# MÁS SEGURIDAD

Magazine

# Tecnología

## para un turismo seguro

Julio 2024

México y Latam / precio $60.00MX

GRUPO EDITORIAL • GRUPO EDITORIAL • GRUPO EDITORIAL • GRUPO EDITORIAL

MS GLOBAL

ESS+®
FERIA INTERNACIONAL DE SEGURIDAD

21 - 23 AGOSTO 2024
Bogotá D.C., Colombia

30 AÑOS
Generando oportunidades
para la industria de la seguridad
en Latinoamérica

# Fuente de tecnologías de última generación

Sea parte de la edición de aniversario de ESS+ y participe de las **nuevas y renovadas actividades**

**ESS+Show case**
Lanzamiento de nuevos productos espacio físico

**ESS+Bussines agenda**
Rueda de negocios
Expositor• expositor •visitante

**ESS+Convergnet events**
Eventos de la Industria

**ESS+Academy**
Capsulas tecnológicas

**ESS+Hackers eticos 2°**
Versión de Hackers Vs Dispositivos

**Promoción global**

**ESS+Time line**
30 años de éxito para una feria sostenible

ESS+CORFERIAS APP

ESS+ SALÓN SE SEGURIDAD LABORAL
POWERED BY: sicur

ESS+ SALÓN DE SEGURIDAD CONTRA INCENDIOS
POWERED BY: sicur

## CONTÁCTENOS Y SEA PARTE DE ESTA EDICIÓN ESPECIAL


**ADRIANA MÁRQUEZ**
Directora Comercial
amarquez@securityfaircolombia.com
Cel.: +57310 334 16 69
Tel.: +57601 7039104 – 7042492

**PATRICIA ACOSTA**
Directora ESS+
pacosta@securityfaircolombia.com
Cel.: +57310 884 84 66
Tel.: +57601 7039104 – 7042492


POWERED BY: sicur | IFEMA MADRID
ORGANIZAN: PAFYC | corferias
GREMIOS ALIADOS: ASIS | COLADCA | ALAS

MEDIOS ALIADOS
MÁS SEGURIDAD Magazine
GLOBAL DEFENSE MAGAZINE

securityfaircolombia.com

HUMBERTO MEJÍA HERNÁNDEZ, / DSE, CPSI
DIRECCIÓN GENERAL
humberto@revistamasseguridad.com.mx

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

BEATRIZ CANALES
COORDINACIÓN EDITORIAL
edicion@revistamasseguridad.com.mx

DG CREATIVE
DISEÑO

TERESA OJEDA
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@revistamasseguridad.com.mx

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

JORGE MERCADO ABONCE
Servicios Jurídicos Integrales
Anzaldo- Martínez-Mercado
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

SÍGUENOS EN:

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

**Revista Más Seguridad** Año 16, No 149, Julio 2024, 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 551894 7067. 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.

# Soluciones tecnológicas y humanas = vacaciones seguras

Las novedades electrónicas contribuyen, al mismo tiempo a que se hagan más agiles los procedimientos, pues hoy seguridad y facilitación van de la mano.

Con lo último en avances tecnológicos en temas de realidad aumentada, virtual y computación cuántica, darán forma a un futuro en el que el papel principal de la tecnología tomará una fuerza potencial en los servicios de seguridad electrónica para las empresas del sector turístico, pero sin dejar a lado al capital humano.

El uso de estas soluciones tecnológicas es primordial en todas las industrias económicas del país, como el caso del sector turístico, ya que hoteles y aeropuertos en esta temporada vacacional, deben brindar, pero sobre todo proteger a los usuarios de los mismos con estrategias eficaces de seguridad en inmuebles y transporte.

Por ello, todas aquellas empresas que ofrecen un servicio especializado a través de personal capacitado, deben adaptarse para evolucionar y lograr la satisfacción y expectativas de los clientes.

Hoy, resulta indispensable para una mejor protección de usuarios en temporada vacacional contar con cámaras de última generación que brinden una mejor videovigilancia, un control de accesos que garantice la seguridad del inmueble y por ende del huésped, cerraduras inteligentes y personal de seguridad física que proteja al usuario final en su estancia, así como en su traslado, en concreto, hacer uso de las herramientas que fabricantes, proveedores, distribuidores e integradores de seguridad electrónica brindará confianza y protección a quien la use.

El uso de tecnologías biométricas como el reconocimiento facial, es una solución que está ganando terreno como un método de acceso seguro y personalizado a las habitaciones y otras instalaciones de los inmuebles, como habitación, aeropuertos u oficinas. Estas herramientas tecnologías ofrecen un nivel alto de seguridad y conveniencia, eliminando la necesidad de tarjetas de acceso físico que pueden perderse o ser robadas.

No es un secreto que la inseguridad en la que actualmente vivimos, nos ha rebasado, y protegernos se ha convertido en una prioridad. Las soluciones tecnológicas nos ayudan a contrarrestar o disminuir, y en algunos casos a erradicar los errores humanos, entonces, estas novedades electrónicas contribuyen, al mismo tiempo a que hagamos más agiles los procedimientos, pues hoy seguridad y facilitación van de la mano, pero siempre en el capital humano.

Tengamos en consideración que el mercado de la protección electrónica cuenta con una amplia experiencia en el desarrollo e implementación de soluciones tecnológicas avanzadas para la seguridad de los hoteles, aeropuertos y otras verticales. Por lo que es imperante tener compromiso con innovación y calidad en los servicios.

# Los Profesionales de LATAM

## Alfredo Yuncoza
## Venezuela

Doctor Honoris Causa en Derechos Humanos. Máster en Seguridad y Defensa. MBA con estudios de Economía. Maestrante en Dirección y Administración Global de Negocios. Egresado de varios diplomados en protección y seguridad, así como del William J. Perry Center for Hemispheric Defense Studies, (National Defense University. USA). Certificado CSSM© (Certified in Security Supervision and Management) y CPO© (Certified Protection Officer) ambas por IFPO. IFSEC Global Influencer Security and Fire 2020 (Reino Unido). Presidente – fundador del Consejo Consultivo Latino de IFPO (USA).

Reconocido por la organización Life Safety Alliance - LSA (USA), entre los Top 40 Global Thought Leaders in Security and Life Safety. Reconocimiento que representa un esfuerzo por aportar mayor objetividad, transparencia y rigor al proceso de identificación de personas influyentes y líderes de opinión en el campo. Ha recibido numerosas distinciones de organizaciones vinculadas a las industrias de la seguridad y la protección, desde Colombia, Perú, Estados Unidos, Inglaterra y Venezuela.

Su trayectoria profesional de más de 40 años ha sido desarrollada para organizaciones nacionales y transnacionales. Miembro de la red de expertos del Global Initiative against Transnational Organized Crime (Suiza). Past Regional Vicepresident (8B) de ASIS International (USA). Actualmente es consultor en gestión estratégica de riesgos en América Latina. Facilitador invitado a diversos eventos internacionales de seguridad en los que ha interactuado con cerca de 14.000 profesionales. Sus más de 600 artículos se publican en medios de Estados Unidos, Reino Unido, España, México, Argentina, Chile y Venezuela, entre ellos Más Seguridad.

5 Nueva serie UPS de Hikvision

6 Lanza Ajax Systems cámaras IP cableadas

10 Nuevos lectores murales de Salto Systems

**15** Biometría facial vs delincuencia

**16** Innovador IDX 2024 de Ingram Micro México

22 Tecnología para turismo seguro

**32** En marcha CIPROCI 2024

**30** Robos a transporte en primer semestre

**38** Combate al crimen organizado

**40** Orion IV nueva placa para blindaje

FUERA DE GRABACIÓN

@MatadorMejia

Humberto Mejía / DSE, CPSI

# La captura inesperada

Su nombre era ya “una leyenda” en la narco-cultura. Para muchos delincuentes era inspiración para ascender en el mundo del hampa, para los cuerpos de seguridad pública y nacional el objetivo a cazar; para los periodistas la “nota de ocho”, mientras que para el colectivo popular una figura que nunca pisaría la cárcel. Pero sucedió lo inverosímil, capturaron a Ismael Zambada García, “El Mayo” y de una forma impensable: engañado y en territorio estadounidense.

“El Mayo” Zambada, es uno de los nombres más famosos en la historia de la guerra contra el narcotráfico, sinónimo de temible poder y corrosiva influencia del mayor cártel de drogas del mundo. Es el último “jefe” de una generación de capos que creó el cartel de Sinaloa junto con Joaquín “El Chapo” Guzmán, a partir de lo que quedó del Cartel de Guadalajara tras su colapso en 1989.

Periodistas mexicanos y estadounidenses afirman que su captura, luego de caminar impune en el mundo del narco por 40 años, se debió a una elaborada operación encubierta del FBI con la que lo engañaron para llevarlo a EE.UU. Otros dicen que fu por una traición del Joaquín Guzmán López, hijo de “El Chapo” Guzmán, algunos afirman se trató de una entrega voluntaria y otros afirman que se trató de una extracción en el territorio mexicano, lo cual tampoco suena descabellado.

Lo que hasta hoy se sabe es que las autoridades estadounidenses lo detuvieron en El Paso, Texas y el gobierno mexicano ni enterado estaba. “El Mayo” ya se ha declarado inocente de múltiples cargos ante un tribunal federal de Texas.

Con insistencia la teoría que más suena es que fue engañado para viajar a EE.UU. como parte de una operación encubierta ideada por el hijo de su antiguo socio “El Chapo”, tras hacerle creer que viajaba al norte de México para inspeccionar posibles lugares para pistas de aterrizaje clandestinas.

A Zambada le daba pánico ser detenido. Para alguien que tuvo cautela durante años, parece increíble que resultara engañado a los 76 años. Quizá era necesario algo extraordinario para poder detenerlo, tal vez el actual gobierno mexicano le deba favores al capo y sus homólogos estadounidenses lo quieren aprovechar para llamar a cuentas al próximo ex Presidente mexicano (por cierto, muy odiado y calificado con el peor mandatario en los últimos años). Por lo pronto varios funcionarios y políticos de todos los niveles de México y EE.UU. deben nerviosos con esta detención.

La pregunta sobre el arresto es ¿por qué ahora? Sin duda el operativo se planeó durante meses. La razón “principal” la expuso el Fiscal General de Estados Unidos, Merrick Garland: “el fentanilo es la amenaza más mortífera que jamás haya enfrentado nuestro país”. También es cierto que el motivo puede ser el año electoral que se vive en EE.UU. que traerá consigo beneficios al gobierno de Joe Biden para impulsar a Kamala Harris e imponerla sobre Donal Trump.

En México poco a nada cambiará: El narco seguirá, la guerra entre cárteles nadie la impedirá, el gobierno actual y el que le sigue solo darán declaraciones y poca acción, la delincuencia mantendrá su rumbo y se fortalecerá mientras la sociedad queda una vez más en medio, solo protegiéndose con lo que tenga a la mano, ahí la seguridad privada y electrónica es la alternativa…

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


Tour Internacional 2024

MÁS SEGURIDAD Magazine

EXPO NAVAL®

ESS+ FERIA INTERNACIONAL DE SEGURIDAD

intersec

NENA THE 9-1-1 ASSOCIATION MEXICO

ASIS INTERNATIONAL™ WOMEN IN SECURITY

SEGURIDADEXPO by Fisa | CHILE

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

# Introduce HIKVISION® nueva serie UPS de alta resistencia

En un mundo cada vez más dependiente de la tecnología digital, la protección de dispositivos electrónicos contra interrupciones de energía y picos de voltaje es más crucial que nunca. Reconociendo esta necesidad, Hikvision anuncia su nueva gama de sistemas de alimentación ininterrumpida-UPS (DSUPS600-X, DSUPS3000-X y DSUPS1000-X) que promete no solo mantener los dispositivos en funcionamiento durante cortes de energía, sino también protegerlos contra las fluctuaciones de energía que pueden causar daños irreparables.

"Las lluvias y los fenómenos climáticos asociados pueden tener un impacto significativo en el suministro eléctrico, lo que lleva a cortes de luz y posibles daños a los equipos electrónicos, además de afectar el tendido eléctrico y los pozos de distribución de energía se generan apagones, picos de voltaje y hasta cortos circuitos que pueden descomponer o quemar los equipos tecnológicos que están conectados al suministro eléctrico, afectando incluso, la operación y productividad de los negocios", comenta Miguel Arrañaga, director regional de Ventas Bajío en Hikvision México.

"Nuestra serie de UPS reduce significativamente el riesgo de daños a dispositivos sensibles causados por sobretensiones y picos de voltaje, garantizando que las operaciones comerciales y las actividades domésticas puedan continuar sin interrupciones durante cortes de energía".

Por otro lado, indica que, dada la creciente preocupación por el aumento de los costos energéticos y su impacto en la eficiencia operativa, los profesionales de TI e instalaciones están cada vez más enfocados en optimizar el uso de la energía: "Los profesionales de IT e instalaciones deben mantener un seguimiento constante del rendimiento energético y estar dispuestos a adaptar nuevas tecnologías y estrategias a medida que estén disponibles. Al tomar estas medidas, los profesionales de TI e instalaciones no solo reducen el costo de la energía, sino que también mejoran la sostenibilidad operativa y la resiliencia de sus infraestructuras tecnológicas".

- Seguridad electrónica ininterrumpida para la temporada de lluvias.
- Las lluvias y los fenómenos climáticos asociados pueden tener un impacto significativo en el suministro eléctrico, lo que lleva a cortes de luz y posibles daños a los equipos electrónicos.

**Características principales de la serie de UPS Hikvision:**

- Capacidad: 3000 VA / 1800 W.
- Batería: 12 V / 9 Ah.
- Seis salidas totales (4 con respaldo y 2 sin respaldo).
- Peso: 5.4 Kg.
- Voltaje de entrada: 85 - 150 V ~ 50/60 Hz.
- Voltaje de salida: 102 - 132 V.
- Dimensiones: 274 x 95 x 139 mm.
- Garantía: 3 años (en la batería aplica 1 año)

Tabla de referencia de consumo en watts (aproximado):
55 Watts = 315 minutos.
65 Watts = 240 minutos.

# Lanza AJAX

# cámaras IP de seguridad cableadas

- Cámaras versátiles con buen funcionamiento tanto para interiores como en exteriores, con una clasificación de protección IP65.
- Solución perfecta, gracias a su avanzada tecnología de transmisión.

Estos dispositivos de videovigilancia están diseñados para proporcionar una vigilancia de alta resolución al tiempo que garantizan una protección de la privacidad de nivel superior. Todas las cámaras ya están disponibles para sus pedidos:

Las cámaras Ajax son versátiles y funcionan bien tanto en interiores como en exteriores, con una clasificación de protección IP65. Su configuración es sencilla y segura gracias a la autenticación sin contraseña. Con varios tipos de matriz y lentes disponibles, pueden satisfacer diversas necesidades de videovigilancia.

Actualmente las cámaras Ajax son una solución perfecta, gracias a su avanzada tecnología de transmisión. Estas se sincronizan con los eventos del sistema, lo que permite a los usuarios acceder rápidamente a los datos de video e iniciar la grabación personalizada y basada en escenarios.

**Características clave:**

•Autenticación segura sin contraseña
•Navegación rápida por el repositorio con tecnología de doble transmisión
•Protección multinivel de la cuenta: autenticación de dos factores, control de sesiones e inicio de sesión con contraseña/datos biométricos
•Mural de video virtual personalizable
•Reconocimiento con IA integrado
•Verificación instantánea de alarmas en alta resolución
•Alcance de iluminación IR de hasta 35 m
•Zona de detección de movimiento personalizable
•Sincronización del repositorio con los eventos del sistema
•Micrófono digital integrado
•Soporte para una tarjeta SD de hasta 256 GB
•Carcasa metálica resistente al agua y al polvo
•Control y configuración remotos

# Soluciones de seguridad basadas en AI innovadoras presenta VIVOTEK

A Delta Group Company

Durante Expo Seguridad 2024, la empresa VIVOTEK demostró la fortaleza diferenciadora de sus soluciones de vigilancia IP y compartió su enfoque 2024: Make Tomorrow Easier, Today!

Durante tres días, los asistentes a Expo Seguridad 2024 pudieron experimentar y conocer como la innovación de los productos de la marca dan forma a un futuro más racionalizado para el público, que permite personalizar un sistema de seguridad rentable y sin fisuras, con soluciones físicas y en la nube.

"A través del concepto, Make Tomorrow Easier, Today, la firma quiere compartir con el mundo la visión innovadora de sus soluciones y productos; así como sus conceptos y directivas en constante evolución. Nuestras soluciones son robustas, porque parten de un objetivo sencillo: añadir valor adicional y conocimientos para los socios y usuarios", comenta Miles Chen, director general de la empresa de soluciones de seguridad para LATAM.

Si analizamos al interior de esta visión, podemos encontrar la guía para que la tecnología se convierta en el mejor aliado de la vigilancia IP, para este 2024 y para el futuro:

Make Analytics Easier presenta el análisis de video Edge AI que integra inteligencia artificial en cámaras y sensores para el análisis de eventos en tiempo real. Las aplicaciones incluyen detección inteligente de movimiento, VCA inteligente, seguimiento inteligente avanzado, análisis de objetos de visión, reconocimiento facial, detección de zonas restringidas, detección de infracciones de aparcamiento, reconocimiento de matrículas y recuento de personas.

Con esto se elimina la necesidad de un servidor dedicado para gestionar el análisis de video, agiliza la puesta en marcha del sistema al tiempo que reduce los costes generales y experimenta una mayor flexibilidad en las aplicaciones analíticas, independientemente del método de despliegue de su sistema.

También la tecnología AI Image Tuning permite a las cámaras ajustar automáticamente sus configuraciones para obtener la mejor calidad de imagen, adaptándose tanto a entornos interiores como exteriores. Este ajuste inteligente no solo mejora la calidad visual, sino que también aumenta la precisión del análisis, incluso en condiciones de iluminación complejas.

Make Cloud Easier se centra en un mundo de vigilancia que encarna la seguridad sin la complejidad. "Diga adiós a las configuraciones desalentadoras y dé la bienvenida a una experiencia de seguridad sin fisuras", la marca a través de su solución completa de vigilancia con IA Vortex une cámaras de red y software en la nube revolucionando la forma de salvaguardar sus espacios ya que mejora significativamente los sistemas de seguridad. Esta herramienta introduce la funcionalidad de Profile, permitiendo la identificación facial y la búsqueda en todas las cámaras de forma instantánea. Además, esta plataforma facilita la búsqueda de matrículas vehiculares en todas las cámaras sin necesidad de licencias adicionales. La integración con KISI añade otra capa de seguridad al proporcionar control de acceso.

Make Search Easier revoluciona su vigilancia con la tecnología de búsqueda profunda impulsada por IA de VAST Security Station. Con Deep Search se puede localizar rápidamente personas y vehículos, convirtiendo horas de búsqueda en segundos, con esto se añade un toque de inteligencia artificial a los dispositivos actuales de vigilancia. Además, con la capacidad de generar informes directamente en el software VSS Pro, los videos relevantes se convierten en evidencia tangible en pocos pasos.

Estos informes, presentados en formato PDF, detallan la fecha, hora y ubicación exactas en las que apareció una cara específica, proporcionando una herramienta eficaz para la gestión y resolución de incidentes. La búsqueda de evidencia se vuelve aún más rápida y sencilla con la integración de Milestone XProtect, Genetec Security Center y las cámaras de IA de VIVOTEK, ya que permite análisis instantáneos de eventos sin servidores dedicados, simplifica la configuración y reduce costos, manteniendo aplicaciones analíticas flexibles.

Make Integration Easier incluye la Alianza de Integración de Soluciones (SIA) de VIVOTEK, que fomenta un frente unificado de sinergia tecnológica, fusionando diversas plataformas de hardware y software para ofrecer soluciones de vigilancia personalizadas. Mediante esta colaboración se construye un ecosistema resistente y adaptado a las diversas necesidades de los usuarios ya que SIA es un ejemplo de integración e innovación en toda la industria.

Impulsado por la tecnología de aprendizaje profundo de vanguardia, el algoritmo avanzado de VIVOTEK eleva constantemente la precisión de detección al reducir significativamente las falsas alarmas. Con capacidades sin precedentes de aprendizaje profundo, los sistemas de vigilancia pueden distinguir amenazas reales de eventos no amenazantes, lo que resulta en seguridad y eficiencia operativa.

Un enfoque fresco que permite la colaboración simple con análisis versátiles de video, soluciones basadas en la nube y capacidades de búsqueda e integración con una amplia línea de productos de vigilancia que invita los usuarios a construir un sistema de vigilancia proactivo que mejora la seguridad mediante la identificación y mitigación de riesgos con soluciones inteligentes de la mano con la firma.

# Se transforma **Vicente López** en una ciudad inteligente

**Buenos Airtes, Argentina.-** Milestone Systems, anunció el éxito de la implementación de sus soluciones en Vicente López, provincia de Buenos Aires, Argentina, las cuales han permitido a las autoridades locales mejorar significativamente los tiempos de respuesta en la aplicación de la ley, gestión del tránsito y manejo de emergencias.

Desde 2012, el municipio ha estado implementando sistemas de videovigilancia. Sin embargo, desde 2020, decidieron llevar esta iniciativa un paso más allá al incorporar tecnología de video basada en datos para fortalecer las operaciones de la ciudad.

El sistema anterior estaba obsoleto, puesto que solo contaba con 120 cámaras administradas por diferentes plataformas de gestión de video, lo que dificultaba la capacidad de las fuerzas de seguridad para responder con rapidez.

Para resolver estos problemas, se requería un VMS de plataforma abierta y cámaras avanzadas. El VMS centralizó datos de ubicaciones remotas e integró numerosas cámaras, sensores y análisis.

**Innovación tecnológica para una vigilancia efectiva y escalable**

El municipio de Vicente López implementó el XProtec® Corporate Video Management Systems (VMS) de Milestone Systems. Este software de gestión de video proporciona una solución integral para la supervisión, análisis y gestión centralizada de datos de video en tiempo real. Además, incorporó XProtect Rapid REVIEW, una solución analítica de video forense que permite una rápida revisión, búsqueda y análisis de datos de video.

Asimismo, se desplegaron cámaras de alta calidad impulsadas por Inteligencia Artificial (IA), de la marca Hanwha Vision, incluyendo modelos como el PNV-A9081R, XNP-6400R y PNM-9085RQZ1. Estas cámaras ofrecen un amplio campo de visión y producen imágenes nítidas y claras de alta resolución, filtrando los desencadenantes irrelevantes para centrarse únicamente en personas, objetos o vehículos, generando solo los eventos que las autoridades necesitan ver para realizar búsquedas forenses eficaces y mejorar la eficiencia operativa, permitiendo así una vigilancia efectiva de áreas clave de la ciudad.

Además, para garantizar la escalabilidad y disponibilidad de los datos de video, se puso en práctica una solución de almacenamiento en la nube a través de Amazon Web Services (AWS). Esta estrategia permitió gestionar la gran cantidad de datos e imágenes de alta resolución generados por el sistema de seguridad de toda la ciudad de manera segura y eficiente.

**Transformación digital de Vicente López**

Gracias a esta inversión, autoridades pudieron implementar el “Anillo Digital”, iniciativa que utiliza la tecnología de reconocimiento de matrículas (LPR) para identificar automotores y detectar posibles delitos. “Casi un millón de vehículos circulan cada día por la autopista Panamericana, gracias a los análisis de LPR, estamos creando listas de seguimiento para analizar los delitos con rapidez, puesto que ahora disponemos de funciones de búsqueda rápidas y parametrizadas y podemos filtrar por tamaño del vehículo, color y otras características”, afirmó Santiago De Jesús, secretario de Seguridad de la Municipalidad de Vicente López.

De igual manera, autoridades diseñaron la estrategia “Puntos Seguros”, una medida innovadora, que consistió en la instalación en la vía pública de tótems equipados con cámaras e intercomunicadores, permitiendo a los ciudadanos establecer contacto directo con el Centro de Vigilancia Urbana mediante un botón de emergencia. Estos puntos están diseñados para asistir tanto en casos de inseguridad como en emergencias médicas, coordinando la respuesta de patrulleros, Defensa civil y bomberos.

“La implementación de análisis de video, incluido el reconocimiento de matrículas de vehículos (LPR) y comportamientos para detectar merodeos, estampidas y aglomeraciones, ha permitido a las autoridades pasar de un sistema de seguridad reactivo a uno proactivo”, concluyó De Jesús.

Gracias a la implementación de tecnologías de vanguardia, Vicente López se muestra como un claro ejemplo de ciudad inteligente, donde la innovación se fusiona con la seguridad ciudadana; la municipalidad demuestra cómo la integración de la tecnología en la gestión urbana puede elevar la calidad de vida de sus habitantes, consolidándose como un claro referente en la región.

CURSOS ALAS

En la segunda mitad del año,

# ¡Certifícate con ALAS!

**JUL**
16 al 19

NUEVO

**Ciberseguridad y Protección de Activos Digitales**

**JUL**
23 al 26

**Alarmas y Detección de Intrusión**

**AGO**
27 al 30

CERTIFICADO DC3

**Ventas para la Industria de la Seguridad**

**SEP**
24 al 27

**Gerencia de Proyectos**

**OCT**
22 al 25

CERTIFICADO DC3

**Video Vigilancia**

**NOV**
12 al 15

**Evaluación de Riesgos de Seguridad**

**DIC**
3 al 6

CERTIFICADO DC3

**Operadores de Cuartos de Control**

## Además tenemos cursos a la medida de tu compañía. Pregunta por ellos.

Alarmas y Detección de Incendios • Alarmas y Detección de Intrusión • Ciberseguridad para Alta Gerencia • Ciberseguridad y Proteccion de Activos Digitales • Control de Acceso • Drones en Seguridad • Evaluación de Riesgos de Seguridad • Evaluación del Retorno de la Inversión • Fundamentos de Seguridad Electrónica • Gerencia de Proyectos • Integración de Sistemas de Seguridad • Inteligencia Artificial en Seguridad • Management 3.0 • Operadores de Cuartos de Control • Redes IP e Inhalámbricas • Seguridad Perimetral • Ventas para la Industria de la Seguridad • Video Vigilancia •

ALAS
ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

**CRISTIAN MOLINA**
Coordinador de Cursos
Whatsapp:
+57 321 6153367

SALTO
inspiredaccess

# Presenta la nueva serie de lectores murales con teclado Design XS: **mayor seguridad y comodidad**

- Nuevo producto representa un gran avance en la tecnología de control de accesos.

Con el fin de facilitar el uso de credenciales físicas, móviles y acceso con código con PIN, el nuevo lector está diseñado con un teclado con relieve y braille para personas con discapacidad visual.

Salto Systems, líder mundial de soluciones de control de accesos y parte del grupo SALTO WECOSYSTEM, presenta la nueva serie de lectores murales con teclado Design XS. Con un diseño elegante e ideal para cualquier espacio, este nuevo producto representa un gran avance en la tecnología de control de accesos. Diseñado para facilitar el uso de credenciales físicas como de acceso móvil, el lector presenta un teclado duradero. Para ayudar a las personas con discapacidad visual, los números y símbolos están grabados en braille de 5 puntos.

El lector mural con teclado Design XS está diseñado para establecer nuevos estándares en el control de acceso inteligente. Con autenticación multifactor y la opción de acceso mediante código PIN, este lector mural proporciona doble autenticación y modos de apertura mejorados que aumentan significativamente la seguridad.

Igualmente, se integra a la perfección en cualquier tipo de instalación. Al estar diseñado para adaptarse a cajas eléctricas estándar, la instalación se realiza sin problemas. El lector mural, en combinación con una unidad de control de acceso Salto BLUEnet, simplifica la infraestructura de red con los últimos avances en tecnología de control de acceso inalámbrico y conectividad. El control de accesos en la nube y las aplicaciones móviles son compatibles, proporcionando un sistema de gestión de accesos eficiente que puede controlar ascensores, puertas correderas, accesos perimetrales y puertas electrónicas.

“Estamos muy satisfechos de introducir en el mercado el lector mural con teclado europeo Design XS”, asegura Marc Handels, director de Innovación Tecnológica y Cofundador de Salto. “Este producto no sólo proporciona funciones de seguridad avanzadas, sino que también ofrece una experiencia al usuario cómoda y sencilla. Creemos que establecerá nuevos estándares en la industria del control de accesos”.

El nuevo lector mural Design XS también ofrece una amplia gama de opciones de credenciales para los usuarios. Con un acceso a credenciales móviles y físicas, los usuarios pueden tocar NFC, tarjetas RFID, llaveros o Bluetooth LE para una entrada rápida y cómoda. Esta versatilidad garantiza que los usuarios puedan elegir el método de acceso que más les convenga.

Design XS ha sido sometido a rigurosas pruebas y cumple todas las certificaciones, lo que garantiza un rendimiento y una fiabilidad duradera. Está diseñado para soportar incluso las condiciones más duras, por lo que es la elección perfecta para ubicaciones expuestas al exterior.

Con el lanzamiento de la serie Design XS, Salto continúa innovando y liderando el camino de las soluciones de acceso inteligente. Salto se compromete a proporciona a sus clientes productos de alta gama que ofrezcan seguridad y comodidad.

Para más información, visite nuestra web: **www.saltosystems.es**

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

30 AÑOS PROFESIONALIZANDO

# PROGRAMA LATINOAMERICANO DE PREPARACIÓN PARA EL EXAMEN DE CERTIFICACIÓN INTERNACIONAL COMO:

CPP® Certified Protection Professional
BOARD CERTIFIED IN SECURITY MANAGEMENT

| PARTICIPANTE | COSTO |
|---|---|
| Socio ASIS | $24,000 M.N. + IVA<br>$1,500 USD + IVA |
| No socio | $28,000 M.N. + IVA<br>$1,750 USD + IVA |

**COORDINADOR**
Lic. J. Rubén Fajardo, CPP, PSP, PCI

**26 SESIONES**
Martes y jueves
17 -21 hrs.

**MODALIDAD**
Presencial y aula virtual

**REPASO**
Retiro intensivo
32 hrs.

**INICIO**
08 DE AGOSTO 2024

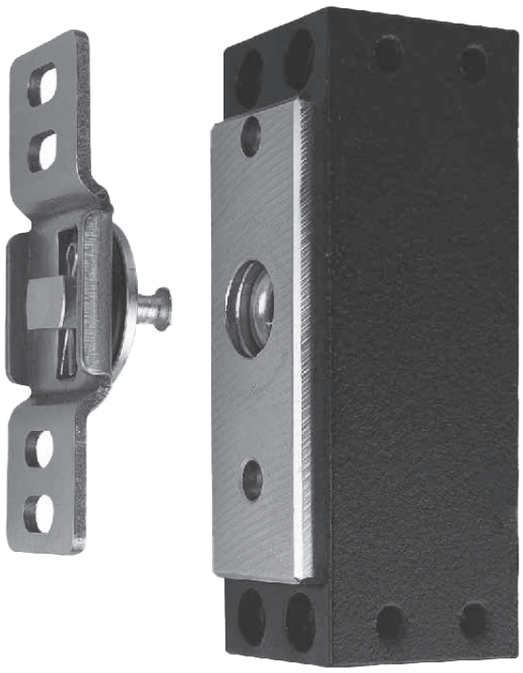
**MAYOR INFORMACIÓN**
( 55 1321 1289
socios@asis.org.mx

# Lanza cerradura ultra compacta de gabinetes **CAMDEN**

**Ontario, Canadá.**- Camden Door Controls lanza su cerradura magnética para gabinetes CX-EPD0009. Con un diseño ultra compacto, es una cerradura de alta seguridad de fácil instalación para prácticamente cualquier puerta de gabinete, como gabinetes de computadora, neveras, casilleros y mostradores de exhibición de tiendas minoristas.

Esta cerradura operada magnéticamente de 12 V o 24 V tiene una fuerza de sujeción increíblemente fuerte de 440 lb (200 kg) y es resistente al agua para uso en interiores o exteriores, lo que la hace ideal para ambientes húmedos, incluidos neveras y congeladores interiores. La CX-EPD0009 también está diseñada para soportar hasta 5 libras de presión de precarga sin atascarse, lo que facilita su instalación y operación.

La cerradura magnética para gabinetes se puede montar en el frente o en el costado con puertas y cajones abatibles o corredizos, y su placa de armadura se ajusta a la alineación de la puerta.



**Acerca de camden door controls:** Camden Door Controls es un proveedor en la industria de productos de bloqueo, control y activación de puertas innovadores, de alta calidad y a precios competitivos. Respalda sus productos con un servicio al cliente, soporte técnico, entrega de productos y garantía superiores. Tiene registro ISO 9001:2018, cuenta con amplias capacidades de desarrollo de productos y mantiene una planta de fabricación de 40,000 pies cuadrados.

OPTEX
Sensing Innovation

www.optexamerica.com

# EL LÍDER MUNDIAL EN SOLUCIONES DE DETECCIÓN

Con soluciones de detección en interiores y exteriores para cada nivel de amenaza, los sensores OPTEX proporcionan flexibilidad, rendimiento y fiabilidad garantizada. Con 45 años de experiencia y más de 25 empresas en nuestra cartera global, OPTEX ha establecido una reputación mundial por su calidad, innovación y excelencia técnica.

## HIGHLIGHTS DEL PRODUCTO:

### REDSCAN Pro Advanced LiDAR Series

Extremadamente fiables y versátiles, los sensores de seguridad REDSCAN PRO utilizan tecnología LiDAR para crear una pared o plano láser virtual de alta resolución de hasta 100 m (330 pies) de largo, ideal para proteger perímetros, edificios, techos y activos.

**Modelos disponibles:**
**RLS-50100V:** 50 x 100 m (165 x 330 ft.), Modelo de interior y exterior
**RLS-3060V:** 30 x 60 m (100 x 200 ft.), Modelo de interior y exterior

### REDSCAN mini-Pro LiDAR Series

Proporciona una precisión y flexibilidad sin precedentes para aplicaciones de alta seguridad, utilizando tecnología de tiempo de vuelo de vanguardia para rastrear con precisión el movimiento objetos. Con una cámara FHD incorporada (modelo RLS-2020V) y cumplimiento de ONVIF, mejora la seguridad con verificación visual y una integración perfecta.

**Modelos disponibles:**
**RLS-2020V:** 20 x 20 m (65 x 65 ft.), modelo de 95° para interiores y exteriores, con cámara FHD
**RLS-2020A:** 20 x 20 m (65 x 65 ft.), 95° modelo de interior y exterior

### CHeKT Video Bridge Series

Potentes dispositivos de puerta de enlace de última generación que permiten la seguridad profesionales para conectar cámaras compatibles con ONVIF, sensores de alarma, sistemas de audio e iluminación a la verificación visual basada en la nube portal impulsado por CHeKT para eliminar el 100% de los despachos falsos.

**Modelos disponibles:**
**CKB-308:** 8 channel PoE-powered CHeKT Video Bridge
**CKB-312V2:** 12 channel PoE-powered CHeKT Video Bridge

**Contact Us:** 800.966.7839

sales@optexamerica.com

# Biometría facial, método seguro contra la ciberdelincuencia: iProov

El mundo se digitaliza a un ritmo increíble y los métodos tradicionales de autenticación, como las contraseñas de un solo uso, no consiguen mantener la seguridad de las organizaciones. A medida que las tecnologías y metodologías de fraude crecen en sofisticación y escala, la verificación biométrica facial ha surgido como uno de los métodos más seguros y convenientes para que las organizaciones verifiquen la identidad del usuario en línea.

Sin embargo, las organizaciones deben comprender que no todas las tecnologías biométricas faciales han seguido el ritmo de los rápidos cambios en el panorama de las amenazas. No todas tienen el mismo nivel de seguridad, resistencia o adaptabilidad a las nuevas amenazas.

Implantar una solución de verificación biométrica facial sin tener visibilidad sobre las amenazas y su evolución, es como construir una casa sin los materiales adecuados para soportar los elementos. Para ser eficaces, las soluciones deben ser resistentes al panorama de amenazas en constante evolución y utilizar la inteligencia sobre amenazas para garantizar que pueden proporcionar el nivel esperado de garantía de identidad.

**América Latina: laboratorio de fraude digital**

"América Latina es un territorio absolutamente líder en fraude digital y estos países están tres años por delante del resto del mundo en términos de ataques biométricos. Vemos ataques en América Latina que no vemos en ningún otro lugar del mundo", afirmó Andrew Bud, CEO.

De acuerdo con técnicos de la empresa, en febrero de este año, un banco latinoamericano fue atacado 100 mil veces en un mes por deepfakes, para configurar una cuenta. Es decir, ciberdelincuentes tratando de penetrar en cuentas de usuarios del banco para cometer su crimen. "Nunca hemos visto 100 mil ataques en un mes contra ninguna institución financiera privada del mundo", recalcó Bud.

"El auge de la IA generativa ha amplificado las vulnerabilidades existentes del conocimiento heredado y los factores de posesión. Los malos actores han utilizado la tecnología como arma para mejorar el relleno de credenciales y las campañas de phishing para maximizar la eficacia de la apropiación de cuentas", agrega Daniel Molina, VP para América Latina.

"iProov Authentication ofrece autenticación biométrica facial basada en ciencia con detección de vida para proteger todo el ciclo del usuario sin comprometer la usabilidad. Un usuario simplemente se autentica con una única credencial, su rostro, para la incorporación, el acceso físico y digital, la recuperación de la cuenta y la vinculación del dispositivo", agrega Molina.

**Comprender las tendencias en los tipos de ataques biométricos**

A principios de 2024, en un informe publicado por la organización sobre amenazas biométricas, en el que se analizan las amenazas a la tecnología biométrica en producción durante el último año.

Entre los principales hallazgos de este informe está: un fuerte aumento de los fraudes por intercambio de caras (fase swap) y ataques de inyección digital en 2023 de 704% en el segundo semestre de 2023, en comparación con el primer semestre del mismo año. Los ataques de inyección están evolucionando rápidamente con nuevas amenazas significativas para las plataformas móviles. Observamos un aumento del 255 % en los ataques de inyección contra la web móvil en el segundo semestre con respecto a los primero seis meses de 2023.

Nadie está a salvo: los ataques ocurren en masa e indiscriminadamente, y no discriminaron ni la industria ni la geografía, lo que sugiere que ninguna organización está a salvo. Los sistemas de verificación basados en movimientos, que utilizan movimientos activos como sonreír, asentir y parpadear, fueron frecuentemente atacados.

iProov Authentication ofrece autenticación biométrica facial basada en ciencia con detección de prueba de vida para proteger todo el ciclo del usuario sin comprometer la usabilidad. Un usuario simplemente se autentica con una única credencial, su rostro, para incorporación, acceso físico y digital, recuperación de la cuenta y vinculación del dispositivo.

**Diferencias entre ataques de inyección digital, intercambios de caras y ataques de presentación**

Los ataques de presentación consisten en presentar un artefacto -como una foto impresa, una máscara de silicona o un video deepfake en una pantalla- a un teléfono móvil o un ordenador, para hacer emular el rostro de una persona.

Los ataques de inyección digital, por otro lado, son ciberataques sofisticados, altamente escalables y replicables que eluden la cámara de un dispositivo (o se inyectan en un flujo de datos). Son mucho más escalables que los ataques de presentación y no requieren la creación manual de un artefacto físico ni ninguna presentación física. Esta escalabilidad impulsa la mayor frecuencia y peligrosidad de los ataques de inyección digital.

Los intercambios de rostros son un tipo de medios sintéticos creados a partir de dos entradas que, en última instancia, superponen otra identidad a la entrada original, "intercambiando" dos rostros en tiempo real. Los intercambios de caras derivados de la IA generativa son la principal preocupación debido a su capacidad para manipular rasgos clave de imágenes o videos.

Muchas soluciones biométricas no están preparadas para defenderse de amenazas cambiantes y sin cartografiar, como los intercambios de rostros y las inyecciones digitales. En respuesta a la amenaza en constante evolución de los ataques sistematizados y escalables, la seguridad debe ser resistente y adaptable, en lugar de simplemente resistente a las falsificaciones establecidas y conocidas.

**¿Por qué es importante la seguridad biométrica?**

La necesidad de una verificación de identidad segura y remota es mayor que nunca. Las organizaciones necesitan saber que sus usuarios nuevos y recurrentes son realmente quienes dicen ser.

La verificación manual de la identidad a distancia ha demostrado ser ineficaz, y el panorama de las amenazas está evolucionando. Delincuentes digitales innovadores están utilizando herramientas avanzadas para crear vectores de amenaza nuevos y ampliamente desconocidos. Todos los métodos de verificación a distancia son vulnerables a herramientas de medios sintéticos, como el intercambio de rostros, ya sean videollamadas totalmente humanas, procesos híbridos con comprobaciones biométricas faciales y supervisión humana, o totalmente automatizados.

En última instancia, los que aprovechan la tecnología de verificación biométrica están en una posición más fuerte para detectar y defenderse de los ataques. Pero hay que elegir la solución biométrica adecuada.

La marca está ampliamente considerado como un proveedor preeminente de soluciones de tecnología biométrica facial, en el que confían destacadas organizaciones de todo el mundo, como la Australian Taxation Office (ATO), GovTech Singapore, UBS, ING, el Ministerio del Interior del Reino Unido, el Departamento de Seguridad Nacional (DHS) de EE.UU., entre otras.

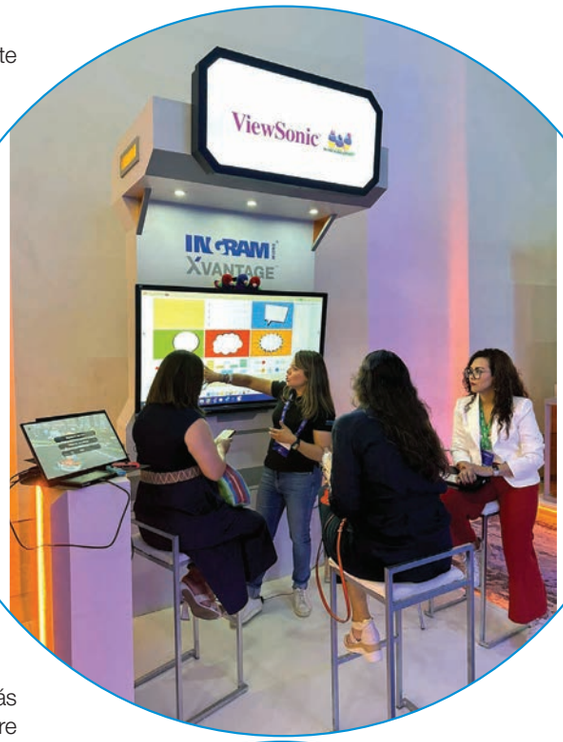
Dada la naturaleza siempre transformadora de la IA generativa y la escalabilidad de los ataques de inyección digital, es imperativo que la seguridad biométrica se gestione de forma activa y adaptable.

Un elemento clave del proceso de seguridad es iProov Security Operations Center (iSOC), el primer sistema global de inteligencia sobre amenazas y gestión activa de amenazas del sector. A través de iSOC, la empresa supervisa el tráfico en tiempo real para detectar patrones de ataque en múltiples geografías, dispositivos y plataformas.

Esto permite una supervisión y aprendizaje continuos de las fuentes, patrones y metodologías de ataque, manteniendo nuestros sistemas biométricos un paso por delante del cambiante panorama de las amenazas.

# Innovador y exitoso IDX 2024 de INGRAM MICRO

**Cancún, Quintana Roo**.- Ante la presencia de casi 700 asistentes, se realizó con rotundo éxito la versión 2024 del congreso IDX de Ingram Micro México, evento donde la firma mayorista con 45 años de existencia en el mercado mundial, dejó ver a sus canales las tendencias a seguir en los próximos meses para las oportunidades de negocio en cloud computing, ciberseguridad, centros de datos, Inteligencia Artificial (IA) e Internet de las Cosas (IoT), pero apuntalando la inclusión e igualdad de género en todas las actividades de la compañía.



## Hacia el futuro

Al inaugurar el IDX 2024, Luis Férez, presidente de Ingram Micro para América Latina, puntualizó: "actualmente vender tecnología es más complicado que antes, porque se requiere mucho más apoyo, entendimiento y mejores skills. Nosotros trabajamos para que nos vean como un aliado integral que pueda ayudarles a complementar una oferta, desde la dimensión, hasta la entrega.

Dijo que los canales y usuarios finales cuentan con una oferta en la nube, ciberseguridad, servicios profesionales y financieros para apoyar los negocios de sus distribuidores.

Los canales asistentes -afirmó- pudieron hacer negocios en el transcurso del IDX 2024, pues tuvieron acceso a precios especiales y descuentos de algunos productos de las marcas patrocinadoras. Aquí el networking es lo más valorado por los canales y fabricantes.

Luis Férez, mencionó que el 35% de los asistentes al IDX fueron mujeres y los 60 fabricantes patrocinadores tuvieron más de 700 reuniones de negocio. Puntualizó que la firma mayorista tiene presencia en 59 países, llega al 90% de la población mundial y trabaja con más de 1500 fabricantes, 125 centros de servicios y logística, así como 25 mil asociados de tiempo completo.

## A paso firme

Entre las novedades del IDX 2024, fue el reconocimiento presencial que se le hizo a Gerardo Romero, como nuevo director general de Ingram Micro México, quien señaló que la empresa apuntala su modelo de negocio en cuatro prioridades estratégicas globales: transformación digital, a través de Xvantage (convertirse de un mayorista tradicional a compañía de plataforma, expansión del portafolio de soluciones avanzadas (incorporación de nuevas marcas), excelencia operativa a través de Xvantage (procesos ágiles para incrementar la satisfacción del canal) y crecimiento del talento y valores ESG de diversidad e inclusión.

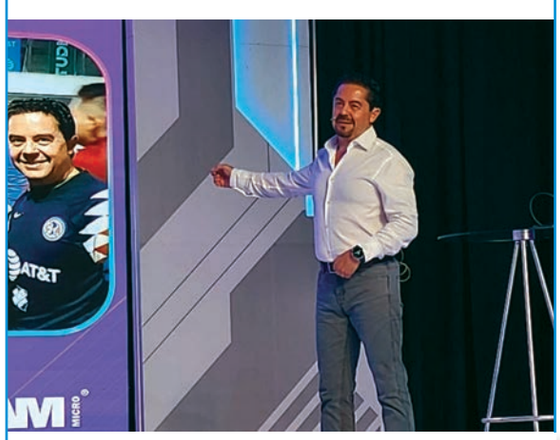
Este año tiene la particularidad que la transformación tecnológica se capitaliza en una tendencia que no tiene revesa, ejemplo es la Inteligencia Artificial que es una realidad.

Gerardo Romero añadió que la apuesta de Ingram Micro está basada en soluciones avanzadas, ciberseguridad, cloud, la nube de marca blanca, servicios de TI administrados, servicios profesionales, logística inversa, soluciones de flujo de caja, servicios de entrenamiento y servicios ITAD.

"Las oportunidades que hay entorno a la Inteligencia Artificial, que trae consigo negocios en el centro de datos, ciberseguridad, cloud y conectividad. Para centro de datos, Ingram Micro está enfocando su estrategia en la adopción de tecnologías hiperconvergentes, servicios gestionados y de consultoría, soluciones de nube híbrida y enfoque en la eficiencia energética y sostenibilidad.

Importante mencionar que el mayorista en la vertical de ciberseguridad, cuenta con un catálogo de soluciones para todo tipo de mercado e industria (SMB, Pymes, Enterprise, entre otras).

Para cerrar, mencionó que Ingram Micro México cuenta con 725 canales activos, más de 25 marcas en ejecución y más de 117 millones de pesos de transacción.




Gerardo Romero, director general de Ingram Micro México

La empresa proveedora de software es un excelente complemento al portafolio de soluciones de coordinación de emergencias de Motorola Solutions.

# MOTOROLA SOLUTIONS adquiere Noggin

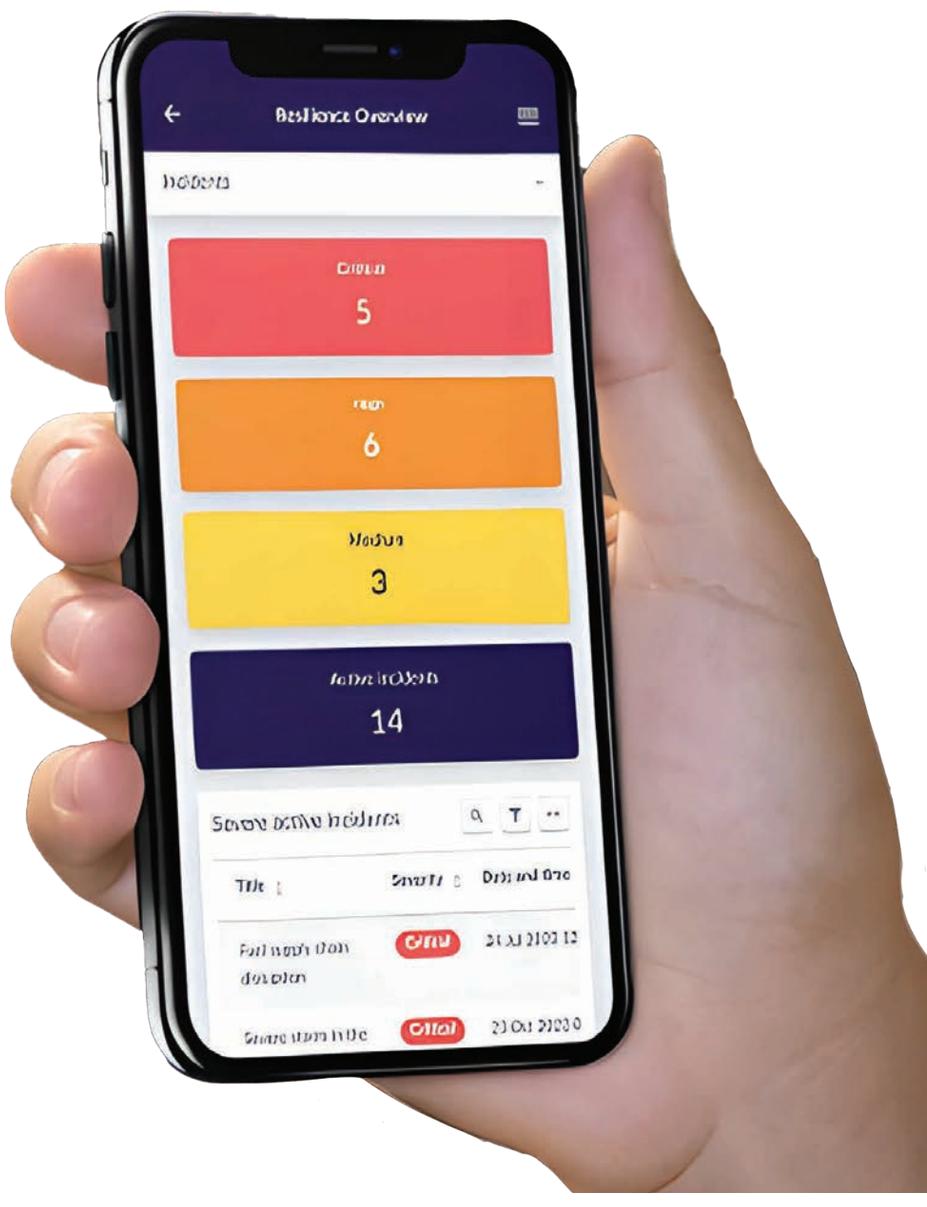
Motorola Solutions adquirió Noggin, proveedor global de software basado en la nube para la planificación de la continuidad del negocio, resiliencia operativa y gestión de eventos críticos (CEM). La empresa tiene su sede en Sídney (Australia) y cuenta con clientes en todo el mundo.

El software de Noggin ayuda a empresas e infraestructuras críticas a anticiparse, prepararse y responder eficazmente a los incidentes. La plataforma integrada de la compañía ofrece flujos de trabajo y listas de comprobación flexibles, mapas integrados y paneles de consciencia situacional para ayudar a agilizar la gestión de incidentes y fortalecer la flexibilidad de las empresas. Con una interfaz única y fácil de usar, el software de Noggin permite a los equipos de respuesta comunicarse directamente, seguir procedimientos unificados y ver la misma imagen operativa durante incidentes cotidianos o emergencias.

"Nuestras inversiones en tecnología para conectar a los necesitados con los que pueden ayudar, son más críticas que nunca", dijo Greg Brown, presidente y CEO de Motorola Solutions. "Noggin permite la resiliencia operativa y las capacidades de gestión de incidentes que son esenciales a medida que las industrias a nivel mundial siguen viendo cómo las amenazas escalan en número y complejidad."

La empresa proveedora de software es un excelente complemento al portafolio de soluciones de coordinación de emergencias de Motorola Solutions, añadiendo planificación de continuidad de negocio, resiliencia operativa y software CEM que ayuda a hacer la seguridad empresarial más accesible y accionable. La adquisición de Noggin refuerza aún más la capacidad de Motorola Solutions para conectar los organismos de seguridad pública y las empresas, permitiendo la colaboración que es fundamental para un enfoque más proactivo de la seguridad.

"Junto a Motorola Solutions, seguiremos ayudando a las compañías a responder y gestionar rápidamente todo tipo de eventos adversos e interrupciones", afirmó James Boddam-Whetham, CEO de Noggin. "Nos entusiasma este nuevo paso en nuestro camino que nos permitirá ofrecer soluciones a una base de clientes más amplia."



# Infostealers: peligro en LATAM

- Mal peligroso y sigiloso, que puede llevar a pérdidas financieras significativas, como el robo de identidad y compromisos de seguridad a gran escala; representan una amenaza grave y persistente en el panorama de la ciberseguridad.

Son múltiples los riesgos y amenazas que rodean la seguridad y muchos los datos e información con los que interactuamos día con día, como personas y como organizaciones. Por ello, la seguridad de la información y la gobernanza de los datos se han convertido en aspectos clave e indispensable en nuestras actividades diarias. Entre las diversas amenazas cibernéticas, los infostealers se destacan por su capacidad para robar información confidencial y sensible con cierto grado de "facilidad" y resulta preocupante su creciente actividad y efectos en América Latina y el Caribe. En las siguientes líneas exploraremos más sobre los infostealers, cómo operan y los grupos criminales más notorios que los utilizan.

Los infostealers son un tipo de malware diseñado específicamente para infiltrarse en sistemas informáticos y extraer información valiosa. Esta información puede incluir credenciales de usuario, datos financieros, información personal y otros tipos de datos sensibles. Los infostealers se distribuyen a menudo a través de correos electrónicos de phishing, sitios web comprometidos y descargas de software malicioso. Su capacidad para operar en segundo plano y sin ser detectados los convierte en una amenaza particularmente engañosa.

El peligro creciente sobre los infostealers radica en su capacidad para robar datos sensibles sin el conocimiento del usuario, se dice que los infostealer son un mal peligroso y sigiloso, que puede llevar a pérdidas financieras significativas, como el robo de identidad y compromisos de seguridad a gran escala. La información robada puede ser vendida en mercados clandestinos, donde puede ser usada múltiples veces para cometer fraudes y delitos. La rapidez con la que los infostealers pueden extraer y transmitir datos a servidores controlados por atacantes los hace extremadamente peligrosos. La información objetivo de ellos puede ser (sin ser limitativa):

**Credenciales de usuario:** Pueden capturar nombres de usuario y contraseñas almacenadas en navegadores web, aplicaciones de correo electrónico y otros programas. Esto permite a los atacantes acceder a cuentas personales y corporativas.

**Información financiera:** Datos de tarjetas de crédito, información bancaria y otros detalles financieros son objetivos comunes. Esta información puede ser utilizada para realizar transacciones fraudulentas o venderse en mercados clandestinos.

**Datos personales:** Pueden capturar información personal, como números de seguro social, direcciones y números de teléfono. Esto puede llevar a robos de identidad y otros problemas relacionados con la privacidad.

Los infostealers se valen de diferentes formas de operar para lograr su objetivo, algunas de las formas más comunes son:

1. Registro de pulsaciones: registran cada tecla que es presionada, pueden capturar contraseñas y datos confidenciales.

2. Escaneo de archivos: buscan y roban archivos específicos del dispositivo.
3. Acceso a contraseñas: roban las contraseñas y credenciales almacenadas en los navegadores web.
4. Captura de pantallas: realizan capturas de pantallas periódicamente para registrar la actividad e información sensible y confidencial.
5. Espionaje de comunicaciones: vigilan los correos electrónicos y conversaciones en tiempo real en búsqueda de información sensible.

**Infostealers y grupos criminales en LATAM**

Los infostealers han presentado un incremento en su actividad en Latinoamérica y el Caribe, los países con mayor actividad* de este tipo en el primer semestre del 2024 son: Brasil (462,938), Argentina (146,427), México (118,784), Colombia (118,700) y Perú (118,566).

Los infostealers más relevantes en la región en el mismo periodo fueron: Lumma, Redline y Risepro. Estos se caracterizan por que es posible encontrarlos como Malware como servicio (MaaS), por sus múltiples capacidades y múltiples canales de C2.

Varios grupos criminales organizados utilizan infostealers como parte de sus operaciones. Estos grupos son conocidos por su sofisticación y la escala de sus ataques. A continuación, se describen algunos de los grupos más notorios:

TA505: Este grupo es conocido por sus campañas de phishing a gran escala y el uso de infostealers como FlawedAmmyy y ServHelper. TA505 ha atacado a instituciones financieras, minoristas y organizaciones de salud en todo el mundo.

FIN6: Este grupo se enfoca principalmente en el robo de datos de tarjetas de pago. Utilizan infostealers para capturar información de puntos de venta (POS) y han sido responsables de algunas de las brechas de datos más grandes de la última década.

Evil Corp: Conocido por desarrollar el infostealer Dridex, Evil Corp ha llevado a cabo numerosos ataques contra empresas en todo el mundo. Dridex es particularmente efectivo para robar credenciales bancarias y ha causado daños financieros significativos.

Para finalizar, es imprescindible mencionar que los infostealers pueden distribuirse de varias maneras, entre las que se incluyen:

1. Correos electrónicos de Phishing: Mensajes diseñados para engañar a los usuarios para que descarguen y ejecuten el malware.
2. Sitios web comprometidos: Páginas web que explotan vulnerabilidades en los navegadores para descargar infostealers sin el conocimiento del usuario.
3. Software malicioso: Programas que parecen legítimos pero que en realidad contienen infostealers.

Los infostealers representan una amenaza grave y persistente en el panorama de la ciberseguridad. Su capacidad para robar información crítica de manera silenciosa y eficaz los convierte en una herramienta poderosa para los ciberdelincuentes. Para combatir esta amenaza, es esencial que las organizaciones implementen medidas de seguridad robustas, como la autenticación multifactor, la educación continua en ciberseguridad y el uso de software de seguridad avanzado.

Además, la colaboración internacional y el intercambio de información sobre amenazas emergentes son fundamentales para mitigar el impacto de los infostealers en nuestra sociedad conectada. Sin mencionar que, con un conocimiento adecuado y la implementación de mejores prácticas de seguridad, es posible reducir significativamente los riesgos asociados con estos ataques cibernéticos.

**Referencias:**
Scitum-SCILabs. (2024). “Los infostealers: ladrones digitales de tu información personal”. Consultado el 29 de junio de 2024 de: https://resources.scitum.com.mx/infostealers-ladrones-digitales/

**Gustavo Guzmán Hernández**
gguzmanh01@gmail.com
Tw @GustavoG_Kc
Articulista Invitado
**México**
Articulista Invitado

# ¡Los ciberataques siguen aumentando!

## Todavía no conocemos las intenciones de los hackers. ¿Es esta la razón?

**São Paulo, Brasil.-** En la era digital, ningún negocio está a salvo y libre de piratas informáticos. Por lo tanto, es fundamental conocer a tus oponentes a través de sus perfiles. También debemos profundizar en el conocimiento de los perfiles de los hackers, conocer sus intenciones, según la Norma ABNT NBR ISO/IEC 27005:2023, tenemos que identificar el Estado Final Deseado de los hackers. Y con este perfil planteado, podremos prospectar qué ataques, a qué nivel de tecnicismo se atacará a las empresas de determinados segmentos. Con esto conoceremos los tipos de ataques.

La inteligencia de amenazas debe incluir este tema para que los responsables de ciberseguridad puedan planificar las medidas de seguridad basadas en el EFD de los hackers.

Los modelos de IA se volverán altamente sofisticados y capaces de manejar diversos conjuntos de datos que son difíciles de descifrar, como los que se encuentran en la web oscura y dentro de formularios de datos “ocultos”.

A medida que los proveedores continúen innovando con la IA, los equipos de seguridad se sentirán más seguros de su capacidad para aumentar los flujos de trabajo de seguridad con datos de inteligencia de amenazas cibernéticas.

Al mismo tiempo, la IA será ampliamente accesible para los profesionales, independientemente de su conjunto de habilidades o nivel de madurez. El personal de nivel junior confiará más fácilmente en las soluciones de IA para gestionar y tomar medidas, ya que el valor añadido y la facilidad de uso han mejorado.

Tanto las empresas como los profesionales deben tener como motor el uso de la IA como herramienta para mitigar los ciberataques.

El ciberataque es muy completo y abarca una amplia variedad de actividades maliciosas realizadas por individuos o grupos con la intención de explotar vulnerabilidades en sistemas informáticos, redes o dispositivos conectados. Estas incursiones digitales pueden tener diferentes objetivos, como:

1. Robo de información y datos sensibles
2. Interrumpir los servicios
3. Aplicar golpes
4. Dañar la reputación de las empresas

A lo largo de los años, con el crecimiento acelerado de la digitalización, los ciberataques han seguido el ritmo de la evolución de la tecnología. Hoy, además de ser extremadamente comunes, estos incidentes son más sofisticados y potencialmente dañinos. Para que te hagas una idea, según Cybersecurity Ventures, se espera que el coste de la ciberdelincuencia alcance los 8 billones de dólares en 2023 y crezca hasta los 10,5 billones de dólares en 2025. Esto demuestra que el tema es de muy alta relevancia y necesita ser tratado con la máxima atención, y tenemos que cambiar nuestras estrategias. Tenemos que: cambiar tu mentalidad, es decir, tenemos que cambiar nuestra forma de pensar, cambiar la forma en que nos enfrentamos a los hackers. Está claro que no está funcionando. No estamos siendo asertivos. ¡Así que tenemos que ver dónde estamos pecando!

Hacer frente a las numerosas amenazas cibernéticas que existen es un gran desafío. Además, es una tarea permanente, que involucra diferentes cuidados y prácticas.

Podemos enumerar algunos tipos de ataques: Ransomware, Phishing, Phishing de ballenas, DoS y DDoS, MITM (Hombre en el Medio), Ingeniería Social, Ataque de contraseña, suplantación de DNS, Fuerza bruta, Ataque XS, Malware, Caballo de Troya, Spoofing, Día Cero, Ataque de espionaje, Ataque de aniversario, Señuelo, entre otros.

El problema, nuestra interpretación y punto de vista, es la falta de mapeo de los perfiles de los hackers, además de conocer los tipos de ataques y las vulnerabilidades más explotadas. Conocer más profundamente tus características y habilidades es conocer tus habilidades e intenciones, es conocer el Estado Final Deseado – EFD.

EFD es la visión del hacker, proporciona la base para hacer planes: cómo implementarán el ataque para hacer realidad sus intenciones. Él decide: cuándo, qué y cómo hacerlo, de acuerdo con las condiciones existentes.

El hacker parte de la situación actual y visualiza un conjunto de condiciones deseadas, que representan el estado que se alcanzará al final del ciberataque. Tenemos que entenderlo a través de un análisis lógico. La siguiente figura muestra lo que debemos entender. Sin esta comprensión, seguiremos perdiendo esta carrera por la eficacia cibernética.

El hacker completa esta visualización con el Enfoque Operacional – cómo se implementará el ciberataque para que pueda cumplir sus intenciones – Estado Final Deseado – EFD.

La principal tarea de los gestores de riesgos cibernéticos es identificar las fuentes de estos riesgos, es decir, sus vulnerabilidades. Hay que mirar al pasado y conocer la frecuencia de los ataques en el contexto del modus operandi de los hackers. Y el tercer y más importante vector es conocer, a través de estudios de Inteligencia, el Estado Final Deseado – EFD. Contaremos así con la Intención, Motivación y Capacidad Técnica del hacker para entrar en el entorno cibernético de la empresa.

Al conocer esta tríada, la empresa seguramente estará mucho más preparada para enfrentar los ciberataques.

Este concepto, originado en el área de los riesgos cibernéticos, debe ser incluido por los gestores de riesgos corporativos como criterio de análisis en otras disciplinas, como la seguridad corporativa, en el contexto de desviaciones de comportamiento que engloban el cumplimiento de la empresa, el fraude corporativo y otros en los que el factor humano es un agente activo.

El EFD, un concepto presente en el estándar de seguridad de la información, ciberseguridad y protección de la privacidad, debe ser aplicado directamente por los gestores de otras categorías de riesgo como metodología para visualizar el riesgo materializado.

De nada sirve conocer los tecnicismos de los ataques y los sistemas de ciberseguridad, sino sabemos cómo se pueden llevar a cabo.

Por eso es importante que el EFD se entienda en su totalidad, para que las defensas preventivas y las acciones de respuesta a emergencias, crisis y continuidad del negocio puedan ubicarse concretamente en los puntos considerados estratégicos.

Este es nuestro gran reto en este siglo XXI de cambios constantes y amenazas disruptivas. ¡¡Nuestro VUCA y BANI World Challenge!! ¡La digitalización no puede ignorar los riesgos!

**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**
Articulista Invitado

# Tecnología para un turismo seguro

La seguridad se ha convertido en un factor primordial, especialmente durante los periodos vacacionales, cuando la afluencia de turistas incrementa considerablemente en aeropuertos y resorts.

Por: Beatríz Canales

Garantizar una experiencia segura y placentera para los huéspedes ha impulsado a la industria hotelera a adoptar soluciones tecnológicas de vanguardia, por lo que empresas líderes en tecnologías de seguridad electrónica y privada como Scati, Seguridad Privada Peninsular, Hikvision, Salto Systems y Serviseg, han desarrollado productos y servicios de vanguardia que no solo protegen a los visitantes, sino que también optimizan la gestión operativa de los establecimientos. Aunado a esta protección, se resalta la protección física ofrecida por guardias, apostados en los hoteles y cubriendo la protección aeroportuaria.

Dichas soluciones avanzadas van desde videovigilancia inteligente y control de accesos hasta el uso de Inteligencia Artificial (IA) y tecnologías biométricas, jugando un papel estratégico en la creación de entornos seguros y confiables, fundamentales para el éxito del sector hotelero, sobre todo en temporadas de alta demanda.

**Seguridad Integral en el sector hotelero**

Scati, el fabricante español ha destacado por su avanzada tecnología en soluciones de seguridad electrónica, ofreciendo una variedad de equipos y plataformas integradas para una gestión eficiente y segura de hoteles y otras verticales.

Al respecto, María Eugenia Sánchez, Key Account Manager de la firma, subraya la amplia experiencia de la empresa: “nuestro compromiso con la innovación y la calidad nos ha posicionado en este

mercado, ofreciendo soluciones que no solo protegen a los huéspedes y empleados, sino que también garantizan la integridad de las instalaciones y propiedades”.

La compañía proporciona una variedad de equipos y soluciones que simplifican la operativa diaria, controlando todos los sistemas desde una única plataforma. Entre estas soluciones se encuentran la videovigilancia inteligente, prevención de fraude, control de accesos y gestión de visitantes, todas ellas integradas para ofrecer una gestión eficiente y segura.

Sus ventajas competitivas en el mercado incluyen tecnología desarrollada por un equipo de I+D que asegura que sus sistemas se mantengan actualizados para enfrentar los desafíos más recientes del sector. Además, destaca por sus soluciones ciberseguras que garantizan una protección robusta y preparada para futuros desafíos, así como por el uso de inteligencia artificial que permite respuestas más precisas a partir del análisis de video.

Un caso de éxito que ilustra la eficacia de las soluciones de la empresa es el Breathless Riviera Cancún Resort & Spa, donde se han instalado más de 300 cámaras que velan por la seguridad de sus huéspedes con la máxima discreción.

En el ámbito de la videovigilancia, se ofrece una gama completa de soluciones. Entre sus productos destacados se encuentra el SCATI VMS, un software de gestión que permite una supervisión integral y eficiente. Complementando este software, SCATI CLOUD proporciona una opción avanzada de grabación en la nube, asegurando que los datos estén siempre disponibles y seguros. Además, integra analíticas de video avanzadas que facilitan la detección de incidentes en tiempo real, y cuenta con servidores de grabación robustos y cámaras de alta definición, incluyendo sistemas de CCTV embarcado, ideales para aplicaciones en movilidad.

Para el control de accesos, SCATI ACCESS se presenta como un software de gestión de primera línea, capaz de administrar de manera

efectiva el acceso a instalaciones críticas. La integración de sistemas es otra área donde SCATI sobresale, gracias a su software de gestión SCATI SENTRY. Finalmente, en el campo de la inteligencia de negocios, SCATI RECKON se destaca como un software de business intelligence que incluye diversos módulos para el análisis detallado de los datos de seguridad.

Estas soluciones integrales de SCATI no solo aseguran la protección de instalaciones y personas, sino que también optimizan la gestión operativa y proporcionan un alto nivel de seguridad en diversos entornos.

**Capital Humano**

La inteligencia artificial está transformando la seguridad hotelera, permitiendo sistemas más proactivos y predictivos. La ciberseguridad está para proteger la información personal y financiera de los huéspedes,

y las tecnologías biométricas como el reconocimiento facial, están ganando terreno como métodos de acceso seguros y personalizados.

De su lado, tenemos a la firma Seguridad Privada Peninsular, adaptando sus servicios a las necesidades específicas de cada hotel.

Saúl Daniel Romero Rodríguez, director de operaciones de dicha empresa de seguridad privada, destaca la importancia de la capacitación y el perfilamiento del personal de protección: “nos enfocamos en la prevención de riesgos y en ser un elemento disuasorio con capacidad de reacción ante eventualidades”.

Explica que cada guardia es capacitado de manera continua para enfrentar situaciones específicas, como conatos de incendio o alertas por extravío de menores. Esta capacitación constante garantiza que el personal esté preparado para reaccionar de manera efectiva y

proporcionar una sensación de tranquilidad y seguridad a los huéspedes.

Durante la temporada alta de vacaciones, Seguridad Privada Peninsular ajusta el número de elementos de seguridad según la afluencia de huéspedes. “No hay un número ideal de guardias; analizamos las necesidades específicas de cada cliente y reforzamos las áreas más vulnerables,” explica Romero. Por ejemplo, en verano o durante el “Spring break”, se incrementa el personal de protección para asegurar una cobertura adecuada y eficiente.

Su servicio de seguridad residencial se centra en proteger y salvaguardar la tranquilidad de los residentes. También ofrece soluciones integrales de seguridad corporativa diseñadas para proteger tanto a los empleados como a los activos de cualquier empresa.

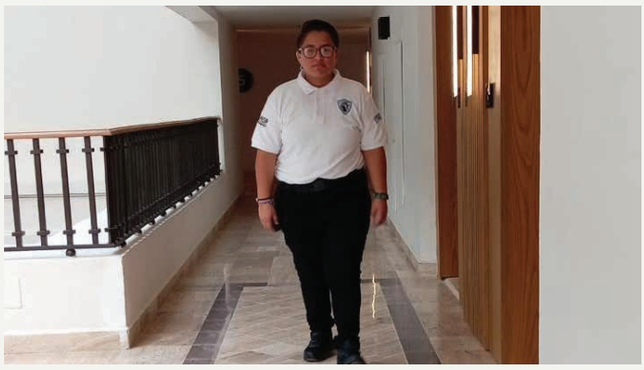
Otro aspecto es la seguridad en tiendas de prestigio, esencial para

proteger la mercancía, prevenir pérdidas y proporcionar un ambiente de compras seguro. La protección en la construcción también es prioritaria con medidas precisas: equipo de protección, señalización clara y supervisión constante para prevenir riesgos.

En el rubro turístico, un sector hotelero con alta seguridad es fundamental para garantizar la tranquilidad de los huéspedes y el personal. La empresa utiliza herramientas avanzadas como CCTV, sistemas de intrusión y controles de acceso electrónicos. Además, ajusta el número de elementos de seguridad según la afluencia de huéspedes, garantizando una cobertura adecuada durante temporadas altas como el verano y el famoso “Spring break”.

**Tecnología en evolución**

Por otro lado, Miguel Arrañaga Alcántara, director regional de ventas Bajío para Hikvision México, explica cómo la empresa ha evolucionado



la seguridad en el sector hotelero con tecnologías avanzadas y equipos especializados, ha trabajado estrechamente con hoteles urbanos y resorts en destinos turísticos de playa: “usamos analíticas de video y soluciones para cuidar áreas comunes, detectar personas extrañas y monitorizar comportamientos”.

Desde sus inicios, Hikvision ha trabajado estrechamente con hoteles urbanos en Ciudad de México, Guadalajara y Monterrey, así como con resorts en destinos turísticos de playa como Cancún, Playa del Carmen, Veracruz y Acapulco: “hemos tenido muchas experiencias desafiantes debido a las condiciones ambientales adversas como lluvia, baja iluminación y perímetros abiertos rodeados de selva,” comenta Arrañaga.

El fabricante ofrece cámaras térmicas, radares y sistemas de inteligencia artificial que permiten una detección precisa y eficiente de movimientos o vehículos, protegiendo así las instalaciones del hotel. Un ejemplo de éxito es Bahía Príncipe en la Riviera Maya, donde Hikvision implementó una solución centralizada para controlar y administrar varios hoteles desde un punto central, optimizando la operación y reduciendo costos.

Para el experto Arrañaga, el uso de soluciones electrónicas para tener unas vacaciones seguras, tanto de los inmuebles como de los usuarios es fundamental, comentando que al encontrarse con quipos de la marca en diferentes inmuebles es sinónimo de calidad, pero sobre todo de seguridad confiable.

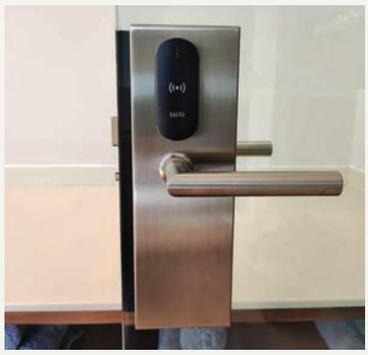
“La seguridad empieza desde uno mismo cuando se sale de casa, y si bien los sistemas son inteligentes, avanzados y realizan varias cosas, como complemento debe existir el factor humano, pero hay que dejar que la tecnología haga su trabajo, hacerlo en conjunto para ganar resultados efectivos”, resalta.

**Cerraduras electrónicas de vanguardia**

Empresa reconocida a nivel mundial por sus soluciones de seguridad electrónica, transforma la experiencia del huésped con tecnologías avanzadas.

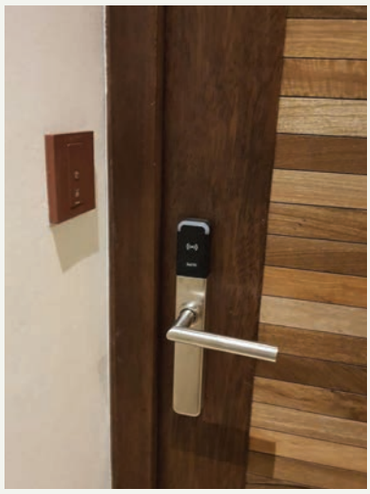
Rubén Estrada Tapia, gerente comercial de Salto Systems para la zona sureste de México, destaca la transición de llaves mecánicas a tarjetas y cerraduras electrónicas: “Salto ha permitido un mejor control y encriptación de las credenciales, ofreciendo un sistema más robusto que mejora la gestión del huésped”.

"Somos una empresa a nivel mundial que ha revolucionado la seguridad en hoteles, sustituyendo las llaves mecánicas por tarjetas y cerraduras electrónicas". Esta transición ha permitido un mejor control y encriptación de las credenciales, que también permite un control total de lo que ocurre dentro de una habitación.



Salto cuenta con dos plataformas, una muy puntual para el segmento de hotelería y otra especial para el nicho de renta vacacional: "Si tienes, por ejemplo, algún departamento o condominio que quieres rentar, puedes tener tu propio control desde tu dispositivo móvil con una solución en la nube, donde es posible generar llaves digitales a través de los móviles a todos los que quieran hacer uso del condominio o la propiedad que tengas.

"Es posible también tener monitoreo en tiempo real de todos los eventos que se generen en la puerta como por ejemplo, puerta abierta, quién accedió, a qué hora salió, y si las baterías están al 30%, puedes enviar una extensión o cancelar también. Esto te da un grado de control mucho más alto, porque la gestión depende totalmente de ti", explica Estrada Tapia.



La eficacia de las soluciones de Salto se refleja en casos de éxito notables. Por ejemplo, un hotel con mil habitaciones que utilizaba otra marca, registraba gastos operativos de $6 mil dólares al año, mientras que al cambiar a Salto, los costos se redujeron a $4,855. "Esto demuestra ahorros significativos debido a la calidad de nuestros productos y tecnologías", afirma Estrada.

Las plataformas de esta importante firma en México y América Latina permiten generar llaves digitales, monitorear eventos en tiempo real y gestionar la seguridad de manera eficiente. Por ejemplo, la plataforma robusta Space puede gestionar hasta 64 mil puertas y 4 millones de usuarios, proporcionando un control preciso y seguro casi en tiempo real.

Finalmente, Daniel Arturo Espinosa Ávila, director general de Grupo Serviseg Cosepros, comparte detalles sobre el papel fundamental que desempeña su empresa en la seguridad aeroportuaria en México. Desde 2001, se ha dedicado a la custodia y cuidado de pasajeros en aeropuertos, líneas aéreas y servicios complementarios dentro de las terminales aéreas, como joyerías y restaurantes.

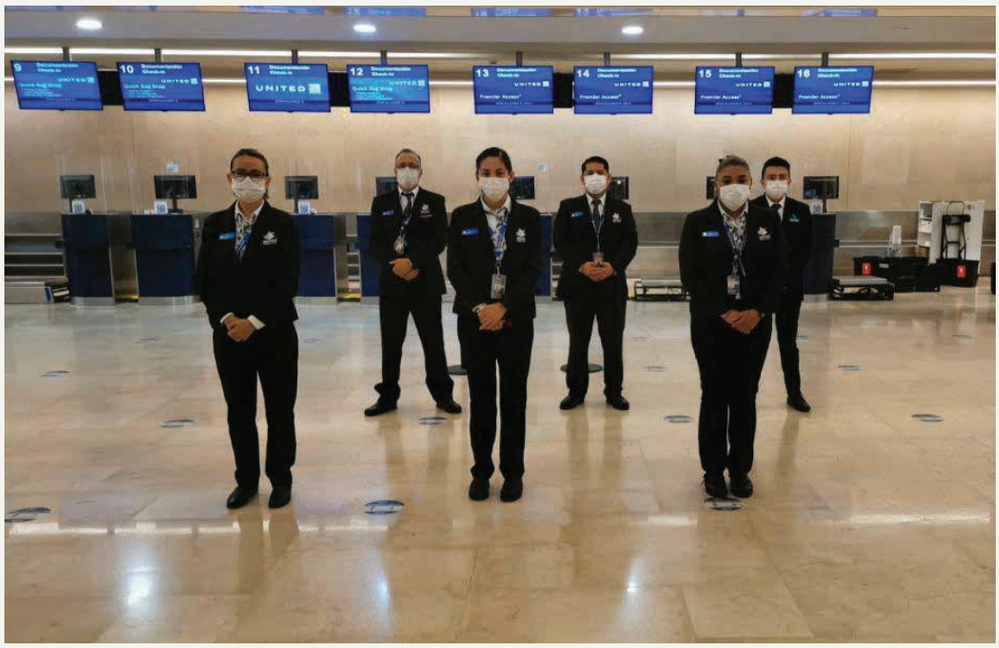
Espinosa Ávila explica que su equipo se encarga de manejar las líneas de ingreso a los aeropuertos, utilizando tecnología avanzada como máquinas de rayos X y detectores de trazas para identificar artículos o sustancias peligrosas: "nuestro trabajo se dedica exactamente a la custodia y cuidado de pasajeros en aeropuertos. El personal está capacitado para vigilar objetos y comportamientos sospechosos, garantizando la seguridad de todos los presentes", señala.

Genetec™

Evolución del control de acceso

Análisis del mercado de control de acceso: Tendencias y mejores prácticas para mejorar tus operaciones de seguridad

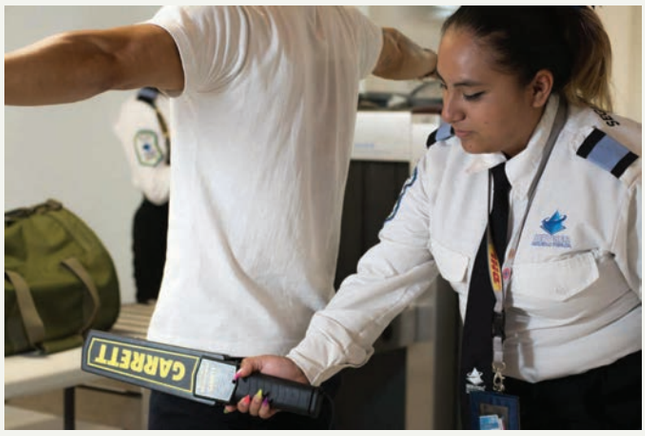
Descarga el whitepaper



La empresa emplea herramientas electrónicas vitales para la protección, incluyendo equipos de rayos X, detectores de metales y arcos de detección. Estas tecnologías son esenciales para realizar revisiones de equipajes de manera eficiente y segura. Espinosa Ávila subraya: “Es primordial. Sin equipos de rayos X, la revisión de equipajes sería manual y mucho más lenta”.

La cantidad de personal necesario para garantizar la seguridad varía según la temporada y el aeropuerto. Este personal adicional asegura un flujo rápido y seguro, sin comprometer la protección.

Grupo Serviseg se distingue por su vasta experiencia y un centro de capacitación y evaluación certificado, que prepara tanto a su personal como a otras compañías. La empresa cuenta con alrededor de 3 mil elementos, de los cuales unas mil 400 están dedicados a la seguridad aeroportuaria en todo México.




En cuanto a la proyección a futuro, el directivo destaca que la empresa está alineándose con las nuevas leyes y estrategias para continuar ofreciendo servicios de alta calidad.

Con una sólida trayectoria y un compromiso inquebrantable con la seguridad, Grupo Serviseg Cosepros continuará fortaleciendo su reputación para ser un referente en el ámbito de la seguridad aeroportuaria en México.

**Consejos y herramientas para unas vacaciones seguras**

La seguridad es vital sobre todo en el sector de la aviación, ya que es una prioridad indiscutible, especialmente durante las temporadas de vacaciones, cuando el flujo de pasajeros aumenta considerablemente.

Al respecto, Eduardo Reyes López, gerente de Seguridad Patrimonial en Schneider Electric y con casi 30 años de experiencia en la salva guarda en la aviación, ofrece una perspectiva única sobre cómo garantizar “vacaciones seguras” a través de una gestión efectiva de riesgos y procedimientos rigurosos.

El experto explica que la gestión de riesgos es el núcleo de los procesos en seguridad aeroportuaria: “las acciones en seguridad aeroportuaria parten de una gestión de riesgos,” enfatiza, destacando la importancia de un enfoque meticuloso y sistemático en la identificación de amenazas y la implementación de estrategias de mitigación. Su labor incluye, establecimiento de procedimientos y evaluación de su efectividad para asegurar una mejora continua.

En los aeropuertos, la seguridad se enfoca en proteger a las personas: pasajeros, colaboradores, visitantes y autoridades, por lo que “la premisa siempre es proteger a las personas y los activos esenciales para las operaciones aéreas,” subraya. Además de las personas, se deben cuidar activos críticos como instalaciones, radio ayudas, plantas de combustibles, torres de control y servidores.

Reyes López comparte algunos consejos para garantizar la seguridad en los aeropuertos a partir de tres elementos básicos:

1.- Personal de seguridad: incluye tanto a personal de seguridad privada como a todos los empleados del aeropuerto, quienes deben estar capacitados para actuar ante amenazas.
2.- Tecnología y equipamiento: arcos detectores de metales, equipos detectores de explosivos, rayos X, sistemas de cámaras y equipos de radiocomunicación son herramientas esenciales.
3.- Procedimientos: estos dictan cómo y por qué se realizan las actividades y se vinculan con las autoridades en situaciones de contingencia.

**Importancia de las herramientas electrónicas**

Las tecnologías modernas han reducido significativamente los errores humanos y han agilizado los procedimientos de seguridad. “Anteriormente los procedimientos eran tardados, tediosos y muy invasivos,” menciona Eduardo Reyes y abunda que con el uso de nuevas tecnologías, estos problemas se han mitigado, mejorando la experiencia de los pasajeros.

El equipo de seguridad varía según el volumen de operaciones y pasajeros, el tamaño del aeropuerto y el nivel de amenaza. Durante

la temporada de vacaciones, el nivel de exigencia es mayor debido al incremento de pasajeros, pero el personal está preparado para ser más ágil sin comprometer la efectividad.

La experiencia de los expertos en líneas aéreas, empresas de seguridad privada y aeropuertos ha dado una visión completa de los problemas y necesidades de seguridad. Esta perspectiva integral ha permitido implementar soluciones estratégicas que benefician a todo el sistema aeroportuario.

Se anticipa, por lo tanto, que las regulaciones de seguridad serán cada vez más estrictas y el uso de tecnologías avanzadas, incluyendo la Inteligencia Artificial, se incrementará. Las nuevas amenazas, como el uso de drones y ataques cibernéticos, requieren desarrollos tecnológicos y personal de seguridad altamente calificado.

"Los aeropuertos son instalaciones estratégicas y claves para el desarrollo económico," finaliza el gerente de Seguridad Patrimonial en Schneider Electric.

Cabe destacar que la seguridad física seguirá siendo una línea de defensa importante contra amenazas a la aviación civil. La innovación con tecnologías como cercados perimetrales inteligentes, cámaras con Inteligencia Artificial y pases de abordar biométricos se perfeccionará cada vez más, aunque ya es esencial para mantener la seguridad en constante evolución.

Este enfoque integral y actualizado en la protección aeroportuaria garantiza que las vacaciones de los viajeros sean seguras y sin contratiempos, proporcionando tranquilidad y protección en cada etapa del viaje.

Rubén Estrada, gerente comercial de Salto Systems

María Eugenia Sánchez, Key Account Manager de Scati

Daniel Arturo Espinosa Ávila, director general de Grupo Serviseg Cosepro

Miguel Arrañaga Alcántara, director regional de ventas Bajío para Hikvision México

Saúl Daniel Romero Rodríguez, director de operaciones de Seguridad Privada Peninsular

Eduardo Reyes López, gerente de Seguridad Patrimonial en Schneider Electric

# En marcha CIPROCI 2024

· Evento líder en seguridad humana y protección contra incendios en Latinoamérica

**Bogotá, Colombia.-** CIPROCI 2024, organizado por Indean y respaldado por la prestigiosa National Fire Protection Association (NFPA), se consolida como un evento transformador para el sector, extendiéndose a varios países: Brasil, Ecuador, Argentina y Colombia, donde se realizará en Bogotá, los días 11 y 12 de septiembre.

**”Uniendo fuerzas para responder a los desafíos de seguridad en latinoamérica.”**

En su versión en Brasil, realizada el pasado 2 y 3 de julio, los resultados superaron todas las expectativas, demostrando un impacto significativo en actualización, normatividad, exposición y networking para el sector, en donde la normatividad y la innovación en el sector fueron los temas de discución más importantes.

Finalizó con una rueda de negocios que fomentó el networking entre los asistentes, demostrando así que CIPROCI 2024 es la mejor plataforma para exponer y posicionarse en el sector de protección “contra Incendios”.

En su versión en Colombia, contará con la participación de entidades como el Gobierno Nacional, el Ministerio del Interior, la Aeronáutica Civil, la Dirección Nacional de Bomberos y Desastres, junto a gremios de aseguradoras, constructoras, diseñadores y fabricantes; garantizando oportunidades para todos, en el epicentro de un movimiento de seguridad sostenible, que acciona hacia el logro de objetivos de desarrollo sostenible relacionados al sector.

**Patrocinadores Oficiales**

Las ediciones anteriores de CIPROCI han sido un éxito rotundo, con logros como el aumento del 250% de sus empresas patrocinadoras en su última versión. Este año, la participación es aún más diversa, contando con marcas como PAVCO Wavin, Impofer, Bosch, Makei Soluciones, Edwards, Mircom, Halligan, Honeywell, Flowcom Group, ASTRA, Top Fusion, CKC, Zeus do Brasil, STI Firestop, Bermad, RDM, Dinamica, TecnoFluidos, Ruhrpumpen, Skop, Avanti, ACO Brasil, Emmeti, HCT Brasil, Samtech, ABB, Sugan, Green BMS, HPELLET, Tubotecnica, Fischer, Tecnomontagens, Siemens, Temon y Condex. En CIPROCI, su marca promueve la innovación, mientras gana exposición y posicionamiento en el sector.

**Una agenda académica como ninguna otra**

Los espacios académicos de CIPROCI 2024 se dividirán en:

1. Los días 9 y 10 de septiembre podrá llevar su profesión al siguiente nivel, sea una autoridad en el congreso con los certificados precongreso NFPA.
2. Los días 11 y 12 de septiembre se ofrecerá una agenda insuperable de conferencias, que abordará normatividad, experiencias y perspectivas de los expertos sobre las tendencias y soluciones más innovadoras, metodología BIM aplicada a la protección contra incendio y conversatorios con líderes del sector público y privado.

“El tema de incendios es como un seguro de vida, esperamos no necesitarlo, pero al momento que se requiera, es importantísimo tenerlo bien hecho”, comentó Diana Leaño. Grupo Empresarial Hypro SAS.

Para conocer todos los detalles de este gran evento, visite: www.ciproci.com

# CIPROCI

## LATINOAMÉRICA - 2024

## Certifícate presencialmente en NFPA, con nuestros Cursos Pre-Congreso.

## 9 y 10 de Septiembre de 2024.

**Hotel Black Tower Premium. Av. La Esperanza #43a-21.**
**Bogotá, Colombia.**

**Conocer los detalles**

ORGANIZA

Indean

PATROCINADOR OFICIAL

NFPA®

# 203 casos de robo a transporte

## 1er semestre 2024

Pese a las acciones que el gobierno es sus tres niveles emprende para combatir el robo de mercancías en tránsito, el primer semestre cerró con la cifra de 203 hurtos registrados, principalmente en los estados de México, Puebla, Jalisco, Guanajuato, San Luis Potosí, Veracruz, Querétaro e Hidalgo. Del total, 98.5 se recuperó en promedio en los primeros 42 minutos del siniestro, gracias a la plataforma SIAMES C5, la cual es un desarrollo propio de la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital (AMESIS). En junio del presente año, se registraron 48 hurtos vs 64 del mismo periodo de 2023, según datos proporcionados por la organización.

Ricardo Bustamante Medina, presidente de la AMESIS, el robo de mercancías en tránsito no ha disminuido, pues los delitos son cada vez más violentos, donde incluso varios operadores lamentablemente han perdido la vida.

Del total de hurtos en carretera, AMESIS identificó, a través de sus afiliados, que el 48% de los robos es cometido contra tractocamiones y remolques, 15% solo remolques, 13% torton, 5% Ram y el 18% en varios. Del total de los eventos, el 98% corresponde a vehículos de transporte de mercancías y el 2% a particulares.

Ante estos datos, Bustamante Medina, refirió que el robo al transporte de carga en México, AMESIS tiene contabilizado, de acuerdo a las cifras obtenidas a través del SIAMES C5 (Sistema Integrador de Aplicaciones Móviles Especializadas en Seguridad) y su PUC (Punto Único de Contacto), lo que también arroja las zonas de alto riesgo donde se registra el mayor porcentaje de ilícitos. Estado de México ocupa el 34%, Puebla 23%, Jalisco 14%, Guanajuato 10%, San Luis Potosí y Veracruz 6%, Querétaro 4%, Hidalgo 2% y el resto del país con el 1%.

En su mayoría, los robos se cometen en las carreteras México-Querétaro, México-Puebla y México-Pachuca; con el 29%, 15% y 12%, respectivamente, según datos obtenidos de SIAMES, la cual es una herramienta diseñada por la asociación para la atención de eventos de robo desde el PUC en coordinación con las autoridades correspondientes a nivel nacional. Está dirigida a los sectores del autotransporte de carga, particulares y mercancías.

Para la AMESIS y sus asociados, los hurtos registrados en la primera mitad de 2024, ocurrieron a nivel nacional en un horario recurrente entre las 05 y las 09 horas. Se estima que el hurto por jamming fue del 81% debido a que las autoridades no han tomado acciones para aplicar la ley anti Jammer, incluso una medida preventiva para inhibir el uso de jammers sería colocar detectores carreteras de estos equipos, los cuales por el solo hecho de portarlos es delito y detención de las personas portadoras.

Cabe hacer mención que el 25 de enero de 2020 entró en vigor en México la llamada “Ley anti jammer”, reforma a distintos artículos de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR y del Código Penal Federal que tuvieron como finalidad reducir los delitos cometidos con bloqueadores de comunicaciones inalámbricas. Hoy esta ley no se aplica.

Es relevante hacer mención que las cargas de abarrotes ocuparon el 30% de los robos, seguido de acero con el 24%, llantas 20%, materia prima 15%, herramientas 09% y varios 7%. Estas cargas tienen mayor demanda y son fáciles de colocar en el “mercado negro”, según datos recabados entre los miembros de la asociación.

“Cámaras y asociaciones del autotransporte de carga, seguridad y rastreo satelital, así como autoridades federales, coinciden que el delito disminuye apenas un par de dígitos semestrales. En los primeros seis meses del año en curso, ya se han registrado a nivel nacional más de 2 mil robos a vehículos de carga, lo cual se potencia por la poca presencia de la Guardia Nacional para el resguardo de las carreteras del país y los pocos paradores seguros para la pernocta de los operadores”, refiere Ricardo Bustamante Medina, titular de la AMESIS.

# amesis MR

Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital A.C.

## 24/365 DÍAS
Atención personalizada de nuestro centro de monitoreo

## SIAMES C5
Uso exclusivo de la plataforma, para comunicación con las autoridades

## TOTAL ACCESO
Consulta a reportes de estadísticas de robos

- Certificación de Monitoristas
- Comité de Tecnología e Innovación
- Comité de Capacitación y Desarrollo
- Comité de Estadísticas del Sector
- Comité de Relación con Autoridades
- Comité de Relaciones Públicas

## SOCIOS ACTIVOS

Tracking Systems de México S.R. de C.V. · sittel Seguridad Satelital · Holkan Rastreo Satelital · skyguardian · skymeduza · ADS LOGIC Telematics · SECUREWITNESS · INFO TRAX · TECNO LOGISTIK · RAINDE · SEGURIDAD 360 .com · ATLANTIDA · TTC · ISIS Seguridad Integral · GEOTRUCKS · GRUPO ALFIL · SEC Soluciones · GPSMonitor Rastreo Satelital · GRUPO PRYSE · DUMAX Smart Tracking · PROTECZONE P.T. Seguridad Total

## SOCIOS ADHERENTES

GPS TRACKER MX Vamos contigo® · SATECH Rastreo Satelital · TSNVISION Technology of Security Vision · RCU Sistemas · GEOTRACKING Rastreo Satelital · Tecno GPS · MAGNI Tracking


c.administrativa@amesis.org.mx
amesis.org.mx

COMUNÍCATE
55 3334 4707

# La mujer en la industria del blindaje y Norma NMX-R-025-SCFI-2009

• La transformación tecnológica lleva inevitablemente un cambio de estrategia, tanto en términos de modernización de la cadena de producción, como en una mayor especialización profesional.

La llegada de Claudia Sheinbaum a la Presidencia de México es un pequeño, pero importante pago a la deuda histórica que hay con las mujeres mexicanas en la búsqueda de la igualdad de género. Es evidente la capacidad de liderazgo que tienen y una visión mas amplia de como debe estar todo organizado.

En la industria del blindaje, sus responsabilidades abarcan ya prácticamente todas las áreas: dirección comercial, ejecutivas de ventas, administrativas, control de calidad en planta, compras, almacén, hojalatería y pintura, blindaje opaco y transparente etc., la transformación tecnológica lleva inevitablemente un cambio de estrategia, tanto en términos de modernización de la cadena de producción, como en una mayor especialización profesional. Esto favorece la mayor entrada de la mujer a la industria con posibilidades de desarrollo profesional sin límites.

Pero tampoco hay que engañarse, el verdadero desafío no es encontrar talento femenino, eso sabemos que abunda, sino que es encontrar a las empresas con el liderazgo y cultura necesarios para que ese talento florezca. Hay compañías excelentes que no tienen problemas en darle retos y oportunidades por difíciles que sean, independientemente del género, pero aún son pocas. Abundan más las que no están preparadas a los nuevos paradigmas.

En la industria seguimos viendo la incapacidad de eliminar los horarios estrictos a cambio de implementar la productividad por objetivos, se tiende a desconfiar de directivos demasiado jóvenes y no digamos si es mujer, para mantener unos modelos operativos que funcionaban con éxito en el siglo pasado, como el de las reuniones maratónicas y que ahora son obsoletas. Aunque la mujer en el pasado ha ejercido eficientemente profesiones técnicas, había estado en la sombra en las fábricas y no se le daba la importancia necesaria a la capacitación femenina que ahora se ha convertido en prioridad.

En México existe la Norma NMX-R-025-SCFI-2009 que establece los requisitos para la certificación de las prácticas para la igualdad laboral entre hombres y mujeres. Busca igualdad e inclusión laboral, además de consolidar la previsión social, a través de la creación de condiciones de trabajo digno, bien remunerado, con capacitación, con seguridad, libre de discriminación, con corresponsabilidad entre la vida laboral y familiar. Las empresas blindadoras que tengan voluntad de estar a la vanguardia en este ámbito deberán cumplir con los requisitos establecidos en la Norma que están divididos en cinco ejes.

Igualdad y no discriminación: se refiere a la adopción de políticas y acciones para la igualdad y la no discriminación entre mujeres y hombres en las comunicaciones internas y externas de la organización, en el reclutamiento, selección y permanencia en el trabajo, en los salarios, incentivos y compensaciones, y en la promoción vertical y horizontal. Previsión social: verifica que las trabajadoras disfruten, sin ningún tipo de discriminación de las prestaciones y beneficios ofrecidos por la organización. Asimismo,

se refiere a la instrumentación de esquemas y mecanismos que permitan a trabajadoras conciliar la vida familiar y la vida laboral. Clima laboral: comprueba la existencia de prácticas e indicadores parra crear un ambiente de trabajo libre de violencia laboral, cuenta con un instrumento que mide el nivel de satisfacción de las trabajadoras en el espacio laboral. Accesibilidad y ergonomía: se refiere a espacios físicos y mobiliarios adaptados a las necesidades de mujeres embarazadas y personas adultas mayores. Libertad sindical: corrobora el derecho de las trabajadoras para constituir organizaciones sindicales y para afiliarse o no a las existentes sin ningún tipo de discriminación.

Además, la Norma establece tres puntos críticos que invariablemente deben ser cumplidos para poder obtener la certificación; Anuncios de vacantes u ofertas de trabajo expresados en lenguaje no sexista y libres de cualquier expresión discriminatoria. Prohibición explícita de exámenes de no gravidez y de VIH como requisito de contratación. Contar con políticas, programas y mecanismos de prevención, atención y sanción de las prácticas de violencia laboral.

Los indicadores de la Norma inciden directamente en la productividad y competitividad de las empresas al mejorar el clima laboral, obtener el potencial de creatividad de las personas por buen clima laboral. Hacer un buen uso del talento al equilibrar las proporciones de mujeres y hombres en la organización. Se reduce la rotación del personal por mayor sentido de pertenencia.

Hacer uso de la marca Igualdad Laboral entre mujeres y hombres en sus productos, documentos e imagen institucional. El uso de la aporta ventajas comparativas respecto a las empresas que no tienen certificación en la Norma, puesto que la sociedad en general y los clientes identifican el compromiso de la organización con la igualdad laboral. Asimismo, internacionalmente y en diversas licitaciones se valora el que una organización cuente con diversos certificados y distinciones. ¿Tu organización está dispuesta y lista para el cambio?

**Ricardo Guzmán**

Director de operaciones en Vínculo Estrategas Comerciales. Amplia experiencia en el ámbito del blindaje automotriz y colaborador comecial a nivel gerencial y directivo en las más importantes blindadoras de México
rguzman@vinculoec.com.mx
**México**

Articulista Invitado

# Ventajas económicas de la reventa de vehículos blindados

La Asociación Mexicana de Blindadores de Automotores (AMBA), establece que un vehículo blindado por alguna de las 10 empresas socias de este organismo ofrece no sólo una tecnología de última generación y un conocimiento óptimo en su fabricación, sino con ello la posibilidad de una potencial reventa de la unidad en alguna de sus compañías integrantes de dicha asociación en el mercado en general.

Los socios tienen una considerable posibilidad de comprar un vehículo blindado usado, si éste fue protegido balísticamente desde luego por la propia empresa, o bien por alguno de los miembros de la AMBA, debido a la solidez técnica que el organismo exige a sus socios para que puedan formar padre de la misma.

Lo anterior, afirma Esteban Hernández, presidente de AMBA, representa una garantía de que el trabajo hecho en ese automotor tuvo procedimientos adecuados y el ahora vendedor tiene muy probablemente una unidad en buenas condiciones. Esta situación, añadió, es uno de los beneficios que tiene un comprador que adquirió un vehículo con algún socio, además de alguna potencial ventaja en materia legal o judicial.

Las compañías miembros de la asociación aplican un sólido procedimiento para que la postventa del vehículo blindado en materia técnica, tenga un adecuado seguimiento, con mano de obra calificada, que permita un correcto rendimiento de los vehículos que han recibido protección balística.

El seguimiento postventa por parte del blindador es importe, en el que procesos como el cuidado de los materiales balísticos, transmisión, caja automática o suspensión, entre otros, son vitales para que el vehículo tenga durante el mayor tiempo posible un funcionamiento correcto y brinde la seguridad que buscan los compradores.

Los vehículos blindados por compañías de AMBA siempre cuentan con la carta de autentificación y su correspondiente Código QR-holograma expedido por la Dirección General de Seguridad Privada, el cual es un documento imprescindible para la venta de los vehículos blindados usados o de segunda mano.

El presidente de la AMBA manifestó finalmente que el organismo trabaja constantemente para fomentar los mejores procediendo técnicos, administrativos y de servicio en favor de la seguridad, la integridad y la economía de sus clientes.

# Evite que vehículos accedan a su propiedad con solución inteligente

- Dahua lanza la solución de entrada y salida de vehículos operada con inteligencia artificial para PyMEs.

Con una nueva solución integral diseñada y creada específicamente para abordar las necesidades específicas de los escenarios de las PyMEs: la solución de entrada y salida de vehículos con Inteligencia Artificial de Dahua.

La gestión de acceso de vehículos ha sido un desafío frecuente para algunas PYMES, como parques industriales y edificios de oficinas, debido a que los métodos tradicionales no pueden verificar de manera inmediata y efectiva la entrada y salida de vehículos, lo que a menudo genera congestiones y largas filas de autos que afectan negativamente la experiencia de conducción.

Para este tipo de empresas sería desastroso que se produjeran robos o incidentes de seguridad dentro de las instalaciones. Por otra parte, el registro manual en papel añade más carga de trabajo al personal de seguridad, sin mencionar la incapacidad de este método para buscar rápidamente los registros de entrada y salida de los vehículos.

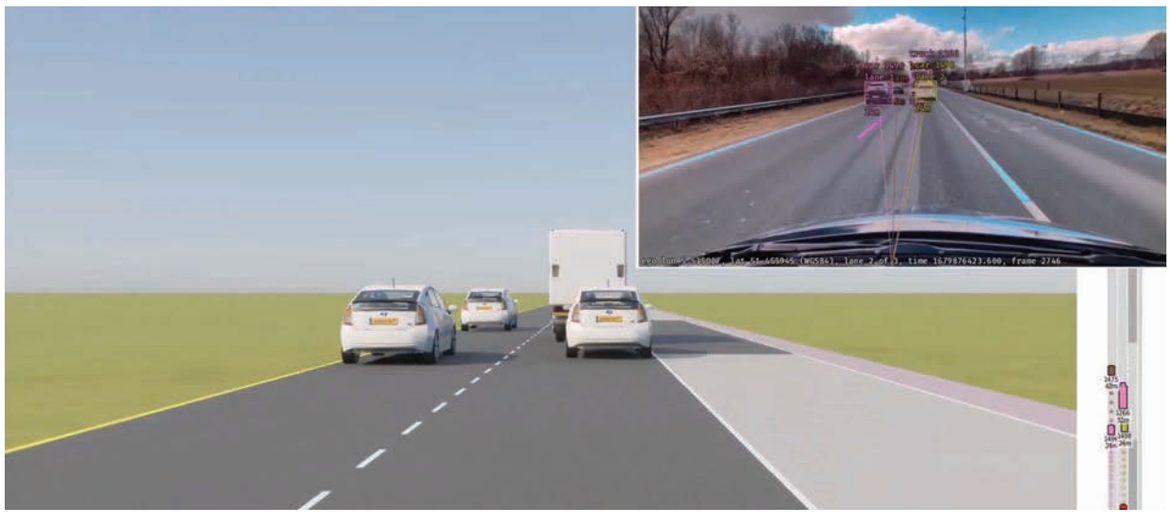
Para solucionar este problema, Dahua Technology, proveedor de servicios y soluciones AIoT centrado en video, desarrolló la solución de entrada y salida de automotores con Inteligencia Artificial. Que permite realizar el acceso automático a los automóviles mediante el reconocimiento automático de matrículas (ANPR), lo que evita que personas ajenas entren en las inmediaciones y otros posibles incidentes de violación de la seguridad. Con funciones de lista blanca y lista negra, el ANPR puede ayudar a evitar la entrada de no autorizados, con una precisión de detección del 98%.

Otro beneficio de esta solución es su sistema sin contacto continuo. Ofrece acceso rápido con manos libres a autos autorizados a través de control de barrera con llave local y/o intercomunicador remoto, aliviando significativamente las congestiones durante las horas pico. En términos de gestión de registros, esta solución permite la verificación y grabación visual, que integra la información de acceso del vehículo con video para un mejor manejo y consulta de los registros.

La solución de entrada y salida de automotores con Inteligencia Artificial de Dahua es, sin duda, una herramienta de acceso a vehículos diseñada con IA que puede mejorar en gran medida la gestión de las PyMEs mediante autenticación inteligente, acceso rápido ininterrumpido y verificación y grabación basadas en video. Ayuda a prevenir incidentes de seguridad como la intrusión o el robo, mejora la experiencia de conducción y permite grabación visual y seguimiento de las unidades. Es ideal para áreas de entrada y salida tanto interiores como exteriores de complejos de apartamentos, hoteles, fábricas, oficinas y otros escenarios de PyMEs.

# La verificación y validación de vehículos autónomos

## exige fusionar el mundo real y virtual



A medida que la industria automovilística avanza hacia el futuro, las empresas se enfrentan al reto de construir vehículos que ofrezcan mayor comodidad, seguridad y conectividad. Se espera que la llegada de los vehículos autónomos y definidos por software (VA/VDS) acentúe esta tendencia y amplíe aún más los límites de la complejidad de los vehículos. Los VA, en particular, requerirán componentes de última generación en múltiples ámbitos, como software, chips semiconductores, sensores y cableado eléctrico, lo que culminará en vehículos más sofisticados nunca antes fabricados.

La complejidad de los vehículos autónomos como sistema de sistemas será sin duda inmensa. Sin embargo, la verificación y validación de la seguridad, fiabilidad y rendimiento de los vehículos autónomos en todos los escenarios de tráfico puede resultar una tarea aún más retadora. Las proyecciones indican que las plataformas de vehículos autónomos tendrán que completar el equivalente a miles de millones de kilómetros de pruebas para garantizar su seguridad y fiabilidad.

Así pues, un reto fundamental para los fabricantes de vehículos autónomos será el desarrollo de métodos de verificación y validación que permitan evaluar rápidamente el rendimiento de estos sofisticados autos en todo tipo de escenarios de tráfico y condiciones climáticas.

Las pruebas en condiciones reales deben complementarse con simulaciones de alta fidelidad que ayuden a los equipos de diseño a recopilar información vital de forma más rápida y rentable. Con un enfoque combinado de pruebas en el mundo real y simulaciones, los equipos de ingeniería en vehículos autónomos pueden identificar casos extremos sobre la marcha y evaluar el comportamiento del unidad en todos los escenarios de conducción de forma más rápida y rentable.

Para llevar a cabo este enfoque combinado real y virtual se necesita una plataforma integrada de desarrollo de VA que pueda probar y volver a probar el funcionamiento del vehículo en escenarios virtuales realistas durante todo el ciclo de vida del diseño. Una plataforma integrada de diseño y simulación de VA permite incorporar los resultados de las pruebas y los datos de simulación al diseño del vehículo, creando un sistema de bucle cerrado que mejora el diseño, el funcionamiento y las características físicas del sistema con datos de alta fidelidad.

Una plataforma de este tipo es posible gracias a un amplio enfoque de digitalización que apoya la creación de un gemelo digital completo del vehículo autónomo, que abarca el diseño, la verificación y validación, la supervisión sobre el terreno y la optimización del hardware, software, producción y ciclo de vida del vehículo.

**La digitalización favorece un enfoque de simulación combinado**

El desarrollo de sistemas avanzados de asistencia al conductor (ADAS, por sus siglas en inglés) y vehículos autónomos es un proceso de ingeniería basado en datos. Se generan, analizan y reincorporan al diseño grandes cantidades de datos en cada paso del ciclo de vida a través del gemelo digital integral. Al traducir los datos en bruto y al transformarlos en conocimientos de ingeniería que impulsan mejoras y optimizaciones se pueden ganar y perder ventajas competitivas.

Todo empieza con la recolección de datos en el mundo real. Normalmente, la cantidad de datos recopilados en una prueba física es inmensa. Las soluciones de recopilación de datos digitalizados incluyen software que puede realizar un análisis inicial de los datos, distinguiendo los datos que son pertinentes para el objetivo de la prueba en cuestión y permitiendo a los equipos tomar decisiones bien informadas sobre el almacenamiento de datos y prioridad de procesamiento.

Los datos capturados se vuelven aún más potentes cuando se convierten al dominio virtual. Los datos de las pruebas reales pueden enriquecer los entornos de los vehículos simulados y la dinámica de conducción, dando lugar a un gemelo digital de mucha mayor fidelidad. Los escenarios capturados durante las pruebas en el mundo real también pueden ser importados y recrearse en una solución de simulación. Una vez en el entorno de simulación, el equipo de ingenieros puede modificar todos los parámetros del escenario, como las condiciones meteorológicas o la velocidad del vehículo, lo que permite a los equipos cuestionar todas las facetas del rendimiento del sistema.

Las simulaciones de alta fidelidad de un gemelo digital completo de un vehículo también presentan el mejor entorno para la identificación de los llamados escenarios “desconocidos-no seguros”. Los equipos de ingenieros pueden utilizar los conocimientos de situaciones reales conocidas en combinación con métodos matemáticos para descubrir escenarios críticos alternativos. Hacerlo en el entorno virtual permite a los equipos descubrir y analizar estos escenarios de forma mucho más eficiente, reduciendo el número de escenarios desconocidos e inseguros y, por tanto, el riesgo en el que se incurre al desplegar sistemas autónomos.

# Seguridad en eventos corporativos empresariales y masivos

Todos los días y cada semana los estadios, eventos y festivales de música concentran en ocasiones decenas de miles de asistentes. Estos eventos multitudinarios son cada vez más frecuentes por lo cual, conlleva una serie de factores de riesgo relacionados con el gran número de asistentes.

En cualquier operativo de seguridad hay dos componentes fundamentales: prevención y anticipación, esto para garantizar la seguridad en grandes terrenos. Es preciso, por tanto, prevenir y anticiparse a los eventuales riesgos mediante la construcción de un plan de seguridad.

Para las características del plan las medidas a diseñar deberán estar basadas en tamaño, tipo y duración del evento, entre otros factores; esto asegura que cada aspecto del plan esté medido y el personal de seguridad pueda reaccionar en tiempo y forma adecuada. Para ello, se deben tomar en cuenta las siguientes condiciones:

1. Evaluación del lugar en el que se va a realizar el evento
2. Estado de sus instalaciones
3. Previsiones meteorológicas.
4. Empleo de barreras y control de accesos
5. Personal de control de accesos
6. Utilización de medios tecnológicos
7. Cámaras de CCTV y detectores de metales
8. Control del aforo
9. Salidas de emergencia
10. Servicio médico
11. Plan de contingencia
12. Plan de evaluación

El objetivo principal de la seguridad en eventos no es responder a las amenazas, sino evitar aquellos problemas que lo produzcan, para ello se debe contar con todas las medidas de seguridad, con el objetivo de la protección en la interacción física de todas las personas que asisten como es el staff, trabajadores, público e involucrados en el evento, de esta manera se podrán evitar riesgos intrínsecos.

Es preciso analizar la proximidad de las zonas de riesgo, las comunicaciones y accesos, para poder disponer de los medios de transporte precisos y, así evitar aglomeraciones, problemas de estacionamiento, entre otros.

Los eventos empresariales y corporativos son aquellos convocados para reunir a las personas relacionadas con una compañía perteneciente al sector económico e incluso áreas afines, a diferencia de simples encuentros sociales. Estos eventos trascienden esa categoría para convertirse en acciones concretas que se integran con la estrategia de marketing de la compañía.

Cuando se trata de eventos empresariales, la creatividad es un aliado clave para diseñar formatos innovadores y efectivos, al que se adapten los objetivos de la empresa sin descartar lo descrito antes sobre las medidas de seguridad que se deben llevar en los principales eventos:

1) Cursos
2) Seminarios
3) Reuniones
4) Ferias y exposiciones
5) Presentación de productos
6) Incentivos para empleados y eventos de fidelización de clientes
7) Eventos de team building para mejorar el trabajo en equipo y tener un mejor impacto social.



**Claudio Oliva López**

DSI.
Cat Security Administration, S.A. de C.V.
rguzman@vinculoec.com.mx
**México**

Articulista Invitado

# AGMEN optimizando la seguridad privada con ChatGPT

- Opción innovadora y versátil que puede transformar significativamente cómo se abordan los desafíos para profesionales del sector.

En el dinámico y exigente campo de la seguridad privada, la tecnología juega un papel crucial en la mejora de eficiencia operativa y efectividad en la gestión de riesgos. En este sentido, la Inteligencia Artificial (IA) se presenta como una aliada poderosa, facilitando tareas que van desde la vigilancia y el análisis de datos, hasta la toma de decisiones estratégicas. Entre estas herramientas emergentes, ChatGPT de OpenAI se destaca como una opción innovadora y versátil que puede transformar significativamente cómo se abordan los desafíos en este sector.

**¿Qué es ChatGPT y cómo puede beneficiar a la seguridad privada?**

Es un modelo de lenguaje desarrollado por OpenAI que utiliza Inteligencia Artificial para comprender y generar texto de manera similar a la de un humano. Su capacidad para procesar grandes cantidades de información, responder preguntas específicas y generar texto coherente lo convierte en una herramienta poderosa para diversos usos en seguridad privada:

1. Análisis de datos y monitoreo: ChatGPT puede analizar grandes volúmenes de datos de manera rápida y efectiva. Esto es crucial para la seguridad privada, donde la recopilación y el análisis de información en tiempo real pueden ayudar a identificar patrones sospechosos, anticipar riesgos y mejorar la respuesta ante incidentes.

2. Asistencia en la toma de decisiones: los profesionales de seguridad privada pueden utilizar ChatGPT para obtener insights rápidos sobre estrategias de seguridad, evaluación de riesgos y protocolos de respuesta. Esto puede incluir recomendaciones sobre la distribución de recursos, medidas preventivas y tácticas de intervención.

3. Capacitación y educación: ChatGPT puede servir como una herramienta de capacitación interactiva para nuevos empleados en seguridad privada. Puede responder preguntas comunes, proporcionar información sobre procedimientos estándar y simular escenarios para entrenamiento práctico.

4. Comunicación mejorada: Facilita la comunicación interna y externa al proporcionar respuestas rápidas y precisas a consultas y solicitudes de información por parte de clientes, empleados y otros interesados en seguridad privada.

**Implementación práctica de ChatGPT en la seguridad privada**

Para aprovechar al máximo ChatGPT en el ámbito de la seguridad privada, es importante considerar lo siguiente:

- Entrenamiento específico: Personalizar el modelo mediante entrenamiento con datos específicos del sector de seguridad para mejorar su capacidad de respuesta y relevancia en contextos particulares.

- Integración con sistemas existentes: Integrar ChatGPT con otros sistemas de monitoreo, análisis de video, gestión de incidentes y plataformas de comunicación para maximizar su utilidad y efectividad operativa.

- Seguridad y Privacidad: Mantener altos estándares de seguridad y privacidad de los datos al utilizar ChatGPT, asegurando que la información confidencial esté protegida en todo momento.

En resumen, ChatGPT representa una innovación significativa en la seguridad privada, ofreciendo capacidades avanzadas de análisis de datos, toma de decisiones y comunicación que pueden mejorar eficiencia y efectividad en todas las facetas de esta industria. Adoptar esta tecnología no solo puede optimizar las operaciones diarias, sino también fortalecer las estrategias de seguridad y protección en un mundo cada vez más complejo y dinámico. Con la aplicación adecuada y una integración cuidadosa, ChatGPT tiene el potencial de elevar los estándares de seguridad privada hacia nuevos niveles de excelencia.

Articulo creado por la IA (CHAT GPT), con instrucciones y conocimientos especializados en sistemas de control de seguridad y calidad.

**Julio Márquez Recillas**
Quality Manager, AGMEN Seguridad Privada.
**México**
Articulista invitado

# Identifique y combata el crimen organizado en el comercio minorista

Una nueva y desafiante realidad enfrenta la industria minorista: el crimen organizado en el comercio minorista (ORC, por sus siglas en inglés). Este tipo de delito, que involucra el robo a gran escala de mercancías por parte de grupos criminales, ha experimentado un aumento significativo en los últimos años, generando pérdidas millonarias para las empresas.

**¿Qué es el ORC?**

Se define como el robo a gran escala de productos minoristas por parte de grupos criminales sofisticados que buscan revenderlos para obtener ganancias. Estos grupos emplean diversas tácticas, desde el robo en tiendas hasta el hurto de carga en tránsito, y a menudo recurren a la violencia e intimidación para lograr sus objetivos.

**Impacto significativo en la economía**

En 2022, el ORC generó pérdidas por más de 100 mil millones de dólares sólo en Estados Unidos. Este tipo de delito no sólo afecta a las grandes cadenas comerciales, sino también a pequeños negocios y emprendedores.

En México, de acuerdo con la Coparmex, uno de cada dos negocios en el país ha sufrido algún tipo de delito y de cada 10 robos a negocios, sólo dos se denuncian (78%). Asimismo, de acuerdo con una encuesta elaborada por la empresa Alto, el robo con violencia a negocios minoristas aumentó 40% en México durante 2022, y según señala la ANTAD, los supermercados y tiendas especializadas pierden más de 13 mil millones de pesos al año por este tipo de delito.

**¿Cómo protegerse del ORC?**

Existen diversas medidas que las empresas pueden tomar para protegerse:

- Capacitar a los empleados para que puedan identificar comportamientos sospechosos y reportarlos a las autoridades.
- Mantenerse actualizado sobre las últimas tendencias del ORC y las nuevas tácticas utilizadas por los grupos criminales.
- Apoyar iniciativas para combatir el ORC, como la Ley de Lucha contra la Delincuencia Organizada en el Comercio Minorista de 2023.
- Establecer relaciones estrechas con las agencias policiales locales para facilitar la respuesta ante un incidente.
- Implementar tecnología de seguridad para proteger la carga en tránsito, como sellos inteligentes y sistemas de monitoreo.

**Aliado en la lucha contra el ORC**

La empresa mundial en gestión de riesgos de la cadena de suministro, Overhaul ofrece soluciones tecnológicas innovadoras para ayudar a las empresas a prevenir el ORC. Su plataforma proporciona visibilidad en tiempo real sobre la ubicación y el estado de la carga en tránsito, lo que permite detectar y prevenir robos de manera oportuna. Además, su equipo de expertos está altamente capacitado para asesorar a las empresas en la implementación de estrategias efectivas para combatir el crimen organizado en el comercio minorista.

**Llamado a la acción**

De acuerdo con la empresa de gestión de software, el ORC es una amenaza que afecta a toda la industria minorista. Es fundamental que las empresas, las autoridades y la comunidad en general se unan para combatir este tipo de delito. Solo mediante un esfuerzo conjunto puede protegerse el sector y garantizar un crecimiento próspero.

# Expertos en **soluciones menos lesivas**

APRINSA

**100 Aprinsa**

**200 Aprinsa**

## Modelos: 100 y 200

Equipo de control electronico inteligente

Estan preparadas para detener actividades violentas e ilegales de individuos, mientras no causa efectos mortales al sospechoso. Ideal para ser usado en recorridos de vigilancia en las calles y estaciones de tráfico, hospitales, cortes de justicia, prisiones, etc.

- **Seguro de usar:** Tecnología probada durante décadas sin efectos mortales
- **Rapido de usar:** Efectivamente controla al sospechoso inmediatamente
- **Fácil de usar:** Paraliza al sospechoso por contacto o a distancia al apretar el gatillo, apuntando el láser
- **Listo para usar:** Precio razonable

@seguridad1 33 3700 7721

**direccion@aprinsa.net**

Miguel Caballero confirma lanzamiento en México de su nueva placa de blindaje para chalecos ORION IV, certificada por la NIJ (Instituto Nacional de Justicia) de EEUU.

# Lanzamiento en México de nueva placa de blindaje para chalecos ORION IV

La compañía global en el diseño y fabricación de prendas de protección balística, Miguel Caballero confirmó la presentación de sus más recientes lanzamientos en Expo Seguridad 2024, la principal exposición del sector en México, y una de las más relevantes a nivel internacional. Dentro de los productos que llevará al mercado mexicano la multinacional, se destaca la placa ORION Nivel IV que obtuvo, recientemente, la certificación del Instituto Nacional de Justicia de los Estados Unidos (NIJ), lo que valida la calidad y altos estándares que ha destacado a la empresa a lo largo de su historia.

El fundador y CEO de la compañía, Miguel Caballero, expresó: “Participar en las principales exposiciones de la industria de la seguridad y la defensa alrededor del mundo ha sido clave para llevar nuestra calidad certificada a diferentes mercados. Expo Seguridad es para nosotros un escenario estratégico que nos permite presentar las novedades que traemos al país como la nueva placa Orion IV, entre otros lanzamientos que reflejan nuestra promesa de innovar para salvar vidas y garantizar el confort de nuestros usuarios”.

Además de la placa ORION IV, la marca presentó otras innovaciones en Expo Seguridad, incluyendo la Tank Top Confort, que ofrece protección balística de niveles II y IIIA con un peso de solo 1.2 kilogramos, y el ION Armor, un chaleco exterior futurista que redefine protección y comodidad.

Con más de tres décadas de experiencia en el sector, Miguel Caballero continúa liderando el mercado Sde protección personal conprendas que no solo cumplen con los más altos estándares de seguridad, sino que también responden a las necesidades de diseño y comodidad de sus usuarios.

Miguel Caballero
CEO de Miguel Caballero

GRUPO ALEM

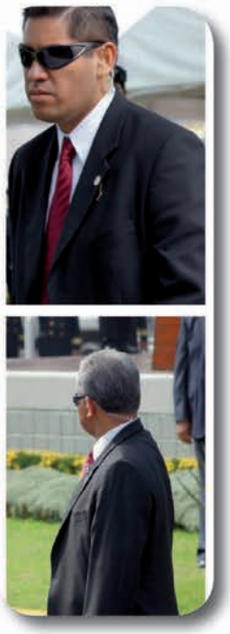
Seguridad Privada Integral S.A. de C.V.

# ¡Garantizamos su tranquilidad!

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

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

**Custodias:** Para todo tipo de transporte de mercancías en tránsito



**Rastreo satelital:** Vehículos particulares, carga o flotillas

**Videovigilancia:** Fija, móvil y remota

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

## www.grupoalem.mx

edgar.seguridad.integral@gmail.com

***+52 564705 2246***

# Creció la adquisición de productos blindados por tema electoral: CNB

- La renta de camionetas blindadas tuvo un incremento del 42%.
- Chalecos y chamarras, fue parte fundamental de las campañas de precandidatos y candidatas.

En medio de uno de los procesos electorales considerado como el más violento del país, el Consejo Nacional de la Industria Balística dio a conocer que candidatos y precandidatos de al menos 22 estados se acercaron a adquirir o rentar productos blindados para reforzar su seguridad.

De acuerdo con datos de la organización Data Cívica, en lo que va del 2024 han sido asesinadas 19 personas precandidatas y candidatas, además se han registrado otro tipo de ataques contra los aspirantes a algún cargo de elección popular como amenazas (14), ataques armados (5), atentados (8) y secuestros (9).

"Para los candidatos, el tema del blindaje fue algo crucial, los números nos dan cuenta de que fue la campaña más violenta que ha tenido México hasta ahora. Hemos visto algunos candidatos usando protección personal y no habló solo de autos blindados, sino de ropa como chalecos y chamarras, fue parte fundamental de las campañas", expresa Gadi Mokotov, presidente de la Comisión Ejecutiva del CNB.

Bajo este panorama, el Consejo asesoró a candidatos, equipos y personal de Secretarías de Seguridad y de casi todos los partidos políticos de 22 estados, entre ellos, Estado de México, Guerrero, Guanajuato, Jalisco, Michoacán, Nuevo León, Puebla y Veracruz.

"Las peticiones de autos, ropa y hasta cuartos blindados está muy ligado a la inseguridad que vive el país, vemos hoy que tanto para los candidatos como para las personas el blindaje ya no es un lujo, es una necesidad para salvar sus vidas y continuar con su trabajo y así la atención a la ciudadanía", agrega Daniel Portugal, vocero del CNB.

Ambos expertos coincidieron en que desde que iniciaron las campañas, se incrementó mes con mes la adquisición de vehículos y ropa blindada, pero no sólo autos nuevos, sino seminuevos. Pero la renta de camionetas SUV tuvo el alza más considerable, ya que en relación con el año anterior creció 42%.

El incremento en la renta, a decir de los expertos, es normal porque muchos candidatos no hacen una inversión tan fuerte, ya que saben solo es para campaña y en caso de que ganen, puede tener una asignada por el gobierno.

Para asegurar la protección, los candidatos deben considerar que el nivel de blindaje debe ser más alto, es decir, deben asegurar que los autos en los que se trasladen tengan niveles de blindaje contra atentados y en cuanto a la ropa tienen que usar chalecos, chamarras, chalecos ejecutivos y otros aditamentos dependiendo del escenario en el que se encuentren.

Otra recomendación de los expertos es la construcción de cuartos de pánico o de seguridad que son habitaciones blindadas que cuentan con sistemas de comunicación con las autoridades y en caso de ser necesario agua, alimentos y oxígeno que les permiten resguardarse de atentados, esto porque justo en el recientre proceso electoral se observo que la delincuencia atacó las casas de candidatos y las oficinas de campaña como en el caso de Morelos.

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

# EXPO SEGURIDAD & TELECOM CENTRO AMERICA

Con la experiencia y éxito de SEGURIEXPO ECUADOR, llega a Guatemala la feria internacional de tecnología en Seguridad y Telecomunicaciones más importante de Centro América.

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

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

Seguriexpo Centroamerica Guatemala 2025 es ideal para:

- Potenciar el proceso de ventas e introducir nuevos productos.
- 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

www.exposeguridadcentroamerica.com

Prensa asociada: MÁS SEGURIDAD Magazine · GLOBAL DEFENSE MAGAZINE

# La inseguridad jurídica en América Latina

• La justicia...aquel principio moral que inclina a obrar y juzgar respetando la verdad y dando a cada uno lo que le corresponde.

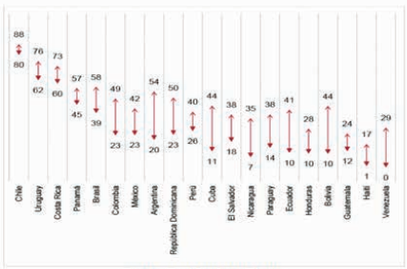
**Quito, Ecuador.**- América Latina, sin lugar a dudas sigue siendo una región rica en cultura, historia y diversidad, sin embargo, también enfrenta desafíos significativos en el ámbito jurídico. La inseguridad en esta área, caracterizada por la falta de confianza en las instituciones legales e incertidumbre en la aplicación de la ley, afecta a la sociedad, economía y estabilidad política.

Es así que las violaciones sistemáticas de la legislación y su desequilibrio, han llevado a América Latina a liderar las reclamaciones ante el Centro Internacional de Arreglo de Diferencias Relativas a Inversiones (CIADI), por parte de inversores extranjeros de los sectores como minería, gas, electricidad, transporte y banca, los cuales concentran la inversión extranjera directa (IED) en la región.

Uno de los referentes y constante evaluador, el Banco Mundial, a través de ciertos indicadores generados en este contexto, muestran que Chile, Uruguay y Costa Rica están entre los países con mayor respeto al Estado de Derecho, mientras que Bolivia, Guatemala, Haití y Venezuela tienen puntuaciones más bajas. Brasil, Colombia, México, Argentina y Perú ocupan posiciones previsibles. La variación en algunos países sugiere procesos alternantes de mejora y empeoramiento regulatorio.

Coparticipa de igual manera la inseguridad, el crimen organizado y el narcotráfico, constituyéndose en los riesgos claves en América Latina.

*Figura 1 Seguridad Jurídica en América Latina: Rango del indicador Rule of Law Banco Mundial*




Fuente: Real Instituto Elcano

Es innegable que la principal causa, es la corrupción que mina la confianza en el sistema legal. Generando una falta de transparencia y ese sinsabor a impunidad, que debilita las instituciones legales y erosiona la credibilidad. (Calduch, 2000).

Otro factor que también se asocia a este problema, es la existencia de normativa compleja y ambigua, la cual a través de leyes y regulaciones a menudo confusas, contradictorias, direccionadas, sesgadas o mal aplicadas, dificulta que los ciudadanos y las empresas comprendan de manera clara y precisa el verdadero alcance de estas reglas, limitando sus derechos y obligaciones.

La inestabilidad política es también otra más de las causas, las cuales a través de los cambios frecuentes en la administración gubernamental llegan afectar la continuidad de la legislación, generando incertidumbre en la aplicación de la ley.

Diremos que las consecuencias que acarrea este grave problema son:

- La desinversión y estancamiento económico, lo que genera una falta de confianza en el sistema legal disuadiendo al potencial inversor, afectando la creación de empleo y la innovación.
- Los litigios prolongados, que a través de procesos lentos y costosos perjudican a las partes involucradas creando incertidumbre sobre los resultados de estas disputas.
- La irremediable vulnerabilidad y afectación de los Derechos Humanos, por su falta de acceso a la justicia y generación de impunidad que socava la protección de los ciudadanos.

Se torna por ello imperioso fortalecer las instituciones judiciales y combatir la corrupción, simplificando la normativa y dar claridad en la aplicación de la ley, así como promover la comprensión de los derechos y deberes legales entre la población lo que contribuirá a una mayor confianza en el sistema, de igual forma compartir buenas prácticas y aprender de las experiencias para mejorar su sistema legal.

En conclusión, la inseguridad jurídica es un obstáculo que América Latina debe superar para lograr un desarrollo sostenible y una sociedad justa. La colaboración entre gobiernos, sociedad civil y sector privado es clave para construir un entorno legal más confiable y equitativo.

**Referencias:**

- Calduch Cervera, R. (2000). "Causas y consecuencias de la inseguridad jurídica en América Latina." Fundación para la Investigación Estratégica (FIE). http://www.fundacionfie.org/uploads/3/1/2/0/31207787/1-_rafael_calduch.pdf
- Causas y Consecuencias de la Inseguridad Jurídica en América Latina. http://www.fundacionfie.org/uploads/3/1/2/0/31207787/1-_rafael_calduch.pdf.
- América Latina y la seguridad jurídica - Real Instituto Elcano. https://www.realinstitutoelcano.org/comentarios/america-latina-y-la-seguridad-juridica/.
- Una epidemia en movimiento: El cambiante panorama de la seguridad. https://www.undp.org/es/latin-america/blog/una-epidemia-en-movimiento-el-cambiante-panorama-de-la-seguridad-ciudadana-en-america-latina-y-el-caribe.
- La inseguridad en América Latina y Caribe - El Orden Mundial. https://elordenmundial.com/mapas-y-graficos/la-inseguridad-en-america-latina/.

**Edison Cadena Ayala**

MSC, CPO, CPOI, CSSM
gerente de la empresa
SEINNATIONAL CIA. LTDA.
Ecuador
rguzman@vinculoec.com.mx
**Ecuador**

Articulista Invitado

# SEGURIDADEXPO®
by Fisa | CHILE

## 25-27 SEPT. 2024
## METROPOLITAN SANTIAGO

# SEGURIDADEXPO: INNOVACIÓN SIN LÍMITES PARA UNA PROTECCIÓN PERSONALIZADA

*¡Visita nuestro sitio web!*

*¡Hablemos! Y agenda una reunión con nosotros*

info@seguridadexpo.cl

+56 9 4481 6922

PATROCINAN

Gobierno de Chile · Ministerio de Hacienda · AMUCH Asociación de Municipalidades de Chile · ANAPCI Asociación Nacional de Protección contra Incendio - Chile · aseva · Bomberos Chile · Cámara Chileno Británica de Comercio · Apesa Chile · conecta logística · InvestChile

GL events

@seguridadexpo

METROPOLITAN SANTIAGO

www.seguridadexpo.cl

ORGANIZA Y PRODUCE

Fisa GL events Group

CO-ORGANIZA

Carabineros de Chile

# Riesgos y amenazas a seguridad y defensa en América Latina

Si bien existen desafíos importantes, también hay oportunidades para construir un futuro más seguro, próspero y pacífico para todos los ciudadanos de la región.

**Buenos Aires, Argentina.-** América Latina, es una región vibrante y diversa, se enfrenta a un panorama complejo en materia de seguridad y defensa. Si bien los desafíos tradicionales como la delincuencia organizada y el tráfico de drogas persisten, nuevos desafíos han surgido en los últimos años, poniendo a prueba la capacidad de los Estados para garantizar la seguridad de sus ciudadanos.

En este análisis, exploraremos en forma sintética los principales riesgos y amenazas que aquejan a la región, tomando en cuenta datos y perspectivas relevantes, e intentando dar respuestas predictivas, nos adentraremos en los oasis de Siwa para exponer posibles escenarios futuros.

**Principales amenazas:**

- **Crimen Organizado Transnacional (COT):** El COT, incluyendo narcotráfico, pandillas y trata de personas, sigue siendo una de las principales amenazas en la región. Los grupos criminales se han vuelto más sofisticados y violentos, infiltrando instituciones y corrompiendo funcionarios públicos. Según la ONU, América Latina concentra el 31% de los homicidios relacionados con el crimen organizado a nivel mundial, conllevando a impacto en la seguridad cuyo resultados son la generación de violencia, inestabilidad y limites el desarrollo económico. Además de debilitar las instituciones democráticas y erosionar la confianza pública.

- **Violencia social:** La alta tasa de homicidios, desigualdad y exclusión social alimentan la violencia social en muchos países de la región. Esta violencia se manifiesta en disturbios civiles, pandillas y feminicidios. Según el Banco Mundial, América Latina tiene la tasa de homicidios más alta del mundo, con 20.1 homicidios por cada 100,000 habitantes. Generando altas tasas de percepción de inseguridad (consolidando una cultura del miedo), obstaculizando el desarrollo humano y el bienestar de las comunidades.

- **Ciberseguridad:** Los ciberataques se han convertido en una amenaza cada vez más grave para los gobiernos, empresas y ciudadanos de la región. Estos ataques pueden obtener de forma ilegal información confidencial, interrumpir servicios esenciales y causar daños económicos significativos. Un ejemplo reciente: en 2021, un ciberataque al Banco Central de Costa Rica provocó la suspensión de sus operaciones durante varios días. Es decir, pueden dañar la infraestructura crítica, el sistema financiero y la privacidad de los ciudadanos.

- **Cambio climático:** Los efectos del cambio climático, como sequías, inundaciones y desastres naturales, exacerban las vulnerabilidades existentes y generan nuevos riesgos para la seguridad. Estos eventos pueden provocar desplazamientos masivos, conflictos por recursos y tensiones geopolíticas. Se estima que para el 2050, hasta 25 millones de personas en América Latina podrían ser desplazadas por el cambio climático, aunado a que afecta la seguridad alimentaria, el acceso a agua potable y la estabilidad regional.

- **Terrorismo:** Si bien la amenaza del terrorismo, en su convergencia con grupos relacionados al narcotráfico, no ha sido priorizado en América Latina por los gobiernos, como en otras regiones, algunos grupos extremistas y células han realizado ataques en los últimos años. La proliferación de armas y la inestabilidad en algunos países podrían aumentar el riesgo de futuros ataques.

Tomando en cuenta las tendencias actuales y los desafíos emergentes, es posible vislumbrar algunos escenarios futuros

para la seguridad y defensa en América Latina:

**Escenario 1 Mayor inestabilidad y violencia:**

- Aumento de la actividad del crimen organizado y la violencia social, impulsados por la pobreza, la desigualdad y la falta de oportunidades.
- Debilitamiento de las instituciones democráticas y el Estado de Derecho, lo que genera mayor impunidad y corrupción.
- Crecimiento de grupos extremistas y células terroristas, aprovechando la inestabilidad social y la proliferación de armas.
- Mayor riesgo de desastres naturales y conflictos por recursos, exacerbados por el cambio climático.

**Escenario 2 Cooperación regional y fortalecimiento institucional:**

- Mayor cooperación regional e internacional para combatir el crimen organizado, el terrorismo y otras amenazas transfronterizas.
- Fortalecimiento de las instituciones democráticas, el Estado de Derecho y la lucha contra la corrupción.
- Inversión en educación, salud y oportunidades económicas para reducir la desigualdad y prevenir la violencia social.
- Desarrollo de capacidades en ciberseguridad y gestión de riesgos para enfrentar las nuevas amenazas.
- Implementación de políticas públicas para la adaptación al cambio climático y la prevención de desastres naturales.

**Escenario 3 un futuro más seguro y próspero:**

- Reducción significativa de violencia y criminalidad, gracias a la cooperación regional y el fortalecimiento institucional.
- Instituciones democráticas sólidas y transparentes, con un Estado de Derecho efectivo y combate efectivo a la corrupción.
- Sociedades más justas e inclusivas, con menores niveles de desigualdad y pobreza.
- Mayor resiliencia ante las nuevas amenazas, como la ciberseguridad y el cambio climático.
- Una región más integrada y próspera, con mayor cooperación y desarrollo sostenible.

El futuro de la seguridad y defensa en América Latina dependerá en gran medida de las acciones que se tomen en el presente. Si bien existen desafíos importantes, también hay oportunidades para construir un futuro más seguro, próspero y pacífico para todos los ciudadanos de la región. Un enfoque integrado e integral que combine medidas de seguridad, desarrollo social y cooperación regional será fundamental para alcanzar este objetivo.

**Llamado a la acción:**

**Gobiernos:** fortalecer las instituciones democráticas, combatir la corrupción, invertir en seguridad y desarrollo social, y promover la cooperación regional.

**Sociedad civil:** participar activamente en la construcción de paz, exigir transparencia y rendición de cuentas, apoyar iniciativas para la inclusión y el desarrollo sostenible.

**Comunidad internacional:** apoyar los esfuerzos de la región para fortalecer la seguridad y defensa, promover el diálogo y la cooperación, y respetar la soberanía e independencia de los países.

Juntos, podemos construir un futuro mejor para América Latina, donde la seguridad, la justicia y el bienestar sean una realidad para todos.

**Edgardo C. Glavinich**

Secretario Nacional.Consejo Argentino para la Seguridad Integrada – CAPSI –
Miembro permanente Global Initiative Against Transnational Organized Crime
**Argentina**

Articulista Invitado

# XIII EXHIBICIÓN Y CONGRESO INTERNACIONAL NAVAL Y MARÍTIMO PARA LATINOAMÉRICA.

EXPO 2024 NAVAL®

**Somos el centro de negocios para las industrias de defensa, construcción naval y de seguridad en Latinoamérica.**

**Participa del principal encuentro profesional del sector, la vitrina perfecta para mostrar tus nuevos desarrollos tecnológicos e innovaciones.**

## [ CONGRESO INTERNACIONAL ]

**Los desafíos para la industria de defensa en el nuevo orden internacional.**

| [ 14.500 ] | [ +88 ] | [+7.000 ] | [ +35 ] | [ +500 ] |
|---|---|---|---|---|
| M² de superficie | Empresas Expositoras | Visitas Profesionales | Países Participantes | Reuniones de Negocios |

*¡Contáctanos!* info@exponaval.cl +56 9 4481 6922

ORGANIZA Y PRODUCE Fisa

PARTNER OFICIAL TECNOLÓGICO option

INVITA SAAB

AUSPICIA PuertoValparaíso CRECIENDO JUNTOS

PATROCINAN Gobierno de Chile · Ministerio de Hacienda · Ministerio de Defensa Nacional

# 17° CONGRESO INTERNACIONAL DE CENTROS DE ATENCIÓN DE EMERGENCIAS

## 23 AL 25 DE OCTUBRE DE 2024

**HOTEL PARADISUS. CANCÚN, MÉX.**

NENA THE 9-1-1 ASSOCIATION MEXICO

**REGISTRATE**

PARADISUS
Cancun • Mexico

nena_911mx | Nena 9-1-1 Mx | www.911latinoamerica.org | Nena 9-1-1 México

>

# Una nueva serie de lectores murales con teclado Design XS: mayor seguridad y comodidad

**Diseñado para establecer nuevos estándares en el control de acceso inteligente. Con autenticación multifactor y la opción de acceso mediante código PIN, este lector mural proporciona doble autenticación y modos de apertura mejorados que aumentan significativamente la seguridad.**

**www.saltosystems.com**

salto
INSPIRED ACCESS