

# MÁS SEGURIDAD

Magazine

**HIKVISION®**

## Safe City



**Seguridad Inteligente, Ciudades Seguras**

Hikvision revoluciona la seguridad urbana con soluciones innovadoras.

Edición 158 | Año 18 | octubre 2025



México y Latam / precio \$60.00MX







# FORO INTERNACIONAL DE SEGURIDAD Y FACTORES HUMANOS

## CAMBIO DE PARADIGMAS

UNA PERSPECTIVA  
DIFERENTE SOBRE LAS  
LESIONES LABORALES



13-14 DE NOVIEMBRE 25

CIUDAD DE MÉXICO  
HOTEL HILTON SANTA FE

**¡No te lo pierdas!**

ORGANIZADO POR



APOYO:



prevencionar.com.mx  
lo primero, tu seguridad



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

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

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

DG DESING  
DISEÑO Y DESARROLLO VISUAL

TERESA RAMÍREZ OJEDA  
INFORMACIÓN  
redaccion@revistamasseguridad.com.mx

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

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

CARMEN CHAMORRO  
CORRESPONSAL ESPAÑA  
corresponsal@globaldefense.com.mx

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

JORGE MERCADO ABONCE  
SERVICIOS JURÍDICOS INTEGRALES  
ANAZALDO-MARTÍNEZ-MERCADO  
DIRECCIÓN JURÍDICA  
juridico@revistamasseguridad.com.mx

ASISTENCIA A CLIENTES  
atencion@revistamasseguridad.com.mx

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

SIGUENOS EN:

-  Revista más seguridad
-  @revmasseguridad
-  revistamasseguridad
-  Revista más seguridad
-  @revmasseguridad
-  Revista más seguridad

Revista Más Seguridad Año 18, No 158, octubre 2025, Publicación mensual de Grupo Editorial MS Global S. de R.L. de C.V., con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 5555272279 / +52 5528732719. Editor responsable: Humberto Mejía Hernández. Certificado de Reserva 04-2022-050614181900-102 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No. 11483 y Certificado de Licitud de Título No. 13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: Grupo Mejía Impresores, calle La Poza No. 72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel: +52 5518947067.

## Seguridad ciudadana con avanzada tecnología

Un “C5” se refiere al Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano, un espacio gubernamental que monitorea cámaras de videovigilancia urbana y coordina servicios de emergencia como seguridad ciudadana, atención médica, protección civil y medio ambiente. Opera el número de emergencias 911, gestiona la alerta sísmica y utiliza aplicaciones para recibir reportes y enviar unidades de respuesta; pero para hacer posible esto, la tecnología juega un papel preponderante para hacer posible toda esta convergencia. Hoy internacionales y grandes fabricantes, así como mayoristas e integradores son parte del engranaje de estos sitios que han salvado en el mundo miles de vidas humanas.

Las funciones principales del C5 son monitoreo y videovigilancia urbana, coordinación de emergencias, pues funciona como el centro neurálgico para atención de emergencias médicas, incidentes de seguridad, protección civil y otros servicios esenciales; atención ciudadana como entidad encargada de recibir y gestionar llamadas de emergencia a través de líneas 911 y 089 (denuncias anónimas); gestión de incidentes para rastreo de vehículos involucrados, guía a los agentes y coordina a los cuerpos de emergencia (policía, bomberos, ambulancias) en la atención de los reportes, así como alerta y prevención para emitir la alerta sísmica y colabora con diversas instituciones para mejorar la seguridad pública y el bienestar ciudadano.

Destacadas marcas de seguridad electrónica, telecomunicaciones, radiocomunicación y telemetría; entre otros, procedentes de Estados Unidos, Asia o Europa mantienen en México y América Latina un importante core de negocios con los C5 y C5i a través de una amplia o profesional red de mayoristas, integradores e instaladores con modernos e imponentes desarrollos, que incluso éstos han sido premiados a nivel internacional en ferias de seguridad electrónica, cómputo o comunicaciones.

A nivel internacional ya no es raro ubicar C2, C4, C5 y C5i de niveles municipales y estatales que mantienen comunicación estrecha y directa con sus gobiernos nacionales. México no es ajeno a esta tendencia.

En nuestro país, hace dos décadas fue creada la asociación civil mexicana para representar oficialmente a la National Emergency Number Association (NENA 9-1-1) y se ha destacado como un organismo especializado en la gestión de los Centros de Atención de Emergencias Latinoamérica. Su actividad se centra en la oferta de cursos y capacitación, así como la certificación del personal e instituciones.

Desde hace más de 2 lustros en México, NENA 911 reúne a líderes de cada entidad de nuestro país y Latinoamérica que dirigen, administran, coordinan y operan Centros de Atención de Llamadas de Emergencia; ello ha contribuido en la formación de profesionales que gestionan llamadas de emergencias, así como con la creación de estándares y certificación de procesos para la atención de emergencias.

Desde 2009 esta organización tiene presencia en varios países de Latinoamérica con más de 100 instructores certificados bajo los estándares de NENA 9-1-1 Internacional. Además, realiza un congreso anual internacional donde fabricantes exponen sus innovaciones en la materia y expertos comparten casos de éxito y tenencias mundiales en situaciones de emergencias, ya sean de tipo social, industrial o natural.

Sin duda, la tecnología es el eslabón mas fuerte en todos los Centros de Atención de Llamadas de Emergencia, ya sea a través de videovigilancia urbana, botones de pánico, líneas telefónicas convencionales o celulares, el posicionamiento GPS, la telemetría o la radiocomunicación, sin olvidar el talento humano que está detrás de cada línea o monitor dando seguimiento a un incidente. 



# Los Profesionales de LatAm

Jaime Iván Ortega González



Oficial superior de Inteligencia de la Escuela Superior de Guerra del Comando General de las Fuerzas Militares de Colombia.  
Más de 21 años de experiencia cooperando con organizaciones internacionales vs crimen y terrorismo, contribuyendo a dismantelar redes internacionales involucradas en el lavado de activos y financiación al terrorismo, tráfico ilícito de medicamentos y narcotráfico.  
Analista internacional de riesgos, contextos, prospectiva y experto investigador de campo.  
Security Risk Prevention  
Auditor Líder OEA HSE ISO 28000 – 31000 – 14001  
Magister Ciberseguridad y Ciberdefensa  
Magister en Inteligencia Estratégica  
Jurado Maestría y Asesor Académico superior 

• Escucha 



NUESTRO

PODCAST

a través de Spotify





- 6** Altronix exhibe novedades para LatAm en ESS+ 2025
- 7** Ajax presentó soluciones contra intrusiones, incendios y videovigilancia
- 9** Autonomous Management Framework (AMF) Plus de Allied Telesis

**Tecnología, IA y ciberseguridad redefinen el control perimetral y de accesos en LatAm**



- 16** Nuevo lector de reconocimiento facial HID Amico
- 27** Celebra Control Seguridad Integral 25 años de existencia

**Tecnología y seguridad para C4 y C5 de México**



- 42** ESS+ 2025 se consolidó con la edición 31



## Homicidio en CCH Sur: C5 aclara llamada de la madre del asesino

El reciente caso alarmante e indignante del homicidio de un joven estudiante del CCH Sur ha generado diversas versiones y polémicas en las redes sociales. A raíz de la difusión de información que sugería que la madre de Lex Ashton N, el psicópata asesino, alertó al 911 sobre las intenciones de su hijo, desmintió esta versión y detalló que la mujer llamó para reportar la ausencia del joven de 19 años. También, dijo que en su habitación faltaban algunos objetos. El C5 ha reforzado su compromiso con la transparencia en la información. Nunca alertó al operador sobre las intenciones asesinas de su vástago.

**Sucesos en CCH Sur:** El lunes 22 de septiembre de 2025, en el estacionamiento del Colegio de Ciencias y Humanidades (CCH) ubicado en la colonia Jardines del Pedregal, alcaldía Coyoacán, Lex Ashton N, de 19 años, asesinó con una guadaña a su compañero Jesús Israel N, de 16. La agresión dejó un empleado de la institución educativa herido. Al tratar de escapar, el presunto responsable se lanzó de un segundo piso y también resultó herido.

Al cierre de edición de Más Seguridad Magazine, el sospechoso seguía hospitalizado bajo custodia. Este lamentable suceso ha puesto en el debate público la seguridad en los centros educativos públicos y la salud mental de determinados jóvenes que sin filtro alguno son aceptados en estos centros de enseñanza. “Estos casos solo se veían en escuelas de EE.UU. o Europa, hoy en México hay que anticiparnos al delito”, señalan expertos.

**C5 se deslinda:** El C5 aseguró que, de acuerdo con el protocolo de atención de y los operadores de la línea de emergencias, la llamada fue registrada y canalizada al área de despacho de la Secretaría de Seguridad Ciudadana (SSC) para su atención inmediata. “Desde el primer momento se actuó en coordinación con las autoridades correspondientes”, indicó el C5 a través de una tarjeta informativa. El personal operativo actuó de acuerdo con los lineamientos de atención ante reportes de emergencia, lo que subraya la importancia de seguir los protocolos establecidos para estos casos; es decir, no hubo error u omisión por parte del operador que tomó la llamada. Simple.

**Colaboración:** El C5 colabora activamente con la Fiscalía General de Justicia (FGJ) de la Ciudad de México en las investigaciones y proporciona información obtenida por las cámaras de videovigilancia y los sistemas de coordinación de emergencias. Los datos y videos del C5 son cruciales para esclarecer los hechos y determinar las responsabilidades. El compromiso de las autoridades es total en este lamentable suceso, el cual ha conmocionado a la comunidad escolar y a la sociedad mexicana.

**Proceso judicial:** Lex Ashton N, presunto responsable permanece hospitalizado bajo custodia, lo que significa que enfrenta cargos penales por los delitos de homicidio y lesiones. El proceso judicial será largo y complejo como casi todos los que ocurren en México; sin embargo, el caso CCH Sur ha puesto de manifiesto la necesidad de fortalecer los mecanismos de prevención de la violencia en las escuelas y de prestar mayor atención a las señales de alerta de los jóvenes. Expertos en seguridad corporativa, salud mental y hasta sociólogos, coinciden y consideran que este tipo de tragedias se pueden prevenir si autoridades, escuelas y padres trabajan en conjunto. Cierro: “después del niño ahogado...”

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

Tour Internacional 2025

**MÁS SEGURIDAD**  
Magazine

**NENA**  
THE  
**9-1-1**  
ASSOCIATION  
**MEXICO**

**EXPO**  
**SEGURIDAD**  
& **TELECOM**  
COSTA RICA

**Expodefensa 2025**  
Feria Internacional de Defensa y Seguridad  
International Defense and Security Trade Fair

**FORO INTERNACIONAL**  
**DE SEGURIDAD Y**  
**FACTORES**  
**HUMANOS**

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





# presentó recientes lanzamientos para la protección contra intrusiones

videovigilancia, protección contra incendios, confort y automatización.

**Bogotá, Colombia.-** Ajax, fabricante europeo de sistemas inteligentes y profesionales de seguridad, presentó sus soluciones en intrusión, protección contra incendios, comunicación y videovigilancia para los mercados residencial y de negocios para América Latina

“En el marco de la Feria Internacional de Seguridad ESS+ 2025, en entrevista con Más Seguridad Magazine, Felipe Hoyos, Director Técnico de Ajax para Latinoamérica, destacó que la compañía cuenta con un departamento específico que cada trimestre se encarga de lanzar novedades y actualizaciones de sus productos y soluciones que están en el mercado.

“Nuestro objetivo es garantizar la privacidad de los usuarios. Es el usuario final quien decide qué empresa, instalador o persona autorizada puede acceder a las imágenes, grabaciones o al control de las cámaras PTZ, y bajo qué condiciones. Además, define cómo actuar ante una confirmación de alarma. De esta forma, Ajax no solo ofrece soluciones en intrusión, automatización, confort e incendios, sino también un completo portafolio en videovigilancia que respalda la seguridad integral del cliente”, afirmó Felipe Hoyos.

En intrusión, la empresa exhibió un nuevo panel de alarma diseñado para instalaciones que están desatendidas como por ejemplo un rancho, una finca o una infraestructura en donde no hay conectividad a nivel de Ethernet y demanda de autonomía con las baterías de Ajax y la posibilidad de extender la cobertura con antenas externas.

También presentó un nuevo sensor de cortina para exterior, con doble infrarrojo pasivo, microondas, banda K y antimasking y que cuenta con una detección antisabotaje por acelerómetro.

Además, exhibió su portafolio de sensores de incendios que pueden ser desde subida repentina de temperatura, detección de humo o monóxido de carbono, para cualquier tipo de instalación a nivel profesional y también con estaciones manuales. En protección contra incendios estos dispositivos están interconectados a los hubs de Ajax, que son un “cerebro” con diferentes posibilidades tanto manuales, a nivel de aplicación o botones y de forma automatizada.

“Cada panel que tiene Ajax o hub permite escenarios de automatización, temperatura, programación horaria, confirmación de alarma o el cambio del modo de seguridad del panel”, aseguró Felipe Hoyos.

Ajax dio a conocer apagadores o interruptores, que se controlan vía inalámbrica desde cualquier parte y que poseen múltiples características para aprovechar de mejor manera el sistema de alarma. Así como las electroválvulas Water Stop, 100% inalámbricas para control de riesgos que permiten cerrar de forma remota el suministro de agua en la estancia protegida por el sistema de seguridad Ajax.

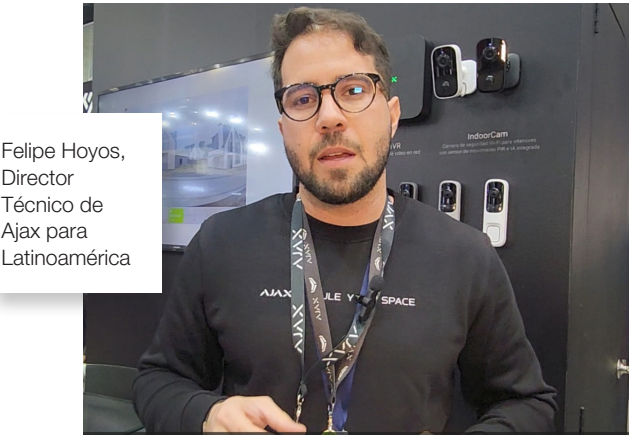
En sistemas de comunicación e intrusión, dio a conocer el SpeakerPhone Jeweller, que permite una comunicación bidireccional con la instalación, protección anti sabotaje avanzada y se puede conectar el panel de alarma con un conmutador que permite hacer audio verificación en el lugar donde está sucediendo el evento.

• Ajax Systems, fabricante de soluciones inteligentes de seguridad y automatización, presentó en la Feria ESS+ 2025 sus últimos lanzamientos e innovaciones en intrusión, videovigilancia, detección de incendios y automatización, dirigidas al mercado residencial y empresarial de América Latina.



Finalmente, en el área de videovigilancia, Ajax presentó dos innovaciones para ampliar su portafolio de CCTV. La primera es un doorbell inteligente, disponible en cuatro colores, que integra dos funciones en un solo dispositivo: por un lado, una cámara de 4 megapíxeles con ángulo de visión de 110° y batería con autonomía de hasta dos horas; y por otro, la capacidad de convertirse en un sensor de movimiento, que se conecta al panel de alarma incluso cuando se pierde la señal de Wi-Fi.

El otro lanzamiento es la Ajax IndoorCam, una cámara de seguridad Wi-Fi para interiores con sensor de movimiento PIR e IA integrada, con conexión inalámbrica y con una resolución de 4 megapíxeles para aquellas instalaciones en donde se requiere una instalación más práctica sin cableado.



Felipe Hoyos,  
Director  
Técnico de  
Ajax para  
Latinoamérica



# exhibe novedades para LatAm en ESS+ 2025

**Bogotá, Colombia.-** Altronix —fabricante de soluciones de transmisión de energía y datos— estuvo presente en la Feria Internacional de Seguridad 2025 ESS+ con la demostración de su línea de productos, que incluyen cargadores de baterías, convertidores de medio, transmisores de video, adaptadores y soluciones de comunicación en red para sistemas de seguridad, control de acceso, videovigilancia y detección de incendios.

Ronnie Pennington, Director de Ventas para las Américas en Altronix, indicó a Más Seguridad Magazine que la compañía, con sede en Estados Unidos, tiene más de 40 años y cuenta con un departamento de más de 3 mil productos de alta calidad, lo cual le permite a la firma ofrecer garantía de por vida, y ese valor es su principal diferenciador en el mercado.

“Somos hechos en Estados Unidos, usamos componentes de buena calidad por eso podemos ofrecer garantía de por vida, no somos el más barato ni el más costoso, somos competitivos. El mercado confía en Altronix como empresa con equipos de buena calidad y nuestros clientes son atendidos directamente por personas, respondemos correos y contamos con un chat en la página web para hablar sobre nuestro portafolio de productos”, explicó Pennington.

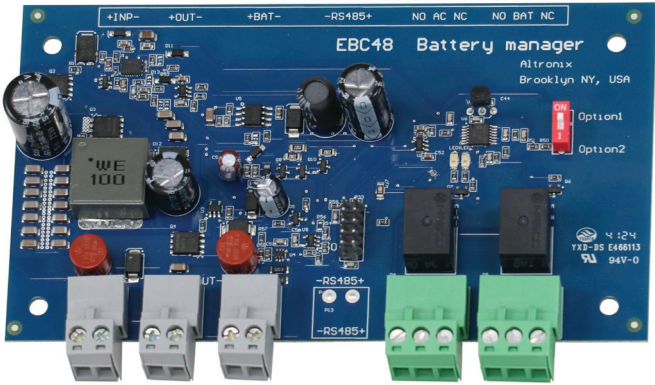
En la Feria Internacional de Seguridad ESS+ 2025, Altronix presentó desarrollos nuevos como: el EBC48, un cargador de batería rápido externo que permite una carga de 16 horas y es ideal para aplicaciones en donde no se dispone de alimentación constante; el NetWay5PQ, un conmutador PoE+ compacto, reforzado y gestionado por red, que conecta directamente al puerto de gestión y cuenta con cuatro salidas de puertos.

También el NetWaySP2BT, un convertidor de medios de fibra a Ethernet que proporciona hasta 180W de potencia a dos dispositivos mediante puertos 802.3bt (4PPoE), y adaptadores como el Pace1STR, un kit adaptador Ethernet de largo alcance diseñado para extender la transmisión de datos y la alimentación a dispositivos IP.

Además, la compañía exhibió nuevas versiones de soluciones existentes como: el PACE1KRT, un kit adaptador Ethernet de largo alcance que transmite datos y alimentación mediante par trenzado en formato compatible con PoE (+); la Serie Trove, una solución de integración de alimentación y control de acceso en un cajón de rack; y la Serie NetWay Spectrum, el gabinete más grande con el que cuenta la empresa y es una solución para desplegar dispositivos de red usando fibra y energía PoE, además recientemente se le agregó otra tarjeta para cuenta con el respaldo de baterías de largo alcance.

Ronnie Pennington aseguró que todas las soluciones de Altronix son compatibles con las principales marcas de control de accesos, videovigilancia, control de incendios y alarmas, incluidas las de origen chino o japonés, países a donde también surte producto.

Todas las soluciones ya están disponibles a nivel mundial y para América Latina a través de distribuidores, desde México hasta Argentina. Específicamente en Colombia, Altronix vende a través de empresas como: SYSCOM, ISTC, Full Protection, Sac Seguridad, Anixter, Silmar, entre otras.



- La empresa tiene más de 40 años, cuenta con un departamento de más de 3 mil productos de alta calidad, con garantía de por vida.
- Exhibió los novedosos productos EBC48, NetWay5PQ, NetWaySP2BT y Pace1STR

Para Altronix, las verticales que son el core de su negocio son control de accesos y videovigilancia. Por volumen, México es la región más importante y la más grande de todas, le siguen República Dominicana, Panamá, Costa Rica, Colombia, Perú y el Caribe con Trinidad y Tobago, Puerto Rico. Chile y Argentina están creciendo constantemente.

El objetivo de Altronix es que sus distribuidores mantengan un stock importante en el país de venta a fin de que puedan despachar un producto en un lapso de entre cinco a 10 días, dependiendo de la cantidad y el tipo de producto. Cabe destacar, que en el mercado de control de accesos, la empresa trabaja con más de 65 socios.

Ronnie Pennington concluyó que Altronix actualmente trabaja en un nuevo proyecto que va a modificar la forma en cómo se hace la instalación de un control de acceso, y afirmó: “Siempre estamos enfocados a los diferentes mercados y aplicaciones. No hay una empresa como Altronix en el mundo, nos enfocamos en fuente de poder para control de accesos, videovigilancia, incendios, alarmas y seguridad”.

Más información: [info@altronix.com](mailto:info@altronix.com)



Ronnie Pennington,  
Director de Ventas para  
las Américas en Altronix



# IDIS<sup>®</sup> presenta en ESS+ 2025 su portafolio de soluciones



**Bogotá, Colombia.-** IDIS, fabricante surcoreano de sistemas de videovigilancia y seguridad, presentó en la Feria Internacional de Seguridad (ESS+) 2025 su línea IDIS AI, que abarca diferentes soluciones de seguridad integral desde cámaras con inteligencia artificial (IA) embebida, equipos de reconocimiento facial, servidores y dispositivos de videovigilancia NVR (Network Video Recorder).

En entrevista para Más Seguridad, Víctor Merino, director regional para IDIS en Latinoamérica, indicó que IDIS tiene casi 30 años en el mercado y originalmente habían estado enfocados en ser fabricantes OEM y SDM, pero hasta hace algunos años decidieron lanzar su marca de forma directa, por lo que, dijo, los productos son nuevos, basados en tecnologías recientes como la inteligencia artificial, NDAA Compliance y muy amigables en el entorno de Ciberseguridad.

“Hay mucha tecnología en el ámbito de la ciberseguridad, ese es el gran factor diferenciador de nuestra marca, la oferta es muy grande, tenemos cámaras de distintos tamaños, modelos y formas, y eso nos permite ser muy flexibles en distintos casos de usos”, explicó Víctor Merino.

En el stand de BTCO —su distribuidor autorizado para la región de Sudamérica— IDIS dio a conocer sus cámaras de seguridad 360 con IA, con protocolos muy seguros y en las que se pueden “correr” aproximadamente 40 algoritmos diferentes de inteligencia artificial; así como servidores para aplicaciones más robustas; y NVR muy competitivos de 8, 16 y 64 canales.

“Otro diferenciador de nuestros productos es la parte técnica, lo robusto que somos en el ambiente de ciberseguridad, cada NVR tiene su propio firewall, eso no es muy común en la industria, y nos da un posicionamiento muy fuerte en instalaciones grandes. Hoy todo corre en la red, de alguna forma estas cajas son muy robustas”, señaló.

Víctor Merino, aseguró que la línea ADIS se ha posicionado fuertemente en el sector bancario en América Latina, aunque

precisó que las soluciones tecnológicas se adecúan a muchas verticales.

Reconoció que, a diferencia de otros países de Latinoamérica, el mercado mexicano tiene diferentes requerimientos en materia de seguridad bancaria con los cuales cumplen, pero que todavía no han atacado de forma efectiva.

“Estamos en esa estrategia, cumplimos 100% con Seproban (Seguridad y Protección Bancaria), y estamos en conversaciones con un banco transnacional muy grande, donde estamos próximos para poder lograr el sponsor para poder venderla (la tecnología) abiertamente en el mercado como Seproban lo exige. México también es a través de distribución, estamos en conversaciones con algunos distribuidores para tener un mejor posicionamiento de la marca”, concluyó Víctor Merino.



Víctor Merino, director regional para IDIS en Latinoamérica

# Poderoso sistema

## Autonomous Management Framework (AMF) Plus de



**Bogotá, Colombia.-** En la Feria Internacional de Seguridad ESS+ 2025, Allied Telesis —fabricante japonés con presencia en más de 100 países— presentó su sistema de administración, virtualización y automatización de datos denominado Autonomous Management Framework (AMF) Plus, el cual también se puede aplicar a la vertical de videovigilancia.

Henry Hernández, Director Regional de Allied Telesis para el Norte de Sudamérica, indicó a Más Seguridad Magazine, que la compañía se caracteriza porque acompaña a los integradores y a su canal de distribución a desarrollar productos y proyectos con el objetivo de hacerles más fácil el desarrollo, implementación, así como el mantenimiento preventivo y correctivo.

“Somos una compañía que está trabajando de la mano con sus integradores y distribuidores, estamos generando demanda en el usuario final, el mejor marketing que tenemos en estos momentos es el usuario final, y es lo que nos está haciendo crecer y cerrar cada vez más negocios”, afirmó Henry Hernández.



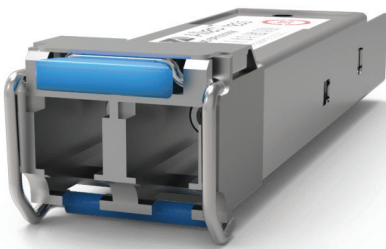
Además, aseguró que cada año la firma presenta nuevos lanzamientos de productos y es propietaria de la tecnología, “no dependemos de terceros, ni en hardware ni en software, el 18% del revenue que tiene la empresa está dedicado al departamento de investigación y desarrollo”, desglosó.

El sistema Autonomous Management Framework (AMF) Plus automatiza las tareas de administración de la red como respaldos, recuperación y aprovisionamiento. La empresa desarrolló este producto en 2017, ya está disponible en el mercado de América Latina y no es exclusivo para videovigilancia, ya que también se puede aplicar en voz y datos, y redes corporativas.

Henry Hernández señaló que el AMF está desarrollado para la gestión, monitoreo y visualización con otros productos de otras marcas, pero aclaró que sólo se va a poder automatizar o virtualizar con equipos de sus propias marcas.

El objetivo de Allied Telesis es diseñar cada vez más producto, pero más que a nivel de hardware, busca que

• La empresa es desarrolladora y propietaria de su tecnología, tanto en hardware como en software, y el 18% del revenue del negocio lo destina al departamento de investigación y desarrollo.



sea todo lo intangible. Recientemente, la empresa lanzó la familia IGS950, una serie de switches de red con capacidad de Power over Ethernet (PoE+).

“Entregamos en las manos del usuario final una herramienta que le haga la vida más fácil en el mantenimiento preventivo y correctivo, que ahorre tiempo y dinero y que pueda dedicar más tiempo a otras labores de su empresa”, concluyó Henry Hernández.



Henry Hernández,  
Director  
Regional de  
Allied Telesis





**¡Aún estás a tiempo!**

Certifícate antes de fin de año y abre nuevas oportunidades

**OCT**

28 - 31



Gerencia de  
Proyectos

**NOV**

25 - 28



Video  
Vigilancia

**DIC**

9 - 12



Operadores  
de Cuartos  
de Control

Si eres **Socio ASIS**, obtendrás **puntos CPEs** en esta actividad



**CRISTIAN MOLINA**

Coordinador de Cursos

Whatsapp:

+57 321 6153367



ASOCIACIÓN  
LATINOAMERICANA  
DE SEGURIDAD



# Presenta LiDar RLS-50100 Pro™ y sistema DAS “EchoPoint™

**Bogotá, Colombia.-** Optex —fabricante especialista en soluciones de detección de seguridad mediante tecnología de detección láser, pasiva e infrarroja activa— dio a conocer en la Feria de Seguridad ESS+ 2025, el sensor LiDar, uno de los más nuevos de su portafolio de productos para detección de intrusiones, y el sistema de fibra óptica EchoPoint.

En entrevista con Hans Klein, presidente en Latinoamérica de Optex, destacó que todos los productos presentados en la Feria de Seguridad ESS+ 2025 ya están disponibles en mercado latinoamericano y son fabricados en Japón y EE.UU.

“Hasta hace pocos meses nuestro hub fue Estados Unidos, pero debido a las tarifas que este país impuso, ahora ofrecemos soluciones directo a cliente, quien puede importar directamente desde Japón, con lo cual se evita tarifas más altas del mercado estadounidense”, explicó Hans Klein.

A parte de los sensores reconocidos con tecnología PIR,

- La empresa lanzó el sensor LiDar, un dispositivo láser sofisticado que cubre una zona de hasta 100 metros, y el sistema de fibra óptica EchoPoint, sensores acústicos distribuidos (DAS).



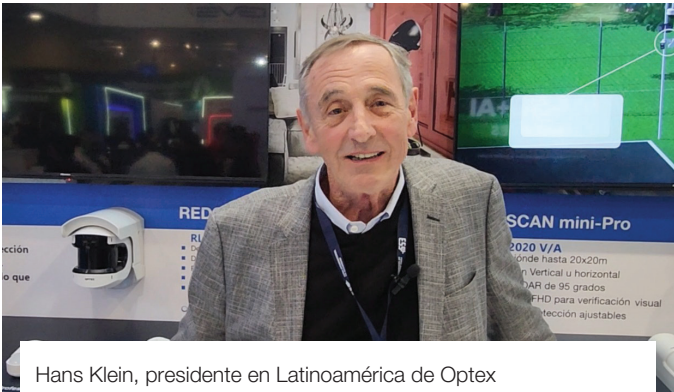
Dual y AIR, se lanzó recientemente el sensor LiDar RLS-50100V, es un dispositivo láser sofisticado que cubre una zona de hasta 100 metros, cuenta con una cámara Onvif integrada y posee la tecnología de detección más precisa y confiable del mercado.

Optex ofrece diferentes modelos de estos sensores LiDar, desde 20mts, 60mts y hasta 100, así como otros productos reconocidos, fotoeléctricos, infrarrojos pasivos y modelos inalámbricos o cableados.

Otras de las novedades que presentó en la exposición es el sistema de fibra óptica EchoPoint, sensor acústico distribuidos (DAS, distributed acoustic sensing), que tiene la capacidad de cubrir hasta 100 kilómetros desde un punto o un controlador de alarma. Este sistema se encuentra instalado y operando desde hace casi tres años para la protección perimetral en el Aeropuerto Internacional Felipe Ángeles (AIFA), ubicado en el Estado de México.

Sobre EchoPoint, Hans Klein indicó que lo más destacado de este sistema de fibra óptica es que mantiene una precisión de 6 metros para localizar la intrusión y puede instalarse en infraestructuras como oleoductos, para detectar tomas clandestinas o para la protección de perímetros largos.

Otro producto que exhibió Optex son los sistemas de detección de intrusos por fibra óptica de la serie Fiber Defender para la protección de perímetros de hasta aprox. 10km. Fiber Defender es la serie más exitosa de Fiber SenSys Inc. (Grupo Optex), de los cuales actualmente están instalados en más de 100 sitios petroleros solamente en Colombia.



Hans Klein, presidente en Latinoamérica de Optex



# Sensor Acústico Distribuido por Fibra Óptica de Largo Alcance



Los sensores acústicos distribuidos (DAS) **EchoPoint™** utilizan la última tecnología en algoritmos de detección y clasificación por fibra óptica para proporcionar la solución más avanzada para aplicaciones que requieren sensores de detección de intrusiones confiables y de localización puntual. Estos avances hacen que los sensores **EchoPoint™** sean una parte clave de la solución en sitios grandes donde se necesita la ubicación precisa de una intrusión.

## Serie EP9000

- Robusta solución para Cercos, Muros, soterrado, ductos, infraestructura de redes de datos
- Opciones de cobertura desde 5km hasta 100km con +/- 2 – 6m de precisión
- Total inmunidad a tormentas eléctricas, campos EMI y RFI
- Con Interfaz Gráfico de Usuario, requiere de 2U de Rack
- Tolerancia al corte y redundancia de sistema
- Instalaciones Híbridas (sobre Cercos y soterrado)





# Tecnología, IA y ciberseguridad redefinen el control perimetral y de accesos en Latinoamérica

• Empresas tecnológicas impulsan un nuevo estándar en control perimetral en LatAm.

Beatriz Canales  
Parte 2 de 2

La firma **Armatura** y sus soluciones de control de accesos, prioriza la protección de datos y la ciberseguridad, superando los métodos tradicionales de autenticación: “Se trata de abrir una puerta con una credencial o reconocimiento facial y también de proteger la información que se genera en cada evento”, explicó Francisco Medina, Integrador de aplicaciones de seguridad electrónica especializado en sistemas de control de acceso de la marca. Subrayó que los sistemas actuales deben garantizar el cifrado de datos sensibles como accesos a zonas restringidas o instalaciones estratégicas.

Una de las innovaciones destacadas es la biometría de palma bimodal, que combina el escaneo simultáneo de la geometría de la palma y de las venas, mejorando la precisión en bases de datos extensas: “Con esta tecnología, incluso en sistemas con miles de registros, se reduce la probabilidad de error y se agiliza el acceso”, detalló. Esta solución ya está siendo adoptada por corporativos en México y otros países de Latinoamérica.

Además, Armatura trabaja en sistemas con bases de datos descentralizadas, donde la información biométrica se almacena de forma segura en el dispositivo móvil del usuario. A través de su plataforma BioHA, las credenciales faciales se resguardan en el teléfono del usuario y se validan mediante un código QR cifrado. “Vamos hacia un modelo en el que el usuario es dueño de sus propios datos biométricos”, afirmó Medina.



Francisco Medina, integrador de aplicaciones de seguridad electrónica especializado en sistemas de control de acceso de Armatura.

**Ajax Systems** impulsa la integración de sistemas inalámbricos en seguridad residencial e industrial. La marca de origen europeo especializada en sistemas de alarma inalámbricos, consolida su crecimiento en México gracias a soluciones que integran seguridad electrónica, automatización, detección de incendios y videovigilancia en un solo ecosistema: “Nuestro objetivo no es solo ofrecer alarmas, sino un sistema de seguridad completo que evolucione con las necesidades del usuario”, explicó Alberto Treviño, gerente de marca de Ajax Systems México.

Sus integraciones permiten controlar desde su app elementos como iluminación, barreras vehiculares o cerraduras magnéticas mediante relevadores inalámbricos. “Aunque no fabricamos control de acceso como tal, nos integramos fácilmente con otros sistemas, y eso nos permite participar en proyectos de cualquier escala, desde viviendas hasta instalaciones industriales”, indicó Treviño. También destacan funciones inteligentes en CCTV, como detección por tipo de objeto y registro cronológico de eventos.

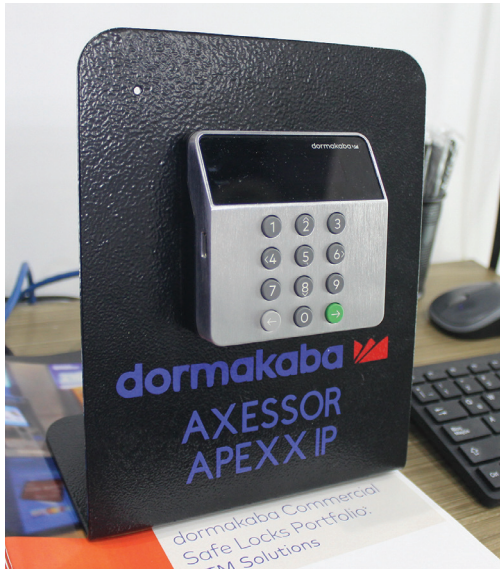
México se ha convertido en una de las regiones de mayor crecimiento para la marca en América: “Cerramos 2024 con un crecimiento del 80% respecto al año anterior, y 2025 ya apunta a superar esa cifra. Las soluciones inalámbricas están transformando el mercado y nuestra tecnología nos ha abierto puertas donde otras marcas no han podido entrar”, afirmó Treviño.



Alberto Treviño, gerente de marca Ajax Systems en México.







**Dormakaba** refuerza su presencia en México y Centroamérica con más de 150 años de experiencia global, continúa expandiendo su portafolio de soluciones de control de accesos en México, Centroamérica y el Caribe. Javier González, desarrollador de negocios regional, explicó que la compañía busca ofrecer “lugares seguros en cada edificación que las personas visitan”, a través de hardware, software y automatización adaptados a distintas industrias como hotelería, automotriz, educativa y bancaria.

Las soluciones más recientes integran tecnología sin contacto, cerraduras digitales y sistemas avanzados de gestión, enfocados en verticales con alta demanda como la hotelería e industria: “Desde operadores automáticos hasta software para gestionar accesos restringidos o salidas de emergencia con certificaciones puntuales, nuestro catálogo cubre cada necesidad”, afirmó González.

El crecimiento se ha consolidado en México y en Costa Rica, Panamá y República Dominicana. La empresa proyecta una expansión aún mayor en regiones donde aún no tiene presencia



total: “Queremos estar donde aún no hemos llegado y fortalecer nuestra posición en donde ya estamos. Nuestra meta es seguir creciendo con innovación y cercanía al cliente”, concluyó.

# 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](http://www.ajax.systems)



Javier González, desarrollador de negocios regional de Dormakaba



**Hikvision** fortalece su portafolio en control de accesos y protección perimetral, migrando de sistemas basados en tarjetas o claves a tecnologías biométricas como huella digital, reconocimiento facial e incluso de iris. “Estas soluciones permiten verificar con mayor



certeza la identidad de las personas y ampliar su uso para control de asistencia, gestión de permisos y administración de visitantes en entornos corporativos, industriales y residenciales”, comentó Miguel Arrañaga, director regional para Hikvision México.

En el ámbito perimetral, la compañía combina cámaras térmicas, radares y sistemas de fibra óptica para cubrir extensiones de varios kilómetros, integrando estas herramientas en su plataforma HikCentral. Esta sinergia permite detectar intrusiones, hacer seguimiento con cámaras y emitir alertas disuasivas mediante altavoces IP, ajustando la respuesta según el nivel de riesgo.

Sectores como el educativo, industrial y de infraestructura crítica han incrementado la demanda de estas soluciones,

priorizando el control de accesos autorizados y la protección de áreas sensibles. “En escuelas, por ejemplo, se aplican sistemas de reconocimiento facial y de placas vehiculares para garantizar que solo personas y vehículos autorizados ingresen a las instalaciones”, afirma el directivo.

La compañía apuesta por la integración de Inteligencia Artificial para optimizar la detección y análisis de eventos, reduciendo la dependencia de la supervisión humana. Entre sus desarrollos más recientes se encuentra AcuSense, una tecnología que permitirá realizar búsquedas de personas o vehículos a partir de descripciones escritas, agilizando la respuesta ante incidentes y reforzando la seguridad integral.



Miguel Arrañaga, director regional Hikvision México

### Desafíos y oportunidades, el futuro.

A pesar del crecimiento sostenido, las marcas coinciden en que el mercado enfrenta grandes retos. Entre ellos, la falta de estandarización en normativas locales, la profesionalización de los integradores y la necesidad de mayor cultura digital entre usuarios finales.

Sin embargo, las oportunidades son vastas. La automatización, los modelos de “seguridad como servicio” y la creciente adopción de herramientas predictivas abren nuevos nichos.

La industria del control perimetral y la de accesos ha dejado de ser un sector meramente físico. Hoy, es un campo que une ciberseguridad, Inteligencia Artificial, movilidad y análisis de datos. Las empresas que lideran este cambio no solo protegen edificios, sino que resguardan la información, las operaciones y la identidad misma de quienes acceden a esos espacios.

Mientras el mercado latinoamericano sigue madurando, las soluciones se expanden con rapidez, y todas las marcas coinciden en una premisa fundamental hoy: el futuro es la seguridad perimetral y el control de accesos. 



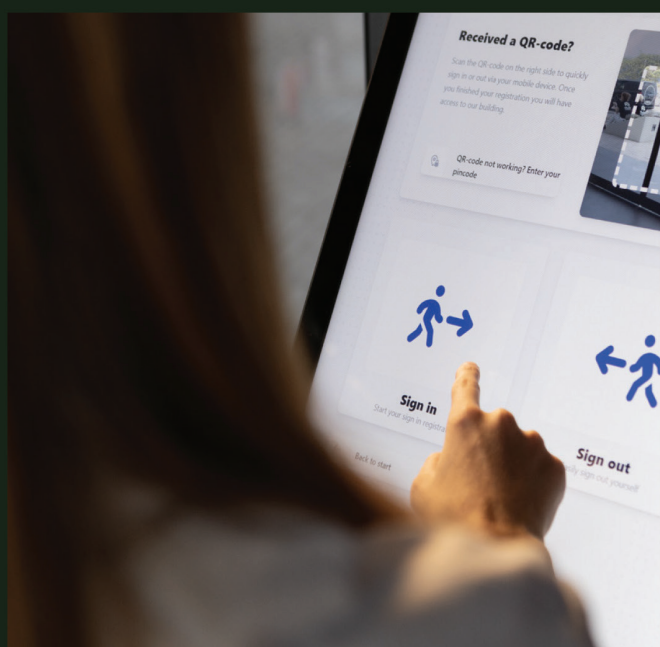


# Impulsando un acceso más inteligente

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](https://saltosystems.com)



Datos de contacto

[marketing.cala@saltosystems.com](mailto:marketing.cala@saltosystems.com)





# lanza HID Amico, lector de reconocimiento facial biométrico

• Esta terminal cuenta con cinco factores de autenticación, y se integra con la mayoría de las plataformas de control de acceso más reconocidas del mercado.

**Bogotá, Colombia.-** Durante la Feria Internacional de Seguridad (ESS+) 2025, el fabricante HID introdujo al mercado de América Latina el lector de reconocimiento facial biométrico HID Amico, una terminal que se caracteriza porque es compatible con su solución de credencialización virtual Origo.

Entrevistado por Más Seguridad Magazine, Jorge Bejarano, gerente Senior de Ventas para la Solución de Credencialización Virtual de HID, destacó que este producto es el primer biométrico dentro del portafolio de la marca y es un desarrollo completamente nuevo para el mercado de biometría facial.

Describió que HID Amico es una terminal capaz de arrancar con 10 mil usuarios, pero puede expandirse hasta 100 mil usuarios en memoria, y además se integra con la mayoría de las plataformas de control de acceso más reconocidas del mercado.

Este equipo cuenta con cinco factores de autenticación, el principal es el de biometría facial, cuyo algoritmo es de Paravisión, certificado por el NIST (Instituto Nacional de Estándares y Tecnología). También es compatible con su solución de credencialización virtual Origo y puede soportar cualquier tarjeta de proximidad en 125 kHz en 13.56 MHz de HID o de terceros, códigos de QR dinámicos o estáticos para aplicaciones de visitantes y una opción de PIN.

Jorge Bejarano afirmó que HID está presente en mercados de segmentos medios y altos, pero especificó que HID Amico se puede aplicar en cualquier vertical en donde hay ingresos masivos y no se puede carnetizar a los usuarios, se requiere un alto nivel de seguridad y se necesita mezclar diferentes tipos de autenticación. Funciona a través de tarjetas virtuales y físicas, así como con biometría facial con altos estándares de ciberseguridad y de privacidad.

“En el mercado existen algunos equipos en la línea alta con un costo más alto, pero uno que combine las cinco soluciones y que tenga la de credencialización virtual de HID no lo hay. Muchos usuarios que han trabajado con la plataforma de credencialización virtual estaban esperando soluciones de biometría facial, pero no se decidían porque tenían que comprar terminales de otros fabricantes que no eran compatibles con las soluciones de credenciales virtuales. Ya tenemos la solución in house, compatible con diversas tarjetas y formatos”, aseguró Jorge Bejarano.

Agregó que este producto es muy competitivo, enfocado para un segmento con una clasificación alta, pero con un precio que está por debajo de otras marcas y con integraciones con una plataforma grande de control de acceso, con toda la calidad y el respaldo de HID.

HID Amico fue presentado oficialmente al mercado global durante la feria ISC West 2025, celebrada del 31 de marzo al 4 de abril en Estados Unidos. Actualmente, la solución ya está disponible en varios países de Latinoamérica. En Brasil, Colombia, Costa Rica y México, se han iniciado procesos de adopción y adecuación conforme a las normativas locales, como parte de su despliegue regional.



Jorge Bejarano, gerente Senior de Ventas para la Solución de Credencialización Virtual de HID



# impulsa soluciones híbridas para Latinoamérica con Cloudlink 210

**Bogotá, Colombia.-** Recientemente, la firma canadiense Genetec, presentó su nuevo dispositivo Cloudlink 210, diseñado para responder a una necesidad creciente en la región: conectar sistemas tradicionales de seguridad con plataformas en la nube bajo un esquema híbrido.

Miguel Castellanos, gerente regional de ventas de Genetec, explicó que la tendencia en Latinoamérica apunta a modelos mixtos: “Los clientes quieren lo mejor de los dos mundos: mantener su infraestructura en sitio y, al mismo tiempo, aprovechar la flexibilidad de la nube. Cloudlink 210 hace posible esa integración”, señaló.

El dispositivo funciona como un puente para que cámaras, sistemas de control de acceso o plataformas de intrusión —sin importar el fabricante— se integren a Security Center, la solución de gestión en la nube de Genetec. Su arquitectura abierta permite trabajar con cámaras bajo el estándar Onvif, controladoras de acceso de Axis o Mercury, y una lista extensa de paneles de intrusión compatibles.

El alcance es transversal: desde instalaciones corporativas hasta sectores críticos, la solución busca simplificar la gestión y reducir costos de operación.

“Hemos tenido casos de éxito en subestaciones eléctricas ubicadas en zonas remotas donde resulta complejo enviar técnicos. Con una sola visita de instalación y conexión a internet, el equipo queda listo para ser monitoreado desde cualquier parte del mundo”, detalló Castellanos.

El lanzamiento en la región andina —Colombia, Ecuador y Venezuela— marca la evolución de un producto previo, el módulo 110, que estaba limitado a video. La nueva versión amplía su alcance a control de acceso



e intrusión, cubriendo demandas más amplias de los usuarios finales.

La compañía también busca acelerar la adopción del Internet de las Cosas (IoT) en la gestión de seguridad. A través de su Security Center, es posible integrar datos provenientes de sensores que van más allá de la seguridad física: sistemas de climatización, bombas de agua, unidades de aire acondicionado o sensores de ruido pueden reportar eventos que se correlacionen con la operación general de un edificio.

“Cualquier fabricante que trabaje con protocolos abiertos como BACnet, Modbus o MQTT puede enviar información a nuestro sistema. Esto amplía la capacidad de correlacionar datos y tomar decisiones operativas más inteligentes”, explicó Miguel Castellanos.

Subrayó que la región aún tiene camino por recorrer en la adopción de estas tecnologías, pero confía en que la necesidad de eficiencia y monitoreo remoto acelerará el proceso.

“Lo que proponemos no es reemplazar, sino complementar. Queremos que las empresas de la región se beneficien de soluciones híbridas, escalables y seguras”, concluyó el directivo. 



- El dispositivo integra video, control de acceso e intrusión en un solo punto de gestión.
- Permite conectar infraestructura clásica con plataformas en la nube de manera segura.
- Casos recientes en subestaciones eléctricas muestran su valor en sitios remotos.



Miguel Castellanos,  
gerente regional de ventas  
de Genetec

# Iniciativas vs la crisis de profesionales en ciberseguridad



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

Articulista Invitado

A nivel global, se estima un déficit de más de 3 millones de profesionales en ciberseguridad; muchas vacantes aún no son cubiertas por falta de personal formado adecuadamente.

Según Fortinet, en América Latina y el Caribe faltan 1.3 millones de especialistas en el sector, y más del 70 % de las organizaciones considera esa carencia como un riesgo operativo importante. Además, la situación genera costosas brechas de seguridad que superan el millón de dólares en más de la mitad de los incidentes cibernéticos.

Las organizaciones y gobiernos deben actuar estratégicamente porque las amenazas modernas —incluyendo ransomware, ingeniería social y ataques avanzados— requieren tanto capacidades defensivas como ofensivas sólidas. La falta de personal entrenado y especializado limita la resiliencia para las organizaciones, las naciones y las regiones, reduce la capacidad operativa y de respuesta ante incidentes, exponiendo sistemas críticos. El reporte del Foro Económico Mundial subraya que solo 15 % de las empresas espera que las capacidades cibernéticas crezcan significativamente antes de 2026, lo que agrava el riesgo, un riesgo real asociado al uso de la tecnología.

ENISA, en su informe sobre el programa CyberHEAD, muestra que los niveles actuales de matrícula y graduación en educación superior aún no satisfacen la demanda y recomienda diversificar currículos, fomentar la inclusión y promover desafíos académicos como parte crucial de la formación. Desde otro ámbito, estudios académicos también apuntan a una falta de habilidades en áreas como seguridad de aplicaciones, ingeniería de requisitos, gestión y cumplimiento en seguridad. Además, se destacan la importancia de habilidades blandas (comunicación asertiva, trabajo en equipo, trabajo bajo presión, entre otras) y diversidad de género, lo cual impacta directamente en la contratación y efectividad del talento.

## Capacidades cibernéticas

Se identifica déficit en estas áreas críticas, siendo también las más buscadas:

- Seguridad de software y aplicaciones
- Criptografía, explotación web y reversión



- Gestión, cumplimiento normativo y auditorías estándar (ISO 27001)
- Habilidades de respuesta de incidentes, y habilidades para responder ante amenazas emergentes, incluyendo IA y computación cuántica

Cabe señalar, que con el avance de IA y la futura llegada de la computación cuántica, es urgente fortalecer la formación en inteligencia artificial aplicada a seguridad (por ejemplo: detección de anomalías, ML adversarial), criptografía post-cuántica y auditoría avanzada.

## Involucramiento de actores: gobiernos, empresas e internacionales

El modelo europeo liderado por ENISA sugiere una aproximación colaborativa: gobiernos, academia e industria trabajando bajo marcos comunes como el “European Cybersecurity Skills Framework” y promoviendo ejercicios, retos y certificaciones estandarizadas. Organismos internacionales como la OIT/ILO y OCDE han insistido en que la formación y el desarrollo de capacidades es clave para reducir la informalidad, mejorar empleo juvenil y elevar resiliencia digital. El modelo de “Cybersecurity Capacity Maturity Model for Nations” (CMM) de la UIT también orienta cómo estados pueden avanzar institucionalmente. Empresas como Fortinet han comprometido la formación de un millón de personas para 2026, subrayando el papel esencial del sector privado en la provisión de capacitación



estructurada y certificaciones reconocidas.

Lo anterior, es factor crítico contra el crimen organizado. El crimen organizado en línea se ha convertido en una industria, con ataques masivos (por ejemplo, México con más de 30 mil millones de intentos en los primeros seis meses de 2024) utilizando inteligencia artificial para escalar sus operaciones. La profesionalización de los defensores es clave para responder a estructuras criminales



igualmente profesionalizadas y con bastos recursos.

Canteras para la ciberseguridad

Aquí dos ejemplos de importancia para la atracción y formación de talentos, desde edades tempranas.

- **Latinamerica Cybersecurity Challenge (LAC)**  
El evento inaugural de LAC fue en Medellín 31 julio 1 agosto 2025, reuniendo jóvenes, expertos y líderes de academia, gobierno y sector privado, con la misión de demostrar el valor del modelo Capture the Flag (CTF) como herramienta de evaluación y capacitación técnica en la región.
- **International Cybersecurity Challenge (ICC) impulsado por la ENISA**  
Desde 2022, el ICC, organizado por ENISA con redes regionales incluyendo LATAM, reúne equipos regionales en pruebas de explotación web, criptografía, reversión, hardware y defensa ofensiva/defensiva. ENISA reporta que los participantes desarrollan más del 50 % de las competencias del European

Cybersecurity Skills Framework y cubren habilidades presentes en más del 80 % de ofertas laborales en ciberseguridad.

Beneficios de la vinculación entre academia, gobierno y sector privado

- Desarrollo de talento local: permiten descubrir y profesionalizar jóvenes antes que migren, abandonen el campo o sean parte de grupos cibercriminales.
- Certificación práctica y redes profesionales: ICC y LAC brindan visibilidad regional e internacional, conexiones con empresas y oportunidades laborales.
- Retroalimentación curricular: colaboración directa con empresas permite adaptar programas académicos a necesidades reales del mercado.
- Inclusión y diversidad: apoyar grupos sub representados amplía la base de talento y mejora resiliencia institucional estándar.

Impacto en el ecosistema digital

La inversión en capacitación y eventos tecnológicos fortalece el ecosistema digital al:

- Elevar la ciberresiliencia nacional frente a amenazas sofisticadas.
- Promover innovación y emprendimiento en ciberseguridad.
- Mejorar la confianza digital de usuarios, inversores y organismos reguladores.
- Generar una comunidad técnica auto-sostenible, reduciendo dependencia de talento extranjero.

Riesgos de no invertir en capacitación cibernética

- Vulnerabilidad persistente: organizaciones que no fortalecen sus capacidades quedan expuestas a ataques disruptivos.
- Pérdidas económicas y reputacionales: brechas de seguridad costosas y sanciones regulatorias.
- Fuga de talento: sin espacios de formación y crecimiento, los jóvenes migran o abandonan la disciplina.
- Brecha digital ampliada: los países con menor inversión se rezagan tecnológicamente frente a regiones más preparadas.

Consideraciones finales

La escasez de profesionales en ciberseguridad en América Latina, representa una amenaza estratégica tanto para lo público como lo privado. La formación efectiva debe combinar educación superior actualizada, entrenamiento práctico, participación en eventos como LAC y el ICC, así como una colaboración estrecha entre academia, gobiernos y sector privado. Estos mecanismos permiten cultivar un ecosistema digital resiliente y preparado para los retos actuales (IA adversarial, cibercrimen profesional) y futuros (computación cuántica).

No invertir en el desarrollo de capacidades cibernéticas implica dejar la defensa digital en manos de actores maliciosos, con consecuencias sociopolíticas, económicas y tecnológicas muy graves. Por tanto, es urgente desplegar políticas públicas, programas educativos y alianzas público privadas que formen a la próxima generación de expertos en ciberseguridad de manera inclusiva, estructurada y sostenible. 

Referencias

- Fortinet (2024), déficit de 1.3 M en LATAM y costos por brechas mayores a US\$1M. Web: Mexico Business News
- ENISA's CyberHEAD framework y recomendaciones para educación superior. Web: enisa.europa.eu+1
- ICC e impacto de competencias ENISA CTF. Web: icc.ecsc.euenisa.europa.eu/en.wikipedia.org
- Estudio académico sobre brecha de habilidades globales en ciberseguridad Web: arXivXivXiv.
- CCBOL 2024 en Sucre, IA y ciberseguridad, participación internacional. Web: panoramaeconomicopma.comumsa-2023.clei.org
- Latinamerica Cybersecurity Challenge 2025 en Medellín, modelo CTF regional.

# ¡MUNDO NAVI!

## ¡Nuevo reto de seguridad corporativa!



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

Articlista Invitado

**S**ão Paulo, Brasil.- Nos adentramos en un territorio marcado por turbulencias impredecibles y cambios exponenciales para los que las empresas y sus líderes no están preparados. Esta es una era en la que todo se reinventa, se replantea y se reprograma.

La nueva normalidad hoy se conoce como Mundo NAVI. En las últimas décadas se han propuesto diferentes modelos para describir la complejidad del entorno global. El mundo VUCA, acuñado en la década de 1990 por el Colegio de Guerra del Ejército de EE. UU., fue sucedido por BANI, propuesto por Jamais Cascio en 2018, y más recientemente, en 2023, el concepto NAVI, concebido por la consultora EY, para caracterizar el entorno empresarial actual.

NAVI – No lineal, Acelerado, Volátil e Interconectado – representa una visión más contemporánea del entorno global, caracterizada por transformaciones intensas, interdependientes e impredecibles, que requieren que las empresas adopten un nuevo enfoque de gobernanza, estrategia y gestión de riesgos.

Los mundos VUCA y BANI no han desaparecido, pero ya no son suficientes para comprender el mundo en el que vivimos. Los eventos actuales se definen más por la no linealidad y la interconectividad, que generan desafíos, imperativos y oportunidades. Cada enfoque trae implicaciones específicas para los líderes de seguridad corporativa.

El mundo NAVI no es simplemente otro nombre para VUCA o BANI; es un entorno más complejo, definido por cuatro características:

1. No lineal: Más que nunca, los líderes operan en un mundo donde el cambio no ocurre a un ritmo constante. Las curvas en S de la tecnología pueden precipitar puntos de inflexión, en los que las innovaciones pasan repentinamente de una mejora gradual a saltos exponenciales. Estos puntos de inflexión se producen con mayor frecuencia y magnitud.
2. Acelerado: El cambio se acelera sin precedentes. La inteligencia artificial (IA) avanza rápidamente; el cambio climático transforma ecosistemas y economías en distintas regiones del planeta; y los escenarios geopolíticos atraviesan mutaciones disruptivas y vertiginosas.
3. Volátil: La política se está reconfigurando y polarizando, lo que aumenta la probabilidad de transformaciones profundas de un proceso electoral a otro. Para las empresas, navegar en este espacio volátil es cada vez más desafiante, con implicaciones directas en la estrategia corporativa.
4. Interconectado: El mundo NAVI es un entorno en el que las tendencias, los eventos y los riesgos están fuertemente interrelacionados. Choques exógenos pueden desencadenar múltiples impactos que, con frecuencia, culminan en resultados inesperados: el conocido “efecto dominó”. Ejemplos claros son la guerra en Ucrania y los conflictos en Medio Oriente, que derivaron en interrupciones en las cadenas de suministro y otras consecuencias globales. La interconectividad exige una visión prospectiva y mayor capacidad de anticipación.

### La brecha de la seguridad corporativa



La gestión de la seguridad corporativa, tal como se practica en la mayoría de las empresas hoy, está profundamente desalineada con el mundo NAVI.

- En una era de cambios acelerados y mayor volatilidad, la seguridad aún se rige por procesos lentos y fragmentados.
- En un contexto de interconectividad creciente, las áreas de seguridad siguen operando como islas desconectadas, sin visión de portafolio ni perspectiva estratégica holística.
- En un entorno no lineal, la adopción de metodologías capaces de modelar y gestionar esta dinámica ha sido limitada y resistida.

Un claro indicador de esta brecha es la ausencia de un Director de Seguridad Corporativa en muchas empresas. En un entorno internacional altamente volátil, la seguridad debe integrarse a la estrategia al mismo nivel que otras áreas críticas del negocio.

### Transformación necesaria en el mundo NAVI

Alinear la seguridad corporativa con el mundo NAVI requiere una transformación integral, que incorpore prácticas como la Gestión Integrada de la Seguridad Empresarial, orientada a una visión más holística y estratégica de la protección del negocio, sus servicios y productos.

Los profesionales de seguridad deben aprender a equilibrar riesgos y beneficios, no solo a limitarlos. Para enfrentar los desafíos emergentes del mundo NAVI, la seguridad corporativa necesita nuevos enfoques, con dos herramientas clave:

1. Ciclo de Inteligencia: orientado al futuro, para identificar señales débiles y anticipar escenarios.
2. Matriz de Riesgos con técnica de Interconectividad: para comprender la motricidad y criticidad de los riesgos, fortaleciendo la toma de decisiones.

### Riesgos emergentes en el mundo NAVI

En este entorno, los riesgos de seguridad corporativa se caracterizan por ser novedosos, con datos insuficientes y sin referencias claras para la toma de decisiones. Este es uno de los mayores desafíos para los gestores de seguridad en la actualidad.





**AFÍLIATE**

ASIS CAPÍTULO  
MÉXICO 217

**\$ 5, 650 MXN**

ASIS INTERNACIONAL

**\$ 125 USD**

**FORMA PARTE DE  
LOS PROFESIONALES  
DE LA SEGURIDAD**

► COMUNÍCATE A:

✉ [SOCIOS@ASIS.ORG.MX](mailto:SOCIOS@ASIS.ORG.MX)

☎ 55 1321-1289

*¿Cómo ser sponsor?*

Escanea el código QR.

**SUMA TU MARCA  
AL MEJOR CAPÍTULO**



**¡CONOCE  
MÁS!**

ESCANEANUESTRO  
LINKTREE

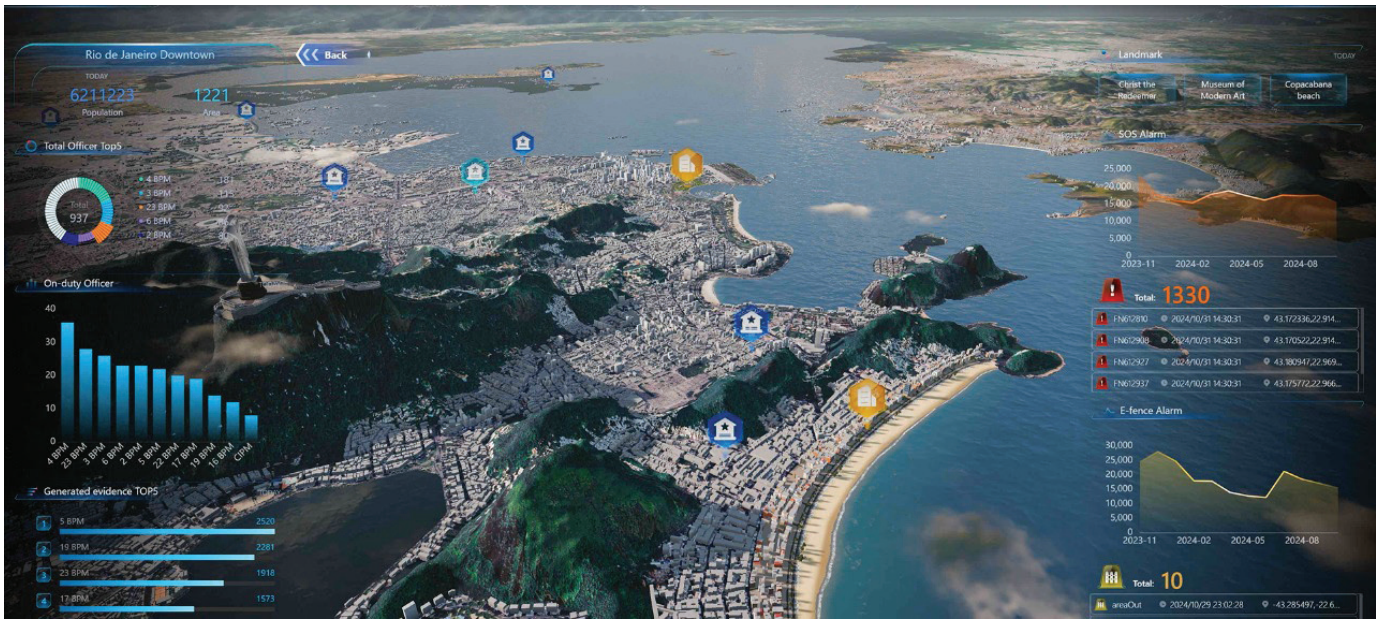


**7 OCTUBRE**

**11 NOVIEMBRE**

**2 DICIEMBRE**





# IA, gestión de datos y alta disponibilidad: la propuesta de **HIKVISION®** para C4 y C5 en México

- IA en borde, centro de datos y software: Hikvision convierte el video urbano en decisiones operativas para C4 y C5.
- Acuseek acelera el análisis forense con búsquedas en lenguaje natural y cruces de rostros, placas y atributos en segundos.
- Alta disponibilidad 24/7 y soluciones móviles (bodycams, torretas, motos LPR) reducen tiempos de respuesta y fortalecen la operatividad con evidencia.

En México, los centros de emergencia ciudadana C4 y C5 dejaron de ser salas tapizadas de monitores para convertirse en nodos de decisiones en tiempo real. En estos espacios se filtra la información crítica, y se coordinan las respuestas policíacas, servicios de protección civil, atención médica, entre otros.

En esa transición, Hikvision llega con una arquitectura tecnológica que busca algo más que “ver”: pretende comprender lo que sucede y anticipar lo que podría ocurrir, sin perder continuidad operativa: “Nuestros centros se diseñan con un esquema de alta disponibilidad; si fallan los servidores de gestión, almacenamiento o equipos de red, el servicio operativo no se detiene. Así debe operar un centro de atención de emergencias con disponibilidad 24/7”, resume Rubén García Soriano, gerente de Soluciones de Gobierno del Centro de Investigación y Desarrollo de la empresa.

El planteamiento descansa en tres capas de inteligencia que se complementan. La primera capa vive en el borde, dentro de las propias cámaras. Bajo el modelo de Inteligencia Artificial Generativa, propio de la **Guanlan**, la analítica embebida reduce falsas alarmas, detecta intrusiones y comportamientos como aglomeraciones, peleas o caídas, y reconoce atributos de personas —vestimenta, accesorios, rasgos— junto con atributos vehiculares —tipo, color, marca, placas o sentido de circulación—. La lógica es filtrar ruido desde el origen para que a la sala de monitoreo solo llegue lo relevante. La segunda capa se despliega en el

centro de datos con servidores de fusión que toman video “plano” o capturas de cámaras inteligentes, incluso de cámaras de otras marcas y lo transforman en metadatos aprovechables, gestionando millones de imágenes generadas por el borde o el centro de datos.

Allí opera **Acuseek**, una tecnología que permite realizar búsquedas mediante lenguaje natural: el operador escribe “dos personas en moto sin casco con mochila” o “grupo encapuchado” y el sistema regresa coincidencias tras cruzar información de atributos generadas en el borde o en el centro de datos. La tercera capa se concentra en el software con **Hikcentral Master**, un VMS/PSIM de gama alta diseñado para la administración de ciudades inteligentes que integra mapas de calor, trazabilidad de personas y vehículos, listas de interés, mapas GPS y, para la alta dirección, gemelos digitales en 3D con funciones de realidad aumentada y virtual. El objetivo es claro: pasar del muro de pantallas a tableros de decisión.

Esa triada técnica se acompaña de una premisa operativa: alta disponibilidad real. La arquitectura está basada en clusters de servidores, brinda inmunidad ante fallas de dispositivos; brindando gran flexibilidad en la escalabilidad de los sistemas, de modo que el monitoreo no interrumpa su servicio, aún cuando algún componente falla.



La promesa de continuidad no es un detalle de ingeniería; es el fundamento de un centro de emergencias que debe procesar llamadas, video, datos de patrullas, policías en calle, placas, rostros y catástrofes naturales de manera ininterrumpida. Rubén García lo sintetiza con un giro práctico: “La continuidad operativa es el principal KPI. Si la pantalla se apaga, el resto no importa, ya que el flujo de información continua sigue analizándose”.

El catálogo de soluciones aterriza esa visión en la calle y en centros de emergencia. **Hikcentral Master** actúa como columna vertebral para administrar ciudades en tiempo real; con base en trayectorias vehiculares y de personas, mapas de calor y listas de interés, comprimiendo análisis masivos de información en vistas ejecutivas que los tomadores de decisiones pueden leer y actuar en segundos.

**Acuseek** democratiza las búsquedas: convierte la descripción humana en una consulta técnica que localiza patrones delictivos, configura detecciones como peleas, disparos, personas armadas o vehículos robados, y devuelve resultados que fortalecen expedientes en fiscalías, tribunales de justicia y asuntos internos.

En campo, las bodycams sincronizan evidencia con el VMS; las patrullas se equipan con torretas inteligentes capaces de ejecutar lectura automática de placas y reconocimiento de personas; y las motocicletas añaden lectura en movimiento para identificar vehículos robados. A esa capa móvil se suman los botones de emergencia ciudadana, una vía alterna al 911 que reduce tiempos de aviso en colonias, corredores comerciales y espacios públicos.

La compañía asegura una presencia tecnológica global en seis estados de la República Mexicana y en más de 18 municipios capitales.

La demanda más dinámica proviene de soluciones móviles y portátiles, por su valor probado



y la manera en que alimentan la trazabilidad operativa policiaca hacia los C4 y C5, las fiscalías y los tribunales. El núcleo de oportunidades sigue estando en los Puntos de Monitoreo Inteligente (PMI): postes que alojan cámaras fijas, analíticas y comunicaciones, y que







ya no se conciben como islas, sino como parte de una red que debe monitorearse para garantizar su estado de salud operativa, latencias y porcentaje de equipos en línea, indicadores cruciales para los C5 y C4.

Los casos de uso que describe el Rubén García comparten una ambición: quitar pasos y optimizar tiempos entre el evento y la respuesta. En la calle, las bodycams no solo documentan; protegen a los agentes y a la ciudadanía, aportando transparencia para auditorías internas.

Las patrullas y motos, con LPR y reconocimiento de personas, permiten capturas dirigidas y recuperación de unidades sin depender de “sospechas” vagas. Los botones de emergencia desahogan tráfico del 911 y desencadenan alertas georreferenciadas que el sistema contextualiza con video cercano.

En la sala, **Acuseek** teje el análisis forense en segundos, con filtros por hora, lugar y tipo de evento, mientras **Hikcentral Master** visualiza rutas de patrullaje, disponibilidad de cámaras y KPIs de salud, y eleva una vista ejecutiva en los gemelos digitales que ayuda a coordinar, en la misma escena, a policía, protección civil y ambulancias.

El impacto esperado se mide en tres frentes. Primero, la eficiencia de despacho: si la ruta detección-clasificación-asignación-arribo pierde fricción, descienden los tiempos de respuesta y crece la probabilidad de contener eventos en curso. Segundo, la evidencia: líneas de tiempo, metadatos, georreferencias y video sincronizado robustecen la cadena de custodia y evitan que un caso se desmorone por una debilidad documental. Tercero, la disponibilidad técnica: el monitoreo de salud permite anticipar caídas, atender microfallos de red, vigilar energía en casetas y sostener un porcentaje alto de cámaras en línea, incluso en contingencias eléctricas o climáticas.

La gobernanza de datos se vuelve un capítulo obligado. Más sensores implican más información personal: imágenes, biométricos, rutas y patrones. La compañía plantea despliegues alineados con marcos de privacidad locales y con políticas de transparencia que distinguen roles y perfiles de acceso, y mantienen bitácoras de consulta para cada interacción con el

sistema.

La narrativa de Hikvision se acopla a ese guión: la tecnología debe sostener tanto la operación cotidiana como la excepcional. La hoja de ruta proyecta un salto de **Ciudades Seguras** a **Ciudades Inteligentes**. La integración con sistemas ITS y de semafización pretende centralizar la información crítica de las ciudades para una toma de decisiones mucho más informada y eficiente, sincronizándose fotomultas con analítica confiable para generar ciudades mucho más ordenadas y seguras, todo desde una misma plataforma, alertas ambientales, desastres naturales, autopistas, estacionamientos públicos para una gobernanza transparente.

“El siguiente paso es consolidar ciudades inteligentes; entender en tiempo real qué pasa y qué puede pasar, para mover recursos a tiempo”.

En el fondo, el mensaje que Hikvision busca posicionar es menos espectacular y más táctico: conectar sistemas, entrenar personas y disciplinar datos. La promesa de valor no está en acumular más fierros, sino en hacerlos conversar para decisiones más eficientes y rápidas. En resumen, democratizar el desarrollo de ciudades inteligentes. 

Rubén García Soriano, gerente de Soluciones de Gobierno del Centro de Investigación y Desarrollo de Hikvision





# 16 CONGRESO

## INTERNACIONAL DE CENTROS DE ATENCIÓN DE EMERGENCIAS

08 AL 10 DE OCTUBRE DE 2025  
HOTEL ROYALTON SPLASH RIVIERA CANCÚN



NETWORKING



CONFERENCIAS  
MAGISTRALES



EXPO NENA



ESCANEA EL QR

PARA ENTERARTE DE TODO LO QUE  
PASA NUESTRO CONGRESO Y  
CONOCER MÁS DE NENA 9-1-1 MÉXICO

HIKVISION



DAHUA  
TECHNOLOGY

CARBYNE

Teltronic  
WE CAN MAKE IT HAPPEN

Priority  
Dispatch

Seguri tech  
INTEGRAL SECURITY

Genetec

ISS  
INTELLIGENT VIDEO. EXPERT.

nimbus  
SECURE SOFTWARE SOLUTIONS

HEMAC

INTRADO

sérmex  
EXPERTOS EN SEGURIDAD

Milesight

RAPIDSOS

milestone

PULSIAM

bambu  
tech services

THINKSAFE  
INGENIERIA

AVAYA

NGA

VIPER

MCM  
BUSINESS TECH-CO

Integraciones  
Electromecánicas

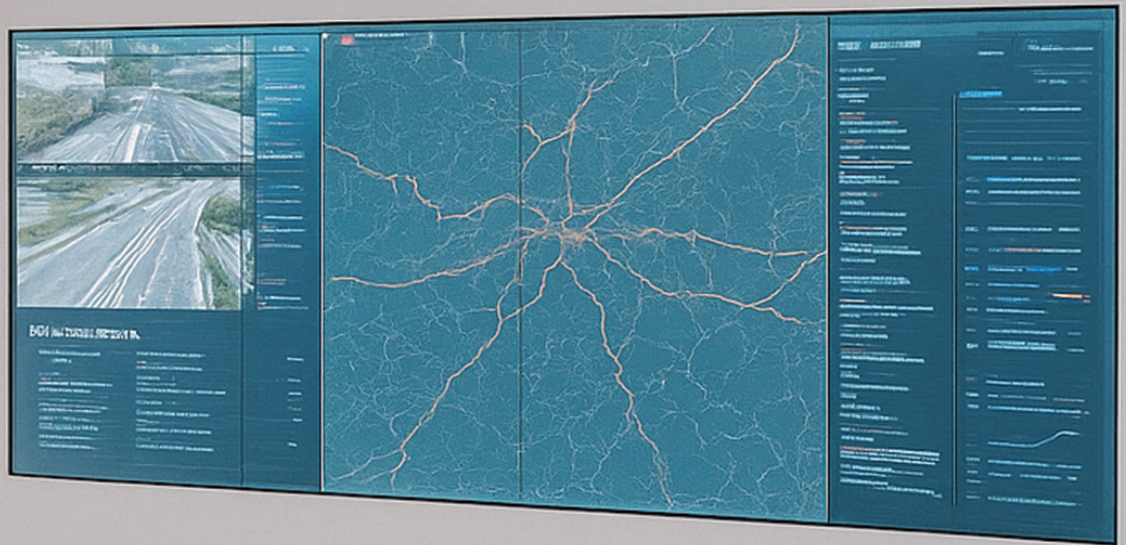
PTT PRO

Aviat



# Tecnología y seguridad convergen en los C4 y C5 de México

Beatriz Canales Hernández



- Integración de sistemas, inteligencia artificial y costos eficientes, la apuesta de Kabat One, Genetec, Hikvision y Uniview.
- Desde México hasta América Latina, los proyectos de videovigilancia y control, buscan salvar vidas y anticipar riesgos.

La seguridad pública se encuentra en un punto de inflexión en el que los Centros de Comando, Control, Comunicaciones, Cómputo y Contacto Ciudadano (C5), junto a los Centros de Comando y Control (C4), son ya infraestructuras críticas para responder a emergencias, coordinar a fuerzas policiales, y prevenir delitos. Y es en este terreno en el que la tecnología dejó de ser un apoyo accesorio: hoy es el centro de la operación.

Empresas como Kabat One, Genetec, Hikvision y Uniview han construido un portafolio de soluciones que incluyen la integración total de subsistemas, el uso de analíticas avanzadas e Inteligencia Artificial. Cada una con su propio sello, pero con un objetivo convergente: salvar vidas y generar ciudades más seguras.

**Kabat One**, el “sistema de los subsistemas”. Niv Yarimi, fundador y presidente de Grupo Kabat y Kabat One, describe la esencia de su solución estrella con una frase: “Nuestro objetivo es integrar lo que ya existe. No se trata de tener más cámaras, sino de hacer que hablen entre sí”.



La plataforma Kabat One se presenta como un ecosistema capaz de integrar telefonía, videovigilancia, bases de datos, GPS, radio, sistemas CAD y video analítico en un solo núcleo.

“El problema que encontramos en los C4 y C5 es que cada sistema funciona aislado. Nosotros los conectamos para que, en segundos, un operador pueda despachar la patrulla más cercana, la ambulancia y hasta los bomberos en caso de un accidente”, explicó Lavimi.

Los resultados hablan: En Morelia, Michoacán, tras la implementación del sistema, los homicidios pasaron de 2,761 en 2022, a menos de mil en 2024, y “solo se logra con tecnología que analiza la data en tiempo real y que automatiza decisiones”, subraya el directivo.

Actualmente, Kabat One opera en Ciudad de México, Michoacán, Tamaulipas, Nayarit, Oaxaca y Chiapas, y comienza a expandirse hacia Perú, Ecuador y Brasil.



Niv Yarimi, fundador y presidente de Grupo Kabat y Kabat One



Michelle Nieto, Vertical Sales Manager para el sector público e infraestructura crítica en Genetec

**Genetec** y la visión unificada. Con más de 25 años de experiencia, la empresa aporta la flexibilidad de integrar múltiples dispositivos en una sola plataforma. Michelle Nieto, Vertical Sales Manager para el sector público e infraestructura crítica en Genetec, lo explica: “Nuestro enfoque es dar una visión unificada al operador. Por ejemplo, Security Center concentra videovigilancia, control de accesos, comunicaciones, analíticos y hasta sensores IoT en un solo tablero”.

La plataforma Security Center incluye el módulo Citigraph, utilizado por la policía de Chicago, que permite integrar información de patrullas, drones y cámaras corporales en tiempo real.

“La Inteligencia Artificial es fundamental porque las cámaras crecen cada año, pero no así la cantidad de monitoristas. Con IA balanceamos



[www.pimecsa.mx](http://www.pimecsa.mx)

## Distribuidores mayoristas en seguridad integral



- Videovigilancia e inteligencia artificial a través de video
- Control de acceso peatonal, vehicular y sistemas de inspección
- Seguridad, videovigilancia e IA en el transporte
- Monitores, LCD y Videowall
- Productos de videoconferencia y pantallas interactivas
- Alarmas e intrusión
- Smart home y productos de consumo



esa ecuación y logramos identificar patrones delictivos, incidentes viales o actividades potencialmente violentas”, explica Nieto.

En México, Genetec está presente en C4 y C5 de 11 estados, especialmente en el centro y norte del país, y mantiene proyectos activos en más de 150 países. Sus soluciones no solo atienden a gobiernos: también se aplican en aeropuertos, puertos, prisiones e incluso centrales nucleares, donde la seguridad no admite margen de error.



Rubén García Soriano, gerente de soluciones de gobierno del Centro de Investigación y Desarrollo de Hikvision

**Hikvision**, inteligencia en tres capas. Para esta empresa, la clave es dotar de inteligencia a cada nivel del ecosistema de seguridad.

Al respecto, Rubén García Soriano, gerente de soluciones de gobierno del Centro de Investigación y Desarrollo de Genetec, detalla: “Hablamos de inteligencia en el borde, en los servidores y en el software. Cada capa aporta eficiencia y reduce tiempos de respuesta”.

En el borde, las cámaras integran analíticas capaces de detectar peleas, aglomeraciones o vehículos en sentido contrario. En los centros de datos, el sistema Acuseek procesa video plano de cualquier marca y lo convierte en información accionable.

Y en el software, la plataforma Hikcentral Master administra millones de imágenes para generar mapas de calor, listas negras de vehículos o gemelos digitales de las ciudades.

Actualmente, Hikvision opera en Puebla, Durango, Sinaloa, Baja California Sur, Querétaro y la Ciudad de México, además de proyectos internacionales en Brasil, Colombia y Chile.

“No se trata solo de prevenir delitos, también de gestionar emergencias como inundaciones o incendios con información en tiempo real”, afirma Rubén García.

**Uniview**, costo-beneficio y visión nocturna a color. Con apenas una década en el mercado, esta compañía se ha posicionado como uno de los cuatro líderes globales en videovigilancia.

En México, su presencia se expande gracias a la combinación de innovación y precios competitivos. Roberto Ávila, gerente de ventas y proyectos de ciudades seguras en Uniview México, destaca la tecnología Owlview, que permite ver a color en condiciones de muy baja iluminación.

“Antes, revisar horas de video era un trabajo difícil. Hoy, con nuestras analíticas de IA en los NVRs, se pueden buscar patrones por palabras: persona con camisa negra, audífonos o paraguas rojo, y el sistema localiza las imágenes en segundos”, explica.

La marca ha instalado más de 10 mil cámaras en alcaldías de la Ciudad de México y equipos en Guanajuato, Mérida y Baja California. Además, su certificación NDAA le abre puertas en Estados Unidos y Canadá, donde otras marcas chinas no pueden participar.

“Nuestro reto es competir de tú a tú con marcas internacionales, y lo hacemos con innovación constante y mejor precio”, asegura Ávila.



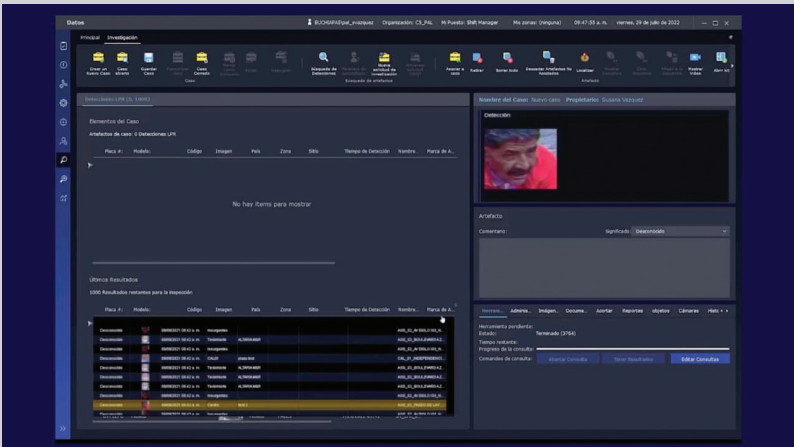
Roberto Ávila, gerente de ventas y proyectos de ciudades seguras en Uniview México

Convergencia hacia ciudades inteligentes

Aunque cada compañía tiene un enfoque particular, todas coinciden en que la seguridad pública no puede limitarse a reaccionar. La tendencia va hacia ciudades inteligentes capaces de anticipar riesgos, integrar sistemas de movilidad, medio ambiente y transporte, así como gestionar información en tiempo real.

Los proyectos de C4 y C5 en México y Latinoamérica muestran que la innovación tecnológica puede reducir homicidios, robos y delitos de alto impacto, siempre y cuando vaya acompañada de una correcta coordinación policial y una visión de largo plazo.

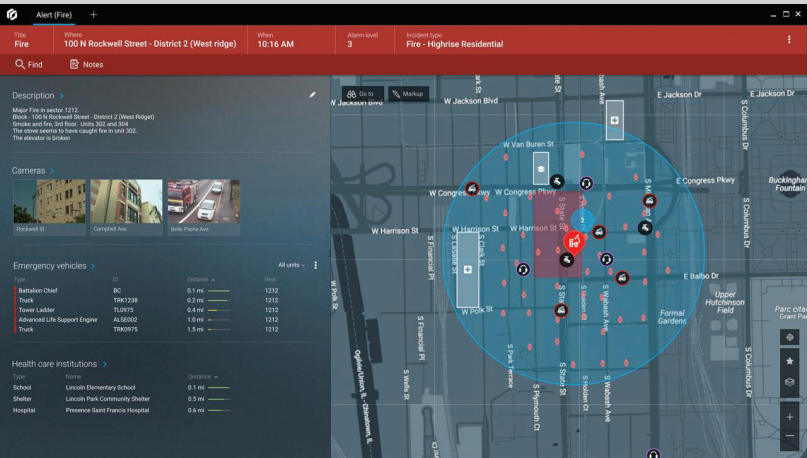
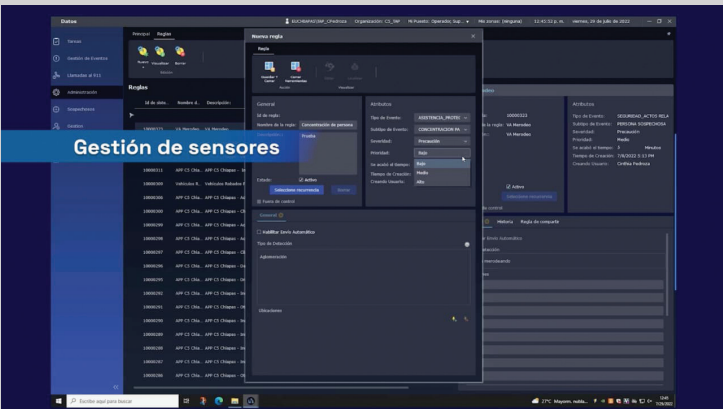
La interoperabilidad dejó de ser aspiración técnica para convertirse en requisito operativo. La “visión unificada” de Genetec, el “sistema de los subsistemas” de Kabat One, las





tres capas de IA de Hikvision y la combinación costo-beneficio + analítica embebida de Uniview, convergen en un mismo punto: disminuir segundos críticos entre el evento y la respuesta. Con reglas claras de datos, flujos guiados y tableros que resuelven — no solo muestran —, el C2, C4 o C5 funciona como un cerebro en tiempo real.

Para **Kabat One**, el reto inmediato es profundizar la automatización de eventos entre agencias y escalar su módulo ciudadano Connect sin sacrificar privacidad. Niv Yarimi lo resume con una meta medible: “Queremos que cada despacho tarde menos, que cada investigación sea más sólida y que cualquier cámara útil se sume de forma segura. Si la tecnología no salva vidas, no cumple su propósito”.



En Genetec, la apuesta pasa por mantener estándares abiertos, gobernanza de datos y ciberseguridad certificada para escalar desde municipios hasta estados completos, sin cambiar de plataforma. Michelle Nieto lo plantea así: “Seguiremos unificando sensores, video, accesos y comunicaciones bajo marcos de privacidad. Que el operador decida mejor y más rápido es la verdadera innovación”.



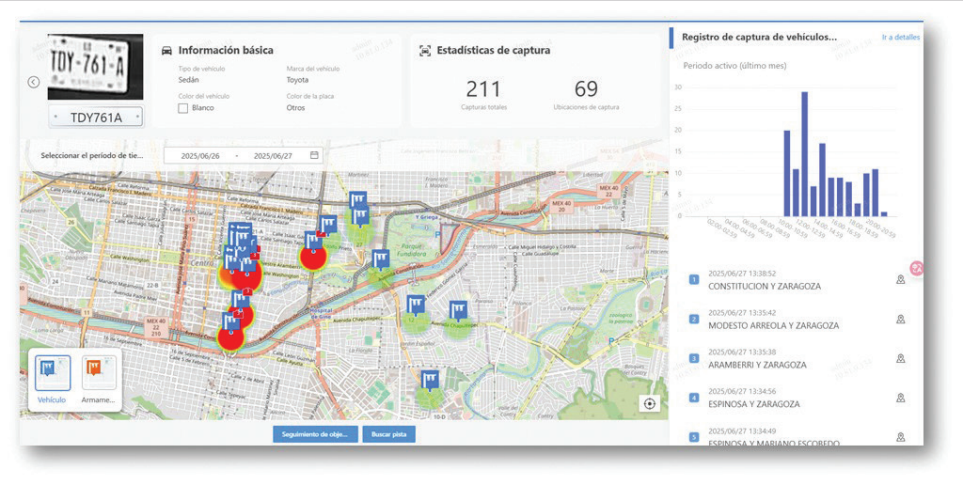
-  **Revista Más Seguridad**
-  **@revmasseguridad**
-  **Más Seguridad Magazine**
-  **revmasseguridad**
-  **Revista Más Seguridad**
-  **Revista Más SEguridad**
-  **Más Seguridad Magazine**

# MÁS SEGURIDAD

Magazine

[www.revistamasseguridad.com.mx](http://www.revistamasseguridad.com.mx)





**Hikvision** llevará su estrategia de inteligencia en el borde, en el centro y en el software hacia tableros ejecutivos con gemelos digitales y mantenimiento predictivo de infraestructura. Rubén García Soriano, cierra con una línea: “Alta disponibilidad 24/7, menos falsas alarmas y análisis a gran escala. La ciudad necesita saber qué pasa ahora y prever qué puede pasar después”.

En **Uniview**, el camino seguirá anclado en el costo-efectivo con IA utilitaria dentro de NVRs, visión nocturna a color (Owlview) y certificaciones como NDAA para abrir mercado en entornos críticos.

Para Roberto Ávila, “buscamos tecnología que cualquiera pueda operar y que rinda en campo. Si la búsqueda por palabras resuelve en segundos lo que antes tomaba horas, estamos haciendo lo correcto”.



Los cuatro actores coinciden en que 2025–2026 será decisivo por la presión de grandes aforos, movilidad, turismo y eventos deportivos. Más que sumar miles de cámaras, la clave será orquestarlas: analíticas coherentes, flujos de despacho auditables, videowalls que prioricen incidentes y módulos móviles — bodycams, torretas inteligentes, motos lectoras— sincronizados con la red de postes y con los CAD/911.

Como sintetiza Niv Yarimi al hablar del cambio cultural que ya se ve en diversos estados: “De edificios monumentales pasamos a decisiones basadas en datos”; Michelle Nieto cierra: “la seguridad no solo reacciona, también anticipa”; Rubén García de su lado, subraya “información accionable en segundos”; y Roberto Ávila concluye “innovación útil, accesible y lista para operar”.

Con esta ecuación, el C4/C5 para de ser sala de pantallas para convertirse en palanca real de seguridad y desarrollo tecnológico en seguridad de alto desempeño.



# AMESIS se suma a estrategia gubernamental

## “Cero Robos” en carreteras

- En esta lucha frontal vs robo de camiones, será crucial robustecer la vigilancia aérea para verificación del balizado de unidades de carga e implementar medidas para la aplicación de la ley antijammer.
- La asociación sumará tecnología satelital de sus empresas afiliadas, quienes dan servicio a un importante número de unidades motrices y de arrastre activas, a través de modernos centros de monitoreo.
- Cuenta con suficientes monitoristas especializados, capacitados y certificados en temas de rastreo, telemetría y manejo de crisis, así como videovigilancia móvil en tiempo real.

Recientemente, el gobierno federal, a través de la Guardia Nacional (GN), presentó la estrategia especial “Cero Robos”, la cual ya se implementa en las carreteras México-Puebla, México-Querétaro y Culiacán-Mazatlán. La Secretaría de Infraestructura Comunicaciones y Transportes (SICT) llevará a cabo cuatro acciones para reforzar la seguridad: cierre de accesos irregulares, instalación de arcos dinámicos, modernización de la infraestructura y la construcción de paradores integrales. A estos mecanismos preventivos oficiales, se suma la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital (AMESIS), una organización pilar en seguridad y rastreo de mercancías en tránsito.

A juicio de la mesa directiva de la AMESIS, en esta lucha frontal de la GN vs robo de camiones, será crucial robustecer la vigilancia aérea para verificación del balizado de unidades de carga, implementar medidas para la aplicación de la ley antijammer y robustecer la comunicación para que sea más estrecha y directa con la GN, dependencia con la que la organización ya mantiene acuerdos y trabajos colaborativos.

“Si bien hemos logrado en AMESIS una reducción de los robos en carreteras del 14% y mantener el 96% de recuperación en casos reportados (oportunos) en un promedio de 45 minutos, el delito no se detiene. En nuestra asociación registramos al cierre de junio del presente, 204 casos de hurtos de mercancías en tránsito. Puebla representa en siniestralidad el 25%, Estado de México 24%, Guanajuato 9%, San Luis Potosí 7%, Hidalgo, Jalisco, Veracruz y Michoacán, cada uno con un respectivo 4%. El resto del país ocupa el 15%. Los trabajos en conjunto con la Guardia Nacional a través de la estrategia Cero Robos, sin duda bajaremos más los índices negativos”, añadió Raymundo Mancera Sandoval, presidente de la AMESIS.

Ante la estrategia anunciada por la Presidenta de México, que comenzó en las carreteras federales México-Puebla, México-Querétaro y Culiacán-Mazatlán, pero se proyecta que llegue a todo el país, será necesario fortalecer los trabajos preventivos de la GN vs robo de camiones, apoyadas con las sinergias del gobierno federal con las organizaciones privadas que se dedican de alguna manera a combatir el robo de camiones, en este caso con los proveedores de telemetría, aseveró el directivo.

En este mismo contexto, como se recordará, el Comandante de la Guardia Nacional, Hernán Cortés Hernández, informó que, en la carretera México-Querétaro se desplegaron 585 efectivos, 194 vehículos, tres helicópteros, dos aeronaves no tripuladas y 20 drones, así como 10 torres para la detección de vehículos con reporte de robo. Y para la identificación y ubicación de los grupos delictivos, se desplegaron cuatro células de inteligencia.

En la carretera México-Puebla, se desplegaron 302 efectivos, 131 vehículos, tres helicópteros, dos aeronaves no tripuladas y 22 drones, así como 10 torres para la detección de vehículos con reporte de robo y cinco células de inteligencia.

En la Maxipista de Mazatlán-Culiacán, 298 efectivos realizan

vigilancia en 143 vehículos, apoyados por dos helicópteros, 12 drones como medios aéreos y cinco torres para la detección de vehículos con reporte de robo, así como cuatro células de inteligencia.

Cabe resaltar que la Secretaría de Infraestructura, Comunicaciones y Transportes, informó que se realiza el cierre de accesos irregulares para reforzar la seguridad en carreteras. En la México-Querétaro se han atendido 17 de 118 accesos; en la México-Puebla ya se cerraron dos y 36 están en proceso.

Se instalarán arcos dinámicos en 12 puntos estratégicos de estas carreteras, así como en diferentes ejes troncales. Se duplicará la capacidad de Caminos y Puentes Federales (CAPUFE) que actualmente tiene 2 mil 142 dispositivos de detección, 155 trabajadores y monitoreo 24 horas.

Al inicio serán 13 paradores integrales, 10 arrancarán las obras este 2025, mediante inversión mixta, y contarán con controles de acceso y seguridad, estacionamientos, servicios, áreas de descanso y esparcimiento, médicas y de alimentos. La meta al 2030 es contar con 30 paradores en la Red Federal de Carreteras.

“A este importante número de elementos y equipos oficiales, AMESIS sumará la tecnología satelital de sus empresas asociadas, quienes dan servicio a un importante número de unidades motrices y de arrastre activas, quienes a través de modernos centros de monitoreo que operan 24/7, tienen cobertura a nivel nacional; adicional, cuenta con monitoristas suficientes, especializados, capacitados y certificados en temas de rastreo, telemetría y manejo de crisis, así como videovigilancia móvil en tiempo real.”





# Inteligencia Artificial (IA) aplicada en la investigación de accidentes aéreos



**Mtro. Eduardo Reyes López**  
Ingeniero en Aeronáutica del IPN.  
Maestría en Dirección Estratégica y  
Gestión de la Innovación. Ha ocupado  
puestos directivos y gerenciales en áreas  
de seguridad de importantes empresas  
del sector aeronáutico, de grupos  
aeroportuarios y protección privada.  
**México**

Articulista Invitado

La importancia de la investigación de un accidente aéreo radica en llegar a la causa raíz y a los factores contribuyentes que produjeron el evento. La precisión en las conclusiones en términos de seguridad, implica una gran responsabilidad por parte de los investigadores para la prevención de futuros accidentes que pudieran ser ocasionados por la misma causa o por factores contribuyentes similares. El sesgo de confirmación subconsciente es parte de la naturaleza del ser humano y en teoría, algo que los investigadores están capacitados para mitigarlo, sin embargo, es casi imposible eliminarlo por completo de sus conclusiones. Este sesgo consiste en interpretar la información conforme a las creencias preexistentes del investigador sobre las causas de un accidente, en lugar de considerar todas las evidencias objetivamente, esto puede llevar a conclusiones erróneas o incompletas sobre lo sucedido, ignorando otras hipótesis que pudieran acercarse más a la causa raíz del evento.

Pero esto es solo un ejemplo en donde la Inteligencia Artificial pudiera jugar un papel preponderante para contribuir a investigaciones más exactas y confiables. La realidad de las cosas es que, aún y cuando hay avances sustanciales en el uso de la IA, para la investigación de accidentes aéreos aún hay mucho camino por recorrer. Un estudio del uso de la IA en tres accidentes aéreos: TransAsia Airways GE235, Air France AF447 y Helios Airways Flight HCY552 comparó las conclusiones generadas por los investigadores y aquellas generadas por ChatGPT siendo totalmente

diferentes e inclusive en algunos casos, variando completamente las versiones arrojadas por ChatGPT para el mismo accidente (<https://www.sciencedirect.com/science/article/pii/S2772662223001984>), pero ¿a qué se debe esto? principalmente a lo que se llama “alucinaciones artificiales” y que consiste en incrustar y producir falsedades aleatorias dentro del contenido generado por la IA, pudiendo contener información falsa o engañosa presentada al lector o espectador como un hecho. A pesar de lo anterior, el uso de la IA, puede ser extremadamente útil como herramienta de apoyo en investigación de accidentes de aviación, pues además de mitigar los errores de interpretación del ser humano, reducirá notablemente el tiempo de una investigación.

### Aplicación de la IA en investigación de accidentes aéreos

Dentro de las bondades que la IA puede aportar al proceso de investigación de un accidente aéreo están:

- Reconstrucción y animaciones del accidente mucho mas confiables y más rápidas de elaborar, actualmente una reconstrucción y animación cuesta alrededor de 50,000 USD y puede llevar hasta meses, con la IA el costo se reduciría sustancialmente y el tiempo de elaboración podría ser de minutos.
- La IA puede comparar directamente los datos de la grabadora de datos de vuelo con las grabaciones del registrador de voz de la cabina y otros datos de señales acústicas para proporcionar una visión más clara de la cronología de los acontecimientos que condujeron a un accidente.
- La IA puede simular el funcionamiento interno de partes y componentes de la aeronave que tuvieron relación con el accidente, bajo diversas condiciones, lo cual puede generar una comprensión más clara y precisa, por ejemplo, de los efectos que el medio ambiente tuvo sobre cierto sistema de la aeronave.
- La IA puede revisar todos los datos disponibles sin tener ideas preconcebidas de lo que podría haber causado un accidente, por lo tanto, tiene el potencial de eliminar todos los elementos de sesgo de confirmación subconsciente de sus conclusiones, ofreciendo así resultados más precisos.



- La IA puede apoyar la creación de una declaración clara del problema, es decir, establecimiento de hipótesis más cercanas a la realidad, delinear las funciones del equipo de investigación de accidentes y el control de preservación de las pruebas originales.
- La IA puede apoyar al proceso de entrevistas de testigos y personal involucrado en el evento, el análisis de las entrevistas, calibrar el tono y el sentimiento, y ayudar a identificar solapamientos o inconsistencias en los testimonios. Puede analizar la fraseología utilizada en entrevistas, informes o incluso políticas para detectar un encuadre cargado de culpa o sesgado que pueda influir en los resultados.
- La IA puede recopilar e integrar datos mediante la extracción y síntesis de información a partir de imágenes de vídeo, registros de audio, fotos del equipo, procedimientos, entrevistas y más.
- La IA puede reconocer patrones y análisis de datos mediante la identificación de tendencias entre conjuntos de datos, vinculación de factores contribuyentes, y destacar los contribuidores sistémicos tales como presiones de tiempo o defectos de diseño.
- La IA puede evaluar si los procedimientos eran prácticos y accesibles en el contexto de las condiciones reales de trabajo.
- La IA ayudar a crear informes claros y sin sesgos.
- A diferencia de los investigadores humanos que pueden tener dificultades para integrar diversas fuentes de información, la IA puede procesar simultáneamente durante y después de los accidentes, fotografías del equipo y escenas documentación técnica incluyendo planos y procedimientos escritos.
- Una aplicación valiosa de la IA en la investigación de accidentes, es su capacidad para identificar factores que contribuyen más allá de las acciones individuales. Las investigaciones tradicionales a menudo se detienen en el nivel de «error humano», pero la IA puede ayudar a las organizaciones a mapear interacciones complejas del sistema.
- Visualizar cómo las decisiones en diferentes niveles organizacionales influyeron en el accidente. Identificar problemas organizativos latentes: Reconocer patrones que sugieren problemas sistémicos más profundos, analizar la presión de producción, cuantificar cómo las demandas del itinerario pueden haber contribuido a la generación de riesgos, evaluar la facilidad de uso del procedimiento, evaluar si los procedimientos eran viables en condiciones reales.
- La IA puede señalar cuando los investigadores están repitiendo conclusiones pasadas, lo que alienta a dar un paso atrás para considerar nuevas posibilidades.
- Quizás lo más importante, los investigadores pueden y deben inducir intencionalmente a la IA a cuestionar sus conclusiones preliminares y finales. Este cuestionamiento deliberado -pedir al modelo que la haga de abogado del diablo o proponga interpretaciones alternativas- puede poner de relieve puntos ciegos y forzar la reconsideración de hechos supuestos o diagnósticos estrechos.

**Desafíos de la IA en la investigación de accidentes aéreos**

No obstante, lo anterior, la IA aún presenta grandes retos y desafíos que tendrá que vencer para poder ser considerada como una herramienta confiable para la investigación de accidentes aéreos:

- **Confianza:** La verdadera pregunta y el principal desafío radica en si la industria de la aviación está preparada para utilizar la IA en casos sensibles como un accidente aéreo. La confianza del público no sólo tendrá que afianzarse más con el uso de tales herramientas, sino que será igualmente vital establecer la confianza y el apoyo de los órganos reguladores y las propias autoridades legales para que las conclusiones de la IA sean admisibles inclusive en los litigios derivados de la investigación del accidente.
- La IA debe erradicar esas alucinaciones artificiales o inducción de falsedades aleatorias dentro de su contenido generado.
- **Posible falta de repetibilidad:** A pesar de que la IA no sufre de sesgo de confirmación, requiere entradas de datos de alta calidad para que sus conclusiones sean lo suficientemente precisas y confiables. Dado que las herramientas de IA aprenden constantemente de los nuevos datos introducidos, la respuesta a una pregunta planteada hoy puede diferir de la respuesta que dé mañana. Si bien estas



respuestas no pueden ser muy diferentes entre sí, la falta de repetibilidad puede constituir un obstáculo para las autoridades reguladoras y los sistemas judiciales que afirman el uso de la IA en las reconstrucciones y análisis de accidentes.

**Recomendaciones para utilizar la IA en investigación de accidentes de aviación**

La IA sirve como un amplificador de las capacidades humanas en lugar de un sustituto, proporcionando ideas y postulados desafiantes, mientras que los seres humanos mantienen la responsabilidad final de las conclusiones y recomendaciones. Las organizaciones interesadas en integrar la IA en sus procesos de investigación de accidentes pueden comenzar con estos pasos prácticos:

- **Comience pequeño:** Comience con aplicaciones enfocadas mientras construye confianza en el enfoque.
- Utilizar la IA para analizar el lenguaje en los informes históricos de accidentes a fin de identificar dónde el sesgo puede haber influido en las conclusiones.
- Haga que la IA genere preguntas de entrevista abiertas para su próxima investigación.
- La IA también puede utilizarse para evaluar la utilidad práctica de los procedimientos frente a las condiciones del mundo real.
- Crear oportunidades para que los equipos de investigación practiquen con herramientas de IA en escenarios de bajo riesgo antes de aplicarlas en accidentes significativos.
- Reconocer las preocupaciones de los profesionales de la seguridad que pueden estar preocupados por la tecnología que disminuye su papel.
- Posicionar a la IA como un amplificador de la sabiduría humana más que como un sustituto.
- Crear protocolos para la privacidad de los datos y el uso de la IA.
- Realizar un seguimiento de cómo la integración de IA afecta a la calidad de la investigación y la implementación de las recomendaciones.
- Simplificar la revisión de documentos: Utilizar la IA para verificar que los procedimientos, las directrices de auditoría y los documentos de capacitación se actualizan sobre la base de los resultados de la investigación.
- Mejorar continuamente las aplicaciones de IA en función de la experiencia del usuario y los resultados de la investigación.

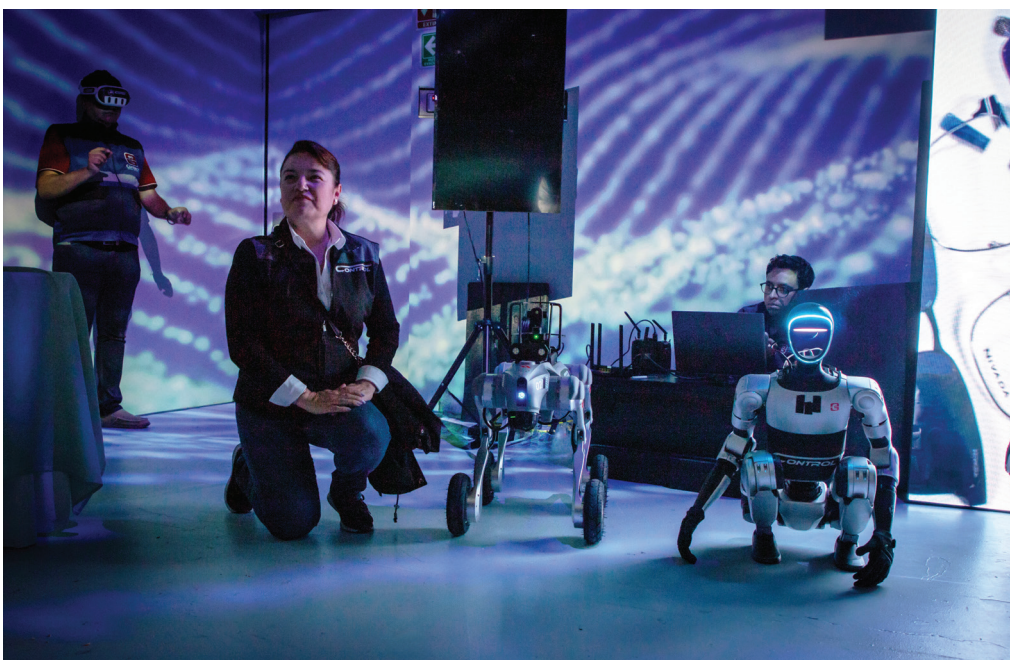
**Conclusión**

La IA aporta potentes capacidades analíticas a la investigación de accidentes, el elemento humano sigue siendo insustituible. El enfoque más eficaz es una asociación bien pensada que aproveche los puntos fuertes únicos de ambas: IA: procesamiento de datos a escala, reconocimiento de patrones, reducción de sesgos, consistencia y análisis incansable de información compleja. Fortalezas humanas: Comprensión contextual, empatía, juicio ético, pensamiento creativo y la capacidad de construir confianza con los involucrados en el incidente. Esta asociación funciona cuando los investigadores humanos mantienen su papel como líderes de pensamiento-guiando la investigación, interpretando los hallazgos a través de su sabiduría experiencial, y haciendo juicios basados en valores sobre lo que más importa. 





# 25 años de liderazgo, innovación y compromiso en la seguridad privada en México



- La empresa mexicana integra tecnología avanzada con capital humano para transformar la seguridad privada.
- Perros robot, humanoides y un Security Operations Center forman parte de la visión a futuro.
- Con más de 4 mil colaboradores, la compañía tiene cobertura nacional en sectores estratégicos.

**G**ruppo Control cumplió 25 años de operación en México y lo celebró con un anuncio que revela el rumbo que seguirá la industria en nuestro país. Benjamín Barona, CEO de la compañía, explicó que la apuesta está en un modelo híbrido de protección, donde la tecnología no sustituye al guardia tradicional, sino que potencia sus capacidades.

“Más allá de cotizar 50 guardias, podemos diseñar un esquema con 15 especialistas apoyados por tecnología, lo que genera mayor trazabilidad, perfiles más profesionales y un retorno de inversión para el cliente”, señaló Barona en conversación con Más Seguridad Magazine.

El concepto se materializa en soluciones que combinan vigilancia física con herramientas tecnológicas. Control opera un Security Operations Center (SOC) que concentra alertas y monitoreo en tiempo real, y al mismo tiempo desarrolla proyectos de innovación que van desde sistemas de videovigilancia hasta la incorporación de perros robot y humanoides.

En estos años, el grupo ha creado divisiones especializadas: Control Elite (guardias armados y escoltas), Control Trust (controles de confianza), Control Response Team (reacción ante emergencias), servicios médicos y ambulancias, además de Contech, el brazo tecnológico que gestiona proyectos integrales. Con ello, la empresa atiende a diferentes sectores industriales como el automotriz, alimentos y bebidas, retail corporativo y plantas manufactureras.

La tecnología no encarece los servicios, al contrario, optimiza los recursos: “No se trata de reemplazar al personal, sino de

transformar sus funciones hacia una mayor especialización. Habrá una reducción natural en ciertas áreas, pero crecerá la demanda de expertos que operen estas herramientas”, puntualizó.

Actualmente, Grupo Control cuenta con presencia en todo el país mediante oficinas regionales y una plantilla de más de 4 mil colaboradores entre personal operativo, administrativo e instaladores. La compañía ha invertido en patrullas, infraestructura y diseño de marca, con el objetivo de transmitir confianza en un sector donde la reputación es clave.

La combinación de experiencia, capital humano y visión tecnológica convierte a esta firma en una de las empresas que marcan pauta en la seguridad privada mexicana. Su apuesta busca responder a un entorno donde los riesgos se complejizan y la eficiencia es indispensable.

## Cinco lustros impulsando un modelo híbrido de protección

Es importante mencionar que el pasado 4 de septiembre, Grupo Control celebró su 25 aniversario con un evento inmersivo que reunió a guardias, colaboradores administrativos, clientes, proveedores y aliados estratégicos, donde la empresa mostró no solo su historia, sino también su visión de futuro: un modelo de seguridad híbrida que combina la fuerza de la tecnología con el valor humano, bajo el concepto de “Control Beyond”.

## Una historia de pasión y legado

“Hoy celebramos 25 años de tener todo bajo Control”, fueron las palabras de Benjamín Barona, CEO de Grupo Control, al dirigirse

a los más de 220 invitados en la gala para clientes. Recordó los orígenes de la empresa y rindió homenaje a Santiago Barona, fundador de Control, cuya visión y tenacidad lograron posicionar a la compañía como referente nacional en seguridad privada integral.

“Aunque ya no esté físicamente, su legado sigue vivo en cada rincón de Control. Él nos enseñó que la seguridad no es solo un servicio: es una misión, una vocación que se honra cada día con responsabilidad y compromiso”, señaló Benjamín Barona.

**Tres eventos, una celebración**  
**Guardias de Control: motivación y orgullo**

La mañana comenzó con un homenaje a quienes representan la primera línea de la seguridad: los guardias. En un ambiente cargado de energía y camaradería, los asistentes vivieron la experiencia inmersiva y recorrieron la historia de la empresa, comprendiendo cómo la innovación marcará los próximos 25 años.

Se reconoció a colaboradores con más de 15 años de antigüedad y se evocó con emoción la memoria de Santiago Barona, fundador de la compañía. Hubo momentos de gran cercanía: dinámicas motivacionales, palabras de los directivos y un desayuno compartido que cerró con el mensaje de Benjamín Barona, Director General.

El guardia Jorge Tomás Soto, resumió el sentimiento colectivo: “Estoy sorprendido de la gran empresa a la que pertenezco, nunca había venido a un evento así; superó por mucho mis expectativas y seguiré siendo parte de la familia Control por muchos años más”.

**Colaboradores administrativos: inspiración y compromiso**

Al mediodía, la celebración continuó con los equipos administrativos de oficinas centrales y foráneas, con representación de ciudades como Toluca, Querétaro, Veracruz, Acapulco, Guadalajara, Monterrey y Saltillo.

Después de la experiencia inmersiva, los asistentes participaron en una conferencia magistral de Matías Montero, quien motivó a los colaboradores subrayando la importancia de formar parte de una empresa que celebra 25 años de historia y que mira con firmeza hacia los próximos 25.

El evento incluyó un espacio de convivencia en la comida, reforzando la unión entre áreas, y cerró con las palabras de Benjamín Barona, quien agradeció el esfuerzo de cada colaborador y compartió la visión de crecimiento e innovación que guiará los siguientes años.

**Clientes, proveedores y aliados: innovación y visión de futuro**

La noche fue el escenario para el evento de mayor proyección, destinado a clientes, proveedores y aliados comerciales. Tras recorrer la experiencia inmersiva, los invitados conocieron de primera mano las nuevas propuestas de seguridad que integran inteligencia artificial, robótica y el Security Operations Center (SOC) como columna vertebral de un modelo de seguridad híbrida.

La conducción del evento estuvo a cargo de la actriz Naomi Hernández, quien dio paso a una serie de videos institucionales y al discurso del Director General, que emocionó y reforzó la confianza en el camino de Control. Posteriormente, un brindis y una celebración marcaron el cierre de la jornada.

En cada momento, el mensaje fue consistente: el



verdadero éxito de Control radica en su gente y en la confianza depositada por sus clientes a lo largo de un cuarto de siglo.

**Innovación al servicio de la seguridad**

Durante la gala, se presentó el modelo de seguridad híbrida que marcará la próxima etapa de la empresa. Proyectos como Control, Contech, Control Trust, Custos, Control Elite y el futuro de Control Beyond reflejan la capacidad de la organización para integrar soluciones tecnológicas de última generación —como inteligencia artificial, drones, monitoreo avanzado y controles de confianza— con la experiencia y compromiso de su talento humano.

“Lo que hacemos no es solo cuidar, vigilar o proteger. Lo que hacemos es generar tranquilidad, confianza y paz. Y lo hacemos innovando”, afirmó el Director General.

**Un futuro profundamente humano**

Pese al impulso tecnológico, en Control la persona sigue en el centro. Con un impacto en la vida de miles de familias, la compañía ha demostrado que la seguridad también se construye desde lo social y lo humano.

Benjamín Barona subrayó: “Este 25 aniversario no es solo un momento para mirar atrás. Es, sobre todo, un compromiso hacia adelante: de seguir creciendo, de seguir innovando y de mantener siempre nuestros valores como norte. El camino recorrido nos llena de orgullo; lo que viene nos llena de emoción”.

**Gratitud y visión**

La noche concluyó con un agradecimiento del CEO de Grupo Control a los asistentes y a todos los que han hecho posible estos 25 años de la firma y con un poderoso mensaje: la seguridad privada en México tiene un futuro más fuerte, humano y tecnológico, y Control seguirá siendo protagonista de esa transformación.



Benjamín Barona, CEO DE Grupo Control y Adrián Barona, director de comunicación





## En seguridad privada, ser diferente importa más que ser “mejor”

La seguridad privada está enfrentando un problema profundo: el sector está muy saturado, los márgenes cada vez más bajos y la mayoría de las empresas parecen casi que “intercambiables”.

El discurso clásico de “tenemos 20 años de experiencia” o “somos tu mejor opción en seguridad” ya no significa ventaja competitiva. En un entorno donde todos prometen lo mismo, el cliente solo compara una variable: precio. Y cuando el precio es el único factor, la calidad, inevitablemente, es la que paga los platos rotos.

### La ilusión de “ser mejor”

El problema con la narrativa de “somos mejores” es que es imposible de comprobar. Es muy subjetiva, genérica y fácilmente cualquiera puede decir lo mismo si quiere.

El resultado es que el mercado de la seguridad privada terminó convertido en un servicio de catálogo: uno más, sin valor agregado ni razones claras para elegir una empresa sobre otra. compañías que hablan de experiencia, innovación y certificaciones pero siguen operando con celulares y WhatsApp en campo.

Es como ver a un cirujano experto operando con tijeras de cocina: conocimiento de alto nivel, pero herramientas inadecuadas.

### El valor de ser diferente

En este escenario, la verdadera ventaja competitiva no es ser “mejor”, sino ser diferente.

- Diferente es entregar trazabilidad y transparencia en tiempo real en lugar de reportes manuales.
- Diferente es usar plataformas de comunicación críticas diseñadas para seguridad en lugar de depender de celulares.
- Diferente es ofrecer evidencia auditable en vez de promesas. Ofrecer tranquilidad que estás cerrando brechas operativas y que cumples con lo que prometes.

La diferencia se vuelve tangible, visible y muy difícil de imitar. Y esa es la clave para escapar de la guerra de precios.

### La resistencia al cambio

Pero el mayor problema es que el sector enfrenta un obstáculo interno enorme. Y que están muy cómodos con lo que ya conocen. En la comodidad de hacer las cosas “como siempre las han hecho”.

Seguir usando herramientas básicas parece “más barato” y “más conveniente” en el corto plazo, pero en realidad genera costos ocultos



gigantescos. Rotación, incidentes innecesarios, fallas de cumplimiento, pérdida de contratos y erosión de reputación. Pero lo más importante. Lo que más se está viendo afectado es la percepción de los clientes cuando ven a un guardia de seguridad desconectado de la realidad, enterrado en la pantalla de su celular.

Las empresas que se resisten al cambio terminan atrapadas en una carrera hacia abajo, a ver quien puede tirar más los precios al piso. Y cuando tu bajas los precios, ¿adivina qué? tu competencia también los baja. Hasta que un día, ya no estás cobrando... estás pagando por trabajar.

Las empresas que invierten en diferenciarse con datos, transparencia y tecnología específicamente desarrollada para seguridad son las que logran atraer clientes premium y construir márgenes sostenibles.

### Diferente vs mejor

La ecuación es simple:

- Mejor = declaración subjetiva.
- Diferente = evidencia objetiva.

Y los clientes que hoy contratan servicios de seguridad profesionales no compran promesas. Compran resultados que puedan auditar. Compran confianza basada en el cumplimiento real. Compran tranquilidad.

### Hacia dónde va la industria

La seguridad privada se encuentra en un punto de inflexión. Y la realidad es que en esta industria (como en todas las demás) el futuro no le pertenece a las empresas que intentan ser “las mejores” dentro de un modelo que ya no funciona, sino a las que rompen el molde y crean nuevas categorías de valor.

En un mercado comoditizado, lo diferente es lo que construye reputación, rentabilidad y sostenibilidad a largo plazo.

La industria de la seguridad tiene que dejar atrás la obsesión por ser “mejor” que la competencia. Ese juego ya está perdido.

El único movimiento estratégico es ser diferente. Porque en este mercado, lo mejor es discutible, pero lo diferente es incuestionable.



**Miguel Rivera,**  
Country Manager México  
miguel@italkptlatam.com  
ITALKPTT

# Comportamiento, coherencia y la seguridad

## que necesita alma: Cuando la experiencia no es suficiente



**Milagros Céspedes Álvarez**  
Coach PNL involucrada en la seguridad desde hace 32 años. Fundadora y directora del Centro de Estudios de Seguridad para Latinoamérica.  
[www.ceslatam.com](http://www.ceslatam.com)  
**Perú**

Articlista Invitada

**Lima, Perú.-** No es la primera ni la última vez que veo situaciones similares. Un profesional de reconocida trayectoria en seguridad comparte un video de una prueba técnica en una red profesional. Como técnica, impecable. Pero para quienes miramos con conciencia, nos percatamos que el personal de la prueba no llevaba ningún equipo de protección personal: ni mascarilla, ni lentes, ni guantes, ni indumentaria adecuada. Ni la más mínima señal de autocuidado.

Lo preocupante no fue el acto en sí, sino la naturalidad con la que se muestra... como si no hubiese nada que cuestionar. Como si la experiencia autorizara a ignorar lo que se exige a los demás.

### ¿Dónde quedó el factor humano en la seguridad?

Para algunos, podría parecer un detalle menor. Para mí, fue un recordatorio de algo que vengo diciendo, y repitiendo desde hace años: La verdadera crisis en seguridad no está en los sistemas, sino en los comportamientos.

La seguridad convencional sigue atrapada en lo demostrativo, centrada en cumplir normas, en exhibir dominio técnico. Pero la seguridad que necesitamos es otra. Una seguridad que reconozca al ser humano como el centro, no como un accesorio del procedimiento.

Y ahí surge la incongruencia; cuando un referente del rubro actúa sin tomar medidas de protección, no solo se pone en riesgo, transmite un mensaje peligroso, normaliza la negligencia, invalida la prevención.

### Seguridad sin conciencia es solo espectáculo.

Hay una brecha profunda entre la seguridad convencional — centrada en lo técnico, lo normativo, lo instrumental— y una visión más evolucionada y humana de la seguridad, donde la persona es el eje.

La seguridad convencional se preocupa por los equipos, protocolos y certificaciones... pero muchas veces olvida al ser humano detrás del equipo, manipulando, evaluando o tomando decisiones bajo presión.

La seguridad humana, reconoce emociones, percepciones, actitudes, valores y comportamientos como factores clave en la gestión del riesgo.

Bajo esta perspectiva, no basta con saber apagar un fuego o probar un polvo químico, hay que preguntarse cómo hacerlo sin comprometer la salud, la coherencia, ni el ejemplo profesional.



Este tipo de incongruencias solo revela que la técnica sigue ganando protagonismo, mientras la dimensión ética, humana y cultural de la seguridad pasa a un segundo plano.

El video no mostraba solo a una persona sin EPP, muestra una cultura profesional que sigue premiando el saber hacer por encima del saber ser. Una cultura que tolera la incoherencia mientras celebra la trayectoria. Y es aquí donde la responsabilidad del profesional con experiencia se vuelve crítica. Tener años en el rubro no otorga inmunidad, otorga un compromiso ético.

### Lo que está en crisis no es la técnica, es el comportamiento.

Porque cuando los comportamientos reales contradicen lo que los manuales promueven, la seguridad fracasa, aunque el sistema funcione.

Este artículo va especialmente para quienes llevan la conciencia de seguridad como bandera, no como eslogan. Para quienes saben que la prevención no se enseña solo con palabras, sino con la coherencia de cada acto. Porque si no reflexionamos ahora, si no revisamos esas conductas normalizadas y cómodas, si seguimos ignorando la incongruencia entre lo que decimos y lo que hacemos, la indiferencia terminará por erosionar el corazón mismo de nuestra cultura de seguridad. Y cuando eso ocurra, la brecha será tan grande que volver a empezar costará muchísimo más: no solo en tiempo o recursos, sino en confianza, credibilidad y vidas.

Esta reflexión no nace del enojo, sino del compromiso. Porque sé que muchos de nosotros creemos en una seguridad con propósito. Una seguridad que no se limita a procedimientos, sino que abraza la responsabilidad de cuidar y cuidarse.

No dejemos que la experiencia se convierta en excusa. Que nuestro comportamiento sea el mejor argumento. Y que la seguridad, finalmente, tenga alma.

Hoy aún podemos elegir ser ejemplo, elegir revisar nuestros hábitos, elegir una seguridad más humana, más consciente, más honesta. Y si al hacerlo nos llaman rebeldes, exagerados o incluso locos... entonces que así sea.

Porque toda transformación comienza con quienes se atreven a ver lo que otros prefieren ignorar.



# Ciudades Cuidadoras: un Nuevo Paradigma Urbano en Latinoamérica



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

**Q**uito, Ecuador.- El concepto de “ciudades cuidadoras” es una respuesta a la creciente necesidad de repensar la planificación urbana desde una perspectiva humana y equitativa, priorizando el bienestar de sus habitantes. Este enfoque va más allá de la infraestructura tradicional para centrarse en quienes requieren cuidados (niños, adultos mayores, personas con discapacidad) y en quienes los proveen. En Latinoamérica, diversos modelos han surgido, impulsados por la necesidad de abordar las profundas desigualdades sociales y de género que caracterizan a la región.

Estos modelos se entrelazan con la visión de la ISO 22341 CPTED Seguridad y resiliencia — Seguridad protectora — Directrices para la prevención del delito mediante el diseño ambiental, que promueve la seguridad por diseño coproduciéndola de la mano de quienes viven y usan cada

zona de las ciudades, y con el naciente Sistema Nacional de Cuidados (SNC) de México.

**Modelos y Buenas Prácticas en Latinoamérica:**  
El desarrollo de ciudades cuidadoras en la región ha adoptado enfoques variados, adaptándose a los contextos políticos y sociales de cada país.

- Bogotá, Colombia: la capital colombiana es un referente con su Sistema Distrital de Cuidado, cuyo pilar central son las “Manzanas del Cuidado”. Estos son nodos urbanos que concentran una amplia gama de servicios gratuitos, como lavanderías comunitarias, atención psicológica y jurídica, y espacios de respiro para las cuidadoras, mayoritariamente mujeres. La buena práctica aquí es la integración territorial de los servicios, reduciendo los “viajes de cuidado” y liberando el tiempo de las cuidadoras.





- Montevideo, Uruguay: Uruguay ha sido pionero en la región con su Sistema Nacional Integrado de Cuidados. A nivel municipal, Montevideo ha complementado este sistema con una política de accesibilidad universal en el espacio público. Se han implementado rampas, señalética podotáctil y semáforos sonoros para facilitar la movilidad de personas con discapacidad y adultos mayores. Esta buena práctica demuestra cómo la infraestructura puede ser una herramienta clave para la inclusión.
- Buenos Aires, Argentina: el programa “Cercanía” ha establecido centros de cuidado en barrios vulnerables, enfocándose en la proximidad y la flexibilidad de horarios. Estos centros ofrecen servicios de cuidado infantil y apoyo a las familias, respondiendo directamente a la necesidad de las madres trabajadoras de contar con un espacio seguro para sus hijos cerca de sus hogares o lugares de trabajo.

#### Avances y Buenas Prácticas en Municipios de México:

La implementación del concepto de ciudades cuidadoras en México ha ganado impulso, con gobiernos locales que adaptan sus estrategias a las realidades de cada ciudad.

- Ciudad de México: ha liderado con la creación de su Sistema Público de Cuidados. Las “UTOPÍAS” de la alcaldía Iztapalapa son un ejemplo destacado de cómo la inversión en infraestructura pública puede ser una herramienta de justicia social y de aplicación de los principios de la ISO 22341 CPTED. Estos complejos ofrecen vigilancia natural, al ser espacios abiertos y bien iluminados, y un control de acceso implícito que se basa en la apropiación comunitaria. Al concentrar servicios como centros de salud, casas de día para adultos mayores y lavanderías, reducen la carga de las cuidadoras y promueven la cohesión social.
- Monterrey, Nuevo León: con el programa “Monterrey me Cuida”, la ciudad se unió a la Alianza Global por los Cuidados. Su enfoque en la corresponsabilidad y en la creación de una red de apoyo tanto física como móvil, que llega a los hogares, representa un paso firme hacia una política de cuidados más integral.
- Guadalajara, Jalisco: la ciudad se ha enfocado en el apoyo directo a los cuidadores a través de programas como “Cuidamos a Quien nos Cuida”, que otorga un apoyo económico a quienes asumen esta labor. Esta es una buena práctica para visibilizar y retribuir, al menos parcialmente, el trabajo no remunerado que históricamente ha recaído en las mujeres.

#### Desafíos y pasos siguientes:

A pesar de estos avances, el camino para consolidar las ciudades cuidadoras en México y Latinoamérica enfrenta desafíos significativos.

- Fragmentación de políticas: los programas de cuidado a menudo dependen de administraciones municipales o

estatales, lo que dificulta su sostenibilidad a largo plazo. Es crucial la coordinación entre los diferentes niveles de gobierno para garantizar un marco legal y presupuestal sólido que no se disuelva con los cambios de gestión.

- Financiamiento: la inversión en infraestructura y servicios de cuidado es alta. Los gobiernos locales deben buscar fuentes de financiamiento sostenibles, incluyendo alianzas público-privadas y la reasignación de presupuestos para priorizar las necesidades de cuidado.
- Participación y Sensibilización: un cambio de paradigma requiere la participación de la sociedad civil y el sector privado. Es necesario sensibilizar sobre el valor del cuidado como un derecho, una responsabilidad colectiva y un motor de desarrollo económico. Los hombres deben ser incluidos activamente en estas discusiones para promover una verdadera corresponsabilidad.
- Inclusión y Accesibilidad: aún existen brechas en la accesibilidad para personas con discapacidad en muchas ciudades. Los proyectos urbanos deben ir más allá de la estética y cumplir con estándares rigurosos de diseño universal. Un paso pendiente es la adopción de normativas como la ISO 22341 CPTED de manera explícita en los códigos de construcción y planeación urbana.

#### Los Cuidados como Pilar Fundamental de ciudades incluyentes y equitativas:

México se ha posicionado como uno de los países más comprometidos en la región en la agenda de los cuidados. Como se destacó en el evento paralelo que se realizó en el marco de la XVI Conferencia Regional sobre la Mujer de América Latina y el Caribe, denominado: “Sistemas Integrales de Cuidados en Movimiento: Aprendizajes desde los UNCT y gobiernos nacionales”, donde se señaló que los cuidados son el pilar fundamental del bienestar y la prosperidad. Tienen la función social del sostenimiento de la vida, la economía y la sociedad; sin ellos, las economías y sociedades se paralizarían.

Este reconocimiento del valor social y económico de los cuidados es el punto de partida para que los gobiernos impulsen políticas que pasen de la esfera privada a la pública. El diálogo en este evento, que reunió a autoridades de México, Chile, Uruguay y Brasil, se convirtió en un espacio para compartir retos y buenas prácticas, fortaleciendo así la agenda regional.

En conclusión, el camino hacia las ciudades cuidadoras en Latinoamérica es prometedor. Los modelos de Bogotá y Montevideo demuestran que es posible crear sistemas robustos y equitativos.

En México, Monterrey y Ciudad de México ya están sentando las bases. El desafío ahora es escalar estas buenas prácticas, asegurar su sostenibilidad y transformar el cuidado de una carga individual a una responsabilidad colectiva, construyendo así entornos urbanos que sean verdaderamente justos y humanos para todos.



# Seguridad corporativa resiliente: convertir la vulnerabilidad en fortaleza



**Edison Cadena Ayala**  
MSC, CPO, CPOI, CSSM  
Gerente de la firma  
SEINNATIONAL CIA.  
LTDA.  
**Ecuador**

Articulista Invitado

“No es el más fuerte de las especies el que sobrevive, ni el más inteligente, sino aquel que mejor se adapta al cambio.” – Charles Darwin

**Q**uito, Ecuador.- En el universo de la seguridad corporativa, la resiliencia, entendida en su acepción más intrínseca, no es solo resistencia ni la capacidad de volver a un estado anterior tras una crisis, sino la aptitud profunda de transformación que permite a las organizaciones absorber los golpes de la adversidad y, en lugar de quebrarse, reconfigurarse para emerger más sólidas. En el terreno empresarial, donde las amenazas ya no son únicamente robos o incendios sino riesgos complejos que incluyen ciberataques, disrupciones globales en las cadenas de suministro, conflictos sociales, pandemias o el desgaste reputacional provocado por la desinformación, la resiliencia deja de ser un adorno conceptual y se convierte en la esencia misma de la seguridad corporativa.

Las organizaciones verdaderamente resilientes en materia

de seguridad no son aquellas que poseen el mayor número de cámaras de vigilancia ni los sistemas de detección más avanzados, sino las que han logrado integrar la seguridad en su cultura interna como un proceso dinámico. La resiliencia organizacional aplicada a la seguridad corporativa consiste en anticipar lo improbable, planificar lo inesperado y, sobre todo, cultivar una cultura capaz de absorber la incertidumbre sin que la operación se fracture. Así, la seguridad deja de ser percibida como un gasto operativo y se convierte en una inversión estratégica que protege los activos tangibles e intangibles: personas, reputación, confianza de clientes e incluso el sentido de propósito.

Los datos recientes refuerzan esta visión. El Business Continuity Institute (2024) encontró que las compañías con programas de resiliencia avanzados reducen hasta



un 40 % sus pérdidas operativas después de un evento disruptivo, mientras que aquellas que basan su estrategia de seguridad únicamente en recursos financieros sufren recuperaciones más lentas y costosas. A nivel de pequeñas y medianas empresas, un estudio desarrollado en Colombia con mipymes industriales (Research Gate, 2024) mostró que la gestión organizativa y operativa —liderazgo participativo, comunicación interna fluida, redes de confianza y planes adaptativos— pesa más que la disponibilidad de capital financiero al momento de superar una crisis. Esto desmonta el mito de que la resiliencia en seguridad se compra: se construye desde dentro, a través de estructuras flexibles, liderazgo comprometido y un sentido compartido de responsabilidad.

El caso de Morgan Stanley durante los ataques del 11 de septiembre en Nueva York es emblemático para la seguridad corporativa. Mientras muchas organizaciones quedaron paralizadas, la empresa había invertido en planes de evacuación, entrenamientos periódicos y protocolos de crisis. La consecuencia fue una respuesta ordenada que salvó miles de vidas. Este ejemplo evidencia cómo la resiliencia no es reactiva, sino fruto de la preparación previa, de la conciencia colectiva y del liderazgo capaz de inspirar confianza en medio del caos. Similar enseñanza dejó la pandemia de COVID-19: organizaciones que habían cultivado cultura resiliente, con equipos entrenados para la continuidad y con esquemas de seguridad híbridos (físicos y digitales), fueron capaces de mantener operaciones esenciales y conservar vínculos con sus clientes, mientras otras quedaron rezagadas.

La resiliencia aplicada a la seguridad corporativa es también una respuesta a los cambios del siglo XXI. Un estudio de BSI (2023) reveló que 8 de cada 10 ejecutivos consideran que la resiliencia es la ventaja competitiva más importante para sostener el crecimiento en entornos de incertidumbre. La data confirma que resiliencia y seguridad no pueden tratarse de manera aislada: cuando se integran en la cultura organizacional, permiten transformar la adversidad en un motor de innovación.

Desde una óptica humanizada, la seguridad

corporativa resiliente parte de reconocer que el eslabón central son las personas. No basta con implementar controles tecnológicos si los colaboradores no entienden el sentido de los protocolos o si no confían en las decisiones de sus líderes. Invertir en programas de capacitación, comunicación transparente y participación activa en los procesos de seguridad fortalece la capacidad de respuesta colectiva. Un guardia, un analista de riesgos o un ejecutivo no pueden reaccionar solos; es el entramado de confianza y cultura organizacional lo que permite que la resiliencia se materialice.

El análisis de la evidencia muestra un patrón claro: las organizaciones que abrazan la resiliencia como parte intrínseca de su seguridad corporativa no solo se recuperan más rápido, sino que utilizan cada crisis como un catalizador para reinventarse. Así, la resiliencia se convierte en un proceso de evolución permanente: las crisis dejan de ser meros episodios traumáticos y se convierten en oportunidades de aprendizaje organizacional, de fortalecimiento cultural y de reposicionamiento estratégico.

La seguridad corporativa resiliente, en consecuencia, no significa blindarse contra todo, porque lo incierto siempre estará presente. Significa aceptar la vulnerabilidad como parte natural del sistema y, desde allí, generar fortaleza colectiva. El valor no radica en regresar a la “normalidad” previa a una crisis, sino en avanzar hacia una versión superior, más consciente y más preparada de la organización. Este es el verdadero sentido de la resiliencia en seguridad: transformar el riesgo en oportunidad y convertir la incertidumbre en una ventaja que refuerza la sostenibilidad a largo plazo.

En última instancia, la resiliencia organizacional aplicada a la seguridad corporativa no es un destino, sino un viaje continuo. Implica cuestionar rutinas, aprender del error, integrar tecnología con criterio humano y entender que la seguridad ya no puede medirse solo en métricas de incidentes evitados, sino en la capacidad de la empresa para adaptarse y evolucionar en un mundo de riesgos líquidos. Así, seguridad y resiliencia dejan de ser conceptos separados y se funden en una sola fuerza estratégica que sostiene la confianza, la reputación y la permanencia de las organizaciones en tiempos de incertidumbre creciente. 

| Cuadro comparativo de hallazgos relevantes: |                                                                        |
|---------------------------------------------|------------------------------------------------------------------------|
| Fuente / Estudio                            | Hallazgo Clave                                                         |
| Business Continuity Institute (2024)        | Reducción del 40% en pérdidas operativas con programas resilientes.    |
| Researchgate – Mipymes Colombia (2024)      | Gestión organizativa y operativa pesa más que el capital financiero.   |
| Bsi (2023)                                  | 8 de cada 10 ejecutivos consideran la resiliencia ventaja competitiva. |

Fuentes consultadas:

Business Continuity Institute. (2024). Organizational Resilience Report. BCI Publications.

BSI Group. (2023). Organizational resilience: Harnessing disruption. British Standards Institution.

Darwin, C. (1859). On the origin of species by means of natural selection. London: John Murray.

Research Gate. (2024). Resiliencia empresarial en tiempos de la pandemia por COVID-19: los factores de éxito de las mipymes industriales. Recuperado de <https://www.researchgate.net/>

Wikipedia. (2024). Resiliencia organizacional. Recuperado de [https://es.wikipedia.org/wiki/Resiliencia\\_organizacional](https://es.wikipedia.org/wiki/Resiliencia_organizacional)





## ESS+ 2025 se consolidó como uno de las ferias más importantes; su edición 31 culminó con éxito

**Bogotá, Colombia.-** Con la afluencia de más de 16 mil asistentes, culminó la edición 31ª de la Feria Internacional de Seguridad ESS+, que, del 27 al 29 de agosto, demostró que la tecnología, y en especial aquellas soportadas en la inteligencia artificial generativa, están presentes en una gran cantidad de sistemas y soluciones que los expositores presentaron durante el encuentro. La feria fue organizada por PAYFC y Corferias y se llevó a cabo en el Gran Salón del recinto ferial.

“Gracias al trabajo aunado entre PAYFC y Corferias, se consolida, edición tras edición, como uno de los encuentros feriales más importantes en materia de seguridad en la región, con cerca de 250 expositores y más de 200 marcas representadas, provenientes de 26 países”, resaltó Laura Silva, jefe de proyecto de la Feria Internacional de Seguridad, Corferias.

Esta edición fue el escenario para que empresas, entidades, generadores de opinión, tomadores de decisiones y el público en general pudieran apreciar el futuro de la seguridad.

De esta manera, la feria se extendió a diversas áreas y actividades, con múltiples focos de atención: sistemas de protección para infraestructuras críticas, supervisión de grandes superficies a través de robots, desarrollos enfocados en la protección humana y el registro en ámbitos educativos, protección humana y sistemas de reacción en casos de incendio, entre otros. “La seguridad y la protección son actividades transversales a todas las áreas de la actividad humana”, comentó la directora de la Feria, Patricia Acosta, quien definió los resultados de la muestra como un éxito, no solo por los negocios que se concretaron, sino también por la importancia de la agenda académica y los seis encuentros gremiales que se adelantaron durante la feria, con 170 conferencistas y expertos, cumpliendo con la transferencia de conocimiento y la exhibición en directo de las innovaciones que marcan el futuro de la seguridad.

### Rueda de negocios, punto de encuentro e impacto

La rueda de negocios contó con la participación de 41 compradores procedentes de Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Panamá, Perú, y República Dominicana y 91 expositores, generando 248 citas con expectativas de negocios por 2.634.200 millones de dólares, evidenciando el potencial del mercado colombiano como centro estratégico regional de negocios.

De esta manera, la Feria Internacional de Seguridad ESS+, cierra la versión 31 y comienza a trabajar en la organización del 2026.

“Agradecemos a todas las marcas que desde que la feria nos ha acompañado y también a todas las que cada año se suman a este reto que nos involucra a todos: la seguridad. Este sin duda es un espacio que se caracteriza por mostrar la evolución de la industria y orgullosamente, nos hemos adelantado al futuro”, puntualizó Patricia Acosta.







# SERCOPP

SERVICES & CONSULT

Servicios de consultoría y  
personal profesional

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

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

📍 Dg. 81i #74C-19, Bogotá, D.C. Colombia

☎ +57 3108052421

✉ gerenciasercopp@gmail.com

[www.sercopp.com](http://www.sercopp.com)





# SECANCOL reduce la siniestralidad con plataforma de gestión de riesgos SARI

- La empresa colombiana adoptó SARI, herramienta que integra análisis de riesgos y reportes en tiempo real.
- La metodología se alinea con Normas ISO 31000 y 31010, garantizando precisión y confiabilidad.
- La digitalización permitió pasar de informes de 50 páginas a reportes ejecutivos de dos.

**Bogotá, Colombia.-** La empresa de seguridad SECANCOL LTDA, que presta servicios de protección intramuros a importantes cadenas de retail y compensación en Colombia, implementó la plataforma digital SARI para análisis de riesgos que ha transformado su operación.

30 años después de su fundación y ya en su segunda generación, SECANCOL Ltda, decidió llevar su modelo de seguridad a un nivel de ciberresiliencia. La compañía implementó SARI (desarrollada por la firma SERCOPP), una plataforma de gestión de riesgos que integra levantamientos en campo, tableros estadísticos con datos oficiales y reportes ejecutivos para clientes corporativos.

“SARI es la descripción perfecta de la tecnología aplicada a la toma de decisiones gerenciales”, resume Verónica Guzmán, CEO de SECANCOL. El objetivo es transformar datos en decisiones con velocidad y foco preventivo.

Antes, la operación enfrentaba tres frenos: estudios de seguridad sin actualizar a tiempo, identificación tardía de vulnerabilidades al inicio de los servicios y comunicación poco digerible para el cliente. Con SARI, la empresa estandarizó el proceso y lo puso en la palma de la mano del equipo operativo.

“Ahora tengo casi el 95% de los análisis de riesgos de mis clientes actualizados”, afirma Verónica Guzmán. La herramienta mide el estado de cada panorama, ordena tareas y entrega a la gerencia un programa de trabajo verificable.

El cambio no sustituyó personas, las potenció. 40 profesionales — coordinadores y analistas— usan la aplicación en sitio y la alta dirección revisa resultados para ajustar recursos: “SARI es autogestión, pero la hace el ser humano”, subraya la CEO. El efecto práctico resulta en menos carga operativa gracias a flujos claros y mejor organización de visitas y seguimientos, con métricas que suben a nivel directivo sin esperar cierres mensuales.

SARI se alinea con ISO 31000 e ISO 31010, lo que refuerza su rigor metodológico y estandariza el lenguaje entre SECANCOL y los clientes. Además, incorpora capacitación mensual y un módulo de reportes ejecutivos que sustituyó informes extensos e inoperantes.

“Ya no entregamos estudios de 50 páginas, sino un informe de dos páginas con información técnica y confiable”, explica Richard Vásquez, director de operaciones de SECANCOL. El equipo dejó atrás el trabajo forense interminable para concentrarse en hallazgos accionables. “La herramienta

ha reducido la siniestralidad en un 75%, lo que representa un ahorro significativo en reclamaciones y pagos asociados a siniestros. El impacto es medible en la reducción de la siniestralidad y en menores reclamaciones asociadas a incidentes.

“La diferencia está en que ahora contamos con información precisa, seria y sustentada en datos oficiales”, detalla Vásquez. La precisión surge de cruzar estadísticas de fuentes públicas con la evidencia levantada por más de mil colaboradores en todo el país, quienes registran incidencias en tiempo real desde teléfonos corporativos. Esos reportes llegan simultáneamente a operaciones y al cliente, habilitando decisiones compartidas en el momento.

SARI también flexibiliza la operación diaria con un módulo de incidencias específicas — accesos, estacionamientos, correspondencia— sin necesidad de correr un análisis completo. Esto acelera la respuesta y mejora la trazabilidad. Para retail y grandes superficies, foco estratégico de SECANCOL, todo esto se traduce en rentabilizar la inversión en seguridad física con indicadores visibles, alertas oportunas y tableros visuales que priorizan riesgos por probabilidad e impacto.

Un factor clave ha sido la coevolución de la herramienta con los procesos internos: “SARI inició con una estructura, pero juntos fuimos más allá”, dice Verónica Guzmán, aludiendo a ajustes de fondo y forma en la presentación de resultados y su integración con protocolos regulatorios. El piloto dio paso a iteraciones y despliegues que hoy convierten a SARI en estándar interno para continuidad del negocio, cumplimiento y seguridad corporativa, añade.

La adopción registra alta aceptación en el equipo operativo porque alivia cargas de tiempo, ordena rutas y facilita la divulgación al cliente. En paralelo, la división tecnológica de SECANCOL crece con videovigilancia, analítica e IA para aportar métricas y evidencia que cierran pérdidas recurrentes: “Es una llave que cerró pérdidas... una herramienta que recomendamos totalmente porque nos permite proteger al cliente y a la empresa de forma elegante y técnica”, concluye Richard Vásquez.

Con despliegue nacional que incluye agencias en principales ciudades y presencia transversal en entornos residenciales, institucionales y corporativos, la combinación personas + datos sostiene la promesa de valor: prevención medible y decisiones que llegan a tiempo. La CEO Verónica Guzmán, lo sintetiza en la ecuación que guía a la compañía: “El hombre y la mujer de seguridad siempre van a permanecer. La tecnología sin criterio no salva a nadie; la tecnología en manos del equipo correcto sí previene, protege activos y sostiene la continuidad del negocio”.



Verónica Guzmán, CEO  
SECANCOL LTDA

# ASOSEC entrega positivo balance del Congreso Nacional de Seguridad 2025

•Autoridades y expertos ratifican la importancia de la vigilancia privada en Colombia.

•Empresarios del sector se muestran optimistas frente al respaldo recibido y reiteran su compromiso de seguir trabajando por la seguridad del país. La ciberseguridad y la tecnología siguen siendo una prioridad.

**B**arranquilla, Colombia.- Como exitoso, calificaron las autoridades y empresarios de la vigilancia privada, el Congreso Nacional de Seguridad 2025, desarrollado recientemente en la ciudad y en el que participaron destacados conferencistas del orden militar, económico y político del país.

El evento que fue liderado por la Asociación Colombiana de Seguridad (ASOSEC), permitió analizar los desafíos que enfrenta el sector, así como también estudiar alternativas de solución frente a los diversos factores que afectan las operaciones del gremio, según lo afirmó la directora ejecutiva de la entidad, Vanessa Cure Anturi.

La dirigente gremial indicó que el Congreso Nacional de Seguridad en su versión 2025, destacó la importancia de fomentar la colaboración entre el sector público y privado para avanzar en el fortalecimiento de la seguridad del país.

“Desde ASOSEC, estamos satisfechos con los logros obtenidos a través de este Congreso Nacional de Seguridad, porque nos permitió un acercamiento importante con las autoridades competentes, y con ello, poner la lupa a esos factores que en gran manera afectan al sector, y ratificar además la relevancia de la vigilancia privada en el país”, puntualizó Vanessa Cure Anturi.

Por su parte, el politólogo y exsenador de la República y conferencista invitado, Jairo Klopotosfky, propuso ante este congreso de empresarios, un proyecto de ley para articular la fuerza pública con la seguridad privada y dar facultades especiales a la Superintendencia de Vigilancia. Klopotosfky, cuestionó que desde el año 2001, el sector empresarial viene afrontando las mismas dificultades que hoy, 24 años después,



sigue exponiendo sin que, a la fecha, se le hayan dado soluciones. Destacó la necesidad de una inclusión y articulación del gobierno nacional con el sector de la seguridad privada.

“El sector de la vigilancia privada, debe unirse y articularse dentro de un proceso nacional, en busca de un mayor fortalecimiento y sostenibilidad económica, lo cual se verá reflejado también en la economía y seguridad del país”, expresó Klopotosfky.

Entre tanto, Juan Carlos Pinzón, diplomático, economista y exministro de Defensa, dijo que la seguridad privada es vital para Colombia, considerando además el gran aporte que le genera a la economía del país, toda vez que emplea a más de 350 mil hombres y mujeres.

En su análisis de contexto geopolítico y de crecimiento económico,

Juan Carlos Pinzón advirtió, que la actual regulación hecha al sector, es muy inconveniente, lo que ha venido causando problemas y efectos negativos en la estabilidad del país.

“La industria de la seguridad privada en Colombia es de gran potencial y goza de un enorme prestigio internacional, y por esta razón debe ser priorizada y debidamente regulada, y debe dársele además un mejor tratamiento que garantice la ejecución de sus operaciones”, aseveró el exministro de Defensa, Juan Carlos Pinzón.

En su mensaje a los empresarios de la vigilancia privada, propuso una mayor inversión en áreas como la ciberseguridad y la tecnología y los invitó a no decaer en su compromiso de seguir trabajando fuertemente por el país, contribuyendo así, con la economía nacional.

“La seguridad y el orden, son fundamentales para el crecimiento del país”, concluyó Juan Carlos Pinzón.





# OSINT: La nueva frontera competitiva en la inteligencia estratégica de América Latina y el Caribe



**Edgardo C. Glavinich**  
Consultor especializado en inteligencia estratégica con experiencia en sectores público y privado. Combina metodologías avanzadas de análisis con aplicaciones prácticas para organizaciones que operan en entornos competitivos complejos. Presidente del Consejo Argentino para la Seguridad Integrada [www.capsi-ar.org](http://www.capsi-ar.org)  
**Argentina**

Articlista Invitado

Análisis estratégico sobre el mercado emergente de inteligencia de fuentes abiertas y su impacto transformacional en el sector privado regional.

Una característica singular del mercado latinoamericano es la coexistencia de abundancia informativa con escasez de capacidades analíticas. La inestabilidad política y la necesidad de transparencia en las actividades gubernamentales están impulsando la demanda de OSINT, especialmente en países como Brasil y México, creando oportunidades sin precedentes para empresas que puedan desarrollar capacidades curatoriales especializadas.

**Buenos Aires, Argentina.-** Vivimos una época en la que el poder ya no reside exclusivamente en el control de recursos físicos o territoriales, sino en la capacidad de procesar, analizar y transformar información en ventaja competitiva. En América Latina y el Caribe, una revolución silenciosa está reconfigurando el panorama de la inteligencia estratégica: el crecimiento exponencial de la Inteligencia de Fuentes Abiertas (OSINT) como activo empresarial crítico.

Los números son contundentes: el mercado de inteligencia de código abierto de América Latina alcanzó un valor de USD 811,31 millones en 2023, y se estima que crecerá a una tasa de crecimiento anual compuesta del 16,4% entre 2024 y 2032, para alcanzar un valor de 3,182.46 millones de USD en 2032. Esta expansión, que cuadruplica el tamaño del mercado en menos de una década, refleja una transformación profunda en cómo las organizaciones privadas conceptualizan y utilizan la información como herramienta de poder.

La tesis central de este análisis es inequívoca: Las organizaciones privadas, especialmente empresas de seguridad e inteligencia corporativa, y las agencias estatales que dominen el arte y ciencia de OSINT desarrollarán ventajas adaptativas críticas en los próximos años. Sin embargo, estas ventajas serán sostenibles únicamente para aquellas organizaciones que aborden OSINT con rigor metodológico, sofisticación ética y realismo estratégico.

**El contexto regional: Un terreno fértil para la inteligencia privada**  
América Latina y el Caribe presentan condiciones únicas que están catalizando la demanda por servicios de inteligencia privada sofisticados. El sector de seguridad privada regional, liderado por México, Brasil y Colombia, ha experimentado un crecimiento extraordinario: en el siglo XXI ha crecido un 60%, y cuanto más crecen las naciones latinoamericanas, mayor es la demanda de servicios a las empresas del sector.

Este crecimiento no es casual. Convergen múltiples tendencias que crean un entorno propicio para la inteligencia privada: el déficit de capacidades estatales ha creado un vacío que las empresas privadas están llenando sistemáticamente; la complejidad del entorno de amenazas, el crimen organizado transnacional, corrupción institucionalizada e inestabilidad política, requiere capacidades analíticas que exceden las metodologías tradicionales de seguridad; la digitalización acelerada ha generado una abundancia de datos disponibles públicamente; y las multinacionales operando en la región junto con empresas locales en expansión requieren análisis de riesgo más sofisticados que los tradicionalmente disponibles.

## La arquitectura económica del mercado OSINT regional

Los datos globales de mercado proyectan un crecimiento extraordinario: el tamaño del mercado de inteligencia de código abierto se valoró en USD 5,146.91 millones en 2023 y se espera que alcance USD 34,941.94 millones al final de 2030 con un CAGR de 28.34% durante el período de pronóstico 2024-2030. Para América Latina específicamente, el mercado regional de USD 811 millones en 2023 representa aproximadamente el 16% del mercado global, una proporción significativa que refleja tanto la demanda latente como el potencial de crecimiento acelerado.

El análisis de la demanda regional revela patrones específicos de adopción: el sector financiero representa el 35% del mercado, requiriendo análisis de riesgo político, monitoreo de fraude y evaluación de contrapartes comerciales; las industrias extractivas constituyen el 28%, necesitando análisis geopolítico, evaluación de riesgo social y monitoreo de grupos activistas; el sector retail y consumo abarca el 18%, demandando análisis de percepción de marca, monitoreo de tendencias de consumo e inteligencia competitiva; y los servicios corporativos especializados representan el 19%, incluyendo empresas de consultoría, bufetes legales y firmas de auditoría que ofrecen servicios de due diligence avanzada.

Los factores diferenciadores del mercado latinoamericano incluyen la complejidad regulatoria, la fragmentación normativa entre países crea demanda por análisis especializado de cumplimiento regulatorio transfronterizo; la volatilidad política, los ciclos electorales frecuentes y los cambios de política súbitos generan demanda constante por análisis predictivo político; la integración económica incompleta, las asimetrías en integración comercial requieren análisis sofisticado de oportunidades y riesgos por mercado; y los ecosistemas criminales complejos, la sofisticación del crimen organizado transnacional requiere capacidades analíticas que frecuentemente exceden las disponibles en el sector público.

## Casos de estudio: Transformación competitiva mediante OSINT

### Caso 1: Grupo energético multinacional – Análisis predictivo de riesgos geopolíticos.

Una importante empresa energética con operaciones en Colombia, Chile y Perú enfrentaba desafíos crecientes relacionados con la inestabilidad política y los conflictos sociales que afectaban sus operaciones. La compañía decidió implementar un sistema integral de inteligencia de fuentes abiertas para anticipar y mitigar estos riesgos.



La metodología desarrollada incluía el monitoreo sistemático de más de 1,200 fuentes digitales, desde medios locales y redes sociales hasta blogs comunitarios y registros de organizaciones no gubernamentales, con capacidades para correlacionar indicadores económicos locales con la probabilidad de conflicto y mantener un sistema de alerta temprana basado en la medición de la percepción social.

Los resultados fueron extraordinarios: la empresa logró anticipar conflictos significativos con un promedio de 45 días de ventaja, reducir en 67% los días de operación perdidos por conflictos sociales, y generar ahorros estimados en USD 12.3 millones durante el primer año de implementación, mientras que el tiempo de respuesta para actividades de relacionamiento comunitario mejoró en 40%.

**Caso 2: Firma de seguridad corporativa – Inteligencia de amenazas integrada.**

Una empresa de seguridad privada con presencia en Argentina, Chile y Uruguay transformó su modelo de negocio mediante el desarrollo de capacidades OSINT especializadas en inteligencia de amenazas. La firma identificó una oportunidad de mercado significativa al ofrecer servicios de inteligencia proactiva a clientes corporativos que tradicionalmente solo contrataban servicios reactivos de seguridad física.

El enfoque desarrollado incluyó la creación de una taxonomía de amenazas específicamente adaptada al contexto latinoamericano, integrando fuentes tradicionales de seguridad con análisis avanzado de redes sociales, desarrollando perfiles dinámicos de grupos criminales con actualización continua y estableciendo un sistema de distribución de inteligencia completamente adaptable según el sector específico de cada cliente.

El impacto en el negocio fue transformacional: la empresa experimentó un incremento del 85% en contratos de servicios premium, expandió sus servicios a 47 nuevos clientes corporativos en 18 meses, desarrolló tres productos de inteligencia propietarios que generaron una facturación anual de USD 2.1 millones, y se posicionó como referente regional en inteligencia de amenazas corporativas.

**Proyecciones y tendencias: El futuro del mercado OSINT regional**

La evolución del mercado de inteligencia de fuentes abiertas en América Latina y el Caribe está siendo moldeada por fuerzas tecnológicas, económicas y regulatorias que convergen para crear un escenario de transformación acelerada durante la próxima década. Las proyecciones

más conservadoras sugieren que el mercado regional triplicará su tamaño actual, pasando de los USD 811 millones actuales a más de USD 3.1 mil millones para 2032, impulsado por factores estructurales que van más allá de simples tendencias coyunturales.

La inteligencia artificial aplicada a la curación de información representa el cambio más fundamental en el horizonte inmediato. Las proyecciones indican que para 2027, aproximadamente el 75% de las capacidades OSINT regionales incorporarán IA para análisis automatizado, pero la diferenciación competitiva continuará residiendo en la supervisión humana especializada y la contextualización cultural. Las empresas más exitosas serán aquellas que logren combinar la velocidad de procesamiento de la IA con la comprensión profunda del contexto latinoamericano.

La consolidación del mercado será inevitable durante la próxima década. Las proyecciones sugieren que aproximadamente el 40% de las empresas OSINT actuales serán adquiridas o se fusionarán antes de 2030, creando jugadores regionales de mayor escala con capacidades más sofisticadas. Paralelamente, emergerá una especialización vertical marcada, con empresas generalistas dando paso a firmas especializadas en sectores específicos como financiero, extractivo, retail y gobierno.

Los modelos de negocio también experimentarán una evolución fundamental. La transición desde modelos tradicionales de consultoría hacia modelos Software-as-a-Service permitirá la democratización de capacidades básicas OSINT mientras se comercializan servicios avanzados a precios premium. Emergerán plataformas OSINT-as-a-Service y servicios especializados como Intelligence Marketplaces que conectarán productores de inteligencia especializados con consumidores corporativos.

**Recomendaciones estratégicas para decisores**

La implementación exitosa de capacidades OSINT en América Latina requiere un enfoque estratégico diferenciado que reconozca las particularidades del mercado regional. Para las empresas de seguridad privada, la clave del éxito radica en entender que OSINT no es simplemente una herramienta adicional sino una capacidad transformacional que puede redefinir completamente su propuesta de valor en el mercado.

Las organizaciones que aspiren a liderar en este espacio deben priorizar el desarrollo de talento especializado por encima de la adquisición de tecnología. La tentación natural de enfocarse en herramientas sofisticadas debe resistirse en favor de construir equipos de analistas que combinen rigor metodológico con comprensión profunda del contexto



latinoamericano. Estos profesionales híbridos constituyen el verdadero activo diferenciador en un mercado donde la información está disponible para todos pero la capacidad de interpretarla correctamente es escasa.

La especialización sectorial emerge como una estrategia superior a la aproximación generalista. El desarrollo de expertise profunda en sectores específicos permite no solo cobrar tarifas premium sino también desarrollar relaciones cliente más estables y profundas, yendo más allá del conocimiento superficial para incluir comprensión íntima de dinámicas competitivas, marcos regulatorios y patrones de riesgo específicos.

Para los servicios de inteligencia gubernamentales, el desafío principal consiste en optimizar la complementariedad entre OSINT y fuentes tradicionales sin sobredimensionar las capacidades de las fuentes abiertas. La integración metodológica efectiva requiere protocolos específicos que permitan combinar inteligencia OSINT con fuentes clasificadas maximizando el valor añadido de cada tipo de fuente.

Las empresas consultoras y de servicios profesionales enfrentan una oportunidad transformacional de integrar OSINT en sus ofertas existentes generando valor incremental significativo. La clave está en reconocer que OSINT no debe ser un servicio separado sino un componente que enriquece y diferencia servicios tradicionales como due diligence, evaluación de riesgos y análisis competitivo.

**Conclusión: El imperativo estratégico de la inteligencia distribuida**

Estamos presenciando una transformación fundamental en la arquitectura del poder informacional en América Latina y el Caribe. La democratización de herramientas de inteligencia, combinada con la explosión de fuentes de información pública, está creando oportunidades sin precedentes para organizaciones que puedan desarrollar capacidades curatoriales sofisticadas.

Los datos son inequívocos: el mercado OSINT regional experimentará un crecimiento exponencial que lo llevará de USD 811 millones en 2023 a más de USD 3.1 mil millones en 2032. Sin embargo, este crecimiento no será uniforme ni automático. Las organizaciones que dominarán este espacio serán aquellas que comprendan que OSINT no es simplemente una herramienta tecnológica sino una disciplina analítica compleja que requiere inversión sostenida en talento, metodología y frameworks operacionales.

**La ventaja competitiva sostenible en OSINT residirá en tres dimensiones críticas.**

Primero, la curación especializada: en un mundo saturado de información, el valor no está en el acceso a datos sino en la capacidad de transformar

información en inteligencia accionable. Las organizaciones que desarrollen capacidades curatoriales especializadas —combinando sistemas de evaluación de credibilidad de fuentes, filtrado inteligente de relevancia, análisis contextual profundo, síntesis estratégica y validación rigurosa— crearán ventajas competitivas defensibles. Esta curación va mucho más allá de la simple recolección de datos para incluir metodologías propietarias que constituyen el verdadero diferenciador en el mercado.

Segundo, la integración operacional: OSINT no puede ser una capacidad aislada sino que debe integrarse profundamente en procesos de toma de decisiones organizacionales. Las empresas que logren esta integración desarrollarán ventajas adaptativas que se amplificarán con el tiempo, transformando no solo cómo recopilan información sino cómo toman decisiones estratégicas fundamentales.

Tercero, la excelencia en especialización sectorial: las organizaciones más exitosas serán aquellas que desarrollen expertise ultra-profunda en sectores específicos, comprendiendo no solo las dinámicas generales del mercado sino las particularidades regulatorias, competitivas y de riesgo de sus industrias objetivo.

El momento de actuar es ahora. Las organizaciones que inviertan en desarrollar capacidades OSINT robustas en 2025-2026 estarán posicionadas para capturar una porción desproporcionada del crecimiento proyectado. Aquellas que esperen encontrarán un mercado ya dominado por jugadores con ventajas de first-mover difíciles de superar.

La transformación que estamos presenciando representa una redistribución fundamental del poder analítico desde instituciones centralizadas hacia organizaciones distribuidas capaces de agregar y procesar información de manera sofisticada. En América Latina y el Caribe, región caracterizada por instituciones estatales frecuentemente débiles y ecosistemas informativos complejos, esta redistribución presenta oportunidades extraordinarias para organizaciones visionarias.

El futuro pertenecerá a aquellas organizaciones que comprendan que en la era de la complejidad informativa, la inteligencia no es un lujo sino una necesidad existencial. OSINT, implementado con rigor metodológico y sofisticación estratégica, representa la diferencia entre liderar la transformación o ser transformado por ella.

**Nota:** Este artículo analiza tendencias regionales y no representa un apoyo de estas prácticas o empresas específicas. Se recomienda siempre verificar la legalidad y ética de cualquier servicio de inteligencia privada en su jurisdicción.







**EXPO**  
**SEGURIDAD**  
**& TELECOM**  
COSTA RICA



**SAN JOSÉ**  
**COSTA RICA**

**12 Y 13 DE NOVIEMBRE 2025**  
**HOTEL BARCELÓ SAN JOSÉ PALACIO**



## Tecnología y Soluciones para un mundo seguro, conectado y confiable.

Con la experiencia y éxito de **SEGURIEXPO ECUADOR** y **EXPOSEGURIDAD GUATEMALA**, llega a Costa Rica la feria internacional de tecnología en Seguridad y Telecomunicaciones más importante del País.

Cada evento nuestros expositores renuevan su confianza y también recibimos nuevas marcas que se suman debido a la gran oportunidad de negocios que pueden generarse en Costa Rica y toda Centro América.

Nosotros les ofrecemos la mejor plataforma de negocios, y los invitamos a ustedes a exponer.

ExpoSeguridad Costa Rica **San José 2025** es ideal para:

- Potenciar el proceso de ventas e introducir nuevos productos en el mercado regional.
- Ampliar la cartera de clientes
- Reafirmar la relación proveedor - clientes
- Posicionar la imagen de la empresa
- Analizar el mercado
- Presentar las últimas tecnologías en materia de seguridad a través de las conferencias agendadas durante el evento
- Hacer crecer su base de real de contactos

Para más información sobre el evento.

**Whatsapp +593 969974897** o envíanos un correo a **info@myestrategia.com**



[www.exposeguridadcostarica.com](http://www.exposeguridadcostarica.com)







## NETWAY SPECTRUM

Switches PoE endurecidos & convertidores de medios de Fibra

- Implemente dispositivos IP en ubicaciones remotas con o sin alimentación local
- Admite hasta 90W por puerto
- La carga rápida de la batería proporciona un respaldo de energía extendido
- Entrada de 115/230 VAC o 277 VAC
- Administre y reinicie dispositivos de forma remota con la administración de energía de red LINQ™
- Garantía de por vida

CORRE CON ELLO™