o socialmente tensionados, comprender el territorio es tan importante como conocer el subsuelo. Y en esa comprensión reside una de las ventajas competitivas más valiosas para cualquier operación extractiva: la capacidad de permanecer, adaptarse y actuar con legitimidad. 

hardtech business impulsa la transición a Smart Cities en Perú

Lima, Perú. – El crecimiento acelerado de las ciudades plantea nuevos desafíos en materia de seguridad ciudadana, movilidad y gestión urbana, impulsando la necesidad de incorporar tecnologías inteligentes y convirtiéndose en una prioridad para las agendas gubernamentales en América Latina. Particularmente, en Perú, la transición hacia entornos urbanos más seguros y eficientes encuentra un respaldo en Hardtech Solutions, compañía con más de 22 años en el mercado peruano, experta en la evolución de la videovigilancia tradicional hacia el ecosistema de las Ciudades Inteligentes (Smart Cities).

En el Perú, Hardtech tiene una operación de alcance nacional, ha consolidado su liderazgo gracias a su especialización en el diseño e implementación de centrales de monitoreo e infraestructura crítica para seguridad ciudadana. Su experiencia en el sector público y privado la posiciona como un actor estratégico en la mitigación del delito y la mejora de la gestión urbana.

Pioneros en seguridad pública e integración tecnológica

Según explicó Jhosep Becerra Pisco, director de proyectos de Hardtech Solutions, entrevistado en el marco de Securitec Perú 2026, la firma es pionera en proyectos de seguridad ciudadana que a la fecha incluyen plataformas integrales de protección urbana. "Nuestras soluciones más grandes y representativas están en el área de seguridad ciudadana. Somos especialistas en el diseño y ejecución de proyectos de manera ininterrumpida desde 2014", señaló el directivo.

Desde hace más de una década, cuando la videovigilancia urbana aún se encontraba en etapas tempranas de adopción en la región, Hardtech Solutions ya elaboraba proyectos complejos que integraban cámaras de alta definición, analíticas de video, sistemas de

radiocomunicación robustos y software de gestión, unificados en centrales de monitoreo de última generación. Esta visión integral permite a los tomadores de decisiones y a los cuerpos policiales coordinar respuestas operativas en tiempo real con altos niveles de eficiencia.

Flexibilidad multimarca y la transición hacia el ecosistema IoT

Uno de los pilares del éxito de Hardtech es su capacidad para

Actualmente, la principal vertical de negocio de la compañía, que sigue siendo la seguridad ciudadana, experimenta una migración orgánica hacia el concepto de Smart City. Este paso implica que las cámaras de seguridad ya no operan de forma aislada, sino que se integran con sensores de Internet de las Cosas (IoT), con sistemas automatizados de semafización y plataformas de gestión de movilidad urbana. El resultado es una red de infraestructura capaz de generar información en tiempo real que permite

la toma de decisiones para mitigar la criminalidad, lograr un desarrollo vial ordenado y una correcta gestión ambiental.

El impacto de la empresa se refleja en el volumen y la complejidad de sus obras. Anualmente, la firma ejecuta entre cuatro y cinco megaproyectos de seguridad ciudadana que demandan un despliegue masivo tanto de obra civil como una importante infraestructura de comunicaciones, y dependiendo de la envergadura y la geografía del lugar, estos desarrollos conllevan periodos de implementación de entre cuatro y siete meses.

Aunque el mercado peruano es su principal prioridad, Hardtech ya proyecta su siguiente etapa de crecimiento con una visión regional. "Nuestro compromiso sigue siendo desarrollar soluciones tecnológicas que fortalezcan la

seguridad ciudadana y la transformación digital del Perú. Sin embargo, el siguiente paso es llevar esa experiencia a otros mercados de Latinoamérica. Colombia y Brasil representan destinos estratégicos para nuestra expansión, por su dinamismo, sus desafíos en materia de seguridad y la oportunidad de aportar soluciones tecnológicas que ya han demostrado resultados exitosos. Estamos convencidos de que la innovación desarrollada en el Perú tiene el potencial de convertirse en un referente para la región", concluyó Becerra.



trabajar bajo demanda, adaptándose a los requerimientos técnicos de cada proyecto. Su experiencia les permite tener un portafolio de alianzas con los mayores fabricantes del sector y trabajando bajo estándares internacionales. De este modo, la empresa integra de forma nativa tecnologías de fabricantes globales como Hikvision, Dahua, Hytera, Dell o Motorola, entre otros. "Trabajamos bajo demanda, la experiencia nos ha permitido manejar e integrar un amplísimo catálogo de marcas, siempre bajo estándares internacionales", subrayó Jhosep Becerra.



TU OPERACIÓN LOGÍSTICA SIEMPRE PROTEGIDA



GPS & RASTREO

Flota · Activos · Carga



VIDEO TELEMÁTICA

IA embarcada · Eventos



DIAGNÓSTICO SCS

OEA · C-TPAT · BASC



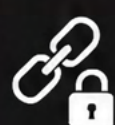
ANGEL GUARDIAN

Control IA/RFID



FLEETCONTROL PRO

Gestión de flota



PREVENCIÓN DE PÉRDIDAS

Robo · Fraude · Merma

OEA**C-TPAT****ISO 28000****BASC****+ 30 AÑOS**

De experiencia

+ 50,000 EQUIPOS GPS

Activos

4 PAÍSES

Méx · Col · EUA · Arg

24/7/365

Sin interrupciones

 contacto@reconsultores.com +52 55 8650 9325**www.recsafe.tech**

El enfoque real de la Seguridad Ciudadana: Reto de la



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

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

Una solución social para una geografía compleja

En entrevista para Más Seguridad Magazine, Carlos Miguel Pérez Chávez, dijo que el núcleo metodológico de la ANCSCI radica en el análisis avanzado de la gestión de riesgos, abarcando desde entornos sensibles como la seguridad escolar hasta los riesgos cotidianos que enfrenta el ciudadano común. Sin embargo, su principal factor diferenciador es el

diagnóstico. Como aseveró Carlos Pérez, el liderazgo, la criminalidad y la vulnerabilidad no se pueden resolver únicamente con el despliegue de fuerzas del orden, se requiere una solución de corte social y sociológico.

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

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

Ante esta realidad, la internacionalización y las alianzas estratégicas son fundamentales. A través de la red internacional de ANCSI, la organización mantiene lazos y representantes en Argentina, Brasil, Bolivia, Ecuador, Colombia, Panamá, México, Estados Unidos, España y Alemania. No obstante,

Carlos Pérez enfatizó que Perú, Colombia y Ecuador comparten una matriz de seguridad ciudadana muy similar, marcando una clara distancia técnica con los modelos de Chile, Bolivia, Brasil o Argentina, cuyas realidades institucionales y criminológicas corren por carriles distintos.

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

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



Carlos Miguel Pérez Chávez,
Presidente de ANCSCI

Ya está en México

Alianza internacional:



MÁS SEGURIDAD
Magazine

CON SEGURIDAD
Magazine Latam



- 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 811 #74C-19 OF. 202 - BOGOTÁ, COLOMBIA



RocketGO
Academy

educación que potencia conocimientos

conocimientos en capacidades para
América Latina

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

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

Su mayor fortaleza en el sector de

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

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

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

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

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

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

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

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

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



Leonardo Garcés
(Colombia), directivo de
RocketGo



Rodolfo Cepeda
(México), directivo
de RocketGo



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



Articlista invitado

Francisco Javier González Fuentes

Presidente de FIBSEM - Foro Iberoamericano de Seguridad y Emergencias



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.

asociación
adisp
directores seguridad

IBEROSEC

CERTIFICACIÓN OFICIAL IBEROAMERICANA
EN SEGURIDAD Y EMERGENCIAS

CON EL AVAL INTERNACIONAL DE

BUREAU VERITAS

RIGOR • INDEPENDENCIA • RECONOCIMIENTO GLOBAL

RECONOCIMIENTO
INTERNACIONAL

ESTÁNDARES
GLOBALES

COMPETENCIAS
ACREDITADAS

RED IBEROAMERICANA
DE PROFESIONALES

MEJORA TU
EMPLEABILIDAD

ÁREAS DE CERTIFICACIÓN

SEGURIDAD
CORPORATIVA

SEGURIDAD
INTEGRAL

CIBERSEGURIDAD

EMERGENCIAS

INTELIGENCIA

PROTECCIÓN
CONTRA INCENDIOS

PREVENCIÓN
DE RIESGOS

TU COMPETENCIA.
TU VALOR.
TU CERTIFICACIÓN.
— IBEROSEC —

SÉ PARTE DEL ESTÁNDAR
QUE IMPULSA AL SECTOR

CERTIFICATE AHORA

www.fibsem.pro

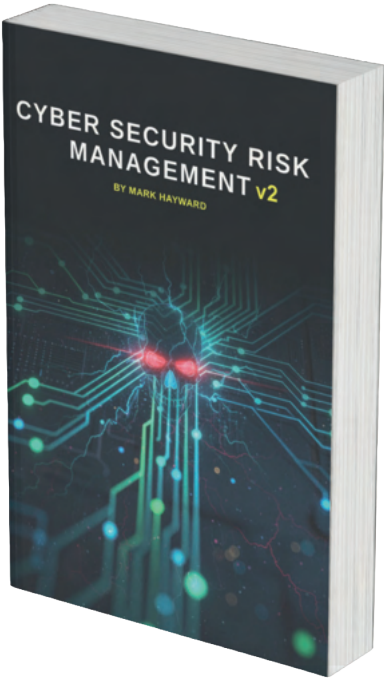
PROFESIONALIZA TU FUTURO. TRANSFORMA TU EXPERIENCIA EN RECONOCIMIENTO GLOBAL.

Agosto - Septiembre 2026 / 41

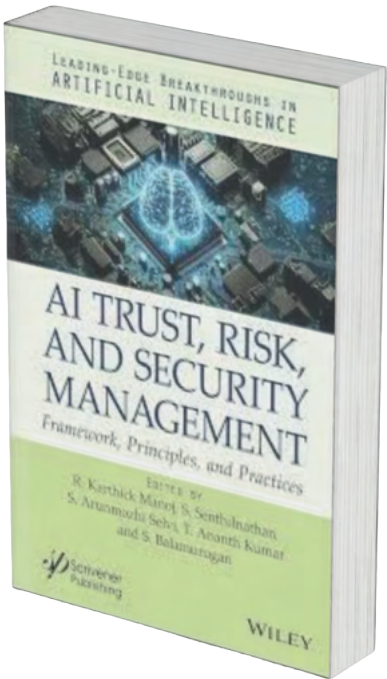
Cyber Security Risk Management v2

Edición: Versión 2 (v2)
Año de publicación: 2026
Autor: Mark Hayward
Editorial: AutomateEd Publishing
(plataforma AutomateEd)

Presenta una guía clara y ordenada para entender y manejar los riesgos de ciberseguridad, enlazando los principales conceptos con marcos reconocidos como NIST e ISO. Pone énfasis en identificar activos esenciales, establecer prioridades frente a amenazas y desarrollar controles efectivos, articulando la relación entre la gestión de riesgos corporativos y la gobernanza de tecnologías de la información.



AI Trust, Risk, and Security Management



Edición: Primera
Año de publicación: 2026
Autor: Obra colectiva; algunos capítulos clave son de Paolo Dal Cin, Daniel Kendzior, Yusof Seedat, Renato Marinho, Cindy Green-Ortiz, Zig Zsiga, Saskia Laura Schröer, Karen Renaud, Merrill Warkentin, George Westerman, entre otros.
Editorial: : John Wiley & Sons, Inc., en coedición con Scrivener Publishing LLC

Explora cómo gestionar la confianza, el riesgo y la seguridad en sistemas de inteligencia artificial. Analiza los principios de Zero Trust aplicados a la IA y examina cómo las amenazas derivadas de modelos generativos pueden afectar estos sistemas. Está dirigido especialmente a consultores y CISOs encargados de incorporar la seguridad de la IA en los esquemas de gobernanza, cumplimiento y gestión de riesgos de las organizaciones.



CAPÍTULO
MÉXICO 217

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



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.

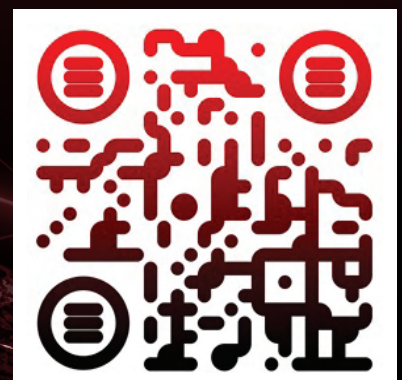
INCLUIDO EN TU MEMBRESÍA ASIS



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

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

¿Qué esperas?



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

