

MÁS SEGURIDAD

Magazine

Revolución tecnológica para seguridad urbana

Edición 156 | Año 18 | junio 2025



México y Latam / precio \$60.00MX



Construyendo ciudades más seguras

Hikvision aprovecha los **dispositivos IoT**, los **análisis de IA** y las **plataformas digitales** para ayudar a los administradores de las ciudades a contar con **soluciones más eficientes**.



Avanzando en la Industria

Somos el fabricante de productos de seguridad más grande del mundo



Innovación tecnológica

Productos y soluciones innovadoras para satisfacer las diversas necesidades de los clientes



Capacidad de producción

Sistema de fabricación automatizado líder en la industria y con entrega flexible



Gestión de calidad

Sistema integral de control de calidad, que cubre todo el ciclo de vida del producto



Liderazgo en ciberseguridad

Proceso seguro por diseño y una amplia gama de certificaciones de primer nivel



Ecosistema de socios

Amplio ecosistema de socios en toda la industria y alrededor del mundo



@HikvisionMx
www.hikvision.com/mx
sales.mexico@hikvision.com

Para más información visita nuestra web o escríbenos a:
sales.mexico@hikvision.com

En el camino de la innovación

tecnológica empresarial

La Inteligencia Artificial nos ha sumergido en herramientas revolucionarias capaz de transformar diversos sectores empresariales.

Hoy día, durante el desarrollo de soluciones tecnológicas, es indispensable que la seguridad esté integrada desde el inicio, en cada línea de código, decisión arquitectónica y proceso de entrega.

Sin embargo, una nueva fuerza está impulsando esta evolución hacia un nivel superior: la Inteligencia Artificial (IA). Gracias a su capacidad para automatizar tareas complejas, detectar amenazas en tiempo real y anticiparse a vulnerabilidades antes de que se materialicen, la IA está redefiniendo las reglas del juego en el ámbito de la ciberseguridad. La IA no solo optimiza los procesos, sino que representa un verdadero cambio de paradigma en la forma en que las organizaciones diseñan, construyen y protegen su software.

En un mundo donde la digitalización avanza a pasos agigantados, las empresas enfrentan nuevos desafíos para mantener la continuidad operativa, la protección de su información y la eficiencia en su comunicación. Por ello las empresas que más rápido adopten tecnologías de ciberseguridad, nube y comunicaciones están un paso adelante en la competitividad del mercado, hoy la Inteligencia Artificial vive en nuestras decisiones cotidianas.

Por otro lado, la Inteligencia Artificial Generativa (IAG) ha emergido como una herramienta revolucionaria capaz de transformar diversos sectores empresariales. Sin embargo, esta no se ha explotado al máximo por diversas causas, como la preocupación de que la automatización sustituya empleos, o la duda al manejo de datos sensibles, así como el temor a una excesiva dependencia tecnológica.

Con el paso del tiempo y una mayor capacitación hemos comenzado a comprender que su utilización nos trae más que ventajas en la innovación continua, personalización de los servicios, lo que deriva en un incremento de la productividad.

Tema en boga es el desarrollo de líderes ejecutivo en la era digital, una forma de adaptabilidad y toma de decisiones basada en datos. Actualmente este liderazgo ha evolucionado drásticamente en las últimas décadas debido al avance de la tecnología y la globalización. Hoy estos ejecutivos deben adoptar herramientas digitales y metodologías basadas en datos para mejorar la eficiencia y la toma de decisiones; en donde adaptan a la era digital con énfasis en la toma de decisiones basada en datos y el uso estratégico de la Inteligencia Artificial (IA).

Uno de los principales retos del liderazgo moderno es la capacidad de adaptación a cambios constantes. La velocidad con la que se actualizan los mercados y la tecnología, requiere que los ejecutivos desarrollen una mentalidad flexible y proactiva. No olvidemos que la IA ha revolucionado la gestión empresarial al proporcionar análisis predictivo, automatización de tareas y personalización de estrategias.

El liderazgo en la era digital requiere un enfoque basado en la adaptabilidad, el análisis de datos y el uso estratégico de la Inteligencia Artificial. Los ejecutivos que integran estas herramientas en su gestión no solo mejoran la eficiencia de sus organizaciones, sino que también fortalecen su capacidad para innovar y responder a los desafíos del mercado. La transformación digital no es una opción, sino una necesidad para quienes buscan liderar con éxito en un entorno competitivo y en constante evolución.

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
DESARROLLO VISUAL Y DISEÑO

TERESA RAMÍREZ OJEDA
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

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

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

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@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
- MasSeguridadMagazine
- revmasseguridad
- Revista Más Seguridad
- Revista Más Seguridad

Revista Más Seguridad Año 16, No 156, junio 2025, Publicación mensual de **Grupo Editorial MS Global S. de R.L. de C.V.**, con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 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.

Cintia Gutiérrez



Cuenta con la Diplomatura en estrategias de ciberseguridad e inteligencia de ciberdelitos, Ciberseguridad, en la Universidad del Norte de Santo Tomé de Aquino, San Miguel de Tucumán. Tramo Pedagógico, UFASTA, Buenos Aires Diplomatura en Dirección ejecutiva de Seguridad, Seguridad UMSA, Buenos Aires. Diplomatura en Robótica, Tecnología, Massachusetts Institute of Technology, Massachusetts. Diplomatura en enseñanza con TICs, University of Cambridge, UK. Licenciatura en Sistemas, Universidad De Belgrano, Buenos Aires.

Actualmente ejerce el voluntariado en ASIS International Argentina, y es Presidenta del Board. Es gerente operativo en seguridad física en Securion S.A.

• Escucha •



NUESTRO
PODCAST

a través de Spotify



MÁS SEGURIDAD

Magazine

Sumario

6

Transformando la seguridad urbana con tecnología inteligente



8 Presenta Ajax Systems IndoorCam

11

Scati resguarda legado del faraón



14 Seguridad industrial en México

14 Ciberseguridad, guerra que no se ve

22

Revolución tecnológica en la seguridad ciudadana



34

En seguridad ISIS es la solución



39 Expo Seguridad Guatemala

46 Fuerza Gremial ASOSEC



Solución web para
buscar y encontrar
personas en
vigilancia y
seguridad privada



Inicialmente en
Colombia 🇨🇴

www.aquitoi.com.co

empresas@aquitoi.com

Whatsapp
+57 3138450831

O escanea el siguiente
código QR:



¡Aquitoi, el lugar donde
podrás encontrar!

Tour Internacional 2025

MÁS SEGURIDAD

Magazine



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

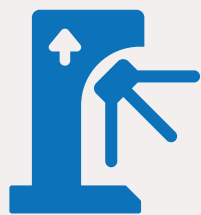


ASOCIACIÓN
LATINOAMERICANA
DE SEGURIDAD

Es tu hora de pertenecer a la comunidad de
protagonistas de la seguridad en Latinoamérica

28 AÑOS
CONECTANDO
profesionales y compañías

TENEMOS
**COMITÉS
NACIONALES**
EN 9 PAÍSES



18 **CURSOS**
ALAS
Cursos Online/InCompany
(a la medida)



REUNIMOS
Fabricantes
Distribuidores
Representantes
de Fábricas
Integradores
Profesionales
Consultores
Gobierno
Usuarios Finales

+765 ²⁹ PAÍSES
SOCIOS EN



51% de nuestros socios son
Usuarios Finales de Seguridad / Gobiernos

Nuestros **SOCIOS CORPORATIVOS**
son las empresas líderes en el mercado mundial

**SOMOS
EXPERTOS**



EVENTOS
El 100% de nuestros
asistentes
recomendarían
nuestros eventos
a un colega



**MARKETING Y
COMUNICACIONES**
Contamos con una
base de 112K
contactos



**NETWORKING Y
NEGOCIOS**
Propiciamos espacios
ideales para el
relacionamiento de
profesionales



CURSOS
12K graduados
en nuestras
certificaciones
internacionales



MANUELA RIVERA
Coordinadora de Membresías
WhatsApp: +57 321 6195464



Transformando la seguridad urbana con tecnología inteligente

Garantizar un entorno seguro y tranquilo es una condición fundamental para el desarrollo sostenible de las ciudades. A medida que aumenta la densidad urbana, también crecen los desafíos en materia de seguridad, lo que exige soluciones tecnológicas más avanzadas para proteger tanto a personas como a los bienes.



El crimen en América Latina continúa en niveles epidémicos. Aunque anteriormente se concentraba en América Central, en los últimos años ha cambiado su epicentro hacia América del Sur y el Caribe. Ante este panorama, los formuladores de políticas públicas en la región han comenzado a reconocer el valor de la tecnología y la innovación como herramientas clave para mejorar la seguridad y optimizar la gestión urbana.

Tradicionalmente, la seguridad urbana dependía únicamente del trabajo humano: cuerpos policiales y vigilancia privada. Sin embargo, con la incorporación de tecnologías de videovigilancia, las ciudades han comenzado a adoptar métodos más eficientes para supervisar sus espacios públicos. Incluso un sistema básico de video seguridad puede hoy facilitar una respuesta más rápida ante incidentes y apoyar de manera significativa las labores de investigación.

Este avance representa solo el inicio de un camino hacia una gestión urbana más inteligente. La evolución hacia ciudades seguras no se limita a la adopción de herramientas digitales, sino que implica una transformación integral basada en el análisis de datos, la automatización y la toma de decisiones informada. Los aprendizajes obtenidos en este proceso, abren la puerta a nuevas aplicaciones que permiten a las ciudades adaptarse y mejorar de forma continua.

Al utilizar soluciones tecnológicas para una asignación más eficiente de recursos y contar con datos precisos en tiempo real, las ciudades inteligentes pueden ofrecer una administración más informada, proactiva y eficiente.

Tecnología inteligente para ciudades más seguras y resilientes

En un entorno urbano en constante transformación, la seguridad ciudadana y la resiliencia urbana requieren un enfoque integral, que combine planificación, innovación tecnológica y sostenibilidad. La adopción de soluciones inteligentes no solo mejora la eficiencia en la vigilancia y gestión del espacio público, sino que también sienta las bases para una mejor calidad de vida en las ciudades.

Bajo el concepto de Smart City, Hikvision ha desarrollado soluciones avanzadas capaces de enfrentar los retos de los núcleos urbanos densamente poblados, como la contaminación, congestión vehicular, dificultades de acceso y desafíos en movilidad y seguridad.

Una de sus principales herramientas es la solución de tráfico inteligente, basada en tecnología de Deep Learning. Este sistema permite una video detección avanzada de vehículos a través de una arquitectura sencilla, de fácil instalación, escalable y con un bajo costo de inversión y mantenimiento. Frente a los sistemas tradicionales, esta tecnología convierte las cámaras de videovigilancia en sensores de alta precisión, capaces de detectar y reconocer vehículos incluso en flujo libre y a altas velocidades.

Los sistemas de tráfico inteligente de Hikvision permiten una monitorización y gestión integral del tránsito urbano e interurbano. Entre sus funcionalidades destacan el reconocimiento automático de matrículas (ANPR), la detección de mercancías, la medición de velocidad, la clasificación del vehículo y la identificación de características como fabricante o color.

La arquitectura del sistema ANPR de Hikvision es flexible y escalable. Las cámaras ANPR distribuidas en las vialidades (Front-End) se encargan de detectar los vehículos y extraer sus parámetros clave. En la parte central del sistema, los grabadores de tráfico (NVR o servidores) pueden instalarse localmente en centros de control, almacenando videos, imágenes y metadatos relevantes. Finalmente, Hik-Central, como plataforma de gestión, permite controlar todos los dispositivos conectados, realizar búsquedas inteligentes, generar reportes y exportar información útil para la toma de decisiones.

Cabe resaltar que la solución de tráfico inteligente de Hikvision permite obtener datos clave sobre el flujo vehicular y las infracciones, lo que facilita una gestión más eficiente del tránsito. Sus cámaras cuentan con sensores GMOS de alta resolución que capturan imágenes precisas incluso a altas velocidades y en condiciones adversas. Incorporan analítica de video embebida y están diseñadas específicamente para detectar y clasificar vehículos en tiempo real. Además, su plataforma abierta permite integrar aplicaciones desarrolladas por terceros, adaptándose a proyectos con necesidades particulares.

Con estas soluciones, Hikvision contribuye a que las ciudades no solo sean más seguras, sino también más eficientes, sostenibles, conectadas y preparadas para los desafíos del futuro.



• Aprovecha la innovación para impulsar la transición hacia un futuro más ecológico, contribuyendo a la lucha contra el cambio climático y atendiendo la creciente demanda de un desarrollo responsable con el medio ambiente.

Obtiene **HIKVISION®** medalla de Plata de EcoVadis

Hikvision recibió la Medalla de Plata de EcoVadis, prestigioso reconocimiento de la plataforma de calificación de sostenibilidad de renombre mundial. Este premio destaca el compromiso continuo de la compañía con prácticas comerciales responsables y su importante contribución a la promoción de un futuro más sostenible, guiado por su filosofía de “Tecnología para un mundo mejor”, marcando un hito clave en la trayectoria global de la compañía hacia la sostenibilidad.

EcoVadis, el proveedor de calificaciones de sostenibilidad corporativa más grande y confiable del mundo, evalúa a las empresas en cuatro áreas críticas: Medioambiente, Derechos Humanos y Laborales, Ética y Compras Sostenibles, al medir las prácticas de sostenibilidad de más de 150 mil empresas en más de 185 países, considerando sus políticas, acciones y resultados.

“Nos enorgullece enormemente que, tras más de 20 años de dedicación, no solo hayamos logrado un crecimiento sostenible para nuestra empresa, sino que también hayamos contribuido significativamente al desarrollo sostenible global”, declaró Huang Fanghong, vicepresidente Senior y Director de cumplimiento de Hikvision. “El reconocimiento de EcoVadis demuestra el progreso que hemos logrado gracias al trabajo y a las sólidas alianzas en toda la cadena de valor y el sector. Pone de relieve nuestro progreso hacia una gobernanza más sólida, prácticas más eficaces y un desempeño de sostenibilidad de gran impacto en todo el mundo. Nos comprometemos a continuar este camino, esforzándonos por cumplir nuestra misión de convertirnos en una empresa responsable”.

Innovando para un futuro más verde

La firma aprovecha la innovación para impulsar la transición hacia un futuro más ecológico, contribuyendo a la lucha contra el cambio climático y atendiendo la creciente demanda de un desarrollo responsable con el medio ambiente. En octubre de 2024, Hikvision se convirtió en la primera empresa del sector de las pantallas LED en recibir la certificación Green Product Mark de TÜV Rheinland.

Esta certificación subraya el cumplimiento de la empresa con los más altos estándares medioambientales, que abarcan áreas como el cumplimiento técnico, el control de sustancias restringidas, la reducción de la huella de carbono y la reciclabilidad.

Impulsando la responsabilidad social en las empresas

En materia de derechos humanos y ética empresarial, la empresa y todos sus empleados cumplen estrictamente el Código de Ética y Conducta Empresarial y la Política Global de Derechos Humanos de la organización. Estos lineamientos garantizan un trato digno y respetuoso para cada persona, a la vez que fomentan un entorno empresarial ético que promueve la integridad, la responsabilidad y la transparencia. Además, la firma extiende su compromiso participando activamente en iniciativas sociales. Desde 2020, ha llevado a cabo el Programa STAR para el Bien Social a nivel global, colaborando con más de 30 ONG y utilizando su tecnología para generar un impacto positivo en el medio ambiente, la fauna y las comunidades locales.

Colaborar con socios para una cadena de valor resiliente

La firma valora profundamente los esfuerzos colectivos para promover la sostenibilidad, como lo reflejan sus exhaustivos requisitos y evaluaciones del desempeño de sostenibilidad de los proveedores para cumplir con altos estándares ambientales y éticos. También utiliza sus tecnologías innovadoras para impulsar una cadena de valor más resiliente, apoyando el crecimiento sostenible de sus socios, tanto en las fases iniciales como finales, creando valor a largo plazo en diversas industrias.

Este último logro refuerza el compromiso continuo de la compañía con el avance de la sostenibilidad y subraya aún más la dedicación de la empresa con los Diez Principios del Pacto Mundial de las Naciones Unidas (UNGC), luego de su participación en 2024. En el futuro, Hikvision seguirá enfocada en crear un impacto positivo duradero mientras impulsa un futuro más innovador y sostenible. 

Lanza Ajax Systems

la IndoorCam



• Cámara de seguridad Wi-Fi con detector de movimiento PIR.

La empresa ha presentado la IndoorCam. Diseñada para hogares, pequeñas oficinas y pequeñas y medianas empresas, combina la flexibilidad Wi-Fi con los estándares de seguridad profesionales de Ajax. Con un canal de comunicación de reserva a través del protocolo de radio Jeweller, IA integrada y transmisión de datos encriptada, la IndoorCam garantiza una monitorización fiable.

Videovigilancia inteligente con IA integrada

Equipado con una cámara de 4 MP, HDR e iluminación IR de hasta 8m, el dispositivo garantiza una calidad de imagen rica en detalles tanto de día como de noche. El sensor PIR detecta el movimiento a una distancia de hasta 4m, mientras que la IA integrada reconoce personas, mascotas o vehículos. La cámara también cuenta con un micrófono de alta sensibilidad y un altavoz de calidad superior para la comunicación bidireccional con supresión de ruido y cancelación de eco siempre activas, que garantizan un audio de alta calidad.

Enfoque centrado en la privacidad

La Ajax IndoorCam ofrece conectividad estable, privacidad e integración perfecta en el sistema de seguridad. La cámara está diseñada con la privacidad y la seguridad en su esencia. Todos los datos del sistema se almacenan de forma segura en la Unión Europea, garantizando el cumplimiento de las estrictas normas de protección de datos de la UE. Las grabaciones de video se encriptan durante el almacenamiento y la transmisión, lo que impide el acceso no autorizado o la violación de datos.

La IndoorCam garantiza una sólida protección de la privacidad de los usuarios finales. Una vez instalado el sistema, solo el usuario final tiene el control: sin vulnerabilidades de seguridad ni acceso oculto. A través de la pestaña Privacidad de la app Ajax, los usuarios pueden gestionar los permisos para las transmisiones en directo y las grabaciones, concediendo o revocando el acceso en cualquier momento. Solo las personas autorizadas, designadas por el administrador del sistema, pueden ver los datos visuales.

Opciones avanzadas de gestión y almacenamiento de vídeo

Las secuencias de vídeo son tan valiosas como la capacidad de acceder a ellas y analizarlas eficazmente. Con el Ajax NVR, Ajax Cloud Storage y una navegación optimizada por el repositorio¹, la IndoorCam garantiza una gestión de vídeo sin esfuerzo, ya sea para la monitorización en directo o la revisión de eventos pasados. JetSparrow, un protocolo patentado de transmisión de vídeo diseñado para el acceso instantáneo a flujos en directo y archivos de vídeo, ofrece una carga de alta velocidad, garantizando que los vídeos en directo se inicien instantáneamente y una navegación fluida por el repositorio sin retrasos.

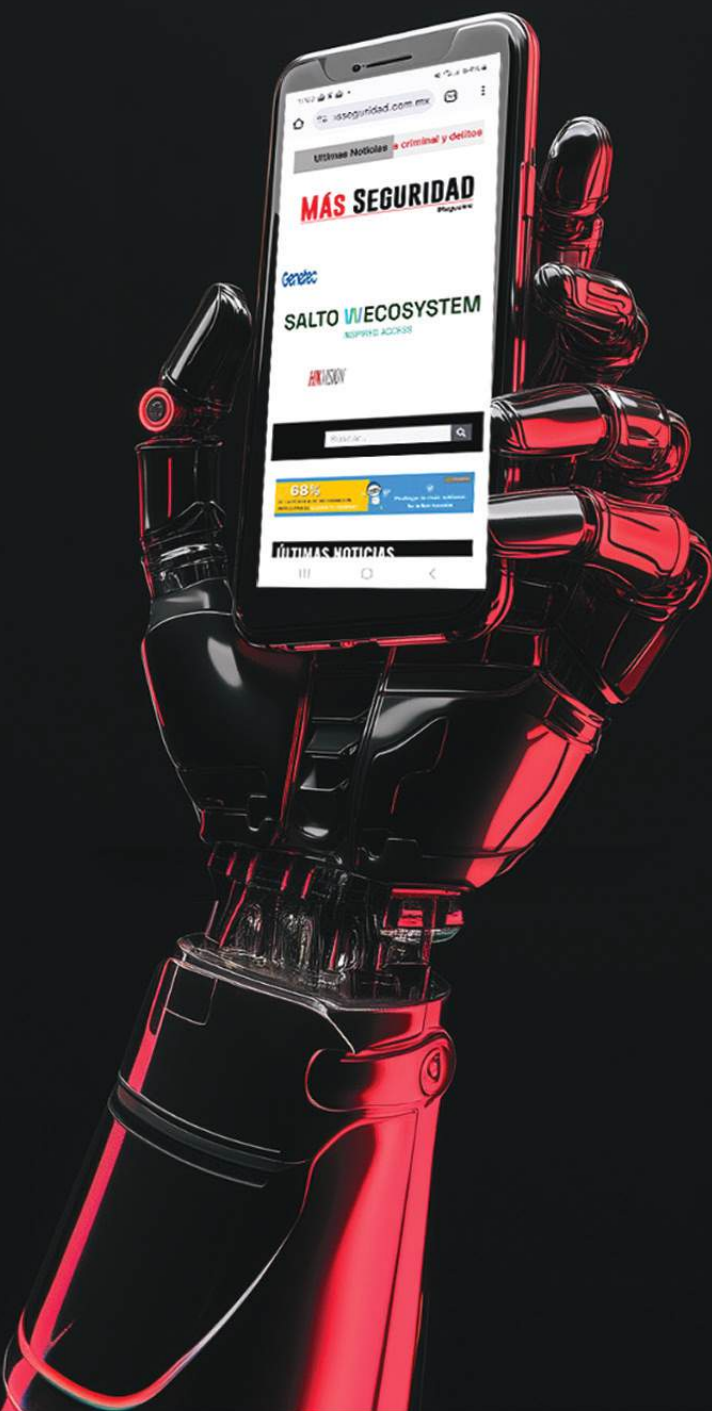
Fiabilidad de la comunicación

Para obtener la máxima fiabilidad, la IndoorCam puede conectarse a un hub Ajax, lo que proporciona un canal de reserva adicional que aumenta la estabilidad general del sistema. Con un alcance Wi-Fi de hasta 500m en línea de visión, la IndoorCam mantiene una conexión estable. Si se pierde la conexión Wi-Fi, la cámara sigue transmitiendo eventos, alarmas y fotos mediante los protocolos de radio seguros y patentados Ajax: Jeweller y Wings. Con un alcance de comunicación de hasta 1.700 metros con un hub, la IndoorCam permanece conectada incluso en grandes espacios.

Al igual que otros productos Ajax, la IndoorCam se integra fácilmente en el sistema de seguridad Ajax. Todo el proceso de integración se realiza sin esfuerzo y en menos de 10 minutos. La vinculación con el sistema de seguridad se realiza en segundos mediante el escaneo de un código QR. Una vez conectada, la configuración de la cámara se puede gestionar mediante las apps Ajax de escritorio y móviles, y la protección contra intrusiones se puede aumentar mediante la sincronización con los detectores Ajax. Al configurar escenarios de vídeo: cuando se activan determinados detectores Ajax, la cámara empieza a grabar automáticamente, proporcionando una verificación visual inmediata de la alarma. 

MÁS SEGURIDAD

Magazine



SÍGUENOS

 Revista Más Seguridad

 @revmasseguridad

 MasSeguridadMagazine

 revmasseguridad

 Revista Más Seguridad

 Revista Más Seguridad

AJAX

DOMINA TU ESPACIO

Todo integrado en un solo sistema.



NDA A
COMPLIANT



www.ajax.systems



DE VERDAD ESTÁS LISTO PARA

EL FUTURO

Contacta a Vigitrón
para tus soluciones
de red en seguridad.



Para más información

Contacte a: Andrés Mosqueda
Representante de Ventas para
América Latina
Cell: 55.2344.9847
Email: amosqueda@vigitrón.com
Sitio web:



es tecnología robusta para la videovigilancia inteligente en México

- Irrompe en nuestro país con soluciones IP para videovigilancia de alta demanda energética.
- La marca ofrece switches PoE con garantía de por vida y soporte técnico especializado.
- Su tecnología permite modernizar sistemas sin recablear, incluso sobre coaxial o par de conductores.

La tecnología de videovigilancia se ha vuelto una herramienta indispensable para industrias, gobiernos y ciudades. En ese interesante escenario, la empresa estadounidense Vigitrón ha iniciado un proceso de expansión en México y América Latina, de la mano de Andrés Mosqueda, gerente de ventas regional, quien desde septiembre del año pasado encabeza la estrategia de introducción en mercados que aún desconocen el alcance de esta marca nacida en San Diego, California.

La compañía cuenta con una trayectoria de 28 años desarrollando soluciones de transmisión de datos y energía, enfocadas en sistemas de seguridad electrónica. Su origen se remonta a la fabricación de transeptores de video para CCTV analógico. Hoy, su portafolio está enfocado completamente en sistemas IP y tecnologías que permiten cubrir largas distancias, resistir ambientes adversos y alimentar cámaras de alta demanda energética.

Mosqueda explica que el portafolio incluye switches PoE capaces de alimentar dispositivos de hasta 90 watts por puerto, extensores Ethernet que aprovechan cable coaxial o incluso dos conductores, y convertidores de medios para redes de fibra óptica. Muchos de estos equipos han sido diseñados pensando en instalaciones complejas, como las que se encuentran en postes urbanos conectados a centros C5. Lo distintivo, afirma, es que todo esto se ofrece bajo una política de garantía de por vida, algo inusual en el mercado.

La integración con fabricantes de cámaras IP como Axis o Hanwha forma parte del enfoque comercial de la marca. La lógica es sencilla: las cámaras requieren conectarse a switches que garanticen estabilidad y alto rendimiento. En ese punto entra la tecnología desarrollada por Vigitrón, capaz de manejar grandes volúmenes de datos de video sin comprometer la red. Andrés Mosqueda destaca que los switches son Jumbo Frame, es decir, aptos para paquetes de video de alta resolución, y que además ofrecen soluciones listas para entornos industriales switch de planta externa” (o “switch OSP” para “Outside Plant”).

Desde el inicio de su operación regional, el ejecutivo ha enfocado sus esfuerzos en dar a conocer la marca. A falta de una estrategia segmentada por industrias, ha optado por una presencia directa con integradores y usuarios finales. A través de visitas técnicas, diseño de proyectos, asesoría especializada y préstamo de equipos para pruebas de concepto, ha

logrado introducir el producto en sectores como la industria automotriz, manufactura y gubernamental.

Durante los últimos meses, el equipo ha sido sometido a condiciones reales por diversos fabricantes e integradores. Las pruebas han dado resultados positivos, según cuenta Mosqueda: “Muchos me dicen que no sabían que este tipo de soluciones existían, y que ahora les resuelve problemas concretos en campo”.

La fábrica en San Diego no solo responde a las necesidades del mercado, también actúa con agilidad. En siete meses, ha desarrollado al menos cuatro nuevos productos, varios de ellos surgidos a partir de requerimientos específicos. Esta capacidad de respuesta le ha permitido a la marca adaptarse a una industria que exige flexibilidad, eficiencia energética y compatibilidad con entornos preexistentes.

El mercado mexicano representa actualmente el 70% del esfuerzo regional. A la fecha, existen alrededor de 10 casos de éxito en el país, algunos aún no publicables, pero que han servido para abrir puertas y generar interés. La marca comienza a ser reconocida no solo por su tecnología, sino también por ser Altamente Confiable por su Garantía de Por Vida y el acompañamiento técnico y el compromiso con cada proyecto.

Vigitrón no solo pone hardware en el mercado, apuesta por formar alianzas técnicas que faciliten la transición de entornos analógicos a sistemas IP de alto rendimiento. La videovigilancia exige más que nunca confiabilidad y potencia; la empresa avanza como una alternativa cada vez más valorada.

¿Por qué elegir Vigitrón?

La empresa que respalda su producto es tan importante como el producto mismo.



Andrés Mosqueda, gerente de
ventas regional



SCATI resguarda el legado del faraón Keops en el Gran Museo Egipcio

Innovación, precisión y respeto por el patrimonio; bajo esa premisa, SCATI ha sido elegida para desplegar su tecnología de videoseguridad en uno de los espacios más simbólicos del mundo: el recinto que alberga el Solar Boat de Keops, una de las embarcaciones más antiguas de la humanidad, con más de 4,500 años de historia.

Ubicada ahora en el Gran Museo Egipcio (GEM), en El Cairo, esta pieza arqueológica única requería un sistema de protección que ofreciera vigilancia permanente sin alterar su entorno museográfico ni interferir con la experiencia de los visitantes. La firma SCATI respondió con una solución a la altura del reto.

El proyecto contempló la instalación de un sistema de cámaras como mini PTZ, discretas y de alta precisión, capaces de ofrecer seguimiento motorizado con visión 4K e infrarroja. Estas se integraron perfectamente a la arquitectura, sin cables visibles ni elementos intrusivos.

Además, se implementaron videograbadores inteligentes y una plataforma de gestión centralizada SCATI VISION, lo que permite supervisar en tiempo real cualquier anomalía desde el centro de control del museo.

Gracias a la analítica embebida en cada dispositivo, es posible detectar movimientos inusuales, accesos no autorizados o patrones de merodeo, activando alertas inmediatas que garantizan una respuesta eficaz y oportuna.

El caso del Solar Boat refleja el compromiso de SCATI con la preservación del patrimonio cultural global, combinando experiencia, precisión tecnológica y sensibilidad arquitectónica. La firma demuestra con creces su liderazgo en seguridad para entornos de alto valor histórico, con soluciones que fusionan Inteligencia Artificial, diseño y control sin comprometer la estética ni la funcionalidad de los espacios más exigentes.



SSOC: SCATI SECURITY & OPERATIONS CENTER



- CCTV
- ACCESOS
- INTRUSIÓN
- PERIMETRAL
- HVAC
- AUDIO IP
- INCENDIOS
- BMS
- OTROS

Presenta Ajax Systems SIM

para transmisión fiable de alarmas



- Tarjeta SIM optimizada para IoT y diseñada para la comunicación entre máquinas.
- Cada SIM está vinculada a su hub designado, lo que impide el uso no autorizado y garantiza que todos los datos transmitidos se procesen de forma segura a través de Ajax Cloud.

La empresa ha anunciado el lanzamiento del servicio Ajax SIM, una solución diseñada para proporcionar una comunicación ininterrumpida entre los sistemas de seguridad y las centrales receptoras de alarmas.

Ajax SIM es una tarjeta SIM optimizada para IoT y diseñada para la comunicación entre máquinas. Preinstalada en los hubs Ajax, se conecta automáticamente a la red más potente disponible en las bandas 2G, 3G y LTE, proporcionando un funcionamiento continuo incluso en zonas con cobertura débil o fluctuante. A diferencia de las tarjetas SIM estándar, que a menudo requieren configuración y activación manual, Ajax SIM está lista para utilizar desde el momento en que el sistema se conecta a la alimentación, lo que aumenta la fiabilidad y la facilidad de uso.

Para los usuarios finales, esto se traduce en una transmisión ininterrumpida de alarmas y eventos, garantizando que las señales críticas lleguen a las centrales receptoras de alarmas sin demora. Para los profesionales de la seguridad, Ajax SIM simplifica el proceso de instalación y ofrece una valiosa oportunidad de ingresos recurrentes.

Cada SIM está vinculada a su hub designado, lo que impide el uso no autorizado y garantiza que todos los datos transmitidos se procesen de forma

segura a través de Ajax Cloud. Estas salvaguardias proporcionan a los usuarios finales la confianza de que su sistema de seguridad está protegido contra interferencias o violaciones en todo momento. Al dar prioridad a la privacidad del usuario, Ajax SIM solo recopila los datos esenciales, como los identificadores de la SIM y del hub, sin almacenar información personal ni realizar un seguimiento de los datos.

Diseñada para aplicaciones de seguridad profesionales, la Ajax SIM ya está disponible en Norteamérica y pronto se expandirá a Benelux, Francia, Italia, DACH, Iberia, LATAM, los países bálticos, Europa del Este, el sudeste de Europa, Ucrania y los países nórdicos, entre otros. A medida que la conectividad móvil se convierte en un estándar mundial, Ajax SIM garantiza que cada sistema suministrado esté listo para funcionar desde el primer día.

El servicio también se introducirá en África (Sudáfrica, Senegal, Costa de Marfil, Mauricio y Kenia), ASEAN (Vietnam, Tailandia y Singapur), Oceanía (Australia y Nueva Zelanda) y MENA (Arabia Saudí). Con esta amplia disponibilidad, Ajax SIM es una solución global diseñada para satisfacer las necesidades de los profesionales de la seguridad y de los usuarios finales de todo el mundo. 

Sensor Acústico Distribuido por Fibra Óptica de Largo Alcance



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

Serie EP9000

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





Seguridad industrial en México, entre la urgencia normativa y el potencial transformador

- México registra más de 500 mil accidentes laborales al año, con un costo estimado de más de 5 mil millones de pesos para el IMSS.
- La industria manufacturera concentra el 90% de los siniestros; el sector automotriz, uno de los más afectados.
- “Cada vez más empresas entienden que la seguridad no solo protege vidas, sino que mejora la eficiencia y reduce pérdidas”: Timothy Castillejos.

A decir de los especialistas, nuestro país reporta más de mil accidentes laborales a diario y se acumulan 14.9 millones de días subsidiados por incapacidad al año; la seguridad industrial ha dejado de ser un “extra” para convertirse en una necesidad estratégica, como lo afirma Timothy Castillejos, gerente técnico-comercial nacional de Euchner México y miembro activo en los comités de la Asociación Internacional de Automatización, quien ha dedicado más de una década a impulsar estándares de protección en maquinaria y procesos industriales.

“Antes, la seguridad era lo último que se analizaba en un proyecto de automatización. Hoy, cada vez más empresas preguntan: ¿cómo hago mi máquina segura? ¿Cómo cuido a mi gente y mis procesos?”

Castillejos subraya que, aunque existe un interés creciente del empresariado por implementar medidas de seguridad, aún persisten grandes retos estructurales: desinformación, poca capacitación, desconocimiento normativo y decisiones basadas más en costos que en eficiencia a largo plazo.



De acuerdo con datos proporcionados por el experto, México enfrenta anualmente entre 450 mil y 500 mil accidentes de trabajo reportados al IMSS, sin contar los que nunca se documentan. Además, alrededor de 250 muertes al año se registran en centros laborales, de acuerdo con el INEGI.

El costo económico es enorme: más de 5,370 millones de pesos anuales en subsidios por incapacidad y pérdidas millonarias por paro de máquinas, fluctuación de personal, multas e ineficiencia operativa:



“Una máquina parada por 10 minutos puede costar millones. Lo han entendido: tener procesos seguros también impacta las utilidades”.

La Secretaría del Trabajo (STPS) y el IMSS son los dos principales órganos reguladores en materia de seguridad industrial. Mientras el IMSS absorbe los costos hospitalarios y determina el pago de primas de riesgo, la STPS supervisa el cumplimiento de 45 Normas Oficiales Mexicanas (NOM) auditables. Cada omisión detectada puede traducirse en sanciones económicas, e incluso la clausura de maquinaria o líneas completas.

“Hay casos donde las multas han alcanzado los 12 millones de pesos por fallas en máquinas”, alerta Castillejos.

Una empresa que incurre en repetidos accidentes no solo enfrenta costos elevados, también pierde competitividad frente a otros mercados: “Los países que lideran en industria, como Alemania o Brasil, ya actualizaron sus marcos normativos. México ha comenzado ese proceso con la NOM-017 y la NOM-004, pero aún queda mucho por avanzar”.

La clave: capacitación e innovación tecnológica

En comparación con otros países latinoamericanos, México se encuentra en una posición intermedia. Aunque aún por detrás de referentes como Alemania o Estados Unidos, ha comenzado a actualizar sus marcos legales y técnicas de control: “Los países que hoy avanzan —como Brasil, Chile o Colombia— entendieron que invertir en seguridad también es ganar eficiencia. En México, debemos continuar ese camino con decisión”, concluye Castillejos.



Timothy Castillejos, gerente técnico-comercial nacional de Euchner México



Expo Seguridad Industrial anunció el lanzamiento de Safety & Fire Conference, programa de conferencias de alto nivel que se llevará a cabo del 24 al 26 de junio de 2025 en el marco de la edición número 17.

Respaldo por la Universidad Internacional del Conocimiento e Investigación (UNICI), institución especializada en programas educativos de protección civil y seguridad laboral, este evento busca elevar la profesionalización en la industria con contenidos especializados y actualizaciones clave en normativas y protocolos de seguridad.

Durante tres días, Safety & Fire Conference ofrecerá un programa dividido en tres ejes temáticos: Fuego, Normas y Protección Civil, proporcionando a los asistentes información relevante y de vanguardia en materia de seguridad.

Los participantes no solo tendrán acceso a ponencias de alto nivel, sino que también recibirán una certificación avalada por UNICI, lo que refuerza el valor educativo y profesional del evento. Además, este nuevo formato representa una evolución del tradicional programa de conferencias de Expo Seguridad Industrial, fortaleciendo el contenido y garantizando una experiencia enriquecedora para el crecimiento de los profesionales del sector.

El evento cuenta con el apoyo de instituciones educativas y asociaciones líderes en la prevención de riesgos y seguridad laboral como NFPA, IIAR, Prevencionar, IPAF, entre otras; consolidándose como una plataforma clave para la actualización y el networking dentro de la industria.

Entre los ponentes destacados que formarán parte del programa se encuentran:

- Jaime Gutiérrez, coordinador de Fomento Económico y Competitividad del Estado de México, experto en desarrollo económico y políticas públicas, quien presentará la conferencia Inversión Segura: Prevención de Incendios como Pilar del Desarrollo Económico, en la que abordará cómo la seguridad

- La evolución del conocimiento en seguridad y protección contra incendios.
- Safety & Fire Conference se celebrará dentro de la Expo Seguridad Industrial del 24 al 26 de junio de 2025 con conferencias especializadas en fuego, normas de seguridad industrial, seguridad en el trabajo y Protección Civil, avaladas por UNICI.

contra incendios es un factor clave para la competitividad y el crecimiento empresarial en el país.

- Cecilia Acosta, directora general México de Seguridad y Bienestar Laboral, reconocida especialista en seguridad laboral, quien impartirá Mapeo de Riesgos Bajo la Metodología de la OIT SAFE WORK. Su ponencia proporcionará herramientas clave para la gestión de riesgos en el ámbito laboral, basadas en estándares internacionales.
- Israel Carrillo, director del CRESTCAP de la OOAD Regional Estado de México Poniente del IMSS, experto en capacitación y gestión de riesgos laborales, quien impartirá una conferencia sobre riesgos de trabajo. En su ponencia, abordará estrategias para la prevención y mitigación de accidentes en el entorno laboral, con un enfoque en la normatividad vigente y las mejores prácticas en seguridad ocupacional.



Uso de la IA: retos y perspectivas para la seguridad

• La IA representa una herramienta poderosa en los procesos de ciberseguridad y ciberdefensa, capaz de detectar amenazas emergentes y proteger activos digitales con una eficacia sin precedentes

tamaños adoptan herramientas basadas en IA para identificar vulnerabilidades, responder a incidentes y mitigar ataques en tiempo real (CISA, 2022).

• Riesgos asociados al uso de IA

El uso de IA en ciberseguridad no está exento de riesgos. Uno de los principales es la opacidad de los algoritmos, lo que puede derivar en decisiones automáticas injustas o discriminatorias. Además, la dependencia excesiva de la IA puede generar una falsa sensación de seguridad. El NIST (2024) advierte sobre los sesgos algorítmicos, mientras que la UNESCO (2021) enfatiza la necesidad de marcos éticos que orienten su desarrollo y aplicación.

• El uso de la IA en grupos criminales

No sólo los gobiernos y las empresas disponen de IA. También grupos criminales y actores estatales maliciosos están utilizando IA para potenciar sus actividades. Según informes de la OEA (2023) y del INCIBE (2022), los cibercriminales emplean IA para automatizar ataques de phishing, evadir sistemas de detección, generar contenido malicioso y realizar deepfakes. Este acceso democratizado

Articlista Invitado

Dr. Gustavo Guzmán Hernández

Académico y experto de Ciberseguridad en Latam, /PN/ITESM/Ciberlac/Coladca Internacional México

En los últimos años, la Inteligencia Artificial (IA) ha emergido como una de las tecnologías más transformadoras de la era digital, impactando profundamente sectores como salud, educación, industria y, de manera particular, la ciberseguridad y la ciberdefensa. Este avance ha generado nuevas oportunidades para la protección de infraestructuras críticas y la detección de amenazas, pero también ha abierto la puerta a una serie de riesgos éticos, sociales y técnicos que exigen una profunda reflexión.

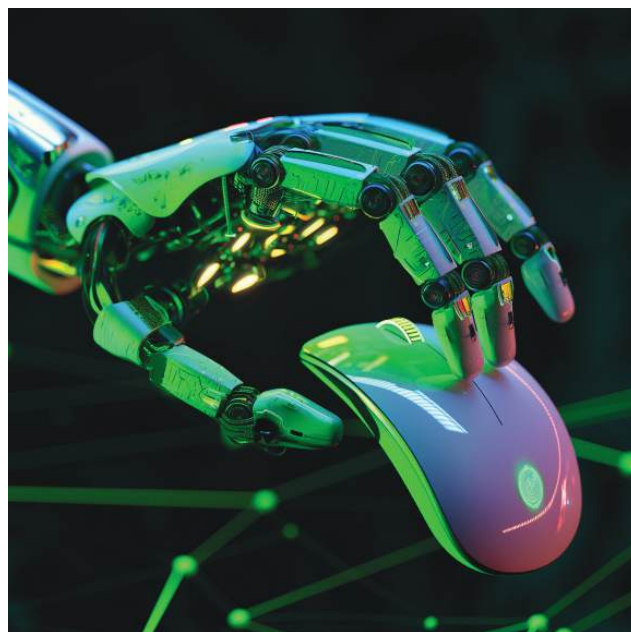
La presente contribución analiza el uso ético y adecuado de la IA en los procesos de ciberseguridad y ciberdefensa desde una perspectiva crítica, informada por fuentes abiertas y confiables como la CISA, el NIST, ISACA, e ITU, entre otras.

• ¿Qué es la Inteligencia Artificial?

La IA se define como la capacidad de una máquina para imitar funciones cognitivas humanas como aprendizaje, razonamiento y resolución de problemas (NIST, 2023). Existen diversas ramas de la IA, entre ellas el aprendizaje automático (machine learning), procesamiento de lenguaje natural (NLP) y la visión artificial. Estas tecnologías se integran cada vez más en soluciones de ciberseguridad, por ejemplo, mediante sistemas de detección de intrusiones basados en IA, que identifican patrones anómalos en el tráfico de red.

• La IA en la vida cotidiana y empresarial

En el ámbito personal, la IA está presente en asistentes virtuales, sistemas de recomendación y aplicaciones de salud. En el sector empresarial se utiliza para automatizar procesos, analizar grandes volúmenes de datos y optimizar operaciones. En ciberseguridad, empresas de todos los



a herramientas avanzadas plantea serios desafíos para la seguridad nacional e internacional.

Los principales afectados por el uso inadecuado de la IA son los ciudadanos, pequeñas y medianas empresas, los defensores de derechos humanos, periodistas y sistemas democráticos. La ONU (2022) ha advertido sobre el uso de la IA para vigilar, manipular informaciones y erosionar la confianza en las instituciones. Las víctimas pueden ser objeto de desinformación, vigilancia masiva o ataques automatizados.

• **Hacia un uso ético de la IA**

El uso ético de la IA en ciberseguridad exige transparencia, responsabilidad y rendición de cuentas. Según la UNESCO y la ITU (2023), los principios éticos deben incorporarse desde la fase de diseño de los sistemas de IA. Asimismo, los marcos normativos como el AI Risk Management Framework del NIST (2023) o las recomendaciones de la ISACA sobre gobierno de IA ofrecen guías para un desarrollo responsable.

• **Recursos para el aprendizaje y la concienciación**

Instituciones como INCIBE, CISA y la OEA ofrecen formación gratuita sobre IA y ciberseguridad. A nivel global, la UNESCO y la ITU promueven programas de alfabetización digital y ética tecnológica. Es imperativo que gobiernos, empresas y ciudadanos accedan a estas oportunidades para reducir las brechas de conocimiento y fortalecer la resiliencia digital.

Finalmente, la Inteligencia Artificial representa una herramienta poderosa en los procesos de ciberseguridad y ciberdefensa, capaz de detectar amenazas emergentes y proteger activos digitales con una eficacia sin precedentes. Sin embargo, su uso también plantea retos éticos, técnicos y sociales que no pueden ser ignorados. La utilización de IA por parte de actores criminales, así como la posibilidad de que refuerce desigualdades o vulnere derechos, subraya la urgencia de una regulación informada, inclusiva y basada en principios éticos sólidos.

Frente a este panorama, es fundamental adoptar una visión crítica y responsable, que promueva el diseño de sistemas de IA centrados en las personas, auditables y alineados con los valores democráticos. La colaboración internacional, el fortalecimiento de capacidades y la educación en ética digital son pilares esenciales para lograr un equilibrio entre innovación y protección. 

Referencias:

CISA (2022). Artificial Intelligence Use in Cybersecurity. Cybersecurity & Infrastructure Security Agency.

INCIBE (2022). Amenazas y riesgos emergentes en ciberseguridad. Instituto Nacional de Ciberseguridad de España.

ISACA (2023). AI Governance: Building Responsible Systems.

ITU & UNESCO (2023). Guidance on AI Ethics for Policymakers.

NIST (2023). Artificial Intelligence Risk Management Framework.

NIST (2024). Bias in Artificial Intelligence Systems.

OEA (2023). Panorama de amenazas digitales en América Latina.

ONU (2022). Informe sobre derechos digitales y tecnologías emergentes.

UNESCO (2021). Recomendación sobre la ética de la inteligencia artificial.

Patrocinador:



Escucha —  —

PODCAST

a través de Spotify



Encuentranos como:

Global Defense MX



Frente al espejo de la ciberseguridad: la guerra que no se ve

No se oyen disparos, pero el frente de batalla está activo: Las armas no son rifles, sino líneas de código, vulnerabilidades en sistemas, correos falsos que parecen reales. En ese territorio intangible llamado ciberespacio, México es blanco frecuente y aún carece de una legislación específica que le permita blindarse por completo.



“La ciberseguridad no es solo una palabra faltante en la ley, es una urgencia cultural que aún no hemos interiorizado”, afirma Gigi Agassini, consultora internacional especializada en gestión de riesgos, privacidad y seguridad digital, fundadora de GA Advisory.

Aunque el país cuenta con artículos en los códigos penales federal y locales que castigan el acceso indebido a información, la ausencia de una ley integral de ciberseguridad —como las que ya existen en la Unión Europea, Canadá o Estados Unidos— deja huecos críticos, y los cibercriminales los aprovechan con precisión quirúrgica.

“El cibercrimen ya es la tercera economía global”, enfatiza Agassini. Solo en 2023, 343 millones de personas en el mundo fueron víctimas de ataques. La proyección para 2025 es alarmante: un costo de 10.5 trillones de dólares, cifra que supera al PIB de muchas naciones: “Y no, tener leyes no es garantía de que los ataques disminuyan. Lo que falta es un cambio de mentalidad y generar una cultura en todos los niveles: ciudadanos, empresas y gobierno”, añade.

Uno de los mayores riesgos es la falsa percepción de inmunidad: “Creemos que los ataques solo son para grandes corporativos. Pero la realidad es que las Pymes, por invertir menos en ciberseguridad, son blanco más fácil”, dice la experta. En un entorno donde las bases de datos se filtran, se comercializan en la dark web y la Inteligencia Artificial se usa para robar identidades y clonar voces, cualquier descuido puede costar millones.

Agassini cita que las instituciones financieras a nivel global alcanzaron pérdidas alrededor de 20 mil millones de dólares en 2024 solo por robo de identidad sintética.

- El cibercrimen ya es la tercera economía global, con un costo estimado de 10.5 trillones de dólares para 2025.
- En 2024, Las instituciones financieras a nivel global registraron pérdidas por 20 mil millones de dólares por fraude de identidad sintética.
- México, aunque carece de una ley específica en ciberseguridad, no significa que no tiene los mecanismos para proceder en casos de ciberataques. Sin embargo, contar con una ley y toda una estructura formal que brinde apoyo y seguimiento a las víctimas de ciberataque, lo alinearía a otros países que desde hace tiempo cuentan con leyes y organismos específicos.

Además, América Latina presenta una tasa de fraude con tarjetas de crédito 97% más alta que en Norteamérica y 222% superior a la de Asia-Pacífico. Más allá de la infraestructura tecnológica, la consultora insiste en la educación digital: “Los passwords más usados siguen siendo 1234 o 123456. Hay que dejar de regalar nuestra información en redes. Nosotros mismos facilitamos el trabajo de los delincuentes”.

Sugiere cambios simples pero efectivos: gestionar contraseñas seguras, actualizar constantemente los dispositivos —incluidas Smart TVs y todos los dispositivos del hogar que se conectan a internet—, educar a la familia, usar antivirus y gestores de claves. “La seguridad comienza en el individuo, se extiende a la familia, a la empresa y al Estado”.

Reuniendo a expertos del sector

Del 24 al 26 de junio, Expo Seguridad 2025 reunirá en la CDMX a más de 400 expositores de 17 países en un espacio de 24 mil metros cuadrados, consolidándose como la feria de seguridad más grande de América Latina. Este año, volverá a contar con el respaldo de la Security Industry Association (SIA), organización global que impulsa la educación profesional en seguridad.

“Habrá conferencias sobre IA, ciberseguridad y sostenibilidad de la seguridad corporativa. Es un espacio donde no solo vez tecnología, sino que te educas, conectas y te anticipas al futuro. No hay que ser experto en seguridad para asistir: la seguridad es responsabilidad de todos”, asegura Agassini.

Cuando tenemos un país con problemáticas visibles e intangibles, y donde el enemigo muchas veces se oculta tras una pantalla, es necesario dejar de subestimar la amenaza digital: “¿Cómo te proteges de algo que no vez? La consciencia es el primer firewall”, concluye la especialista.



Gigi Agassini, CEO GA Advisory.



Nueva plataforma de EDGE

para monitoreo de infraestructuras críticas

En la pasada LAAD 2025, la mayor exposición del sector de defensa y seguridad de América Latina que tuvo lugar en Río de Janeiro, se presentó una innovación que promete revolucionar la protección de infraestructuras críticas: el DISCOVERY-CIM. Esta tecnología proviene del Grupo EDGE, uno de los principales grupos mundiales de tecnología avanzada y defensa que se ha estado expandiendo en América Latina. El DISCOVERY-CIM tiene como objetivo ser una plataforma de Monitoreo de Infraestructuras Críticas (CIM) de nueva generación, diseñada para ayudar a las organizaciones a proteger y monitorear sus activos esenciales.

El sistema fue desarrollado en conjunto por dos empresas del Grupo EDGE: ORYXLABS, proveedor global de soluciones avanzadas de seguridad digital que ayuda a las empresas a monitorear, proteger y optimizar sus activos críticos y entornos conectados, y BEACON RED, integrador líder de sistemas especializado en soluciones de capacitación, tecnologías avanzadas y desarrollo de capacidades de seguridad nacional.

El DISCOVERY-CIM ofrece protección en tiempo real, mayor conciencia situacional y análisis predictivos para la protección de infraestructuras críticas y monitoreo de oleoductos. La plataforma es la adición más reciente a la familia de productos DISCOVERY, expandiendo el portafolio de Gestión de la Superficie de Ataque Externo (EASM) de ORYXLABS para entornos críticos de Tecnología Operacional (OT). Está específicamente diseñada para monitorear la integridad de oleoductos externos y sistemas de protección ambiental en tiempo real.

Mediante el uso de tecnologías avanzadas para prevenir riesgos ambientales a lo largo de los oleoductos y la tecnología de fusión de sensores gestionada por BEACON RED, el DISCOVERY-CIM permite que los usuarios detecten y respondan proactivamente a amenazas como fugas, accesos no autorizados y riesgos ambientales. Además, la plataforma integra soluciones de monitoreo y seguridad de fibra óptica de última generación para mejorar la seguridad de la infraestructura y la resiliencia operativa.

Rogério Lemos, CEO de ORYXLABS, comentó: "El DISCOVERY-CIM está transformando la forma en que las empresas protegen sus activos críticos. Nuestra colaboración con BEACON RED combina

seguridad digital de vanguardia y estrategias de mitigación de riesgos, dotando a las organizaciones de monitoreo en tiempo real, análisis inteligentes y conocimientos predictivos para anticipar amenazas emergentes y mantener la integridad operativa".

Con detección de amenazas en tiempo real, análisis inteligentes y capacidades de monitoreo de vanguardia, el DISCOVERY-CIM establece un nuevo estándar para el monitoreo y la seguridad de infraestructuras críticas.

Infraestructuras críticas

Redes de energía, oleoductos, hospitales y sistemas de telecomunicaciones, son esenciales para el funcionamiento de la sociedad moderna y la economía global. La protección de estas infraestructuras se ha convertido en una prioridad creciente entre los países, especialmente en el contexto de la intensificación de los riesgos derivados del cambio climático.

La Cumbre del G20 de 2024, bajo presidencia de Brasil, fue un ejemplo de ello.

En esa ocasión, los líderes globales destacaron la importancia de invertir en infraestructuras resilientes, capaces de afrontar los desafíos ambientales y cibernéticos del futuro. En su presidencia del BRICS, Brasil también ha puesto el tema en la agenda, con iniciativas orientadas a movilizar inversiones en infraestructuras más seguras y adaptadas a los cambios climáticos.

Los impactos de problemas en estas estructuras se pudieron observar en el país en 2024, cuando inundaciones devastadoras afectaron al estado de Río Grande do Sul. Las intensas lluvias causaron daños significativos al sistema eléctrico, interrumpiendo el suministro de energía y afectando importantes carreteras, además de perjudicar el abastecimiento de agua en diversas ciudades. Este evento, que afectó a millones de personas y resultó en decenas de muertes, evidenció la fragilidad de las infraestructuras esenciales frente a desastres naturales, destacando la urgencia de invertir en tecnologías de monitoreo y resiliencia para proteger estos sistemas contra futuros riesgos climáticos extremos.

Programa de gestión de amenazas cibernéticas

• ¡Un proceso para aumentar la resiliencia!

Articlista Invitado

Antonio Celso Ribeiro Brasileño

PhD, Doctor en Filosofía en Ciencias de la Seguridad Internacional, Cambridge International University, Inglaterra. Presidente de Brasileiro INTERISK. abrasiliano@brasiliano.com.br
Brasil

São Paulo, Brasil.- La gestión de amenazas es la base de todo programa de ciberseguridad exitoso para ofrecer una mayor resiliencia. No podemos olvidar que, en este mundo extremadamente volátil, con cambios rápidos, la única certeza es tener incertidumbres todo el tiempo. Por lo tanto, la Resiliencia Cibernética debe tener las siguientes capacidades:

1. **Anticipación:** La capacidad de prepararse para eventos inesperados o improbables mediante el desarrollo de capacidades y funciones predictivas necesarias para hacer frente a cualquier tipo de evento inesperado, tanto favorable como adverso. Esto también significa estar preparado para aprovechar las oportunidades potenciales que ofrecen los cambios en contextos externos frente a los competidores.
2. **Resistir y absorber:** Capacidad de soportar situaciones adversas y absorber impactos, recuperándose después de perturbaciones. Volver a un estado normal más allá del mantenimiento y la restauración de la funcionalidad de la organización, con un enfoque en el avance de los procesos y capacidades de la organización.
3. **Resistir y absorber:** Capacidad de soportar situaciones adversas y absorber impactos, recuperándose después de perturbaciones. Volver a un estado normal más allá del mantenimiento y la restauración de la funcionalidad de la organización, con un enfoque en el avance de los procesos y capacidades de la organización.

Las capacidades anteriores contribuyen significativamente a la mejora de las posturas de seguridad. En el caso de las amenazas que se materializan, debemos evolucionar desde la corrección de riesgos ad hoc y la gestión de amenazas a medidas proactivas basadas en eventos que puedan materializarse, incluso con una probabilidad poco común. Por esta razón, compartir inteligencia de amenazas ayuda significativamente a la triple postura de anticipar, resistir y responder de manera adaptativa.

El trabajo conjunto aumenta la conciencia y la responsabilidad en todas las áreas de la empresa, en consecuencia su resiliencia y el ciclo de vida de las operaciones.

Un estudio de IBM, publicado en 2023, demostró que la gestión de amenazas, con cuatro vectores de seguridad,

reduce en gran medida la impotencia de las empresas ante eventos cibernéticos disruptivos. Son los siguientes:

1. Limite su exposición al entorno de amenazas mediante la implementación:

Descubre lo que los delincuentes saben sobre ti. Supervise la web oscura para recopilar información sobre las amenazas a su organización, empleados, redes y datos en la web oscura, antes de que lo hagan los delincuentes. Es decir, estudia el EFD – Efecto Final Deseado de sus agresores, según la norma ISO 27005.

- Mantenga a sus empleados actualizados sobre las prácticas de seguridad más efectivas.
- Edúquelos sobre los riesgos asociados con los ataques de phishing y la mala higiene de las contraseñas, y actualice regularmente a sus empleados sobre las formas de protegerse a sí mismos y a su organización.
- Mejore la planificación de la respuesta a incidentes en todo el ecosistema.
- Trabaje con las partes interesadas y los socios de su organización en todo su ecosistema para desarrollar y actualizar periódicamente planes de respuesta a incidentes que aborden específicamente las amenazas de su industria.
- Practique la simulación de respuestas a incidentes para verificar que los protocolos se ajustan a la realidad.





2. Integre y amplíe la seguridad avanzada en todas las cargas de trabajo y servicios de IA mediante la implementación:

- Asegurar el proceso de desarrollo e implementación de IA.
- Proteja cada paso de la canalización de IA, incluidos los datos utilizados para entrenar, probar y ajustar los modelos, los propios modelos de IA y el uso responsable de los modelos de IA para respaldar una seguridad de infraestructura sólida.
- Ampliar la gobernanza de la IA y la responsabilidad ética. Una gobernanza sólida es esencial para una IA fiable.
- Trabajar con los socios para establecer directrices claras para el uso de la IA; auditar periódicamente los sistemas de IA para comprobar su imparcialidad, sesgo y sesgo; y ayudar a garantizar que los resultados de la IA se alineen con los valores y la ética organizacionales más amplios.
- Utilice marcos de seguridad para inspirar confianza en los sistemas de IA. Utilice marcos estandarizados que ofrezcan enfoques estructurados para proteger los sistemas de IA. Estos marcos cubren aspectos esenciales como la privacidad de los datos, la integridad del modelo, los controles de uso y la supervisión continua.

3. Proteja las credenciales controlando la proliferación de datos e identidades mediante la implementación:

- Implemente una protección de datos sólida.
- Proteja los datos confidenciales dondequiera que residan, ya sea en las instalaciones, en la nube o en entornos híbridos. Para proteger los datos en movimiento, utilice el cifrado, implemente controles de acceso sólidos y supervise las transferencias de datos.
- Consolide las soluciones de identidad.

- Trabaje para eliminar los datos desconectados y los silos de identidad. Esto implica integrar los sistemas de gestión de identidades en un marco unificado y holístico, a menudo denominado enfoque de “tejido de identidad”.
- Cambie las tornas de los adversarios con la detección proactiva de amenazas impulsada por IA. A medida que los actores de amenazas intensifican el uso de la IA para desarrollar y escalar ataques basados en credenciales, intensifique el uso de la IA y el aprendizaje automático para detectar amenazas más rápido y responder a los ataques de manera más efectiva.

4. Solucione los errores de autenticación antes de que los atacantes puedan entrar mediante la implementación:

- Amplíe significativamente el uso de MFA. Priorice la MFA para todos los empleados y socios que acceden a los sistemas. Esto proporciona una capa adicional de protección para las aplicaciones y los servicios de red, incluso si las contraseñas se ven comprometidas.
- Modernizar la estrategia de identidad. Además de expandir el uso de MFA, desarrolle e implemente una estrategia de identidad integral, adaptable y escalable.
- Alinee la estrategia con los cambiantes requisitos operativos y de seguridad y mejórela a través de auditorías periódicas.
- Reduzca la complejidad de TI y SI. La creciente complejidad de TI y SI dificulta la administración eficaz de identidades seguras y ralentiza la respuesta a las amenazas legítimas. Para contrarrestar la complejidad, invierta en herramientas y tecnologías para plataformas de identidad más sencillas y cohesivas.

Con la operacionalización de estos vectores de seguridad, en la gestión de amenazas, las empresas tendrán una postura proactiva, integrada con respuestas adaptadas a los escenarios planteados. De esta manera, no será impotente e inerte ante eventos disruptivos. 

Revolución tecnológica para seguridad urbana

•Soluciones de videoseguridad y control de acceso, adaptadas a proyectos locales y nacionales.

Beatriz Canales

En un escenario no desconocido para México y América Latina, las emergencias se presentan en cualquier momento. Susana viaja en su auto rumbo al colegio de Miguelito, en un abrir y cerrar de ojos son impactados por un camión de carga que se pasa un alto y como era de esperarse, huye del lugar. Los ciudadanos prestos al hecho, hacen uso de las herramientas idóneas para prestar ayuda de inmediato. La activación de botones de emergencia, llamadas al 911 y cuerpos de emergencias que vengan en auxilio de las víctimas son vitales. Las autoridades al ser alertados del accidente, ponen en acción el rastreo del vehículo causante del siniestro; el despliegue de ayuda y seguimiento del infractor se hace oportuno por el actuar de la ciudadanía a través de las diferentes soluciones que hoy se utilizan para la protección de las personas.

La seguridad ciudadana ha dejado de ser un concepto exclusivamente ligado a la vigilancia presencial para convertirse en un campo liderado por la tecnología avanzada. Desde la Inteligencia Artificial (IA) hasta plataformas colaborativas en la nube, donde el sector tecnológico ha revolucionado la forma en que se protegen las ciudades, los negocios y las comunidades.

Portafolio de soluciones de Motorola Solutions

Esta firma ha consolidado su presencia en América Latina con inversiones millonarias en el rubro y con un enfoque claro en la seguridad pública y empresarial con el desarrollo de un amplio portafolio de productos y soluciones que abarcan desde comunicaciones de misión crítica hasta videovigilancia avanzada y control de acceso.

Iván Kraljevic, ingeniero senior de preventa, destaca que “uno de los principales diferenciadores de Motorola es la robustez y calidad de sus sistemas, capaces de seguir operando incluso cuando colapsan otras redes”.



Sobre la seguridad en la ciudadanía, el especialista explica: “La entendemos como la protección integral del bienestar de la población, abarcando la defensa de sus derechos, libertades, integridad física y bienes materiales. Operando siempre dentro del marco legal correspondiente, nuestro enfoque está en desarrollar tecnología que contribuya a mejorar la seguridad pública en todos sus aspectos. Esto incluye no solo el ámbito policial, sino también la atención a emergencias de salud y la respuesta ante siniestros, como incendios y rescates, con el objetivo de mitigar cualquier amenaza que afecte la integridad y bienestar de las personas”.

Una segunda área de gran relevancia para la empresa es la bioseguridad, que implica el uso de tecnologías avanzadas en el ámbito de la videovigilancia, como cámaras fijas, móviles, corporales y montadas en vehículos, así como Inteligencia Artificial para el reconocimiento automático de placas, amenazas, situaciones anormales y patrones faciales: “Estas soluciones son clave para la

ACOMPÁÑANOS A NUESTRAS REUNIONES MENSUALES

14 ENERO		11 FEBRERO		4 MARZO		1 ABRIL	TU MARCA AQUI
6 MAYO						24 JUNIO	
8 JULIO						5 AGOSTO	TU MARCA AQUI
2 SEPTIEMBRE		7 OCTUBRE		11 NOVIEMBRE	TU MARCA AQUI	2 DICIEMBRE	

AFÍLIATE Y SÉ PARTE DE NUESTRA COMUNIDAD


**MEMBRESÍA
INTERNACIONAL**

125 USD

 CAPÍTULO
MÉXICO 217
**MEMBRESÍA
CAPÍTULO MÉXICO**

\$5,650 MXN

 CAPÍTULO
MÉXICO 217
**RENOVACIÓN
CAPÍTULO MÉXICO**

\$3,750 MXN

Contáctanos en Linktree*

#ASISxTlyPARATI



seguridad, complementadas con herramientas de investigación que permiten búsquedas rápidas en fuentes de video, tanto para acciones policiales como forenses. Participamos activamente en este campo con marcas reconocidas como Avigilon y Pelco. Además, otro pilar importante es el desarrollo de soluciones de software para comando y control, que facilitan la comunicación entre las fuerzas de seguridad y la ciudadanía, la gestión de emergencias y la consolidación de alertas, entre otras funciones críticas”.

Uno de los mercados clave para Motorola Solutions en la región es el sector empresarial, donde su solución de Radio alert maximiza la integración entre radiocomunicaciones y videoseguridad, brindando mayor eficiencia y productividad a industrias como la minería, el retail, hotelería y la manufactura.

Además, sus soluciones están diseñadas para mejorar la detección de amenazas y simplificar la seguridad en escuelas, hospitales y estadios, con un enfoque claro en automatización y colaboración entre empresas y agencias de seguridad pública.

Motorola Solutions ha implementado sistemas de seguridad avanzados, como los C4 y C5, que juegan un papel clave en la seguridad ciudadana a diferentes niveles: municipal, estatal y nacional, tanto en México como en otros países. Estos sistemas son altamente escalables, lo que les permite adaptarse a las necesidades de ciudades importantes y regiones más pequeñas. Cabe destacar que una de las principales características que diferencia a Motorola Solutions, además de su calidad, robustez y confiabilidad, son sus sistemas de seguridad avanzados, como los C4 y C5, que juegan un papel clave en la seguridad ciudadana a diferentes niveles: municipal, estatal y nacional, tanto en México como en otros países.

Al ser sistemas altamente escalables, les permite adaptarse a las necesidades de ciudades importantes y regiones más pequeñas. En situaciones críticas de seguridad pública, los equipos de radiocomunicación no pueden fallar, ya que de ellos dependen vidas humanas. Incluso en condiciones extremas, como el colapso de redes celulares por tráfico excesivo; las redes de comunicación de seguridad pública deben seguir funcionando de manera ágil, segura y confidencial.

Esta alta disponibilidad y resistencia de los sistemas de Motorola, tanto en videovigilancia, comando y control como en comunicaciones móviles terrestres, asegura operaciones ininterrumpidas y confiables, lo que es fundamental para la seguridad en todos los niveles. Motorola Solutions ha crecido de manera notable, con una presencia significativa en mercados como México, Brasil, Argentina y Chile, donde colaboran estrechamente con socios locales para implementar proyectos de alto impacto en seguridad.

Adaptabilidad para cada entorno

Hikvision es la empresa global de la videovigilancia en México y América Latina, proporcionando tecnologías avanzadas como el reconocimiento facial, cámaras térmicas y sistemas de gestión de video (VMS).

Miguel Arrañaga Alcántara, director de ventas para zona Bajío, destaca que realizan pruebas exhaustivas durante uno o dos años antes de lanzar un producto, garantizando que sus soluciones sean “100% confiables y adaptadas a las necesidades locales”. Un ejemplo es la instalación de más de 300 postes de pánico y cámaras de videovigilancia en la ciudad de Querétaro, lo que ha mejorado la seguridad pública y la movilidad.



Hikvision ofrece soluciones avanzadas de videovigilancia, como cámaras fijas, móviles y perimetrales, además de analítica de video e inteligencia artificial para detectar anomalías, identificar vehículos robados, realizar reconocimiento facial, y mucho más. Estas soluciones permiten una seguridad eficiente en diferentes escenarios, como el control de tráfico, el monitoreo de aglomeraciones o la detección de incendios forestales.

Sus tecnologías están presentes en más del 60% de los centros de control y monitoreo (C4 y C5) en México. Estos centros utilizan cámaras de videovigilancia, analítica de video y herramientas de Inteligencia Artificial para tareas de seguridad pública, como la detección de amenazas, el control de tráfico y la identificación de vehículos o personas involucradas en incidentes.

El directivo aclara el concepto de “ciudad segura”, que se basa en la combinación de herramientas tecnológicas avanzadas (como la videovigilancia y la IA) y el factor humano para mejorar la calidad de vida de los ciudadanos. Cada ciudad o municipio tiene necesidades particulares, por lo que no se puede aplicar una solución estándar en todos los casos. Las soluciones se adaptan a las características y contextos específicos, como la ubicación geográfica o los riesgos que enfrentan, ya sea en zonas costeras o rurales.

La compañía se consolidó en el campo de la videovigilancia y tecnologías de seguridad, con una oferta amplia que abarca desde cámaras de vigilancia hasta sistemas de control de acceso y analítica de video impulsada por Inteligencia Artificial (IA). Sus soluciones destacan en sectores clave como ciudades inteligentes, transporte, retail, hospitales, educación, banca y energía, proporcionando tecnologías avanzadas como el reconocimiento facial, cámaras térmicas, entre otros.

Uno de los productos estrella es HikCentral Professional, una plataforma unificada que centraliza la gestión de videovigilancia y control de acceso, utilizada en grandes infraestructuras como ciudades y organizaciones de seguridad pública.

Se enfatiza que la marca ha destacado por su capacidad de innovación, invirtiendo en Inteligencia Artificial y deep learning para mejorar sus sistemas de analítica de video. Sus soluciones permiten una mayor precisión en la detección de amenazas y mejoran la toma de decisiones en tiempo real.

Miguel Arrañaga Alcántara, director de ventas en Hikvision para zona Bajío

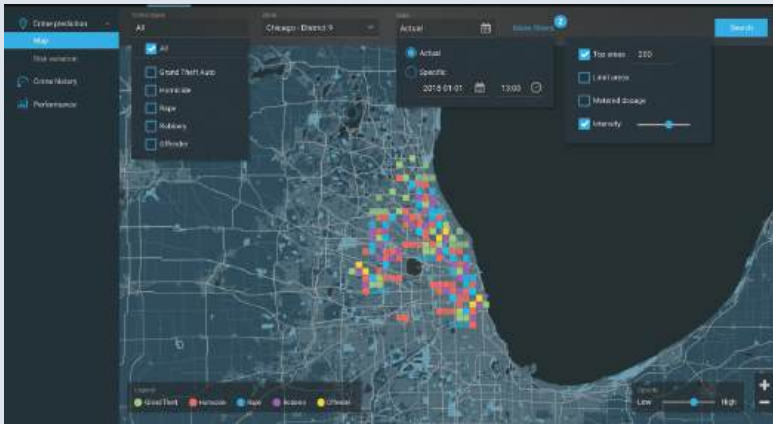
Un enfoque proactivo y preventivo

Genetec apuesta por la ciberseguridad y la protección de la privacidad como pilares de sus soluciones.

Michel Nieto, Vertical Sales Mánager para el sector público en México, menciona que la plataforma Security Center permite anticiparse a los riesgos “utilizando datos en tiempo real para identificar patrones y prevenir incidentes”. La empresa ha implementado soluciones en once estados de México, adaptándose a centros de monitoreo tanto pequeños como grandes.

Con una clara estrategia de expansión que incluye la apertura de oficinas en países como Brasil, Colombia, Chile y México, además del fortalecimiento de su estructura comercial en la región y productos estrella, la firma ofrece Security Center y Security Center SaaS, además de soluciones unificadas que integran control de acceso,





Michel Nieto, Vertical Sales Mánager para el sector público en Genetec México

Videovigilancia colaborativa en la nube

Eagle Eye Networks ha revolucionado el mercado con sus soluciones de videovigilancia en la nube para la gestión centralizada de video dentro de su extenso portafolio de servicios para la seguridad electrónica. Esta empresa ha revolucionado el mercado con sus soluciones de videovigilancia colaborativa, enfocándose en mejorar la seguridad en grandes áreas urbanas y ciudades.

Las soluciones de Eagle Eye Networks son altamente flexibles y se pueden aplicar tanto en proyectos grandes como pequeños. Estas soluciones son utilizadas por una amplia variedad de sectores, desde gobiernos hasta industrias privadas, y se adaptan a diferentes escalas

de implementación, como en la Ciudad de México, donde se han instalado alrededor de 13 mil cámaras en un periodo de cuatro meses

Al respecto, María Luisa Sánchez y Dulce Escobar, México Sales Manager e Inside Sales LATAM respectivamente, explican que la empresa se centra en el concepto de video colaborativo, con el objetivo de crear entornos más seguros, especialmente en grandes ciudades: “La plataforma es flexible y escalable, lo que permite integrarse con diferentes soluciones tecnológicas para adaptarse a las necesidades particulares de cada ciudad y comunidad”.

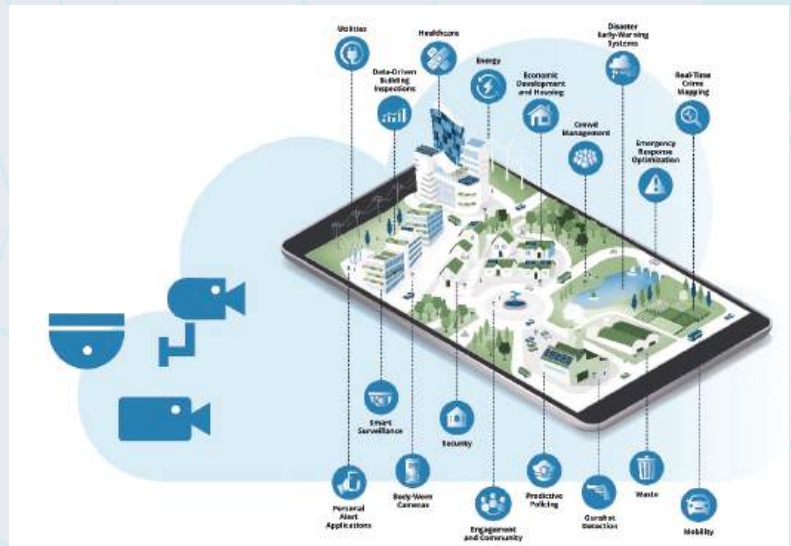
Otras soluciones importantes incluyen:

Security Center es la base para los centros de monitoreo de emergencias, y puede adaptarse según el nivel de complejidad de cada uno:

- C2: Municipios pequeños que requieren módulos básicos como videovigilancia y control de acceso.
- C4: Municipios más grandes o con áreas turísticas o industriales, que necesitan módulos más avanzados, como reconocimiento facial y de placas.
- C5: El nivel más avanzado, que utiliza análisis en tiempo real para gestionar incidentes de forma más eficiente, integrando información de los C2 y C4, y proporcionando análisis como mapas de calor para identificar áreas de mayor incidencia delictiva.

Esta compañía apuesta por la ciberseguridad y la protección de la privacidad como pilares de sus soluciones, que se pueden implementar en la nube, localmente o en modelos híbridos. Su liderazgo en la región ha sido impulsado por una creciente demanda de tecnologías de seguridad avanzada en mercados como el transporte, la energía, y las ciudades inteligentes.

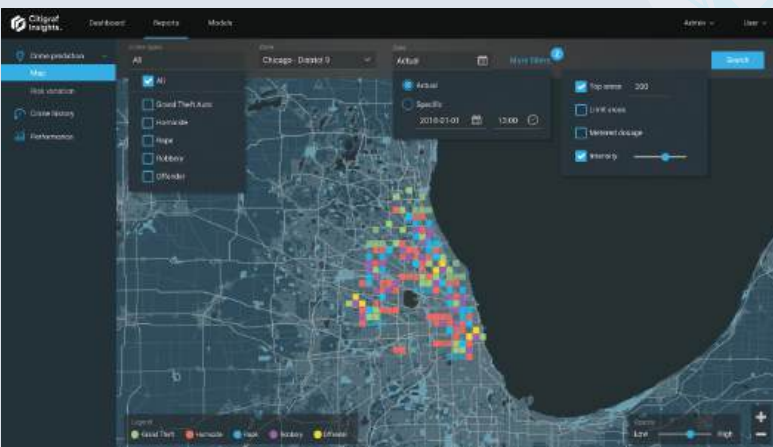
El férreo compromiso con la región se refleja en la reciente expansión de su equipo directivo, con la incorporación de Jason de Souza como director general para Latinoamérica y el Caribe, para liderar la estrategia y seguir fortaleciendo las relaciones con socios e integradores locales.



La firma ha implementado soluciones llave en mano en los centros de monitoreo C4 y C5, que incluyen cámaras, botones de pánico y otras tecnologías para crear entornos más seguros. Estas soluciones están diseñadas para mejorar la seguridad en zonas de alta delincuencia, como las implementaciones en diversas alcaldías de la Ciudad de México, donde las tecnologías de esta firma han ayudado a reducir los niveles de inseguridad.

Un ejemplo es Eagle Eye Cloud VMS, una solución que permite la gestión centralizada de video, diseñada específicamente para empresas y ciudades inteligentes. Este sistema es altamente escalable y ofrece características como grabación en la nube, encriptación avanzada y compatibilidad con cámaras digitales y analógicas, lo que permite a los clientes preservar su infraestructura existente sin necesidad de reemplazarla.

La videovigilancia en la nube se adapta a múltiples sectores, incluyendo retail, hospitales, logística, ciudades inteligentes, y escuelas, proporcionando una plataforma abierta para integraciones con terceros, lo que facilita la recopilación de inteligencia empresarial y mejora la seguridad operativa. María Luisa Sánchez subraya que “operar completamente en la nube asegura la disponibilidad y seguridad de los datos”.





Eagle Eye Networks ha crecido de manera significativa en América Latina, consolidándose como líder en videovigilancia. La compañía, que atiende a más de 80 países, ha expandido sus operaciones en la región, estableciendo una oficina en Medellín, Colombia, desde donde apoya a socios locales y clientes en mercados clave como México, Argentina, Perú y Paraguay.

Integraciones para un ecosistema seguro

FullTime es referente en monitoreo y rastreo en América Latina. José Alves Dosantos Neto, gerente comercial para LATAM, destaca que la empresa ofrece “un ecosistema completo de soluciones, brindando un soporte 100% humanizado”. Entre sus productos se incluyen FullTrack, para el rastreo satelital, y FullCenter, una plataforma que gestiona eventos de seguridad provenientes de paneles de alarma.

Alves Dosantos nos comparte la visión de la empresa en materia de seguridad ciudadana, un tema clave en la actualidad. FullTime, una multinacional con sede en Brasil y con presencia en toda Latinoamérica, lleva casi dos décadas desarrollando soluciones de seguridad electrónica. Entre sus productos destacan aplicaciones orientadas a mejorar la vigilancia y protección de las ciudades, colaborando con C4 y C5 para el monitoreo eficiente de espacios públicos.

“FullTime no solo se limita a vender seguridad electrónica, ofrecemos un ecosistema completo de soluciones”, comenta Alves. Entre estas soluciones se encuentra una aplicación diseñada para ser utilizada tanto por ciudadanos como por gobiernos locales: “Con Eficienty, las personas pueden activar botones de alerta para



reportar incidentes como violencia de género, personas sospechosas o vandalismo, enviando la información directamente al centro de monitoreo del C4 o C5”. Esta integración con centros de comando y control permite una respuesta más rápida y efectiva.

Además de Eficienty, la marca ofrece soluciones que permiten a los ciudadanos y empresas colaborar en la seguridad de sus comunidades: “Nuestra aplicación permite a los usuarios no solo reportar incidentes, sino también acceder a cámaras de seguridad compartidas en barrios o vecindarios con ingresos controlados”, explica Alves. Esta colaboración comunitaria ha demostrado ser una herramienta poderosa en la reducción de delitos en áreas urbanas.

El compromiso de FullTime con la seguridad va más allá de la simple venta de productos. La empresa asegura que sus sistemas estén “100% actualizados y operativos en todo momento”, para que las autoridades y los ciudadanos confíen plenamente en sus soluciones. “Nuestro objetivo es proporcionar tranquilidad a las comunidades y garantizar que siempre haya una respuesta rápida ante cualquier emergencia”, subraya Alves.

La empresa ha implementado sus soluciones en diversas ciudades de Latinoamérica, como Buenos Aires y Bogotá, donde alcaldías han adoptado las herramientas para prevenir delitos como la violencia de género. En otro caso, en Perú, la instalación de cámaras y sirenas en hogares ha logrado reducir drásticamente los índices de robo.

Con una expansión constante y un enfoque en la tecnología, la firma de seguridad busca consolidarse como líder en soluciones electrónicas, no solo en Latinoamérica, sino en otros continentes: “Queremos que cuando se hable de seguridad electrónica, se piense automáticamente en FullTime”, concluye el ejecutivo.

Bolide: desarrollo de soluciones de vanguardia

El principal diferenciador de Bolide Technology Group es su capacidad para desarrollar analíticas avanzadas, que implementan en sus productos destinados a proyectos de ciudades seguras.

Bolide ofrece un extenso portafolio de sistemas de videovigilancia inteligentes con analíticas avanzadas al borde, soluciones en la nube y opciones móviles, todas diseñadas para satisfacer las necesidades del mercado de la seguridad electrónica.

Con más de 30 años de experiencia como pionero en videovigilancia, Bolide también ha centrado sus esfuerzos en soluciones de seguridad para el transporte y la protección de bienes móviles, proporcionando monitoreo y rastreo en tiempo real para garantizar la seguridad en entornos de movilidad.

“Nuestras cámaras de videovigilancia con analíticas al borde generan alertas en tiempo real para los centros de comando, ayudando no solo a crear municipios más seguros, sino también más eficientes”, afirma Alejandro Salinas, vicepresidente de Bolide.

Entre los productos más destacados se encuentra una cámara





SMARTCITY EXPO LATAM CONGRESS

10 - 12 JUNIO 2025
PUEBLA, MÉXICO
CENTRO EXPOSITOR
Y DE CONVENCIONES

En el 2025 celebramos 10 ediciones de pensar en grande, de presentar las ideas más innovadoras, de reunir a investigadores, empresarios y líderes políticos para implementar acciones que dejen huella en nuestras comunidades, creando sociedades sostenibles, innovadoras, tecnológicas e inclusivas. Juntos, forjamos el futuro que América Latina necesita.

+100
Alcaldes

+300
Ciudades
Nacionales e
Internacionales

+200
Instituciones
y Empresas

+300
Ponentes

+50
Medios de
comunicación

+10,000
Asistentes

+20,000 m²
de evento

CONGRESO

ZONA EXPO

NETWORKING



Contáctanos

+52 (55) 2697 8336

info@smartcityexpolatam.com

www.smartcityexpolatam.com



**¡Regístrate ahora
y sé parte de la
revolución urbana!**



ANFITRIÓN

SEDE

ORGANIZADO POR

UN EVENTO DE





multisensor con cuatro sensores internos, que permite una visualización de 360°. Este equipo se distingue por integrar analíticas avanzadas sin licenciamiento adicional, lo que permite a Bolide adaptarse rápidamente a los cambios del mercado y personalizar nuevas soluciones de vanguardia.

Las cámaras de Bolide incluyen analíticas avanzadas al borde, como reconocimiento facial, reconocimiento de placas y detección de objetos. Entre sus modelos más destacados se encuentra:

Cámara Multisensor Bolide BN9108R/NDAA

Cumpliendo con las normativas NDAA, esta cámara es una herramienta clave para entornos urbanos más seguros. Su diseño 4K para exteriores incluye cuatro lentes ajustables que permiten cubrir un campo de visión de 360°, ideal para el monitoreo integral de espacios públicos como parques, avenidas y áreas estratégicas de la ciudad.

Ofrece transmisión en cuatro canales con una resolución de hasta 8MP por canal y una velocidad de 25/30 FPS, garantizando imágenes de alta definición. Con tecnología Starlight y WDR de 120 dB, su rendimiento es excelente en condiciones de baja iluminación. Además, cuenta con un iluminador de doble fuente (IR y luz cálida) para maximizar la visibilidad nocturna.

Su diseño robusto y versátil está certificado con IP67 e IK10, lo que la hace resistente al agua y al vandalismo, perfecta para su uso en exteriores y bajo condiciones climáticas adversas. Con funciones inteligentes en sus cuatro canales simultáneamente, esta cámara es una solución indispensable para cualquier proyecto de Ciudad Segura, proporcionando monitoreo eficiente y una rápida respuesta ante incidentes.

Bolide Technology Group es una empresa norteamericana con presencia global, incluyendo oficinas en Latinoamérica y la Ciudad de México. Su capacidad para desarrollar soluciones personalizadas y rápidas para cada cliente, independientemente de la región o las necesidades específicas, es uno de los aspectos clave que distingue a la marca.



Iván Kraljevic, ingeniero senior de preventa para el tema de combate y control en Motorola Solutions para LATAM y el Caribe.



Michel Nieto, Vertical Sales Mánager para el sector público en Genetec México



María Luisa Sánchez, Sales manager para Eagle Eye Networks



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



José Alves Dosantos Neto, gerente comercial para LATAM en FullTime



Dulce Escoba, Inside Sales LATAM para Eagle Eye Networks



Alejandro Salinas, vicepresidente Internacional de Bolide Technology Group



ARMORING
GROUP



**¡SUPREMACÍA EN
BLINDAJE TOTAL!**

+52 55 1957 7956

[in](#) [v](#) [d](#) [f](#) [@](#) [@armoringroup](#)

www.armoringgroup.com



MÉXICO

Lago Onega 236,
Anáhuac 1a sección, Miguel Hidalgo,
C.P. 11320, CDMX



SWEBOR

El acero flexible redefine la seguridad en América Latina: Swebor

Swebor es la compañía que fortalece su presencia como proveedor estratégico para la industria del blindaje, no solo en el ámbito nacional sino también en Centro y Sudamérica: “México es nuestra plataforma para abastecer desde Guatemala hasta Chile”, afirma Federico Forastieri Appel, director general de Swebor Latam.

Esta firma, que llegó a México en 2019, atiende a más de un centenar de empresas blindadoras registradas ante la Secretaría de Seguridad y Protección Ciudadana y a un número indeterminado de firmas en proceso de formalización o que operan únicamente bajo marco fiscal.

El crecimiento del blindaje civil se concentra en el nivel NIJ 3A, diseñado para detener municiones de armas cortas como 9 mm o .44 Magnum. Este segmento representa el 70% del mercado en las metrópolis como la Ciudad de México, Monterrey o Guadalajara. A medida que se desplaza hacia zonas fronterizas, el patrón se invierte. En estados como Tamaulipas o Sonora, el 70% de la demanda responde a protección contra armamento de uso militar, como AK-47 o AR-15, cumpliendo con normas europeas FB5 y FB6.

Las soluciones se adaptan a cada necesidad mediante aceros que van desde los 2 hasta los 10 milímetros de grosor. Entre sus desarrollos más avanzados se encuentra el blindaje espaciado: una combinación de placas de 600 Brinell con cámaras de aire intercaladas, capaces de resistir incluso municiones perforantes calibre .50. Esta tecnología ya se utiliza en unidades de las secretarías de la Defensa Nacional (DEFENSA) y de Marina-Armada de México (SEMAR), así como fiscalías estatales.

El fenómeno no es exclusivo de México. En países como Ecuador, el repunte de la violencia ha detonado una demanda intensa: “En Ecuador, el 70% del blindaje se orienta a protección contra armas largas”, explica Forastieri. Swebor ya proyecta abrir oficinas en Quito o Bogotá para acortar tiempos de entrega y fortalecer el soporte técnico regional. En Chile, el comportamiento del

- La firma introduce a México su acero balístico de 650 Brinell: flexible, más liviano y tres veces más económico que la cerámica.
- Hasta 160 empresas en el país cuentan con registro para operar en blindaje.

mercado es similar, con énfasis en municiones de guerra y requerimientos normativos más estrictos.

El equipo de Swebor apuesta por un modelo de asesoría especializada con ingenieros en metalurgia y balística que trabajan con los clientes para seleccionar el acero adecuado según el tipo de amenaza, el nivel de riesgo y las condiciones del vehículo. Este acompañamiento incluye soporte posterior a la venta en caso de siniestros, algo poco habitual en el mercado.

Sobre el costo, Forastieri es enfático: blindar un vehículo puede duplicar su valor, pero se trata de una inversión crítica, pues “hoy día hay soluciones para prácticamente cualquier tipo de unidad. No es exclusivo de camionetas premium. Cada vez más familias protegen a sus hijos, no solo a ejecutivos”, apunta.

Las proyecciones de la compañía son cautas. La incertidumbre económica y el cambio de gobierno en México ralentizaron el primer semestre. Aun así, Swebor prevé un repunte en la segunda mitad del año, particularmente en los niveles altos de blindaje, impulsado por el sector público y Fuerzas Armadas.

“No se trata solo de vender acero. Se trata de garantizar que un blindaje funcione cuando más se necesita. Por eso insistimos en estándares internacionales, pruebas certificadas y asesoría profesional desde el primer contacto”, concluye el director general de Swebor.



Federico Forastieri Appel, director general de Swebor Latam.

SWEBOR ARMOR

HECHO PARA DURAR



SWEBOR



@Swebot.lat



Swebot lat



Swebot_lat



@Swebot_lat



Swebot



5521634234



contacto@swebor.mx



www.swebor.mx



Santa Fe No. 170 Int.5-2-06, Col. Santa Fe,
Alcaldía Álvaro Obregón, CDMX

La ingeniería mexicana que protege a las fuerzas del orden

- La firma se consolida como una empresa clave en la fabricación de vehículos tácticos y ejecutivos en México. Con presencia en América Latina, ofrece soluciones personalizadas para las fuerzas de seguridad.

Nuestro país ha priorizado la seguridad los últimos años, por lo que la industria del blindaje tiene un papel esencial en la protección de civiles y fuerzas del orden. Entre los actores más relevantes del sector, destaca la empresa Blindajes ETTS, con más de 15 años en el mercado, que fortalece día a día su lugar como una de las más importantes compañías en la fabricación de vehículos tácticos y ejecutivos.

“Nos especializamos en dos tipos de productos: los vehículos blindados para uso personal y los tácticos, diseñados específicamente para cuerpos de seguridad”, explica Gadi Mokotov, director general de la compañía.

Con una planta principal en Zapopan, Jalisco, y otras instalaciones en Lerma, Estado de México, y en Ecuador, ETTS ha expandido su producción para consolidarse en el mercado latinoamericano. Su fortaleza radica en la capacidad de fabricar unidades a la medida, garantizando tiempos de entrega más cortos en comparación con otros competidores internacionales.

“El blindaje en México ha alcanzado un nivel de calidad y profesionalismo que nos coloca como referencia global. Actualmente somos el segundo mercado más grande del mundo, después de Brasil”, afirma Mokotov.

El corazón de ETTS son sus vehículos tácticos, creados para enfrentar los desafíos de seguridad en distintos niveles. Con camionetas pickup adaptadas y unidades tipo SWAT con blindaje avanzado, su catálogo abarca soluciones para operativos especiales, retenes y traslado de reos.

Al respecto, el directivo señala: “Estos vehículos están diseñados para que las fuerzas de seguridad puedan moverse de manera ágil y protegida en situaciones de alto riesgo. Incorporamos tecnologías como visión nocturna y cámaras de monitoreo para ofrecer un control total del entorno”.

La empresa ha colaborado de manera activa con instituciones como el Ejército Mexicano, Armada y Guardia Nacional, así como diversos cuerpos de policía estatal y municipal, desarrollando unidades adaptadas a las condiciones operativas de cada corporación.



Si bien el sector del blindaje depende en gran medida de las políticas de seguridad de cada administración, Mokotov considera que la industria continuará creciendo.

“Vemos una intención clara del gobierno actual por fortalecer las fuerzas del orden con equipamiento adecuado. En ETTS, más que vender vehículos, diseñamos herramientas de trabajo que se ajustan a las necesidades reales de quienes protegen al país”, sostiene.

En el ámbito internacional, la firma exporta a distintos países de América Latina, donde la fabricación local de este tipo de unidades es escasa. Esto les da una ventaja competitiva al reducir costos y tiempos de entrega, además de garantizar disponibilidad de refacciones y mantenimiento.

Con una producción promedio de 50 vehículos tácticos al año y una estrategia enfocada en la innovación, Blindajes ETTS continúa siendo un referente en seguridad y blindaje, apostando por el talento y la ingeniería mexicana. Mokotov enfatiza: “La calidad de nuestros vehículos es 100% mexicana, desde el diseño hasta la entrega”.





CREAMOS LA SOLUCIÓN IDEAL PARA TI

Nos especializamos en **BLINDAJE**
con un nivel de **excelencia**
que asegura tu **protección**
y completa **satisfacción**.

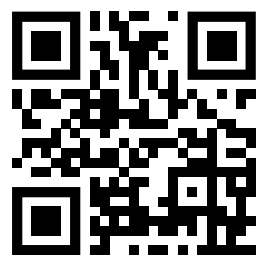


VEHÍCULOS TÁCTICOS

  55 6010 7863

www.etts.com.mx

Visita nuestro sitio:





Articulista Invitado

Alejandro Rojo M.

CPP, DSI, DAS, DES, CPO, CSSM, DhC.,
director general Commander Seguridad Privada
México

Superación

Estimados colegas y amigos es un honor y privilegio dirigirme a ustedes. El trabajo continuo y la constancia son fundamentales para alcanzar el éxito, sin duda este no ha sido un camino fácil, pero ha valido la pena para marcar la diferencia en mi persona.

Recuerdo mis inicios en el sector de la seguridad, empezando como guardia intramuros allá por el año 1988 en Inter-Con, con esos nervios e inexperiencia, pero con todas las ganas de aprender.

La necesidad, la familia y los sueños de cumplir metas, fueron los impulsos por los cuales me esforcé, crecí y mejoré; colaborando con grandes empresas donde el interés de aprender y la disposición, me permitieron seguir aprendiendo de esta hermosa profesión.

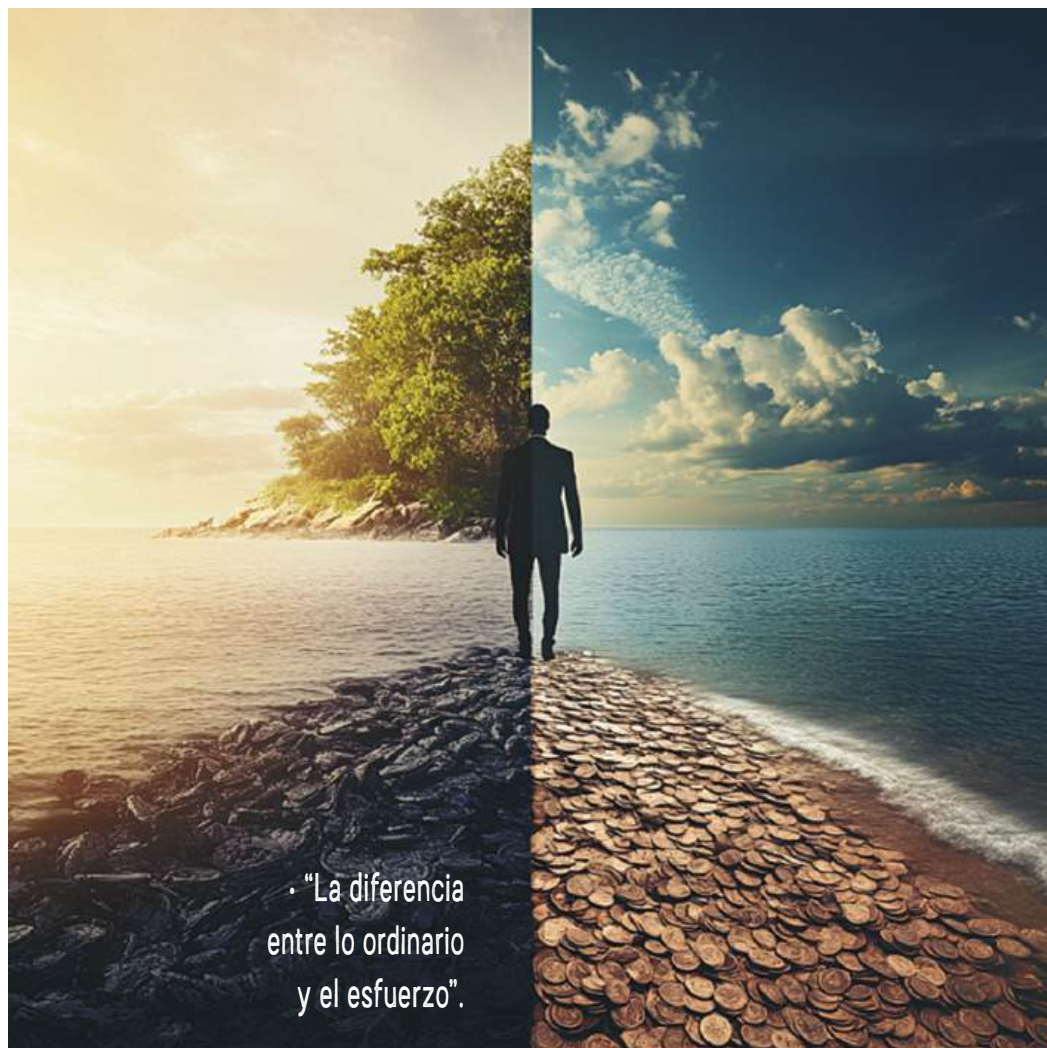
Fueron dos años en los cuales estuve en el mismo puesto (guardia), pero cada día que pasaba me enamoraba de la profesión, si bien hubo días buenos, también malos, pero nada me detuvo para dar mi máximo esfuerzo, aunque parece un trabajo fácil no lo es, ya que la misión de proteger y prevenir incidencias es toda una responsabilidad.

Al pasar de los años fui cambiando de empresas y adquirí más experiencia, pero nunca me conformé con estar en el mismo puesto, así que fui tomando cursos para certificarme en diferentes áreas de seguridad privada y diferenciarme de los demás de manera constante.

El estar más comprometido me abrió las puertas a nuevos puestos o proyectos y me dio una visión más clara de lo que quería lograr. Sin duda la preparación es la base del éxito, por eso es importante estar en constante cambio de crecimiento y aprendizaje.

No podemos ir a la "guerra sin armas", por es importante tener una buena preparación para cumplir con el cargo otorgado. A lo largo de mi carrera he tenido diferentes tipos de retos y obstáculos que he superado, considero que el secreto para el crecimiento (aunque puede haber más factores) radica en mantenerse preparado y actualizado, pertenecer a diferentes asociaciones a fines a tus intereses profesionales, rodearte de personas que también tengan el mismo sueño o intereses, por eso me he rodeado de personas con mucha experiencia y conocimientos de los cuales llevo el buen ejemplo.

Si tuviera que agradecer a grandes mentores y maestros, no terminaría de mencionarlos, colegas, compañeros y colaboradores, que han contribuido a mi crecimiento personal y profesional.



• "La diferencia
entre lo ordinario
y el esfuerzo".

Cada uno de los certificados que he hecho a lo largo de mi carrera, me han ayudado a fomentar mi capacidad de encontrar soluciones a los obstáculos, en este momento se abre un capítulo nuevo en mi vida profesional, y estoy listo para trabajar duro y demostrar que estoy a la altura de este nuevo reto.

La invitación va para todos aquellos jóvenes y a las nuevas generaciones que están interesados o que están incursionando en esta profesión de seguridad, no se desesperen sean disciplinados, siempre aprendan algo nuevo, confíen en sus mentores sean disruptivos y no tengan miedo a intentarlo, tengan miedo de pensar qué hubiese pasado si no lo hubiera intentado.

El hecho de pertenecer a diferentes asociaciones como ASIS, AMEXSI, CNSP, AMESP, entre otros, te puede proyectar a conocer varias formas de pensamiento, disruptivos, analíticos, nuevos horizontes.

Algo que también he aprendido a lo largo de los años es que en el ramo de la seguridad ningún día será idéntico al anterior, siempre hay cosas nuevas que hacer, retos que afrontar, desafíos que superar, sin embargo la satisfacción por haber alcanzado estas soluciones es increíblemente satisfactoria.

Me encantaría conocer más casos en donde estos u otros consejos ayuden a impulsar a las nuevas generaciones, para que juntos podamos compartir la experiencia de decir "soy de ese pequeño grupo que paso de ser un guardia a un director".

Liderazgo en seguridad

Articulista Invitado



José Ruiz

CPP® PCI® PSP® CLSD® ASIS Internacional, director de Seguridad en Four Seasons Hotels and Resorts, con más de 20 años de experiencia, posiciones senior en Hyatt Hotels and Resorts, Costa Palmas y CSO en multinacionales.
México

• La seguridad no es solo proteger lo que ya tenemos, sino construir bases de lo que podemos alcanzar.

(Parte 2 de 2)

En la primera parte de este artículo, estimado lector se habló del poder del líder en los momentos decisivos, así como el trabajo bajo presión. En esta segunda entrega se hablará sobre la confianza y como transformar los desafíos en oportunidades a través del liderazgo.

El arte de ganar confianza en esta industria

La confianza es la moneda más valiosa de un líder. En el ámbito de la seguridad, adoptar estándares globales y mejores prácticas no es solo una obligación técnica, sino una estrategia para ganar influencia en la organización. Cuando basas tus gestiones en métodos claros y medibles, transformas la percepción de la seguridad, déjame darme el lujo de citar aquí un cliché que a muchos puede sonar repetitivo, pero es solo la verdad: cuando logras demostrar la rentabilidad de las medidas de gestión, seguridad deja de ser un gasto y se convierte en una inversión estratégica que impulsa las metas.

Respira profundo por un momento, tomate unos segundos para separar tus ojos de este texto, luego vuelve aquí e imagina esto:

El director de seguridad entra a la sala de juntas tras un evento crítico... No hay excusas, no hay dudas. Presenta datos, soluciones y un par de opciones como planes de acción que no solo resuelven el problema, sino que protegen el futuro de la empresa, y solo necesita el apoyo y la aprobación de alguno de estos dos planes por parte del equipo. ¿Puedes imaginar cómo te sentirías si fueras uno



de los asistentes a esa reunión? Pues, estimado/a colega, esa es la diferencia entre un administrador y un líder visionario.

Transformar desafíos en oportunidades

Según la Encuesta Nacional de Victimización de Empresas 2024 (INEGI), el sector servicios en México enfrentó grandes retos en 2023, siendo el segundo más afectado por el crimen. Sin embargo, no todo es adversidad. La inversión extranjera directa en turismo sigue siendo una muestra de confianza en el potencial del sector, alcanzando \$2,374 millones de dólares en 2024 (al tercer trimestre). Arrollador, ¿no? ¡caray! volvamos a razonar esto: Departamentos y casas con servicios de hotelería 59.7% Hoteles 34.7% total: ¡94.4% de la inversión!

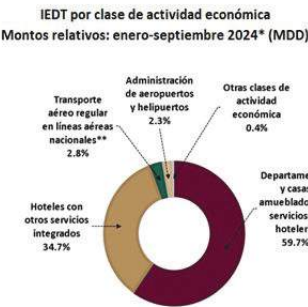
Pregunta Clave

Antes de la pregunta, piensa un poco que tú y yo somos los líderes de seguridad que protegen y colaboran en dar paz mental a los clientes y partes interesadas en la industria con más crecimiento en el país, por tanto, nuestras capacidades técnicas y habilidades humanas de liderazgo y gestión del cambio debiesen estar a esa misma altura. Aquí viene la pregunta, solo responde para ti mismo y con mucha sinceridad, ¿Crees que en nuestro gremio estamos unidos liderando el cambio o simplemente reaccionando a él?

Al final del día, la seguridad no es solo proteger lo que ya tenemos, sino construir bases de lo que podemos alcanzar. Agradezco mucho que hayas llegado hasta aquí, te mando un fuerte abrazo con mi admiración y respeto por elegir esta desafiante tarea en la que tú y yo estamos en el mismo barco.

Indicador de Inversión Extranjera Directa Turística 1999-2024*				
Año	IED	IEDT	Participación de la IEDT del total	
1999	\$13,960.3	\$797.3	5.7%	
2000	\$16,248.7	\$809.2	4.9%	
2001	\$10,057.2	\$507.4	5.1%	
2002	\$24,099.2	\$495.5	2.1%	
2003	\$18,250.0	\$547.6	3.0%	
2004	\$25,015.6	\$561.1	2.2%	
2005	\$25,795.8	\$1,529.1	5.9%	
2006	\$12,366.4	\$1,624.3	7.6%	
2007	\$32,393.5	\$1,499.2	5.9%	
2008	\$29,563.9	\$1,137.9	3.9%	
2009	\$17,850.5	\$667.6	3.7%	
2010	\$27,190.0	\$927.8	3.4%	
2011	\$25,632.5	\$1,017.2	4.0%	
2012	\$31,769.3	\$1,070.4	7.2%	
2013	\$46,364.4	\$1,347.5	2.8%	
2014	\$30,351.3	\$832.0	2.7%	
2015	\$35,363.9	\$561.8	1.6%	
2016	\$31,189.4	\$795.2	2.5%	
2017	\$34,017.9	\$1,800.9	5.3%	
2018	\$34,101.0	\$1,116.2	3.3%	
2019	\$34,617.1	\$1,251.0	3.6%	
2020	\$28,214.7	\$1,213.0	4.3%	
2021	\$13,760.0	\$2,172.3	6.5%	
2022**	\$36,312.9	\$4,494.2	12.4%	
2023***	\$36,296.0	\$2,776.1	7.6%	
2024*	\$35,737.5	\$2,374.9	6.6%	
Total	\$749,639.3	\$35,080.4	4.7%	

Fuente: Datatur, Sector, Gobierno Federal



En el campo de la seguridad privada



es la solución

Con más de 20 años de servicio, Ingeniería en Sistemas Integrales de Seguridad Privada (ISIS), sobresale en el sector de la protección intramuros en nuestro país. Las verticales de negocio que ofrece, da respuesta a las necesidades actuales que hoy el sector de la protección necesita. Raymundo Mancera Sandoval, director general, resalta el avance que en el presente ISIS ofrece en el campo de la seguridad privada.

- Seguridad intramuros y vigilancia para empresas privadas para el manejo de almacenes fiscalizados, hoy son las principales líneas de negocio.



“Sin duda, la contratación de servicios de seguridad privada ha venido creciendo de manera importante bajo las condiciones que marca la ley para este sector. Las empresas de seguridad ya nos convertimos en coadyuvantes de la seguridad pública, porque somos a lo que le llaman el primer respondiente en caso de un incidente o por un acto inseguro”.

El portafolio de servicios de ISIS, incluye vigilancia intramuros, protección al transporte a través de custodias de acompañamiento, y la parte de monitoreo mediante el rastreo satelital. “En cuanto a las diferentes industria a las que se les presta el servicio se encuentra el sector manufactura y empresas de almacenamiento de mercancía. La vertical de negocio más importante de Sistemas Integrales ISIS es la vigilancia intramuros (cuidado de instalaciones hacia el interior, o sea accesos principales, accesos vehiculares, controles de entrada, salida de mercancía y áreas de resguardo especial), básicamente. Hoy nos dedicamos a un mercado muy especializado, que es la vigilancia para empresas privadas que tienen concesión para el manejo de almacenes fiscalizados, no cualquier empresa lo hace”.

Presencia territorial

La empresa opera en toda el área metropolitana, básicamente en el Estado de México, Aeropuerto “Benito Juárez” y “Felipe Ángeles”, la zona del Bajío, desde Querétaro hasta San Luis Potosí con oficinas en Querétaro, Irapuato, León, Salamanca y Silao, ciudades con la mayor concentración con servicio de seguridad intramuros. En la parte de protección del transporte, la tienen por toda la República Mexicana, concentrado orígenes en Querétaro y hacia Veracruz.

Expansión y Proyección

La empresa de seguridad privada se consolida y continúa adaptándose a los cambios y exigencias en el entorno de la protección reforzando su expansión en el corredor Querétaro-San Luis Potosí; y parte del oriente del país, específicamente Puebla y Tlaxcala. “En los últimos cinco años tuvimos un crecimiento de entre el 20 y 40%, el cual se ha sostenido que se ha venido sostenido y hemos crecido de manera importante. La proyección de crecimiento operativo se ha complicando por el tema de los aranceles, ya que trabajamos con plantas de manufactura”, añade el directivo.

Actualmente cuenta con una plantilla laboral de más de 1500 personas, y una flotilla de más de 50 unidades. Los cambios a la nueva reglamentación laboral por parte de la STPS (Secretaría del Trabajo y Previsión Social, ha hecho que la empresa de seguridad privada se alinee y se concentre a las nuevas disposiciones en lo que respecta al tema de las jornadas laborales, de prestaciones, demandas y ley silla, afectando la rentabilidad de la empresa.

La propuesta de Raymundo Mancera es clara con respecto a las regulaciones locales y estatales de empresas de seguridad y es que se cumplan con esas obligaciones “quizás hacer más exhaustiva, frecuente y extensa la revisión por parte de las autoridades del IMSS, SAT, STPS, para que las empresas del sector (entre 3 mil y 4 mil registradas), concluye. ISIS, en voz de su director general es seguir colaborando con las autoridades para mejorar las estrategias de seguridad, apoyando y coadyuvando para que los operativos sean exitosos.



Raymundo Mancera Sandoval, CEO de ISIS, Seguridad Integral.



**Creamos entornos
seguros**

Expertos en custodia de mercancías

Servicios

- Guardias intramuros
- Custodia al transporte
- Monitoreo CCTV
- Rastreo GPS
- Seguridad electrónica
- Control de confianza



55 1089 1089



ventas@isis-seguridad.com.mx



www.isis-seguridad.com.mx

Diseño de políticas públicas municipales para la gestión de riesgos socio-urbanos

Articulista Invitada

Mercedes Escudero Carmona

Presidenta CPTED México ICA Chapter & presidenta ASIS International Capítulo 311 México



• CPTED como parte del Modelo de Seguridad Humana.

Las ciudades, como organismos vivos y complejos, enfrentan una creciente gama de riesgos socio-urbanos que amenazan el bienestar de sus habitantes y la sostenibilidad de su desarrollo. Desde la delincuencia y la violencia, hasta los desastres naturales exacerbados por la vulnerabilidad social, estos desafíos demandan respuestas integrales y proactivas por parte de los gobiernos locales.

En este contexto, el diseño de políticas públicas municipales que integren los principios de la Prevención del Delito a través del Diseño Ambiental (CPTED) dentro de un modelo de seguridad humana y resiliencia se erige como una estrategia fundamental para construir comunidades más seguras, inclusivas y capaces de afrontar la adversidad.

La urgencia de abordar los riesgos socio-urbanos en el ámbito municipal:

Los municipios, como la unidad de gobierno más cercana a la ciudadanía, se encuentran en una posición estratégica para comprender y abordar las dinámicas específicas de los riesgos socio-urbanos. La proximidad permite identificar vulnerabilidades particulares, comprender las complejas interacciones entre factores sociales, económicos y ambientales, para diseñar soluciones adaptadas a las necesidades y características de cada territorio. Ignorar estos riesgos puede acarrear costos humanos, económicos y sociales significativos, erosionando la confianza ciudadana, obstaculizando el desarrollo y perpetuando ciclos de vulnerabilidad.

La Prevención del Delito a través del Diseño Ambiental (CPTED) al tener como premisa el diseño y la gestión

del entorno construido y por construir pueden influir en el comportamiento delictivo y la percepción de seguridad. Al intervenir en aspectos como la vigilancia natural, el control de acceso, el refuerzo territorial, el mantenimiento y la gestión de actividades, CPTED busca reducir las oportunidades para el delito y fomentar un sentido de propiedad y seguridad entre los residentes.

Integrar los principios de CPTED en las políticas públicas municipales implica ir más allá de la respuesta reactiva al delito y adoptar un enfoque proactivo que aborde las causas subyacentes y las oportunidades situacionales. Esto puede traducirse en regulaciones de planificación urbana que promuevan espacios públicos seguros y bien iluminados, directrices de diseño para viviendas y edificios que incorporen medidas de seguridad pasiva, y estrategias de gestión del espacio público que fomenten la apropiación positiva por parte de la comunidad.

Seguridad humana y resiliencia: un marco conceptual amplio:

El concepto de seguridad humana trasciende la visión centrada en la ausencia de violencia física, abarcando un espectro más amplio de amenazas que afectan la dignidad, el bienestar y las oportunidades de las personas. Esto incluye la seguridad económica, alimentaria, de la salud, ambiental, personal, comunitaria y política. Un modelo de seguridad humana reconoce la interconexión de estos ámbitos y la necesidad de abordarlos de manera integral.

La resiliencia, por su parte, se refiere a la capacidad de individuos, comunidades y sistemas para anticipar, resistir, absorber, adaptarse y recuperarse de manera eficiente de



las tensiones y los choques. En el contexto socio-urbano, la resiliencia implica fortalecer la capacidad de las comunidades para hacer frente a una variedad de riesgos, desde eventos climáticos extremos hasta crisis económicas y brotes de violencia.

Integrando CPTED en un modelo de seguridad humana y resiliencia municipal:

La articulación de CPTED dentro de un modelo de seguridad humana y resiliencia a nivel municipal ofrece un marco poderoso para el diseño de políticas públicas transformadoras. Esta integración implica:

- **Diagnóstico integral de riesgos:** identificar y analizar los riesgos socio-urbanos específicos del municipio, considerando no solo las amenazas directas (delincuencia, desastres), sino también las vulnerabilidades subyacentes (desigualdad, exclusión social, falta de acceso a servicios básicos).
- **Enfoque multidimensional:** abordar los riesgos desde una perspectiva que considere sus dimensiones: social, económica, ambiental, espacial y sus interconexiones.
- **Participación ciudadana:** involucrar activamente a la comunidad en la identificación de problemas, el diseño de soluciones y la implementación de políticas, fomentando un sentido de propiedad y responsabilidad compartida. La aplicación de principios CPTED puede ser más efectiva cuando se realiza en consulta con los residentes locales, quienes tienen un conocimiento invaluable de su entorno porque son los nativos expertos del territorio.
- **Diseño urbano sensible a la seguridad:** incorporar los principios de CPTED en la planificación urbana, el diseño de espacios públicos, la construcción de viviendas y la gestión de la infraestructura para reducir las oportunidades de delito y mejorar la percepción de seguridad. Esto puede incluir la mejora de la iluminación, la creación de espacios abiertos y visibles, el diseño de rutas peatonales seguras y la promoción del uso mixto del suelo.
- **Fortalecimiento de la cohesión social:** implementar programas que fomenten la interacción social, la construcción de redes de apoyo comunitario y el fortalecimiento del capital social como elementos clave de la resiliencia y la prevención del delito. Espacios públicos bien diseñados bajo principios CPTED pueden actuar como catalizadores para la interacción y conectividad social.
- **Gestión ambiental y adaptación al cambio climático:** integrar consideraciones de riesgo ambiental y adaptación al cambio climático en la planificación urbana y la gestión de la infraestructura para reducir la vulnerabilidad a desastres naturales y otros eventos extremos. Un diseño urbano resiliente puede minimizar los daños, facilitar la recuperación y establecer una cultura de seguridad con visión preventiva y, así, dejar de ser reactivos solamente.
- **Gobernanza colaborativa:** fomentar la colaboración entre las diferentes partes involucradas (stakeholders) tanto de las autoridades gubernamentales municipales (seguridad, planificación urbana, desarrollo social, medio ambiente), la sociedad civil, el sector privado, la academia, los residentes y usuarios del espacio para abordar los riesgos de manera integral y coordinada.
- **Monitoreo y evaluación:** establecer procesos, procedimientos, métricas y mecanismos de seguimiento y evaluación para medir la efectividad de las políticas implementadas y realizar ajustes basados en la evidencia.

La adopción de políticas públicas municipales que integren CPTED en un modelo de seguridad humana y resiliencia puede generar una serie de beneficios, entre los que destacan:

- **Reducción de la delincuencia y la violencia:** al abordar las oportunidades situacionales y fortalecer la cohesión social.
- **Mejora de la percepción de seguridad:** fomentando un entorno construido que promueva la vigilancia natural, así como el sentido de propiedad y pertenencia.
- **Aumento de la resiliencia comunitaria:** fortaleciendo la capacidad de las comunidades para afrontar y recuperarse de situaciones traumáticas.
- **Promoción de la inclusión social:** creando espacios públicos seguros y accesibles para todas las personas.
- **Desarrollo urbano sostenible:** integrando consideraciones de seguridad y resiliencia en la planificación de mediano y largo plazo.
- **Mayor confianza ciudadana:** al demostrar un compromiso del gobierno local con la seguridad y el bienestar de sus habitantes.

Desafíos y oportunidades:

La implementación de este enfoque integrado presenta



desafíos, como la necesidad de superar la fragmentación institucional y política, movilizar recursos financieros y técnicos; así como garantizar la participación de la comunidad. Sin embargo, también ofrece oportunidades de gran impacto para transformar las ciudades en entornos más seguros, resilientes, incluyentes, sociales y habitables para todas las personas.

Para concluir. Diseñar políticas públicas municipales para la gestión de riesgos socio-urbanos con CPTED en un modelo de seguridad humana y resiliencia no es solo una necesidad, sino una inversión estratégica en el futuro de nuestras ciudades. Al adoptar un enfoque proactivo, integral y participativo, los gobiernos locales pueden construir comunidades más seguras, resilientes y donde el bienestar de cada ciudadano sea una prioridad fundamental.

El momento de actuar es ahora, para diseñar juntos futuros urbanos donde la seguridad humana y la resiliencia sean los pilares de un desarrollo sostenible e inclusivo.

Liderazgo 360

Articulista Invitada


Milagros Céspedes Álvarez

Coach PNL, Directora y Fundadora del Centro de Estudios de Seguridad para Latinoamérica. Involucrada en el mundo de seguridad desde hace 32 años. Miembro del Consejo Fundador de la Comunidad de Women In Security LAC de Asis Internacional. Perú

Lima, Perú.- Nos encontramos en una era donde los desafíos del liderazgo han dejado de ser lineales e imaginables. Hoy, las organizaciones enfrentan escenarios de incertidumbre constante, transformación digital acelerada y una creciente exposición a riesgos emergentes, muchos de ellos invisibles, como el cansancio mental, estrés crónico, fatiga, percepción alterada, desconexión humana o la deshumanización tecnológica.

Frente a este escenario, el liderazgo tradicional, basado exclusivamente en el control, planificación y supervisión, ya no es suficiente. Liderar hoy, requiere algo más profundo, más humano y más estratégico. Requiere activar tres inteligencias que conviven en cada líder: emocional, cognitiva y estratégica.

El primer pilar de este nuevo modelo de liderazgo, es la inteligencia emocional. Lejos de ser un “complemento blando”, se ha convertido en una habilidad crítica para tiempos inciertos. Permite reconocer y gestionar las propias emociones, leer el entorno emocional del equipo y crear espacios donde las personas se sientan escuchadas, valoradas y seguras.

Un líder con inteligencia emocional:

- Sabe regular el estrés propio y el de su equipo.
- Promueve entornos de confianza y comunicación abierta.
- Detecta signos tempranos de fatiga, desmotivación o crisis emocional.

En contextos donde la salud mental se ha vuelto un tema prioritario, esta inteligencia dejó de ser opcional, es necesario que forme parte del sistema de protección de las personas y de la organización.

Pero conectar con las emociones no es suficiente si no somos capaces de pensar con claridad en medio del caos, de la incertidumbre. Aquí entra en juego la segunda dimensión clave del liderazgo: la inteligencia cognitiva.

La inteligencia cognitiva permite analizar, aprender y decidir con pensamiento crítico. Un liderazgo que no permite que lo arrastre la urgencia, sino que toma distancia emocional para evaluar, priorizar y actuar con base en la información y situación.

Un líder con inteligencia cognitiva tiene:

- * Capacidad de desaprender y reaprender rápidamente.
- * Juicio lógico en la toma de decisiones.
- * Adaptabilidad frente a escenarios nuevos o complejos.

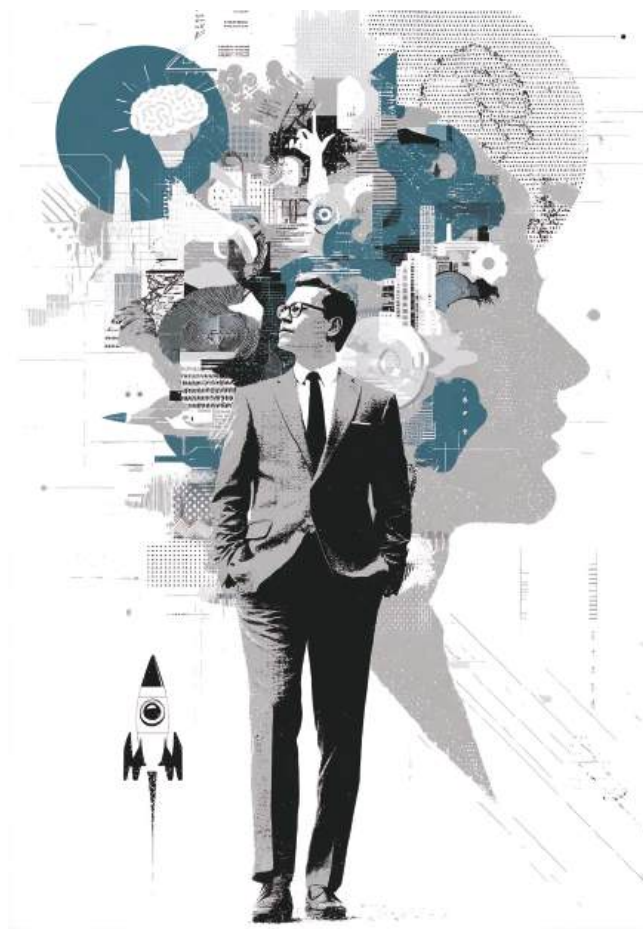
Actualmente los líderes necesitan procesar datos, leer tendencias, entender riesgos y actuar con claridad en entornos ambiguos. Sin pensamiento, no hay dirección.

Sin embargo, pensar bien no es suficiente si no hay una dirección clara. Comprender el presente debe ir de la mano con anticipar el futuro, y para eso, el liderazgo necesita también activar su inteligencia estratégica.

Esta tercera dimensión, la inteligencia estratégica tiene la capacidad de conectar el presente con el futuro, de alinear lo operativo con lo esencial, y de anticiparse antes que reaccionar.

Un líder con pensamiento estratégico:

• Cómo liderar con inteligencia emocional, cognitiva y estratégica en entornos complejos.



- Entiende que toda acción tiene un impacto humano, organizacional y reputacional.
- No improvisa, diseña y adapta con propósito.
- Integra personas, procesos y tecnología en una visión lógica.

En un entorno de riesgos emergentes, como los derivados de la Inteligencia Artificial, el cambio climático o la disrupción tecnológica, esta capacidad es esencial para guiar a otros con rumbo y coherencia.

El verdadero liderazgo integra las tres inteligencias. No se trata de elegir una de ellas sino de equilibrarlas en función a la situación, al equipo y al momento. La inteligencia emocional permite contener, la cognitiva comprender y la estratégica actuar con sentido.

Liderar con las tres es pasar del control a la conciencia, de la reacción a la anticipación, del procedimiento a la cultura.

El liderazgo del futuro no se define por lo que se logra, sino por cómo cuida, piensa y transforma. Y en tiempos donde la tecnología avanza más rápido que nuestra capacidad de asimilarla, un líder valioso será aquel que comprenda el impacto humano de cada decisión, y guíe desde la emoción, el pensamiento y la visión.

“El liderazgo que transforma no es el que controla más, sino el que siente con empatía, piensa con claridad y actúa con propósito. Porque solo quien lidera con conciencia puede guiar a otros con seguridad en tiempos de incertidumbre”.

Expo Seguridad & Telecom Centroamérica prende las alarmas... en la innovación

- La primera edición de la muestra en Guatemala superó las expectativas y se consolida como el nuevo epicentro latinoamericano para fabricantes, integradores y distribuidores del sector.
- Más de 1,600 asistentes profesionales acudieron al evento en solo dos días.
- Participaron 36 stands, 120 marcas y más de 15 fabricantes directos.
- Se realizaron 40 conferencias especializadas en tendencias y soluciones de seguridad.

Ciudad de Guatemala, Guatemala.- Cuando Leonardo Luna Varas, presidente de Expo Seguridad & Telecom Guatemala, pensó en llevar a la región un encuentro especializado en tecnología y soluciones para la industria de la protección y el resguardo, apostaba por un mercado potencialmente fuerte, pero subestimado; lo que no imaginó fue que la respuesta del ecosistema sería abrumadora.

“Nos vamos contentos”, resumió Luna al cierre de la primera edición de la feria: el evento reunió a más de 1,600 asistentes profesionales en tan solo dos días, duplicando las expectativas iniciales. A lo largo del recinto ferial se distribuyeron 36 stands que representaron a más de 120 marcas de seguridad electrónica, muchas de ellas con presencia directa de los fabricantes.

La cita congregó a los principales distribuidores e integradores de Guatemala, El Salvador, Nicaragua, Costa Rica y Honduras, convirtiéndose en un escaparate regional



sin precedentes: “El público que asistió fue un nicho ávido de conocimiento. Hemos logrado que se encuentren cara a cara los fabricantes con los usuarios finales”, enfatizó Luna, destacando uno de los valores diferenciales del evento: su enfoque práctico y de networking real.

En el marco del encuentro se desarrollaron 40 conferencias especializadas, donde expertos abordaron temas clave como vigilancia inteligente, ciberseguridad, automatización, control de accesos y nuevas amenazas emergentes. La agenda académica fue, según los organizadores, un imán para profesionales y decisores que buscaban actualizarse y comparar soluciones.

La respuesta del sector no se limitó al número de asistentes. También hubo una alta participación de fabricantes internacionales, muchos de los cuales no solo se presentaron este año, sino que ya confirmaron su regreso en la próxima edición: “Muchos no apostaron por una primera feria, pero los que vinieron se convencieron de que habían perdido la oportunidad de mostrarse. Hoy ya están comprometidos para el próximo año”, relató Luna.

La visión a futuro del equipo organizador no se detiene. Para 2026, el calendario contempla la realización de nuevas ediciones en Nicaragua, Paraguay, Guatemala y Ecuador, consolidando una red de ferias hermanas que llevarán la bandera de la seguridad electrónica por toda Latinoamérica.

“La industria va a crecer, y tendrá mayores escenarios para mostrar todas las soluciones que año a año desarrolla”, sostuvo el presidente de la feria.

Buena parte de este éxito tiene su origen en la estrategia previa de la organización, que durante más de una década ha desarrollado 22 foros temáticos en diferentes ciudades del continente. Estos encuentros permitieron mapear nichos, generar comunidad y establecer vínculos con los canales locales antes de lanzar una feria de esta envergadura: “Sin los 10 años que llevamos haciendo foros, no hubiéramos podido encontrar el momento ni el lugar ideal para esta primera feria en Centroamérica”, reconoció.

Leonardo Luna Varas aprovechó para agradecer el respaldo del medio especializado **Más Seguridad Magazine**, que han acompañado la evolución del proyecto desde su origen: “Esta revista ha estado con nosotros desde hace 11 años, cuando iniciamos con los foros y eventos de seguridad, apostando por la profesionalización del sector”, rememoró.

Expo Seguridad & Telecom Guatemala llegó para quedarse como el reflejo de una industria en transformación que empieza a hablar con acento propio, desde el corazón de América Latina.

Simbolismo religioso en el terrorismo contemporáneo



Articlista Invitado

Edison Cadena Ayala

MSC, CPO, CPOI, CSSM
gerente de SEINNATIONAL CIA. LTDA.
Ecuador

Quito, Ecuador.- El uso de símbolos sagrados en actos terroristas pone de manifiesto una dualidad inquietante: la fe, fuente de consuelo y unión, se distorsiona cuando se utiliza para justificar la violencia. Movimientos extremistas reinterpretan emblemas ancestrales, dotándolos de un aura mística que legitima sus intenciones y desvirtúa el mensaje religioso. Este fenómeno nos invita a cuestionar cómo la manipulación simbólica puede convertir lo que une en un arma de división.

Desde tiempos inmemoriales, la religión ha otorgado identidad y pertenencia a las comunidades por medio de rituales y símbolos concebidos para brindar consuelo. No obstante, en ciertos contextos, estos mismos elementos se han transformado en instrumentos para legitimar la violencia. Resulta conmovedor ver cómo, en momentos de crisis, el símbolo que una vez inspiró paz se degrada y se utiliza para fines de dominio.

Durante épocas como las Cruzadas y la Inquisición, líderes utilizaron la fe con fines políticos, transformando símbolos sagrados en emblemas de poder. Hoy, grupos extremistas recurren a este mismo recurso para construir ideologías que apelan a la emoción y fomentan la división. Cada signo o caligrafía posee el poder de conmovernos, transmitiendo historias de dolor y esperanza, aunque su mensaje se vea empañado por la violencia.

El verdadero poder de un símbolo radica en su capacidad de conectar con el alma. Cuando se apropia de manera desvirtuada, se traiciona su significado original y se hiere la fe de aquellos que lo ven como un puente hacia la paz. Esta manipulación exige que observemos con empatía tanto a las víctimas como a las comunidades que, pese al fanatismo, mantienen viva la esencia de sus creencias.

Ejemplos de esta resignificación se evidencian en organizaciones que, adoptando emblemas tradicionalmente asociados a la paz, transmiten mensajes de martirio y destino divino. Con un lenguaje visual cargado de misticismo, transforman imágenes de consuelo en llamados a la acción. La difusión de estas narrativas, especialmente a través de redes sociales, refuerza una identidad basada en la distorsión del mensaje original.

Es fundamental recordar que estos casos no reflejan la esencia de ninguna fe, sino desviaciones utilizadas para fines de radicalización y control. La manipulación del simbolismo religioso polariza comunidades y

“El terrorismo nace del odio, se basa en el desprecio de la vida del hombre y es un auténtico crimen contra la humanidad”. **Juan Pablo II**



perpetúa ciclos que dificultan el diálogo interreligioso y la reconciliación. Comprender esta dinámica nos invita a diferenciar la genuina expresión espiritual de la instrumentalización mística que fomenta la violencia.

La resignificación del simbolismo religioso para fines violentos es una paradoja que hiere la esencia misma de la fe genuina. Cuando emblemas destinados a unir, transforman su mensaje en instrumentos de radicalización, la sociedad se ve forzada a cuestionar la integridad de sus creencias. Reconocer esta distorsión se convierte en un llamado a resguardar el significado original de los símbolos sagrados, restaurando su capacidad de inspirar paz y unión. Solo a través del diálogo y la empatía podremos devolver a la fe su papel como puente hacia la esperanza y la cohesión social.

Autoridad sin liderazgo: el riesgo que nadie vigila

Articulista Invitado

Pedro Oré



Miembro de Asis Internacional. Oficial Certificado de Protección – CPO. Oficial Certificado en Investigaciones – CIO. Máster in Business Administration. Máster en Gestión y Dirección de Equipos. Profesional en Administración de Negocios Internacionales. Oficial de Mar de la Marina de Guerra del Perú (r).
Perú.

Lima, Perú.- En el universo corporativo, donde abundan los procesos y las tecnologías más sofisticadas, seguimos dejando fuera una de las variables más determinantes (y más subestimadas) en la ecuación de la seguridad organizacional: el liderazgo ineficaz.

Sí, ese liderazgo que no aparece en los informes trimestrales ni auditorías, pero que genera pérdidas silenciosas, erosiona la cultura interna y, en casos extremos, habilita fallas estructurales que ningún sistema de vigilancia puede prevenir.

En el mundo de la seguridad, el liderazgo es un multiplicador: Potencia o destruye. No hay punto medio. Un mal líder puede convertir una política impecable en letra muerta, una estrategia brillante en burocracia vacía, o un equipo capacitado en una agrupación apática, reactiva y silenciosa.

El problema es que estos costos no se ven a simple vista, pero están en las decisiones que no se toman, en las alertas que no se comunican, en las renuncias no explicadas y en los errores que, por miedo o hartazgo, nadie se atreve a corregir.

¿Qué te parece si conocemos tres formas silenciosas en que el mal liderazgo destruye la seguridad?

- Cultura de silencio: cuando el líder impone miedo o indiferencia, el equipo aprende a callar. Y en seguridad, el silencio no es neutral, es combustible para el riesgo. Si un colaborador nota una anomalía pero percibe que su jefe no escucha, no reacciona o, peor aún, castiga al mensajero, simplemente deja de informar. Bienvenido al terreno fértil de las crisis.
- Desconexión emocional: la seguridad no es solo técnica, es emocional. Un equipo conectado, que siente orgullo y pertenencia, cuida. Un equipo que se siente desprotegido o despreciado, simplemente cumple (y a veces ni eso).

La verdadera prevención comienza en el liderazgo. Seamos claros, un buen líder reduce incidentes.

Cuando el líder falla en conectar, inspirar y contener, la protección se vuelve mecánica, sin alma, y por tanto, frágil.

- Falta de visión sistémica: El mal líder piensa en tareas, no en propósitos. Se obsesiona con los reportes y los procedimientos, pero desconoce el impacto real del contexto humano en los indicadores. Ve el “qué”, pero no el “por qué”. El resultado: una seguridad orientada al cumplimiento, no al compromiso. Y ya sabemos lo que ocurre con las reglas sin convicción.

¿Por qué seguimos tolerando malos líderes?

Porque medimos lo que es fácil de medir, porque confundimos experiencia técnica con capacidad de liderazgo, porque seguimos promoviendo jefes que “saben del tema”, pero no saben de personas, y en seguridad, donde la colaboración, la comunicación y la anticipación son vitales, eso es una bomba de tiempo con cuenta regresiva con súper velocidad.

¿Solución?: valorar el liderazgo como un activo estratégico de protección

La verdadera prevención comienza en el liderazgo. Seamos claros, un buen líder reduce incidentes, ¿cómo? Generando confianza, escuchando con intención, dando sentido al trabajo cotidiano, construyendo equipos emocionalmente seguros y motivados. No se trata de convertir al jefe de seguridad en un coach espiritual. Se trata de entender que el riesgo también es humano, y que liderar con inteligencia emocional, humildad y visión es parte fundamental de cualquier estrategia robusta de protección.

Invertimos millones en infraestructura, en consultorías, en sistemas, en certificaciones, pero si no atendemos el factor humano del liderazgo, todo eso seguirá operando sobre cimientos frágiles. La pregunta que toda empresa debería hacerse es sencilla, pero incómoda:

“¿Quién cuida a los que cuidan?”

Y más aún: “¿Quién los lidera?” Porque si el liderazgo no inspira, no comunica, no protege, entonces el riesgo ya entró, y les aseguro que no tocará la puerta.



La Extorsión

Articlista Invitado

**José Jaramillo Díaz**

Mg., CPP Ejecutivo en seguridad integral con más de 30 años de experiencia, Magister en Gestión de Riesgos, Estrategia Marítima. Es CPP (Certified Protection Professional) de ASIS International y consultor en Sistemas Integrales de Seguridad. Es además docente internacional para la Certificación CPP y expositor en foros nacionales e internacionales.

Perú

· Es importante considerar que existen numerosas personas que, aprovechándose del contexto, buscan obtener beneficios, principalmente económicos, mediante llamadas falsas.

(Parte 1 de 2)

Lima, Perú.- La extorsión es un delito que se materializa cuando el extorsionador obliga a una persona u organización a entregar dinero, bienes u otras ayudas, para lograr esto hace uso de la intimidación, la amenaza o incluso el uso de la fuerza. Estas acciones afectan directamente la libertad y el patrimonio de quien la sufre. La gravedad de la extorsión se incrementa, de acuerdo a quien o quienes la ejecutan, llegando a considerarse en muchos de los casos como delincuencia organizada, de conformidad con la forma en que se lleve a cabo.

Las extorsiones pueden presentar diversos objetivos, y no siempre es la obtención de dinero. Algunos de los más comunes son: Obtener Dinero o Bienes Materiales, es el objetivo más frecuente, exigiendo a la víctima pagos en efectivo, transferencias bancarias o el empleo de criptomonedas; Ejercer Poder o Control, se busca mantener influencia o someter a personas u organizaciones, afectando considerablemente su capacidad de toma de decisiones y autonomía; Forzar a Tomar Decisiones o Tener Ciertas Conductas, se utiliza para obligar la entrega de información, cambio de votos, renunciar a un determinado cargo; Obtención de Información sensible y/o Confidencial, es una forma específica de las extorsiones cibernéticas y buscan acceder a bases de datos de entidades diversas como financieras, empresariales, gubernamentales, entre otras; Venganza o Castigo, aunque es la menos común de las extorsiones, el objetivo no es el económico, lo que se busca es perjudicar a la víctima por encima del beneficio económico. En todos los casos, el mecanismo básico es siempre generar temor, miedo y la presión psicológica para conseguir el objetivo deseado.

Es fundamental comprender que los procesos de extorsión generalmente comienzan con la recopilación de información sobre la víctima. Para ello, los extorsionadores recurren a diversas fuentes y técnicas, que se describen a continuación:

- A. Uso de noticias públicas o eventos sociales.-** Los extorsionadores aprovechan información disponible públicamente a través de medios de comunicación abiertos, como noticias, eventos sociales y rumores difundidos en redes o canales informativos.
- B. Marcaje o espionaje físico.-** Consiste en la observación directa de la víctima para recolectar datos relevantes que puedan ser utilizados en el proceso de extorsión.
- C. Ingeniería social.-** Mediante técnicas de manipulación psicológica, los delincuentes inducen a las personas a proporcionar información voluntariamente. Esto puede lograrse a través de encuestas, concursos, correos electrónicos engañosos, entre otros métodos.
- D. Acceso a bases de datos.-** Se realiza mediante el acceso ilegal a bases de datos de personas, empresas, instituciones u organizaciones, de donde se obtienen datos como nombres, teléfonos, direcciones de correo electrónico, domicilios e incluso información financiera.
- E. Redes sociales.-** Las redes sociales representan una fuente significativa de información sensible, ya que muchos usuarios publican detalles personales que pueden ser aprovechados por los extorsionadores.



- F. Correos electrónicos fraudulentos y técnicas de hackeo.-** A través del envío de correos que aparentan provenir de fuentes confiables, los delincuentes buscan obtener información directa o infectar dispositivos mediante técnicas como phishing, sniffing/snooping, inyecciones SQL, y el uso de rootkits, keyloggers, gusanos, virus o troyanos.
- G. Uso de terceros.-** Los extorsionadores se comunican con familiares, amigos, empleados u otras personas cercanas a la víctima, haciéndose pasar por entidades o individuos de confianza para obtener información de forma indirecta.
- H. Llamadas telefónicas aleatorias.-** Se realizan llamadas al azar con el objetivo de recolectar datos personales de quienes contestan, así como información sobre sus familiares.

La extorsión no actúa de manera aislada, sino que se encuentra profundamente interrelacionada con otras economías criminales, como se describe a continuación:

- I. Lavado de dinero.-** Existe una tendencia creciente a invertir las ganancias obtenidas de manera ilícita en mercados legales, con el objetivo de legitimar los fondos provenientes de actividades delictivas, incluida la extorsión.
- II. Tráfico de drogas.-** La extorsión se vincula al tráfico de drogas a través del control territorial. Los grupos criminales cobran "impuestos" por la venta y distribución de estupefacientes en zonas específicas, consolidando su poder económico y social.
- III. Trata de personas.-** Las redes de trata de personas aprovechan la migración ilegal para extorsionar y manipular tanto a las víctimas como a sus familiares, explotándolos económica y emocionalmente.

Continuará...

Vigilancia y seguridad privada: la clave está en la especialización

Articuliasta Invitado



Leonardo Borrero

Especialista en administración de la seguridad
Seguridad Magister en administración de cadenas de suministro.
Colombia

- Las empresas que prioricen el aprendizaje continuo liderarán el mercado, ofreciendo soluciones adaptadas a cada industria.

Bogotá, Colombia.- En un mundo donde las amenazas evolucionan y los riesgos se diversifican, el personal de vigilancia y seguridad privada enfrenta el reto de actualizar y especializar sus habilidades. La certificación inicial proporciona una base operativa, pero la verdadera diferencia radica en la especialización según cada línea de negocio. PROISO CONSULTORES ha identificado que la capacitación segmentada no solo mejora el desempeño, sino que fortalece la percepción de seguridad y confianza en el servicio prestado.

Más allá de la formación convencional

Las academias de formación en seguridad brindan entrenamiento certificado, pero este no es suficiente para responder a los riesgos específicos de sectores como el hospitalario, industrial, logístico o financiero. Es aquí donde entran en juego las técnicas de Reskilling y Upskilling.

- Reskilling (Recalificación): capacitación en nuevas habilidades para asumir roles distintos. Ejemplo: un vigilante de control de accesos que recibe formación en defensa alimentaria, aprendiendo a identificar riesgos de contaminación, aplicar protocolos de bioseguridad y reforzar la seguridad en áreas críticas de producción.
- Upskilling (Mejora de habilidades): perfeccionamiento de competencias existentes. Ejemplo: un vigilante hospitalario que se capacita en gestión de pacientes agresivos y protocolos de emergencia, desarrollando habilidades avanzadas en comunicación de crisis y manejo de situaciones de alto estrés sin comprometer la seguridad del entorno.

Beneficios de la especialización

- Diferenciación competitiva: empresas con personal altamente capacitado ofrecen un valor agregado real.
- Reducción de riesgos: Mayor capacidad para identificar amenazas y responder eficazmente.
- Fidelización del cliente: Los clientes confían en empresas que entienden sus necesidades específicas.
- Optimización de costos: Equipos especializados operan con mayor autonomía y eficiencia.
- Mayor satisfacción del personal: La capacitación fomenta el crecimiento profesional y reduce la rotación.

Caso de éxito

Un claro ejemplo del impacto de la especialización ocurrió en Agrícola Himalaya, donde nuestra compañía transformó la cultura de seguridad de la empresa. Los vigilantes, formados en seguridad física, no contaban con competencias en defensa alimentaria. Mediante un enfoque de aprendizaje experiencial y gamificación, que combinó teoría con simulaciones prácticas, lograron aplicar nuevas estrategias en inspección de carga, control de accesos y detección de riesgos en la producción.

El resultado: reducción de vulnerabilidades, mejora en la capacidad de respuesta y fortalecimiento de la seguridad en la planta, convirtiendo a la seguridad privada en un pilar clave dentro de la estrategia de inocuidad en toda su cadena de producción.

El alto costo de no especializarse

Si bien especializar al personal puede considerarse una inversión

significativa, no hacerlo resulta aún más costoso, tanto en términos operativos como en la alta rotación del personal, lo que genera costos adicionales en procesos de selección, inducción y entrenamiento recurrente. Paradójicamente, el riesgo de especializar al personal es que estos se vuelvan más atractivos en el mercado y busquen nuevas oportunidades. Sin embargo, cuando los vigilantes sienten que encajan en su rol, que su labor es valorada y que tienen oportunidades de crecimiento dentro de la empresa, es más probable que permanezcan en la organización, reduciendo así la fuga de talento y fortaleciendo la cultura organizacional.

Un caso que lo ejemplifica ocurrió en un hospital donde un vigilante, sin formación en seguridad hospitalaria, no supo manejar una contingencia en la madrugada. En una unidad de urgencias, un paciente psiquiátrico en estado crítico se tornó violento, intentando agredir al personal de salud y dañar el mobiliario. El guardia, sin formación en manejo de crisis hospitalarias ni protocolos de contención de pacientes agresivos, reaccionó de forma incorrecta: en lugar de aplicar técnicas de intervención seguras, utilizó fuerza desmedida, lo que derivó en una lesión grave del paciente y una demanda contra el hospital.

La falta de entrenamiento no solo afectó la operatividad del hospital, sino que generó costos legales, reputacionales y operativos. Además, la rotación del personal de seguridad en la institución aumentó, ya que los vigilantes asignados a la unidad, al no contar con el entrenamiento adecuado, preferían abandonar el cargo antes que enfrentarse a situaciones que no estaban preparados para manejar. En contraste, en entornos donde los vigilantes han recibido una formación especializada y saben exactamente cómo actuar en situaciones críticas, se sienten más seguros en su puesto, comprometidos con su labor y con menos intención de abandonar la empresa.

En conclusión, la seguridad privada no puede depender de una formación genérica. Adoptar estrategias de Reskilling y Upskilling, junto con una segmentación precisa del conocimiento, es la clave para fortalecer las competencias del personal y elevar la calidad del servicio.

Las empresas que prioricen el aprendizaje continuo liderarán el mercado, ofreciendo soluciones adaptadas a cada industria. nuestra firma ha demostrado que la especialización y el aprendizaje experiencial generan un impacto positivo en la seguridad y la continuidad del negocio. La protección no es estática: evoluciona, y con ella deben evolucionar quienes la ejercen.



fuerza gremial que profesionaliza la seguridad privada en Colombia



- Representa a más de 30 empresas de seguridad privada y 30 mil trabajadores en Colombia.
- Impulsa reformas normativas y combate la informalidad en el sector.
- Ofrece certificaciones y capacitaciones avaladas por universidades y entes técnicos.

Beatriz Canales

Barranquilla, Colombia.- La Asociación Colombiana de Seguridad (ASOSEC®) ha tejido, a lo largo de más de tres décadas una red de alianzas, formación, defensa jurídica y liderazgo gremial que la posiciona como un actor relevante en el sector de la seguridad privada del país.

“Somos una asociación civil sin ánimo de lucro que promueve el desarrollo del sector de la seguridad privada en Colombia. Nacimos a mediados de los años 90 en la región Caribe, y en 2012 nos consolidamos de manera independiente”, señala Gabriel Berrío Álvarez, presidente de **ASOSEC**, en entrevista exclusiva para **Más Seguridad Magazine**.

ASOSEC® representa actualmente alrededor de 30 empresas y a cerca de 30 mil trabajadores del sector de la seguridad privada. Su labor abarca asesoría jurídica, acompañamiento administrativo, representación gremial ante entidades de gobierno, así como el impulso a reformas normativas.

Una de sus mayores luchas es contra la informalidad: “La proliferación de empresas ilegales sigue siendo uno de los principales desafíos del sector. Por eso, pedimos mayor vigilancia y control por parte de la Superintendencia de Vigilancia y Seguridad Privada”, enfatiza Gabriel Berrío.

Desde sus oficinas en Barranquilla, lidera espacios de articulación como el Congreso Nacional de Seguridad, que en su edición 2024 puso sobre la mesa temas como cambio climático, terrorismo y gestión de riesgos, generando mesas de trabajo entre autoridades, empresarios y académicos.

Una de las apuestas más visibles ha sido el fortalecimiento profesional del recurso humano del sector, vía una robusta agenda de capacitación que abarca desde

el personal operativo hasta el administrativo y directivo; asimismo, ASOSEC ofrece webinars, talleres, diplomados y certificaciones avaladas por entes técnicos.

Los temas son variados: derechos humanos, uso progresivo de la fuerza, inteligencia corporativa, lavado de activos, seguridad electrónica, liderazgo, marketing y gestión del riesgo bajo ISO 31000: “Buscamos que nuestros afiliados estén a la vanguardia no solo en normatividad, sino en innovación tecnológica y mejores prácticas internacionales”, explica el presidente de ASOSEC®.

Además del trabajo local, la organización ha tendido puentes con asociaciones de México, Panamá, Ecuador y otros países de la región. En Colombia, participa en un Comité Intergremial de Seguridad junto a otras asociaciones, y su presidente es miembro activo de redes de apoyo y calidad institucional para el Caribe colombiano.

“Queremos fortalecer alianzas internacionales que nos permitan intercambiar conocimiento, homologar certificaciones y avanzar juntos en el desarrollo del sector. La seguridad es transversal a todas las actividades productivas y requiere estándares globales”, afirma Gabriel Berrío.

Consciente de su rol en el tejido social, ASOSEC® también promueve la inclusión de mujeres en puestos de liderazgo, el cumplimiento normativo y el respeto a los derechos laborales. Además, apuesta por la transformación digital y el fortalecimiento de la comunicación institucional como pilares de confianza pública.

De cara al 2025, su meta es crecer al menos dos afiliados por mes y consolidarse como el gremio nacional de referencia en seguridad privada: “Queremos un sector fuerte, visible, profesional, y con una representación gremial que verdaderamente defienda los intereses de las empresas serias”, concluye Gabriel Berrío Álvarez. 

ASOSEC[®]

ASOCIACIÓN COLOMBIANA DE SEGURIDAD

20 CONGRESO NACIONAL 25 DE SEGURIDAD

Contexto Geopolítico, Impacto y
Estrategias de Crecimiento en el
Sector Empresarial



17, 18 y 19
Septiembre



BARRANQUILLA
Colombia



COUNTRY
INTERNATIONAL HOTEL

Inscríbete Aquí



Apoyan:

CON SEGURIDAD
Magazine Latam

MÁS SEGURIDAD
Magazine



📞 312 686 4435 - 301 539 7542

📞 605 305 6398

🌐 www.asosec.co

Cómo tener éxito en la gestión de seguridad corporativa



Articulista Invitado

Nelson Castro

Head of Trust and Safety at Rappi Int., CPP,
MBA University of Liverpool, England
Colombia

Enfoque para organizaciones tecnológicas

(Parte 1 de 2)

Bogotá, Colombia- A lo largo de mi carrera profesional, después de haber usado el uniforme militar y pertenecer al servicio secreto, posteriormente enfocando mi visión a la empresa privada permitiendo mejorar mis alcances profesionales y de liderazgo en empresas tecnológicas, ostentando mi cargo actual Head of Trust and Safety para la organización Rappi Internacional, fui invitado por **Más Seguridad Magazine** a compartir mis pensamientos y experiencias en un tema apasionante para mí que es la seguridad corporativa aplicada a corporativos tecnológicos y que seguramente será del agrado de todos en relación a algunas estrategias clave para los profesionales de seguridad, particularmente aquellos dedicados a compañías tecnológicas.

La gestión de la seguridad corporativa ha evolucionado significativamente, y hoy más que nunca es esencial incorporar prácticas de seguridad efectivas y adaptadas a los desafíos específicos del entorno tecnológico y aún más en América Latina, donde se exige una combinación de conocimientos tradicionales de protección y comprensión profunda de las dinámicas empresariales. Las empresas deben integrar la seguridad en todas las fases del desarrollo y adaptarse constantemente a las amenazas emergentes, sin sacrificar la innovación.

A medida que los riesgos evolucionan, también lo deben hacer las estrategias y las herramientas de seguridad. -Es fundamental que los líderes de protección, especialmente aquellos dedicados a las empresas tecnológicas, lideren con visión estratégica, integrando la seguridad en la cultura organizacional y ayudando a la firma a alcanzar sus objetivos de manera segura y eficiente-. Para ello se debe tener un comienzo sobre lo básico tal como:

1. **Definición y establecimiento de los requerimientos de seguridad desde el inicio:** el cual considero como primer paso en la gestión de seguridad corporativa en empresas tecnológicas estableciendo claramente los requisitos de seguridad al inicio de cualquier proyecto. Tal vez esto genera un esfuerzo mayor en relación a la protección de datos, gestión de accesos y respuesta ante incidentes. Si miramos en detalle estos parámetros, aseguramos que la

seguridad no sea un añadido posterior -como suele ocurrir en algunas organizaciones-, sino un pilar fundamental desde el comienzo.

2. **Documentación robusta de procesos y políticas:** quiero resaltar este aspecto para lograr trazabilidad y control, lo cual es imperioso crear documentación exhaustiva que detalle todos los procesos, políticas y procedimientos relacionados con la seguridad. Esta documentación no solo facilita el seguimiento y la verificación de la implementación, sino que también establece una base sólida para la mejora continua y aspectos de compliance.
3. **Implementación de herramientas de gestión de versiones:** No obstante es serlo sino parecerlo y para ello las herramientas de gestión de versiones son cruciales para garantizar trazabilidad, especialmente cuando se trata de código fuente y documentación. Estas herramientas permiten rastrear cambios y verificar que se mantengan los estándares de seguridad en cada nueva iteración del softwares o programas de gestión.

Continuará...





EXPO
SEGURIDAD
& TELECOM
COSTA RICA



SAN JOSÉ
COSTA RICA
12 Y 13 DE NOVIEMBRE 2025
HOTEL BARCELÓ SAN JOSÉ PALACIO



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

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

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

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

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

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

Para más información sobre el evento.

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

www.exposeguridadcostarica.com



Tecnología que protege



**Un espacio donde
usted podrá:**

- **Posicionar su marca** entre los líderes que mueven la industria.
- **Generar contactos** clave para nuevas oportunidades de negocio.
- **Participar** en la mayor red de networking del sector.



**Reserve su stand en
securityfaircolombia.com
o escaneando el código QR**



GREMIOS ALIADOS



ORGANIZAN



MEDIOS ALIADOS

