

MÁS SEGURIDAD

Magazine

19

ANIVERSARIO

¡Y vamos
por más!

Octubre 2026/ No. 165 / Año 19



México y LaTAm /precio \$60.00MX





CAPÍTULO
MÉXICO 217

Contáctanos en nuestro linktree

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



Afíliate y sé parte de nuestra comunidad.


**MEMBRESÍA
INTERNACIONAL**
130 USD


CAPÍTULO
MÉXICO 217
**MEMBRESÍA
CAPÍTULO MÉXICO**
\$5,650 MXN


CAPÍTULO
MÉXICO 217
**RENOVACIÓN
CAPÍTULO MÉXICO**
\$4,687.50 MXN

BENEFICIOS *Membrería*



Reuniones mensuales con conferencistas
de 1.er nivel (sujeto a disponibilidad)



Comunidades temáticas para
intercambiar conocimiento.



Webinars sin costo con instructores
certificados y cursos que otorgan CPE's.



Newsletter semanal con información
relevante.



Presencia del capítulo en los mejores
eventos de seguridad en México.



Chat privado exclusivo para socios
activos.



Convenios con descuentos exclusivos
en productos y servicios.



Acceso a guías y estándares de ASIS
Internacional.



Bolsa de trabajo especializada
en seguridad.



Conexión con más de 34,000
profesionales de seguridad en el mundo.

Más información 55 1321 1289
socios@asis.org.mx

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

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

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

DG CREATIVE
DISEÑO Y DESARROLLO VISUAL

CLAUDIA IVETTE MARTÍNEZ GUTIÉRREZ
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

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

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@globaldefense.com.mx

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

JORGE MERCADO ABONCE
SERVICIOS JURÍDICOS INTEGRALES

ANAZALDO-MARTÍNEZ-MERCADO
DIRECCIÓN JURÍDICA
juridico@revistamasseguridad.com.mx

ASISTENCIA A CLIENTES
atencion@revistamasseguridad.com.mx

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

SÍGUENOS EN:

 Revista Más Seguridad

 @revmasseguridad

 revistamasseguridad

 revmasseguridad

 Revista Más Seguridad

 Revista Más Seguridad

 Más Seguridad Magazine

Revista Más Seguridad Año 19, No 165, Octubre 2026, Publicación mensual de **Grupo Editorial MS Global S. de R.L. de C.V.**, con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 5555272279 / +52 5528732719. Editor responsable: **Humberto Mejía Hernández**. Certificado de Reserva 04-2022-050614181900-102 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No. 11483 y Certificado de Licitud de Título No. 13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: Grupo Mejía Impresores, calle La Poza No. 72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel: +52 5518947067.

La Inteligencia Artificial nos alcanzó

En el mundo, la Inteligencia Artificial -IA- ya está presente en todos los sectores industriales y México no es ajeno a esta tendencia pues se ha vuelto una poderosa arma y muchos no la están aprovechando en sus operaciones. Hoy, el rastreo satelital, videovigilancia, control de accesos y operaciones financieras, entre otros nichos de la seguridad, ya son usuarios de la IA.

Rastreo satelital y seguridad en transporte de carga

Al respecto, la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital -AMESIS-, señaló que hay un “bombardeo” de motores de IA como LLMs y SMLs, con lo que muchas compañías están creando, pero el reto es entender cómo usarlos y atreverse a usarlos. La tendencia en el mundo es que estas herramientas lleven a un avance agigantado en los próximos tres años.

Dentro de la AMESIS había empresas que se dedicaban a generar proyectos de videovigilancia, control de accesos o automatizaciones, pero siempre existían limitaciones en el software existente en el mercado. Hoy con motores como LLM, permite rastrear objetos y personas dentro del área de trabajo, movimientos o actividades sin falla alguna, creando un agente al saber utilizar Cloud.

Respecto al monitoreo y localización de vehículos de carga, se enfrentan a requerimientos especiales como conexión a internet, avisos vía celular sobre apertura de puertas, encendido de motores o botones de pánico. Hoy os asociados de AMESIS a través de una torre de control virtual, ofrecen monitoreo dedicado, con agentes especializados dentro de sus sistemas.

Para la AMESIS, la IA combate el robo al transporte de carga al pasar de un simple rastreo satelital reactivo a modelos predictivos que anticipan los atracos con minutos u horas de ventaja.

La IA puede analizar grandes volúmenes de datos históricos y en tiempo real para identificar patrones y predecir posibles robos. Al detectar anomalías como desvíos de ruta, paradas no programadas o cambios bruscos de velocidad, puede alertar a las empresas de rastreo y autoridades...

Integración de IA y Seguridad Híbrida en infraestructuras críticas

Otro ejemplo de esta tendencia es la compañía internacional Prosegur Security, quien afirma que en un entorno global donde las amenazas evolucionan a ritmo acelerado y los eventos imprevistos desafían constantemente el orden establecido, el enfoque tradicional de la seguridad ha dejado de ser suficiente. Hoy, la protección efectiva exige una evolución estructural hacia la Seguridad Híbrida, un modelo integral que orquesta la más avanzada tecnología, el análisis de datos en tiempo real y la operación humana altamente capacitada.

En México, el impacto de un fenómeno meteorológico para las operaciones de una empresa no termina cuando éste se aleja. Inundaciones, interrupciones eléctricas, daños en instalaciones, restricciones de movilidad, pérdida de conectividad y riesgos para el personal pueden comprometer cadenas de suministro y detener operaciones durante horas o incluso días.

Para Prosegur, la tecnología tiene mayor valor cuando forma parte de una estrategia de continuidad prediseñada. El primer paso es realizar una evaluación de riesgos para identificar los activos, procesos y zonas cuya interrupción tendría mayor impacto. Posteriormente, se pueden definir niveles de cobertura, protocolos de escalamiento y mecanismos de comunicación entre seguridad, operaciones y responsables de la infraestructura.

La empresa ha consolidado este nuevo paradigma apoyándose en su Centro de Operaciones de Seguridad Inteligente (ISOC, por sus siglas en inglés). El mensaje central de esta transformación es claro: la IA y el análisis masivo de datos no llegan para reemplazar al personal de seguridad, sino para potenciar y complementar su capacidad de acción. Al procesar grandes volúmenes de información en tiempo real, los profesionales pueden anticiparse a los riesgos antes de que se materialicen. Aquí solo dos ejemplos de IA para la seguridad corporativa, pero aplicaciones y casos de éxito ya son muchos. 🌐



¡Cumplimos 19 años!

Estamos de festejo por el cumpleaños de nuestra publicación **Más Seguridad Magazine**. Gracias al apoyo de patrocinadores, lectores, colaboradores, fuentes de información y articulistas invitados llegamos al año 19 de la creación y publicación ininterrumpida de este medio especializado, que además hoy goza de la aceptación de la industria a nivel nacional e internacional.

Aciertos, errores, frustraciones, evolución constante y mucho empeño definen el trabajo editorial y publicitario que a lo largo de estos años hemos desarrollado ¿Y saben qué?

¡Vamos por más!

Gracias por ser parte de la familia Más Seguridad Magazine



5 Más video para vigilar y más espacio para guardarlo con Hikvision

6 Productos de Ajax compatibles con ONVIF

8

Incorpora PIMECSA la marca LAMPRO



12

Bull Safe: la evolución de la caja fuerte



15 Seguridad vs incendios

20 Nace el Ecosistema Queretano de Ciberdefensa

26

Nueva oferta en custodias ofrece SAMAHE



42 SAR-IA de Colombia a México

44 ESS+ integración tecnológica y oportunidades de negocio

48 Repetirá Expo Seguridad Bucaramanga en 2027

Sumario



El libro

“La Seguridad Privada en el Estado Mexicano”

Recientemente se presentó el libro “La Seguridad Privada en el Estado Mexicano”, obra que recopila cinco décadas de evolución de esta industria en nuestro país, la cual es fuente de empleo para un millón de familias. Su aporte en nuestro país representa aproximadamente el 1.25% del Producto Interno Bruto (PIB) nacional, equivalente a un valor de mercado superior a los 469 mil millones de pesos, según datos ofrecidos por Armando Zúñiga Salinas, presidente de ASUME - Agrupaciones de Seguridad Unidas por México.

Es importante subrayar que de acuerdo con el Instituto Nacional de Estadística y Geografía (INEGI), el PIB nominal de México en el segundo trimestre de 2026 se situó en 37 billones 530 mil 380 millones de pesos corrientes a precios de mercado, por lo que el mencionado 1.25% de este PIB de la seguridad privada equivale a 469 mil 129 millones 750 mil pesos.

Zúñiga Salinas, también vicepresidente de comunicación de la Confederación Patronal de la República Mexicana -Coparmex-, refirió: “hay muchas actividades relacionadas con la seguridad privada, lo que más identificamos son los guardias, los que vemos en centros comerciales, en empresas. Pero también está la tecnología, el rastreo vehicular, las cámaras de seguridad, los C5 -Centros de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano-, el monitoreo. Todo eso, si lo sumamos, de acuerdo con el INEGI, es el 1.25% del PIB, aproximadamente.

El titular de ASUME dijo que los cuatro principales sectores que demandan mayoritariamente servicios de protección privada son empresas, instalaciones estratégicas, traslado de valores, gobierno y zonas residenciales.

Regresando al mencionado libro, según versiones de quienes ya lo tienen o leyeron, afirman que ofrece una visión jurídica, institucional, empresarial y académica sobre su papel dentro de una concepción integral de la seguridad corporativa en nuestro país.

El líder de ASUME manifestó que la obra tiene como objetivo plasmar la historia de 50 años de la seguridad privada que surgió con lo “veladores” y en la actualidad es un sector de los que más empleos generan en México.

Los coordinadores de ese libro fueron Armando Zúñiga Salinas, presidente de ASUME; Carlos Matute, investigador del IMEESDN y Jaime Domingo López, del CCE.

Al respecto, la senadora Juanita Guerra -apreciada y consentida de varios empresarios de la seguridad privada en México-, posteó en una de sus redes sociales que dicha obra abre una reflexión necesaria sobre la evolución de este sector en nuestro país, su profesionalización y la importancia de fortalecer los mecanismos de coordinación con las instituciones del Estado, reconociendo su carácter complementario en las tareas de prevención, protección y construcción de entornos seguros.

Dijo que los desafíos en materia de seguridad requieren instituciones sólidas, profesionalización, corresponsabilidad y una visión de Estado que permita construir soluciones de largo plazo en beneficio de México”.

No quiero fastidiar la algarabía por la presentación del libro, pero hay que mencionar que la seguridad privada es uno de los sectores que mayor rotación de personal ostenta, que tiene un registro medio-bajo ante la seguridad social y la capacitación de su fuerza laboral -básica- es cuestionable; eso sin contar las prácticas desleales de prestados de servicio irregulares -“patito”-. Es cuanto...

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

MÁS SEGURIDAD

Magazine

Tour Internacional 2026

EXPO 2026
NAVAL

1-3 DICIEMBRE
ESPACIO RIESCO
AV. EL SALTO 9000, MURCIARRABA

3^o
CUMBRE
GLOBAL DE
SEGURIDAD

IX
CONGRESO
INTERNACIONAL
DE SEGURIDAD
PRIVADA
CONFEVIP

EXPO
SEGURIDAD
TELECOM
COSTA RICA

EXPO
SEGURIDAD
TELECOM
PANAMÁ

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

Más video para vigilar y más espacio para guardarlo

HIKVISION®



El crecimiento de la videovigilancia ha cambiado la escala de los sistemas de seguridad. Empresas, comercios, instalaciones públicas y otros espacios operan con un número cada vez mayor de cámaras que generan grabaciones durante todo el día. Ahora, el reto se traduce en conservar esa información durante el tiempo necesario sin que el almacenamiento crezca al mismo ritmo que la cantidad de video.

Una grabación puede contener miles de imágenes en las que buena parte de la escena permanece sin cambios. Mientras una persona o un vehículo atraviesa el campo de visión de una cámara, el edificio, el pavimento, una pared o cualquier otro elemento del fondo puede mantenerse prácticamente igual durante largos periodos. Procesar toda esa información bajo los mismos parámetros implica destinar capacidad de almacenamiento a zonas que aportan poca variación a la imagen.

Es en este punto donde entra Hik-IA Encoding de Hikvision, una tecnología que incorpora inteligencia artificial al proceso de codificación del video para determinar qué elementos de una escena requieren mayor nivel de detalle y cuáles pueden someterse a una compresión más elevada.

El sistema identifica los objetos relevantes mediante el modelo de inteligencia artificial Hik-IA y establece regiones de interés o ROI dentro de la imagen. Personas, vehículos y otros elementos dinámicos pueden conservar mayor definición, mientras que las partes estáticas de la escena reciben una compresión más intensa. De esta manera, la imagen no se trata como un bloque uniforme y la cantidad de datos generados puede reducirse sin modificar la resolución ni la velocidad de cuadros.

Hik-IA Encoding puede reducir entre 30% y 50% las necesidades de almacenamiento en promedio. El impacto es mayor en proyectos con cientos o miles de canales y largos periodos de conservación, ya que el sistema analiza cada escena y aplica una mayor compresión en las zonas con poca actividad, mientras conserva el detalle de los elementos relevantes.

Cabe destacar que, en uno de los escenarios de referencia publicados por la compañía, un proyecto con 2,000 canales, video de 1080p a 2 Mbps y un periodo

de conservación de 90 días requeriría 403 discos duros con un esquema convencional. Con Hik-IA Encoding, la cantidad se reduce a 202 unidades. La diferencia

representa cerca de la mitad del hardware de almacenamiento utilizado en ese escenario, además de una menor demanda de espacio en rack y electricidad.

La inteligencia artificial llega al proceso de codificación de video

Hik-IA Encoding incorpora IA al códec para analizar cada escena antes de comprimirla. Conserva mayor detalle en las zonas con movimiento y aplica una compresión más alta en las áreas estáticas, reduciendo así la tasa de bits y el volumen de datos generado.

Este funcionamiento busca resolver una de las dificultades habituales de los sistemas de videovigilancia de gran escala. Mantener una alta calidad de imagen y conservar grabaciones durante largos periodos requiere una capacidad de almacenamiento considerable. Esta tecnología aborda esa demanda desde la propia generación del video, antes de que los datos lleguen al almacenamiento.

La tecnología utiliza el estándar H.265 y mantiene la resolución y la velocidad de cuadros del video. Su compatibilidad con decodificadores H.265 y dispositivos de terceros permite incorporarla a entornos que utilizan este estándar sin modificar el formato de reproducción. Hikvision señala que este proceso no afecta el análisis de inteligencia artificial que se realiza posteriormente sobre el video.

El sistema está disponible en cámaras de red y PTZ DeepinView X, cámaras Ultra, equipos con ColorVu 3.0, DVR y productos de seguridad a bordo,

con planes de ampliar su presencia a otras líneas. Su

uso contempla campus empresariales, cadenas minoristas, espacios públicos e instalaciones críticas, donde la cantidad de grabaciones puede representar una demanda importante para la infraestructura de almacenamiento. 



Los dispositivos de video ahora son compatibles con ONVIF

Otra gran novedad para los productos de video Ajax: las cámaras y los NVR Ajax ahora son compatibles con ONVIF®. Esta actualización permite la integración directa de los dispositivos de video Ajax en los ecosistemas de vigilancia de terceros existentes, incluidos los NVR y los sistemas de gestión de video (VMS).

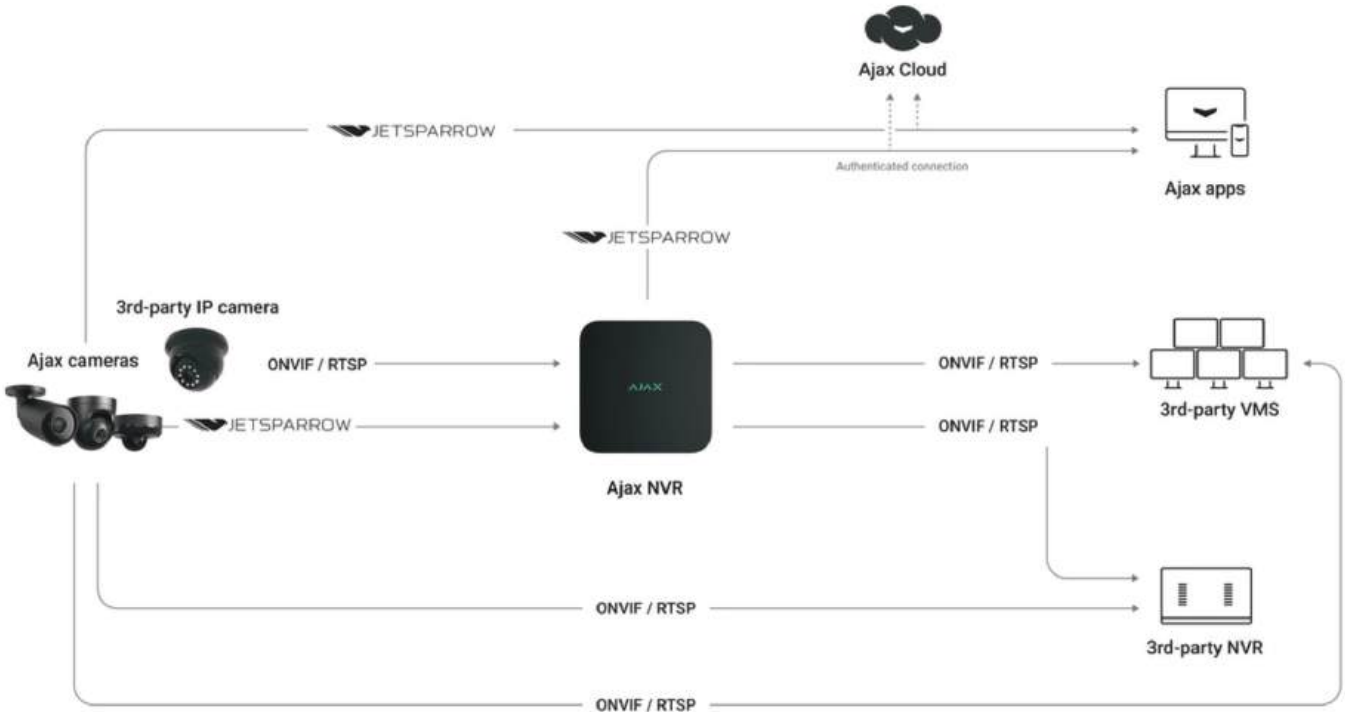
La integración abre numerosas oportunidades para actualizar y modernizar las instalaciones existentes añadiendo cámaras Ajax, lo que aporta funciones de seguridad más avanzadas a un sitio. Otra opción es integrar Ajax con VMS potentes como Milestone, Genetec, Axxon y Digifort.

La conexión ONVIF® está soportada por los siguientes dispositivos Ajax:

- NVR: grabador de video en red
- TurretCam: cámara IP de seguridad cableada
- BulletCam: cámara IP de seguridad cableada
- DomeCam Mini: cámara IP de seguridad cableada
- IndoorCam: cámara de seguridad Wi-Fi

ONVIF® (Open Network Video Interface Forum) es el estándar mundial para integrar dispositivos de seguridad basados en IP en un sistema unificado. Garantiza una comunicación perfecta entre cámaras de video, NVR, plataformas VMS y otras soluciones de seguridad, independientemente del fabricante. Esto significa que los profesionales pueden integrar los productos de video Ajax en la infraestructura existente manteniendo un alto rendimiento, fiabilidad y una transmisión de datos cifrada. La seguridad ya no está limitada por barreras de compatibilidad: está hecha para adaptarse.

Gracias a la conexión ONVIF®, las cámaras y los NVR Ajax ahora pueden transmitir flujos de video directamente a clientes de terceros utilizando el protocolo ONVIF® estándar, sin pasar por Ajax Cloud. Esta implementación es conforme con el Perfil S de ONVIF®, lo que permite la transmisión de video y de audio basada en RTSP, así como la codificación H.264 para la compresión de video. El Perfil S es el estándar de referencia de ONVIF®



- DoorBell: video timbre
- Para configurar la conexión ONVIF®, las apps Ajax deben actualizarse a las siguientes versiones o posteriores:
- Ajax Security System 3.25 (iOS/Android)
 - Ajax PRO: Tool for Engineers 2.25 (iOS/Android)
 - Ajax PRO Desktop 4.20 (Windows/macOS)
 - Ajax Desktop 4.21 (Windows/macOS)

Qué es ONVIF® y cómo se implementa en los productos de video Ajax

y es utilizado habitualmente por la mayoría de los fabricantes de sistemas de vigilancia. Como resultado, los dispositivos Ajax pueden integrarse fácilmente con la gran mayoría de los sistemas de gestión de video existentes.

Los dispositivos de video Ajax incorporan codificación ONVIF® H.265 (HEVC), transmisión de eventos de detección de movimiento y reconocimiento por IA, control del amplio rango dinámico (WDR) y otros ajustes de imagen; no son conformes con ningún perfil ni complemento ONVIF®.

SIGUENOS EN NUESTRAS REDES:

07-09-2010 17:55:47



/pimecsa mx



/pimecsa



/pimecsashop

SUBJECT IDENTIFIED
MALE

H78B34
CAMERA 3B101



1.82
86 KG
AGE 24

Empresa dedicada a la distribución de sistemas en seguridad electrónica, electricidad y telecomunicaciones. Ofrecemos soluciones integrales en videovigilancia, control de acceso, redes y sistemas eléctricos, con un enfoque profesional, eficiente y adaptado a las necesidades de cada cliente.



PIMECSA

Innovación en seguridad electrónica

Mayorista en seguridad electrónica

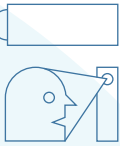
Distribuidor de soluciones tecnológicas

Ingengería y acompañamiento en proyectos

**EFICIENCIA Y PROFESIONALISMO
EN CADA CONEXIÓN**



Innovación



SYSTEM RESPONSE
HQ2977
LV - 0J
65/19
SYST 23



PIMECSA

Innovación en seguridad electrónica

Incorpora a su portafolio de soluciones de marca

L A M P R O

“En PIMECSA buscamos desarrollar LAMPRO, principalmente desde nuestro modelo de distribución mayorista, aprovechando la capacidad comercial, cobertura y conocimiento del mercado para identificar oportunidades y generar demanda. La intención es que PIMECSA funcione como un aliado estratégico para el crecimiento de la marca en México, acercando sus soluciones a distribuidores, integradores, empresas y diferentes canales comerciales, construyendo una relación de largo plazo basada en objetivos compartidos, comunicación constante y desarrollo conjunto del mercado”

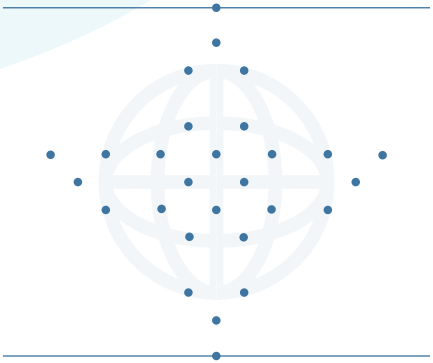
Refiere Alfredo Sánchez Cruz, CEO de PIMECSA.

Importante resaltar que PIMECSA es una empresa 100% mexicana especializada en la distribución mayorista de soluciones de seguridad

electrónica y tecnología, cuyo compromiso es acercar al mercado nacional productos y soluciones de marcas reconocidas, brindando a los clientes y socios comerciales atención, asesoría y acompañamiento durante el proceso comercial, además de mantener la vanguardia tecnológica, ampliando constantemente su portafolio y generando oportunidades de negocio que permitan acceder a soluciones confiables, innovadoras y competitivas.

Respecto a la adhesión de LAMPRO, especialista en comunicación visual, pantallas LED, señalización digital, videowalls e iluminación, el objetivo es desarrollar una marca con presencia y crecimiento sostenido dentro del mercado mexicano, particularmente en sectores que buscan modernizar sus espacios y mejorar la experiencia de sus usuarios, aprovechando la experiencia en

distribución y la red comercial para identificar las verticales con mayor potencial.



-Dicha alianza representa una oportunidad para ampliar la oferta de soluciones tecnológicas y llevar a la marca a nuevos clientes, canales y sectores del mercado mexicano.



De acuerdo con el directivo, la expectativa de PIMECSA se centra en:

- **Desarrollar** nuevos canales comerciales.
- **Incorporar** la marca a su red de distribuidores e integradores.
- **Generar** nuevos proyectos y oportunidades de negocio.
- **Incrementar** gradualmente la presencia de LAMPRO en México.
- **Posicionar** sus productos como alternativas competitivas dentro de sus diferentes segmentos.

Entre las verticales a los que está dirigida la estrategia para LAMPRO, destacan: eventos y entretenimiento (conciertos, ferias, festivales y exposiciones); retail y comercio (centros comerciales, cadenas de tiendas, boutiques y puntos de venta), corporativos y empresas que requieren soluciones de comunicación visual y señalización digital; movilidad (aeropuertos, centrales de autobuses y sistemas de transporte colectivo) y logística; hoteles y turismo, restaurantes y bares, espacios públicos y proyectos gubernamentales como parques, plazas, centros culturales y ayuntamientos, todo ello aprovechando la experiencia comercial, cobertura y capacidad de distribución de PIMECSA.

“Buscamos que LAMPRO sea una marca que crezca de manera sostenible dentro del portafolio de PIMECSA, generando beneficios tanto para el fabricante como para nuestros socios comerciales, distribuidores, integradores y clientes finales de diferentes sectores”, refirió Alfredo Sánchez Cruz.

Visión de la alianza PIMECSA – LAMPRO

En PIMECSA están ciertos que una marca no crece únicamente por

tener un buen producto, requiere contar con un equipo comercial que conozca el mercado, identifique oportunidades y construya relaciones de largo plazo, que no solo sea la tradicional de compra - venta. PIMECSA aportará conocimiento del mercado mexicano, capacidad comercial, distribución y cercanía con los clientes; LAMPRO por su parte la tecnología, soluciones y una propuesta de valor para abrir nuevos canales.

Experiencia probada

En otro orden de ideas, el CEO de PIMECSA, destacó que el principal core de negocio de la empresa es la distribución mayorista de soluciones de seguridad electrónica, infraestructura y tecnología, a través de un enlace especializado entre fabricantes, canales de distribución, integradores y usuario final, acercando productos de marcas reconocidas, además del acompañamiento y asesoría comercial y técnica para facilitar la selección de las soluciones adecuadas de acuerdo con las necesidades de cada cliente de los sectores público y privado.

En la actualidad, la firma atiende a nivel nacional a empresas de los sectores comercio y retail, corporativo, distribución y logística, industria, educativo, laboratorios, salud, seguridad privada, hotelería y turismo, transporte y gobierno es sus tres niveles.

La firma representa a los fabricantes PSA, Seagate, Streamax, ZKTeco, DSC, Siemon, UNV, Western Digital, Hikvision, Dahua, LAMPRO, Hytera, MAXHUB y Uniarch.

Durante los últimos dos años, PIMECSA ha participado en diferentes proyectos y oportunidades comerciales relacionadas con segu-

ridad electrónica y tecnología, atendiendo requerimientos de empresas con presencia nacional y múltiples puntos de operación.

Dos de sus proyectos más relevantes es la colaboración con Grupo Salinas, participando en el suministro y atención de soluciones de seguridad electrónica para diferentes necesidades y ubicaciones en territorio nacional. El otro es la relación comercial con NADRO y empresas relacionadas, donde ofrece soluciones tecnológicas para la modernización de sus instalaciones como videovigilancia, control de acceso, entre otras.

Buscamos -acotó el directivo- generar valor para los fabricantes y socios de negocio mediante cobertura comercial, disponibilidad de producto, conocimiento del mercado y desarrollo de nuevas oportunidades de negocio a través de un vasto portafolio de productos. Somos de los pocos mayoristas que ofrecen tantos valores agregados al integrador y usuario final.



Alfredo Sánchez Cruz, CEO de PIMECSA.

Mercury fortalece y agiliza la expansión del control de acceso

con los nuevos módulos S4 I/O

Cypress, CA.— Mercury Security, experto mundial en hardware de control de acceso de arquitectura abierta y marca de HID, anunció su nueva familia de módulos Mercury S4 I/O. Esta nueva generación de módulos inteligentes está diseñada para ayudar a las organizaciones a modernizar y ampliar su infraestructura de control de acceso físico, aprovechando la infraestructura existente.

A medida que las organizaciones amplían sus instalaciones, adoptan tecnologías en la nube y móviles, y responden a los requisitos cambiantes de ciberseguridad, muchas también buscan formas de modernizar una infraestructura de control de acceso obsoleta, sin asumir el costo y las interrupciones que implican los reemplazos repetidos de hardware. Los módulos Mercury S4 I/O amplían la confiable arquitectura de controladores inteligentes de la compañía con una plataforma segura y modular que permite a las empresas ampliar sus sistemas de manera más eficiente, mantener los sistemas operativos y prepararse para futuros requerimientos tecnológicos.

“La infraestructura de seguridad debe mantenerse durante años, incluso cuando la tecnología continúa evolucionando”, afirmó Steve Lucas, vicepresidente de ventas de Mercury Security. “Diseñamos la plataforma S4 para que los clientes puedan continuar ampliando y adaptando sus sistemas con el tiempo y proteger las inversiones que ya han realizado. Estos módulos representan la siguiente evolución del ecosistema de control de acceso de Mercury, al ofrecer una postura de ciberseguridad más sólida, un mejor rendimiento del sistema y la incorporación de una opción de alta densidad que reduce la huella general del sistema”, agregó.

Instalación más sencilla. Mayor eficiencia

A medida que los armarios de TI y las salas de equipos continúan reduciendo su tamaño, los integradores de sistemas enfrentan una presión cada vez mayor para hacer más con menos espacio físico. La plataforma Mercury S4 aborda directamente este desafío. El nuevo módulo de interfaz de lectores MR54-S4 ofrece capacidad para cuatro puertas en el mismo espacio que anteriormente ocupaba un módulo de interfaz de dos puertas, duplicando efectivamente la capacidad de puertas dentro de la misma huella física. Cada módulo admite hasta 12 entradas y hasta 8 lectores en una sola unidad. Al aumentar la densidad de puertas

Concebida desde la seguridad, la plataforma permite a las organizaciones ampliar su capacidad mientras protegen sus inversiones existentes.

dentro de una huella existente, los integradores reducen la complejidad de la instalación mediante un cableado simplificado y una mayor confiabilidad, mientras que las organizaciones amplían su capacidad, sin agregar paneles ni ocupar espacio valioso.

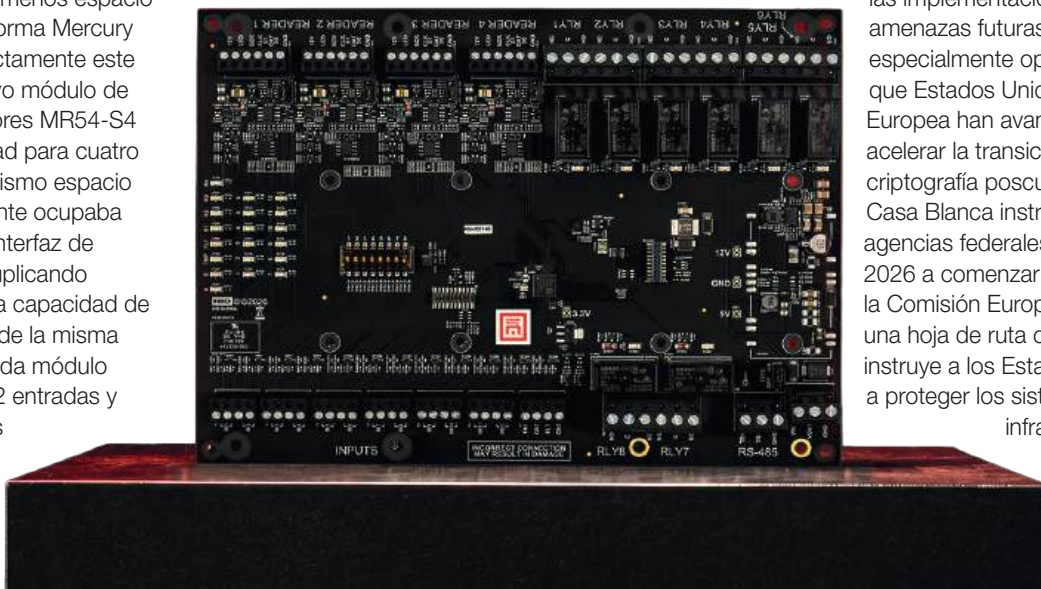
Seguridad desde el diseño. Construido para defender

La ciberseguridad fue una consideración central durante todo el desarrollo. Los módulos Mercury S4 I/O incorporan una arquitectura de seguridad desde su concepción, con protecciones basadas en hardware diseñadas para abordar las ciberamenazas y las expectativas regulatorias en evolución, al tiempo que proporcionan la resiliencia necesaria para entornos de seguridad física de misión crítica.

Las protecciones incluyen un arranque seguro (secure boot), que establece una raíz de confianza basada en hardware al impedir que se ejecute firmware no autorizado o manipulado. Sobre esta base, la confianza aplicada por hardware mediante un Secure Access Module EAL6+* —una certificación de seguridad de alto nivel de Common Criteria— protege la gestión de claves, mientras que la capacidad de criptografía poscuántica amplía esta protección para ayudar a salvaguardar

las implementaciones frente a amenazas futuras. Esto resulta especialmente oportuno, ya que Estados Unidos y la Unión Europea han avanzado para acelerar la transición hacia la criptografía poscuántica, con la Casa Blanca instruyendo a las agencias federales en junio de 2026 a comenzar su migración y la Comisión Europea publicando una hoja de ruta coordinada que instruye a los Estados miembros a proteger los sistemas de

infraestructura de alto riesgo y críticos para 2030. Lo más importante es que



la plataforma se alinea con marcos de referencia reconocidos de la industria, incluidos el Center for Internet Security (CIS), el National Institute of Standards and Technology (NIST) y los requisitos en evolución de la Cyber Resilience Act (CRA), para ayudar a reducir el riesgo y respaldar el cumplimiento a largo plazo.

Abierta. Flexible. Preparada para el futuro

En lugar de exigir un reemplazo completo del hardware a medida que evoluciona la tecnología, Mercury diseñó la plataforma para incorporar capacidades futuras mediante una arquitectura modular. Para las organizaciones que gestionan cientos o incluso miles de puertas, esto significa menos reemplazos de paneles, menos recableado y menos visitas de técnicos a las instalaciones. Debido a que la mano de obra suele representar el mayor costo de una actualización de infraestructura, reducir estas intervenciones en sitio puede disminuir significativamente los costos durante el ciclo de vida, al tiempo que permite a los equipos de seguridad modernizarse a su propio ritmo.

En conjunto, la familia de módulos Mercury S4 I/O proporciona a las organizaciones una base flexible para ampliar los sistemas de control de acceso, preservando al mismo tiempo la apertura, la interoperabilidad y la protección de las inversiones que durante mucho tiempo han definido las implementaciones basadas en Mercury.

Mayor rendimiento. Mayor resiliencia

Basada en la arquitectura abierta de Mercury, la

familia S4 combina una ciberseguridad más sólida y una mayor capacidad de procesamiento, proporcionando 6 veces más memoria y 8 veces más almacenamiento que las generaciones anteriores, junto con una amplia interoperabilidad dentro de un diseño modular que se adapta a medida que evolucionan los requerimientos de los clientes. La plataforma admite compatibilidad tanto hacia adelante como hacia atrás, lo que permite a los responsables de seguridad actualizar su infraestructura de manera gradual mientras minimizan las interrupciones en las implementaciones existentes.

Estas prioridades de diseño reflejan estrechamente lo que Mercury está escuchando del mercado. A través de la investigación continua de la industria que realiza la compañía sobre las necesidades de los profesionales de control de acceso, continúan surgiendo temas claros en torno a mantenerse al día con la evolución de los estándares de ciberseguridad y protección de datos, así como la importancia de la compatibilidad hacia adelante y hacia atrás en la planificación de la infraestructura futura. Estos hallazgos ponen de manifiesto la creciente demanda de plataformas de control de acceso que equilibren la modernización con la protección de las inversiones a largo plazo. 🌐

MÁS SEGURIDAD

Magazine

Síguenos



Revista más seguridad



Revista Más Seguridad



@revmasseguridad



Revista Más Seguridad



Revista Más Seguridad



@revistamasseguridad



Revista Más Seguridad

www.revistamasseguridad.com



la evolución de la caja fuerte

Seguridad física, diseño y tecnología conectada en una nueva generación de soluciones para proteger lo que más importa.

Durante décadas, la caja fuerte ha cumplido una función esencial: proteger mediante acero, cerraduras, refuerzos y mecanismos diseñados para resistir ataques físicos.

Pero el mundo cambió.

Hoy sabemos dónde está nuestro vehículo, controlamos una alarma desde el teléfono y recibimos notificaciones de nuestras cámaras en tiempo real.

En un mundo cada vez más conectado, ¿por qué una caja fuerte sigue siendo un objeto aislado?

Xmart RT nace para cambiar ese concepto.

Bull Safe ha desarrollado una nueva generación de cajas fuertes capaces de formar parte activa de la infraestructura de seguridad de una empresa.

“Ya no se trata únicamente de resistencia física. Se trata de añadir una nueva capa de información y control sobre lo que ocurre alrededor de la caja fuerte”, afirma Luis Felipe Cobos García, CEO de Bull Safe.



Saber. Controlar. Autorizar. Supervisar. Reaccionar

Con Xmart RT, una organización puede tener visibilidad sobre equipos instalados en diferentes ubicaciones, gestionar accesos y autorizaciones y conocer eventos relevantes sin necesidad de estar físicamente frente a cada caja fuerte.

Para empresas con decenas o cientos de sucursales, el cambio es significativo: La caja fuerte deja de ser un punto aislado y pasa a formar parte de una red de seguridad.

Tecnología sin renunciar al acero

En Bull Safe creemos que la tecnología no sustituye a una buena caja fuerte. La complementa.

Para Luis Felipe Cobos García, la evolución tecnológica de estos productos no implica dejar atrás los principios que históricamente han definido su seguridad. Una caja conectada sigue teniendo que cumplir primero con su función esencial: proteger físicamente aquello que se encuentra en su interior.

Por eso, Xmart RT parte de la experiencia de Bull Safe como fabricante de soluciones de seguridad física. Construcción en acero, sistemas de bloqueo, refuerzos estructurales y diferentes niveles de protección continúan siendo la base.

Sobre esa estructura se incorpora tecnología. Resistencia física e inteligencia conectada en un mismo producto.

De la seguridad tradicional al lujo

Xmart RT representa nuestra visión sobre el futuro de la seguridad, pero Bull Safe es mucho más que tecnología conectada.

Fabricamos cajas fuertes tradicionales para hogares, comercios y empresas, además de soluciones especiales para el resguardo de efectivo, documentación y activos de alto valor.

También desarrollamos una línea en la que la seguridad forma parte del diseño

Cajas fuertes de lujo, acabados especiales e interiores personalizados permiten integrar el producto en residencias, oficinas, boutiques y espacios donde la estética es tan importante como la protección.

Dentro de esta categoría destacan nuestras soluciones para relojes, joyería y colecciones de alto valor, diseñadas para proteger y presentar piezas excepcionales dentro de un entorno creado específicamente para ellas.



Fabricamos seguridad. desarrollamos tecnología

Uno de los principales diferenciadores de Bull Safe es reunir fabricación, desarrollo de producto y tecnología dentro de una misma empresa.

Esto nos permite trabajar desde una caja fuerte convencional hasta soluciones especiales para corporativos, cadenas comerciales o proyectos con múltiples ubicaciones.

La seguridad física seguirá necesitando acero, resistencia y buenos mecanismos de protección. Pero cada vez estará más conectada, ofrecerá más información y permitirá mayor control.

“Creemos que el futuro de la seguridad está en encontrar el equilibrio entre la protección física y las posibilidades que ofrece la tecnología”, afirma Cobos García.

Bull Safe trabaja en ese punto de encuentro entre ambos mundos.

Bull Safe

Cajas fuertes tradicionales. Soluciones de lujo. Tecnología conectada.

Xmart RT – La evolución de la caja fuerte hacia un mundo conectado.

bullsafe.com

Seguridad contra incendios

clave para atraer inversión y elevar competitividad de México

La seguridad contra incendios debe convertirse en un componente estratégico de la infraestructura y la competitividad de México, particularmente ante el crecimiento industrial, el nearshoring y la llegada de nuevas inversiones al país, afirmó David Morales Reinoso, presidente de la Asociación Mexicana de Rociadores Automáticos contra Incendios (AMRACI).

En la inauguración de la 9ª Expo Fire, el dirigente advirtió que el desarrollo económico no puede medirse únicamente por el capital invertido o la infraestructura construida, sino también por la capacidad de las instalaciones para proteger vidas, preservar empleos y garantizar la continuidad de las operaciones ante una emergencia.

Destacó que en México ocurren diariamente alrededor de 260 incendios urbanos y no urbanos, mientras que durante la última década miles de personas han perdido la vida por exposición al fuego no controlado o por la ignición de materiales inflamables.

A las pérdidas humanas se suman importantes daños económicos para empresas, trabajadores, familias, aseguradoras y comunidades.

• **AMRACI plantea una norma nacional homologada ante el crecimiento industrial, el nearshoring y la llegada de nuevas inversiones**

David Morales sostuvo que la protección contra incendios debe dejar de verse como un gasto y ser reconocida como una inversión estratégica. “Proteger una inversión significa proteger a sus trabajadores; proteger la continuidad de una empresa significa proteger el bienestar de toda una comunidad”, señaló.

En este contexto, destacó que México vive una oportunidad histórica por la relocalización de cadenas globales de suministro, fenómeno que está impulsando la construcción de parques industriales, centros logísticos, plantas manufactureras y nueva infraestructura.

Sin embargo, consideró indispensable que los sistemas y medidas de protección contra incendios sean incorporados desde la etapa de diseño de los proyectos.





“No puede existir una verdadera competitividad ni una relocalización inteligente si la seguridad contra incendios no se incorpora desde la etapa de diseño de cada proyecto”, enfatizó.

Uno de los principales llamados de AMRACI Industria Contra Incendio, es avanzar hacia una Norma Oficial Mexicana de Seguridad Humana y Protección contra Incendios, que permita establecer criterios homologados en todo el país.

Esta propuesta que contó con el apoyo del presidente de la Confederación de Cámaras Industriales (Concamin) Alejandro Malagón Barragán, plantea que esta regulación sea moderna, verificable y sustentada en la gestión integral del riesgo, con requisitos claros y medibles para edificios públicos, industrias, establecimientos comerciales y viviendas.

El presidente de AMRACI, señaló que una norma nacional permitiría fortalecer la supervisión, facilitar la digitalización de procesos y reducir espacios para prácticas irregulares o desleales.

También consideró que impulsar esta regulación desde la Secretaría de Economía debe entenderse como una decisión estratégica para generar certidumbre a los inversionistas, fortalecer la competitividad y proteger el patrimonio nacional. Como referente de los esfuerzos que pueden realizarse a nivel estatal, destacó la Norma Estatal de Seguridad Humana y Protección contra Incendios de Jalisco, al considerar que representa un avance para homologar criterios y fortalecer las condiciones de seguridad.

Morales llamó a aprovechar la experiencia

existente en México y construir una estrategia conjunta entre gobierno, industria, organismos de evaluación de la conformidad, especialistas y sociedad.

Destacó también la importancia de fomentar una cultura de prevención desde las primeras etapas de formación.

Reconoció el trabajo de Virginia Sendel Iturbide, fundadora y presidenta de Fundación Michou y Mau, por sus 28 años de labor en favor de niñas y niños víctimas de quemaduras.

Asimismo, destacó que el programa “Aprende a Mantenerse Seguro” ha llegado en dos años a más de 80 mil niños y 3 mil docentes en dos estados de la República.

El reto, planteó, es incorporar de manera permanente estos conocimientos en los programas educativos y, posteriormente, en los libros de texto.

Otro de los desafíos, dijo, está relacionado con la preparación de los especialistas del sector. La digitalización, los nuevos materiales, los sistemas automatizados, el almacenamiento de alta densidad y la complejidad de las nuevas instalaciones requieren profesionales cada vez más capacitados.

AMRACI ha trabajado durante más de una década con CONOCER y otros integrantes de la cadena de valor para fortalecer la profesionalización y certificación del sector. Este esfuerzo ha permitido certificar a más de 500 profesionales.

Finalmente, AMRACI llamó a las autoridades, empresas y sociedad a convertir la seguridad contra incendios en una prioridad nacional.

Sostuvo que México tiene la oportunidad de atraer inversiones, fortalecer su infraestructura y aprovechar el crecimiento industrial, pero advirtió que ese desarrollo debe ir acompañado de seguridad, prevención y resiliencia. 🌐

Día del Bombero

La emergencia no termina al apagar el fuego, uno de cada ocho bomberos presenta estrés postraumático

Cuando ocurre un incendio, un accidente o un rescate, los bomberos suelen estar entre las primeras personas en llegar. Sin embargo, el fuego interno no siempre se apaga cuando regresan a la estación. La exposición recurrente a pérdidas humanas, lesiones graves, peligro extremo y decisiones tomadas bajo alta presión también pueden dejar consecuencias emocionales que no son visibles de inmediato.

De acuerdo con un informe internacional publicado en el National Library of Medicine, que analizó 138 estudios, se reveló que el 14.3% del personal de primera respuesta (como bomberos, paramédicos, policías, etc.) expuesto a las actividades habituales de su profesión presenta trastorno de estrés postraumático. En el caso específico de los bomberos, la proporción cambia al 12.1%, lo que equivale a uno de cada ocho elementos afectados.[1]

En el marco del Día del Bombero en México celebrado este 22 de agosto, MSA Safety, empresa experta en seguridad industrial, lidera una campaña para visibilizar y generar conciencia de una realidad que aún enfrenta estigmas: quienes brindan la primera respuesta ante una emergencia, también necesitan una primera respuesta para cuidar su salud mental.

La iniciativa se realizará en colaboración con el Cuerpo de Bomberos de Querétaro, quienes, a través de una serie de entrevistas realizadas en sus instalaciones, comparten sus experiencias del día a día con el objetivo de generar

conciencia de la relevancia de la salud mental.

A esta campaña se suma el Consejo Regional Latinoamericano y del Caribe de Salud Mental (CRLyC), asociación sin fines de lucro, a través del Programa: Sistema Nacional de Apoyo, Consejo Psicológico e Intervención en Crisis por Teléfono (SAPTEL), que ofrece orientación, apoyo psicológico e intervención en crisis emocional mediante una línea gratuita, misma que se pondrá a disposición para los bomberos de México.

La campaña tomará lugar en dos partes, la primera consistirá en un webinar informativo presentado por el Director Operativo del Cuerpo de Bomberos de Querétaro, José Fernando Palacios Ugalde, llamado “El Bombero Profesional y su Salud Mental” donde el especialista hablará de la relevancia del cuidado de la salud mental para cuerpos de emergencia, así como del éxito del programa que ya se tiene activo desde hace más de 5 años en el Departamento de Bomberos que lidera. En el mismo espacio, se develará por primera vez el vídeo creado por MSA Safety en colaboración con el Programa de Atención Psicológica del Cuerpo de Bomberos de Querétaro, el cual se continuará promoviendo a través de las redes sociales de la marca.

En la segunda etapa, MSA Safety junto con CRLyC-SAPTEL lanzarán un manual informativo como recurso para la atención psicológica y la intervención en crisis. El material ayudará a los cuerpos de bomberos de toda Latinoamérica a reconocer señales de alerta, brindar una orientación inicial y facilitar la canalización a especialistas, sin sustituir la valoración profesional, dicho documento ya se encuentra en fase de planeación y se planea sumar a más instituciones especializadas para su óptimo desarrollo.



La emergencia invisible después del servicio

De acuerdo con la NOM-035-STPS-2018[2], un acontecimiento traumático severo ocurre durante el trabajo (como explosiones, derrumbes o incendios graves) e implica peligro mortal o lesiones severas que pueden causar estrés postraumático. Por ello, la Norma exige a las instituciones o empleadores identificar y canalizar a quienes se expongan a estas situaciones para recibir atención necesaria en salud mental.

“Queremos cuidar la parte que no se ve: no solo lo que sucede durante una emergencia, sino el silencio que viene después. Nuestro personal enfrenta batallas internas de distintos tamaños por las tragedias que atiende todos los días”, explicó Fernando Palacios, director operativo del Cuerpo de Bomberos de Querétaro.

Las afectaciones a la salud mental pueden manifestarse con síntomas como alteraciones del sueño, ansiedad, crisis de pánico, irritabilidad,

requisitos mínimos para los programas de seguridad, salud ocupacional y bienestar en los departamentos de bomberos y organizaciones de respuesta a emergencias).

“Me preguntaba si podíamos hacer algo para evitar que una situación así ocurriera dentro del Cuerpo de Bomberos de Querétaro. A partir de ahí comenzamos a buscar un modelo que permitiera prevenir, identificar señales y acompañar a nuestro personal en el día a día”, señaló Gabriela Dorantes Arzate, directora del Instituto de Capacitación de Bomberos Querétaro.

El esquema comienza después de un incidente crítico, cuando el equipo realiza una plática informal que funge como una sesión grupal de desactivación emocional. Si se identifica una necesidad adicional, el elemento puede acceder a atención individual a través de psicólogas especialistas en manejo de crisis, que elaboran y dan continuidad a un plan de tratamiento de salud mental personalizado; el cual permanece como



aislamiento, depresión o estrés postraumático. En situaciones graves y sin atención oportuna, también pueden relacionarse con pensamientos o conductas suicidas.

“No a todos nos afecta un mismo incidente de la misma manera. A algunas personas les impacta más atender a un niño; a otras, ver a una persona mayor que le recuerda a alguien de su familia. Cada persona tiene una forma distinta de procesar lo que sucede”, añadió Palacios.

Atención temprana para evitar que el silencio se convierta en crisis

El Cuerpo de Bomberos de Querétaro comenzó a desarrollar su Programa de Atención Psicológica (PAP) en 2021. Su origen está relacionado con la muerte por suicidio de un integrante de otra corporación de emergencias a la que pertenecía Gabriela Dorantes, una experiencia que llevó a la cofundadora del PAP, a plantear la necesidad de crear un esquema preventivo, el cual se tornó aún más relevante a partir de la publicación de la NOM 035, específicamente posterior al esquema de la NFPA 1500 (la norma que fija los

un recurso fijo para su equipo, proporcionado por sus directivos.

De acuerdo con el PAP, aproximadamente 10% de sus elementos se encuentra en tratamiento de manera rotativa conforme lo van requiriendo, aunque las personas atendidas cambian conforme reciben el alta o surgen nuevas necesidades.

“La verdadera conmemoración de los bomberos en su día radica en entender que su salud mental es tan prioritaria como el fuego que combaten. Quienes llegan primero para ayudar a los demás no deben quedarse solos después de la batalla. Por ello, el equipo de MSA Safety refrenda un compromiso que trasciende del equipamiento físico de pies a cabeza. Al liderar esta campaña y sumar esfuerzos con aliados clave, pondremos juntos a disposición herramientas de prevención y atención de salud mental que asegurará que los bomberos de México y Latinoamérica cuenten con un respaldo integral dentro y fuera del campo de acción”, finaliza Karla Hernández Mendoza, LATAM Segment Marketing Manager / FIRE PPE de MSA Safety.

“Secure by Design and Default Playbook” por la ENISA



Introducción

En la actualidad, nadie compra un automóvil y espera tener que instalarle después el cinturón de seguridad o las bolsas de aire. Damos por sentado que llega de fábrica con frenos que funcionan, bolsas de aire calibradas y una carrocería pensada y diseñada para absorber un impacto antes de que llegue a quien va adentro. Esa expectativa nos parece de sentido común porque la industria automotriz tardó décadas de accidentes, litigios y regulación en aceptar una idea incómoda: la seguridad no puede depender de que el conductor sea perfecto. Con el software y los dispositivos conectados —el router/modem de la casa, la cámara del negocio, el sistema que controla una línea de producción— seguimos, en cambio, atrapados en la etapa anterior a esa aceptación. La gran mayoría de los productos digitales todavía llegan al mercado con la puerta técnicamente abierta, confiando en que alguien, en algún momento, tenga el conocimiento y la voluntad de cerrarla. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) acaba de publicar este año una guía que ataca exactamente ese supuesto, y vale la pena entender por qué su planteamiento, aunque técnico en apariencia, es en realidad una propuesta profundamente humana.

Desarrollo

El documento se llama, sin rodeos, “Secure by Design and Default Playbook”, y su destinatario no es la gran empresa con un ejército de analistas de seguridad, sino la pequeña y mediana empresa que fabrica un dispositivo conectado con un equipo reducido, presupuesto ajustado y, muchas veces, sin nadie cuyo trabajo sea exclusivamente pensar en ciberseguridad. Ahí radica su primera virtud estratégica: en lugar de repetir el discurso genérico de “la seguridad es responsabilidad de todos”, reconoce que exigirle sofisticación a quien no tiene los recursos para ella es, en la práctica, una forma elegante de garantizar que nada cambie. La propuesta de la ENISA distingue dos momentos que solemos confundir. Uno es diseñar el sistema para que resista el ataque desde su arquitectura misma —lo que llama “seguro por diseño”—, y otro es decidir con qué configuración ese sistema sale de la fábrica hacia el mundo real —lo que llama “seguro por defecto”. Un producto puede estar excelentemente diseñado y, aun así, llegar al usuario con la contraseña “admin/admin” activada, el cifrado apagado y todos los puertos abiertos, simplemente porque nadie decidió explícitamente lo contrario.

Por otro lado, es interesante cómo la guía organiza veintidós principios en cuatro familias que, leídas con atención, describen una filosofía coherente y no una lista de trámites. Los “fundamentos arquitectónicos” son las decisiones estructurales que se toman una sola vez pero que determinan todo lo demás: trazar fronteras de confianza explícitas entre un componente y otro, otorgar únicamente el privilegio mínimo indispensable, y construir con la lógica de que cualquier capa de defensa puede fallar, por lo que ninguna debería sostener sola el peso de la seguridad. La “integridad operacional”, en cambio, es el trabajo cotidiano de mantener eso vivo: vigilar registros de actividad, gestionar parches con método, y —quizás el punto más subestimado— diseñar pensando en cómo un usuario común, sin formación técnica, interactuará con la seguridad del producto. El “endurecimiento por defecto” traslada esa filosofía al momento exacto en que el producto se enciende por primera vez: nada de credenciales universales, nada de comunicación sin cifrar por comodidad, cada dispositivo con una identidad propia e irrepetible. Y la “protección guiada” acepta, sin cinismo, que el error humano seguirá ocurriendo, así que, en lugar de sermonear al usuario, el sistema debe advertirle con claridad cuando se aparta de un estado seguro y ofrecerle un camino de un solo clic para regresar a él.

Quizás la apuesta más audaz del documento no está en los veintidós principios, sino en cómo propone demostrarlos. Durante años, el cumplimiento de la ciberseguridad se ha resuelto con documentos: reportes que alguien redacta para una auditoría, se archivan y nadie vuelve a mirar hasta la siguiente revisión, meses o años después, cuando el sistema ya cambió por completo. La ENISA plantea sustituir esa fotografía fija por lo que llama “atestaciones procesables por máquina”: afirmaciones de seguridad codificadas en un formato que una computadora, no solo un auditor humano, puede verificar automáticamente en cada versión del producto.

La idea, en esencia, es que un sistema de entrega de software pueda negarse por sí mismo a publicar una actualización si no trae adjunta la prueba verificable de que pasó un análisis de vulnerabilidades, de la misma manera en que un elevador moderno se detiene solo si detecta que un mecanismo de seguridad falló, sin esperar a que un inspector humano lo note en su próxima visita programada. Es una propuesta que traslada la confianza de la promesa escrita a la evidencia continua, y que resulta particularmente generosa con las empresas pequeñas: automatiza precisamente el trabajo de revisión manual que ellas no tienen capacidad de sostener.



Conclusión

Conviene preguntarse, la próxima vez que desempaquemos un dispositivo conectado a internet, si en verdad tenemos que configurar su seguridad nosotros mismos o si esa responsabilidad debió resolverse antes de que la caja llegara a nuestras manos. Culpar al usuario por una contraseña débil es, muchas veces, una forma cómoda de no preguntarle al fabricante por qué el sistema permitió esa contraseña en primer lugar. El planteamiento de la ENISA no es una curiosidad regulatoria europea reservada a ingenieros: es una invitación a cambiar el ángulo desde el cual toda la sociedad discute la ciberseguridad, pasando de exigir vigilancia eterna a las personas hacia exigir diseño responsable a quienes construyen la tecnología. La llamada a la acción es doble. A quienes desarrollan o fabrican productos digitales, incluso en talleres pequeños o startups de dos personas, la invitación es a preguntarse hoy mismo si su producto llegaría seguro al usuario aunque este nunca tocara una sola configuración. Y a quienes simplemente usamos tecnología todos los días, la invitación es a dejar de conformarnos con “así viene de fábrica” como excusa, y empezar a exigir, como ya exigimos cinturones de seguridad, que lo seguro sea, sencillamente, la única opción disponible.



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

Articlista Invitado

Referencia

- European Union Agency for Cybersecurity. (2026). ENISA secure by design and default playbook: A practical guide to secure by design and default principles for SMEs. <https://www.enisa.europa.eu>



Nace el ECOSISTEMA QUERETANO DE CIBERDEFENSA

para fortalecer la
protección digital de las
PyMEs de Querétaro

Querétaro, México. — Con el objetivo de fortalecer la resiliencia digital, reducir los riesgos de ciberataques y brindar a las pequeñas y medianas empresas herramientas prácticas para proteger sus operaciones, información y continuidad de negocio, se implementará en Querétaro el Ecosistema Queretano de Ciberdefensa (EQC), una iniciativa coordinada por SILIKN, OWASP Capítulo Querétaro y la Subcomisión de Ciberseguridad e Infraestructura de la Comisión de Tecnologías de Información de COPARMEX Querétaro, con la participación de especialistas, organizaciones empresariales, instituciones académicas, proveedores tecnológicos y otros actores del sector.

El Ecosistema Queretano de Ciberdefensa parte de una premisa: la ciberseguridad de las empresas no debe depender únicamente de la adquisición de tecnología, sino

concientización del personal, monitoreo y documentación de eventos, seguridad de redes y mecanismos de respaldo y recuperación ante incidentes.

Uno de los elementos centrales del Ecosistema Queretano de Ciberdefensa será establecer una visión de ciberseguridad accesible para las PyMEs, evitando que la falta de personal especializado o de grandes presupuestos se convierta en una barrera para implementar controles básicos y efectivos. El modelo contempla diferentes niveles de madurez, de manera que una organización pueda comenzar con controles esenciales y avanzar progresivamente hacia capacidades más sofisticadas conforme aumenten sus necesidades y recursos.

Asimismo, el Ecosistema promoverá que la responsabilidad de la ciberseguridad sea asumida desde la dirección de las empresas. Cada organización deberá contar



de una gestión ordenada, proporcional y continua del riesgo. Por ello, la iniciativa buscará acercar a las PyMEs queretanas una metodología práctica que les permita identificar qué deben proteger, conocer sus principales riesgos, determinar sus brechas de seguridad, establecer prioridades y construir planes concretos para reducir riesgos.

La propuesta contempla un proceso gradual que comenzará con la identificación de los activos y procesos digitales críticos de cada empresa, incluyendo sitios web, correo electrónico, información de clientes, sistemas administrativos, equipos de cómputo, redes, servicios en la nube y respaldos. A partir de este diagnóstico se determinarán los riesgos relevantes y se establecerán medidas de protección de acuerdo con el impacto potencial que tendría un incidente sobre cada negocio. El enfoque busca que las empresas puedan concentrar sus recursos limitados en aquellas acciones que realmente reduzcan su exposición.

Entre las medidas que podrán formar parte de los planes de protección se encuentran la prevención de malware y actualización de sistemas, cifrado de comunicaciones, seguridad de servicios en la nube y contratación de proveedores, protección de información, fortalecimiento de equipos y cuentas de usuario, capacitación y

con claridad sobre los riesgos que enfrenta, las medidas que implementará, los recursos necesarios y los responsables de dar seguimiento a su ejecución. El resultado esperado será un plan de trabajo priorizado, vinculado con los riesgos identificados y sujeto a revisión periódica.

La iniciativa también pondrá especial atención en la cadena de suministro, considerando que una empresa puede verse afectada por vulnerabilidades presentes en proveedores, servicios digitales, plataformas en la nube o terceros con acceso a sus sistemas. Para las organizaciones con mayores niveles de exposición se contempla profundizar en la evaluación de riesgos, análisis de brechas, definición del apetito de riesgo, planes de mitigación y mecanismos de monitoreo continuo.

Otro componente fundamental será la medición y mejora continua. La ciberseguridad no será entendida como un proyecto que termina después de instalar una herramienta o completar un diagnóstico, sino como un proceso permanente que deberá adaptarse a la evolución del negocio, la tecnología y las amenazas. El modelo contempla revisiones periódicas para identificar nuevos activos, verificar la implementación de controles, actualizar prioridades y determinar los recursos que requiere cada organización.



Desencriptación y
recuperación total
de datos tras
ataques ransomware



Escanea
Evalúa y fortalece
tu defensa digital



La defensa ya no es solo física. También es digital

Para las empresas que, por su tamaño, actividad, dependencia tecnológica, información manejada o impacto potencial, requieran un nivel superior de protección, el Ecosistema podrá incorporar procesos más avanzados de evaluación y gestión de riesgos. Estos podrán incluir análisis de brechas frente a controles reconocidos, planes formales de mitigación, monitoreo continuo, gestión de riesgos de la cadena de suministro, administración de la superficie de ataque y otras capacidades especializadas.

“El objetivo es que ninguna PyME queretana tenga que esperar a sufrir un incidente para comenzar a protegerse. Queremos construir un ecosistema en el que conocimiento, capacidades técnicas, empresas, especialistas y organizaciones empresariales trabajen de manera coordinada para elevar el nivel de ciberdefensa de nuestro estado”, señaló Víctor Ruiz, fundador de SILIKN.

El Ecosistema Queretano de Ciberdefensa buscará convertirse en un punto de articulación entre el sector privado, la comunidad técnica, especialistas en seguridad, academia y otros actores relevantes, generando mecanismos de colaboración, capacitación, diagnóstico, acompañamiento y desarrollo de capacidades.

La iniciativa tendrá como prioridad que las PYMEs puedan pasar de una visión reactiva —actuar únicamente después de un ataque— a una estrategia preventiva basada en identificar, proteger, detectar, responder y recuperar, principios que permiten estructurar la gestión de la ciberseguridad como un proceso integral.

Con el Ecosistema Queretano de Ciberdefensa, Querétaro busca avanzar hacia un entorno empresarial más resiliente, en el que la protección de la información, la continuidad operativa y la confianza digital formen parte de la competitividad de las empresas.

La coordinación estará a cargo de SILIKN, OWASP Capítulo Querétaro y la Subcomisión de Ciberseguridad e Infraestructura de la Comisión de Tecnologías de Información de COPARMEX Querétaro, junto con otros organismos, especialistas e instituciones que se incorporen a esta iniciativa.

Cuatro fases para fortalecer la ciberdefensa de las PyMEs

Las acciones del Ecosistema Queretano de Ciberdefensa se desarrollarán en cuatro fases:

- **FASE 1.** Curso “Ciberseguridad + IA para dueños y directivos de PYMES”.
- **FASE 2.** Capacitación General en Ciberseguridad Práctica para Pymes, acreditación, networking, webinars y contenidos continuos, además de formar parte del “Directorio de Empresas Ciberseguras de Querétaro”.
- **FASE 3.** Consultoría y Capacitación personalizada para Pymes participantes.

- **FASE 4.** Centro de Respuesta a Emergencias Informáticas, que operará como un mecanismo centralizado de apoyo para atender emergencias de ciberseguridad en las PyMEs. Funcionará como un servicio de primera respuesta ante incidentes para proporcionar contención y coordinación de alertas tempranas dentro de la red empresarial del estado.

EQC y organizaciones aliadas impulsan acciones de ciberseguridad e inteligencia artificial para fortalecer a las PYMES

Como punto de partida de este programa, EQC, en conjunto con otras organizaciones participantes, convoca a dueños y directivos de pequeñas y medianas empresas al curso en línea “Ciberseguridad + IA para dueños y directivos de PYMES”, actividad que dará inicio a la Fase 1 de un programa de acciones orientado a fortalecer la protección digital y la capacidad de respuesta de las empresas ante los nuevos riesgos asociados al uso de la Inteligencia Artificial por parte de los ciberdelincuentes.

En un entorno en el que la IA está siendo utilizada para desarrollar ataques más rápidos, sofisticados y difíciles de detectar, las PYMES enfrentan riesgos crecientes para la seguridad de sus datos, recursos financieros, operaciones y la información de sus clientes.

Como parte de la Fase 1, el curso brindará cuatro horas de capacitación con herramientas prácticas para identificar las principales vulnerabilidades de una empresa, reconocer los nuevos riesgos potenciados por la IA, proteger información, operaciones, recursos y clientes, definir acciones prioritarias de protección y elaborar un plan de protección de 30 días que permita comenzar a actuar de manera inmediata.

La capacitación se llevará a cabo los días 5 y 6 de octubre de 2026, de 1:00 a 3:00 p. m., en modalidad online y con instructor en vivo. El cupo será limitado. La inversión es de \$1,000 pesos mexicanos e incluye la presentación y el manual del participante, el cual incorpora la guía para desarrollar el Plan de Protección. Se tiene contemplado realizar estas capacitaciones cada dos semanas, por lo que les invitamos a estar atentos a las próximas fechas y convocatorias.

Como parte de la continuidad del programa, el monto de inscripción será considerado como descuento para la consultoría en ciberseguridad contemplada en la Fase 3, permitiendo a las empresas avanzar de la capacitación y el diagnóstico inicial hacia la implementación de medidas concretas de protección.

Con esta iniciativa, EQC y las organizaciones participantes buscan promover una cultura de prevención y preparación entre las PYMES, ayudándolas a dejar atrás una postura reactiva frente a los incidentes y avanzar hacia una estrategia de ciberseguridad que les permita proteger sus activos, mantener la continuidad de sus operaciones y responder de mejor manera a las amenazas emergentes impulsadas por la Inteligencia Artificial.



LA INDUSTRIA DE LA SEGURIDAD EVOLUCIONA. TU CONOCIMIENTO TAMBIÉN.

Actualiza tus conocimientos, fortalece tus habilidades y sigue creciendo con Formación ALAS. Descubre programas especializados para profesionales de la seguridad.

FORMACIÓN OPERATIVA

	Alarmas y Detección de incendios		Alarmas y Detección de Intrusión		Control de Acceso
	Fundamentos de Seguridad Electrónica		Integración de Sistemas de Seguridad		Operadores de Cuartos de Control
	Redes IP e Inalámbricas		Seguridad Perimetral		Video Vigilancia

FORMACIÓN GERENCIAL

	Ciberseguridad para Alta Gerencia		Evaluación de Riesgos de Seguridad		Evaluación del Retorno de la Inversión en Seguridad
	Gerencia de Proyectos		Management 3.0		Ventas para la Industria de la Seguridad

NUEVAS TECNOLOGÍAS

	Drones en Seguridad		Inteligencia Artificial en Seguridad		Hacking Ético
---	----------------------------	---	---	---	----------------------

CAPACITA A TU EQUIPO CON CURSOS IN COMPANY

Desde 6 participantes, con contenidos, fechas y horarios adaptados a tu organización.

APRENDE. ACTUALÍZATE. SIGUE CRECIENDO.



MANUELA RIVERA

Encargada de Cursos

WhatsApp: +57 304 2738724

Email: cursos@alas-la.org



ASOCIACIÓN
LATINOAMERICANA
DE SEGURIDAD

Síguenos en nuestras redes
sociales como @alasseguridad

IA aplicada a Seguridad Integral: 10 soluciones destacadas.

Durante décadas, la seguridad integral se apoyó en una idea sencilla: ver para reaccionar. Cámaras, arcos detectores y centros de monitoreo generaban enormes volúmenes de información que, en la práctica, dependían de la atención de un operador (en ocasiones cansado) frente a decenas de pantallas. Hoy esa lógica está cambiando de fondo. La inteligencia artificial (IA) ya no se limita a registrar lo que ocurre: interpreta, prioriza y anticipa. Desde la detección de armas en tiempo real hasta la búsqueda en video mediante una simple frase escrita, pasando por robots de patrullaje y plataformas que analizan millones de fuentes abiertas para alertar sobre riesgos cercanos, la IA se está convirtiendo en el nuevo sistema nervioso de la protección de personas, activos e instalaciones.

En México, el impulso del Mundial 2026 aceleró esta adopción. En este artículo revisamos solo algunas de las muchas soluciones que existen en el mercado y lo

que significan para quienes diseñan y operan estrategias de seguridad, algunas de estas soluciones fueron mostradas en las pasadas exposiciones GSX 2026 de ASIS Internacional e Intersec 2026.

- **1. Ambient.ai:** Plataforma de IA que convierte las cámaras existentes en detección activa de amenazas. Filtra alarmas falsas y prioriza incidentes para el GSOC.

Más información: ambient.ai

- **2. ZeroEyes:** Detecta armas de fuego visibles con las cámaras actuales. Cada alerta la valida una persona en su centro de operaciones 24/7 antes de enviarla, para reducir falsos positivos.

Más información: zeroeyes.com

- **3. Omnilert:** Detecta armas con IA y verificación humana, y activa protocolos de respuesta automática (avisos, cierres, notificación a autoridades).

Más información: omnilert.com

- **4. Evolv Express:** Arco de revisión con sensores e IA que detecta armas ocultas sin detener el flujo de personas. Se usa



*El Estadio Azteca en Ciudad de México, el 28 de marzo de 2026.
Rodrigo Oropeza
(Getty Images)*



Cortesía: IA

en estadios, escuelas y recintos masivos.

Más información: evolv.com

- **5. Verkada (AI-Powered Search):** Videovigilancia en la nube con búsqueda en lenguaje natural (por ejemplo, "persona con chamarra roja en el estacionamiento") y alertas generadas por IA. Más información: verkada.com
- **6. Genetec Security Center:** Plataforma que unifica video, control de acceso y LPR (lectura de placas) en un solo sistema, con nuevas funciones de IA presentadas en Intersec 2026. Más información: genetec.com
- **7. Dataminr Pulse for Corporate Security:** Monitorea millones de fuentes públicas en tiempo real y lanza alertas tempranas de eventos (protestas, desastres, incidentes) cercanos a instalaciones, personal o viajeros. Más información: dataminr.com
- **8. Knightscope (robot K7):** Robots autónomos de seguridad que patrullan con cámaras, LPR y sensores, y funcionan como un "guardia" complementario. Más información: knightscope.com
- **9. Hanwha Vision (analítica en el borde):** Cámaras con IA integrada ("edge") que clasifican objetos y detectan comportamientos. Su informe de tendencias 2026 pone el foco en una IA fiable y ética. Más información: hanwhavision.com
- **10. Videovigilancia activada por texto (tendencia):** Modelos de visión y lenguaje que permiten configurar reglas y buscar en el video escribiendo instrucciones, sin programar analíticas. Más información: Publikt Digital

La inteligencia artificial no sustituye al profesional de la seguridad, pero sí redefine su papel. Las soluciones analizadas muestran una tendencia clara: menos tiempo reaccionando a falsas alarmas y más tiempo tomando decisiones con información oportuna y confiable.

Sin embargo, la tecnología por sí sola no garantiza resultados. Su valor depende de una buena integración con los procesos, la infraestructura existente y, sobre todo, con las personas que la operan.

Antes de adoptar cualquier herramienta, conviene evaluar su precisión real, su compatibilidad, su impacto en la privacidad y la solidez del proveedor en un mercado que se consolida rápidamente. La seguridad integral del futuro será híbrida: algoritmos que vigilan sin descanso y criterio humano que valida, decide y actúa. Las organizaciones que entiendan este equilibrio no solo estarán mejor protegidas, sino también mejor preparadas para anticipar el riesgo en lugar de solo responder a él.



MBA. Armando García Sánchez,
CPP
Gerente de Consultoría & TI
Timur Latinoamérica
[linkedin.com/in/armando-garcia-sanchez/](https://www.linkedin.com/in/armando-garcia-sanchez/)
México

Articlista Invitado

Fortalece



Consultoría el servicio de custodias de mercancía

“Innovación constante, servicio al cliente y respuesta inmediata son las prioridades de la empresa. Desde hace 18 años nos encontramos en constante evolución, lo que nos ha permitido crecer como empresa y ofrecer un vasto portafolios de servicios. Hoy potenciamos las custodias con la implementación de tecnología en plataformas y rastreo satelital para más de 20 grandes clientes a quienes atendemos a nivel nacional con más de 100 viajes por día”, refiere Edgar Aguilera, director ejecutivo de SAMAHE Consultoría en Prevención de Riesgos.

SAMAHE, firma especializada desde hace 18 años en seguridad intramuros, análisis de riesgos, escoltas, seguridad electrónica y custodias, se ha diferenciado en el sector al ofrecer servicios hechos a la medida de cada cliente, lo cual le ha permitido crecer exponencialmente y ser fuente de empleo para más de 300 familias a nivel nacional.

Respecto al servicio de custodias de mercancías en tránsito, implementa GPS de última generación con mejoras constantes en software y hardware para obtener analíticas y ofrecer data a los clientes. Desarrolla su área tecnológica con videovigilancia a bordo y monitoreo 24/7. Las firmas Baby Creysi, Bicileyca, Grupo Dragón, Grupo Viso y diversos laboratorios han confiado a SAMAHE el traslado de sus mercancías punto a punto.

“Hace unos meses estuvimos en Taiwán en una feria de intercambio de tecnología, precisamente para entregar valores agregados a los clientes e incrementar la seguridad de las mercancías en tránsito. Entonces, buscamos dos vías de negocio: mejorar el servicio y distribuir algún software o producto tecnológico que podamos comercializar en América Latina. Uno de los softwares que tenemos en la mira, ayuda a tener un mayor control de accesos a medios digitales. Es como un guardia de seguridad, pero digital”, comenta el ejecutivo.

Es importante destacar la novedad en el servicio de custodias: la implementación del análisis y síntesis de información en ruta. Esto permite entregar datos clave a los clientes —como rutas, horarios y número de incidentes— para que puedan tomar decisiones informadas orientadas a reducir la siniestralidad y los riesgos..

Los clientes toman la decisión -afirma Edgar Aguilera-, pero nosotros que los acompañamos, les damos

- Con tecnología de punta en rastreo satelital atiende a más de 20 grandes clientes.
- Las operaciones se supervisan desde las ciudades de México, Estado de México y Ciudad del Carmen (Campeche).

retro y feedback que pueden visualizar. Implementamos videovigilancia a bordo, audio en cabina, botones de pánico, etc. Reforzamos el binomio capital humano y tecnología. Las operaciones de las custodias se supervisan en las Ciudades de México, Estado de México y del Carmen (Campeche).

“La compañía busca la excelencia en el servicio — sin masificarlo— y lograr un buen retorno de inversión, asegurando que no se pierdan el control ni la calidad. El objetivo es mantener la cartera con la satisfacción garantizada, lo que a su vez asegura la permanencia del capital humano de SAMAHE y, finalmente, retribuir a los socios con márgenes de ganancia justos.

En el corto plazo, la compañía planea incursionar en el segmento de ciberseguridad, principalmente mediante la búsqueda de software impulsado por inteligencia artificial que le ayude en la operación diaria con información precisa y en



Ejecutivos de SAMAHE: Edgar Aguilera, director ejecutivo; Santiago Aguilera, director general y Marco Antonio Gómez, director administrativo.

CUSTODIA DE MERCANCÍAS EN TRÁNSITO



- Custodias
- Tecnologías en custodias
- Guardias intramuros
- Análisis de riesgo y vulnerabilidades

**Tecnología en ruta,
Destino seguro...**

ventas@samahesecurity.com • contacto@samahesecurity.com
www.samahesecurity.com.mx • 55.8464.6151



SOLICITA INFORMACIÓN

tiempo real. Asimismo, se está analizando incursionar en otras dos verticales: el traslado de valores y la logística.

18 años de actividades

Marco Antonio Gómez Patiño, director administrativo de SAMAHE Consultoría en Prevención de Riesgos, rememora que la firma se ha mantenido vigente durante casi dos décadas gracias a sus servicios insignia en escuelas, hospitales, clínicas, unidades habitacionales, fábricas, tiendas de autoservicio, corporativos e instalaciones estratégicas para el Estado. La suma de experiencias de sus fundadores y colaboradores a través de diplomados y cursos, tanto en México como en el extranjero, ha sido vital para su permanencia en el sector.

La interacción con el cliente es esencial para entregar un servicio de calidad. Hoy se conocen sus necesidades de protección y esto exige resultados acordes. Como empresa no puedes ni debes quedar rebasado; eso se llama atención y calidad en el servicio, las cuales logramos con inteligencia operativa en nuestras verticales más robustas: guardias intramuros, custodias y choferes custodios. Reforzamos las operaciones con una implementación sólida de tecnología como body cams, GPS, rondineros o rastreadores», afirma Marco Gómez.

La gama de servicios también incluye consultoría, análisis de riesgo, exámenes de polígrafo realizados por psicólogos especialistas, capacitación para guardias intramuros, custodios y escoltas, así como clases de tiro. Además, la empresa cuenta con una representación en París, Francia, para determinados esquemas de capacitación continua e innovación.

Para concluir, el director administrativo agrega que SAMAHE está inmersa en la vertical de videovigilancia, ya que participó en una norma del CONOCER y su figura está registrada en el Diario Oficial de la Federación (DOF). De igual forma, todos sus monitoristas están certificados en dicha norma y sus servicios de videovigilancia también se ofertan a clientes específicos para el monitoreo de instalaciones y guardias.



MÁS SEGURIDAD

Magazine

Síguenos



Revista más seguridad



Revista Más Seguridad



@revmasseguridad



Revista Más Seguridad



Revista Más Seguridad



@revistamasseguridad



Revista Más Seguridad

www.revistamasseguridad.com



Inteligencia Artificial fortalece al rastreo y seguridad en transporte de carga:



En la actualidad el concepto de la Inteligencia Artificial -IA- está presente en todos los sectores industriales del mundo. México no es ajeno a esta tendencia pues se ha vuelto una poderosa arma y muchos no la están aprovechando en sus operaciones. El rastreo satelital y la seguridad para el transporte de carga tienen un gran aliado que le permite, entre otros rubros, reducir el robo o accidentes.

Alejandro Corona, miembro del Comité de Tecnología de la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital -AMESIS-, señaló: “Hoy tenemos un bombardeo de motores de IA como LLMs y SMLs, con lo que muchas empresas están creando, pero el reto es entender cómo usarlos y atreverse a usarlos. La tendencia en el mundo es que estas herramientas nos lleven a un avance agigantado en los próximos tres años”.

Enfatizó que dentro de la AMESIS había empresas que se dedicaban a generar proyectos de videovigilancia, control de accesos o automatizaciones, pero siempre había limitaciones en el software existente en el mercado. Hoy con motores como LLM, permite rastrear objetos y personas dentro del área de trabajo, movimientos o actividades sin falla alguna, creando un agente al saber utilizar Cloud.

Respecto al monitoreo y localización de vehículos de carga, se enfrentan a requerimientos especiales como conexión a internet, avisos vía celular sobre apertura de puertas, encendido de motores o botones de pánico. Hoy las empresas de AMESIS a través de una torre de control virtual, ofrecen monitoreo dedicado, con agentes especializados dentro de sus sistemas.

“Estamos resolviendo para los clientes, antes como prestadores de servicio nos costaba trabajo implementar nuevas tecnologías, porque los manuales vienen en otros idiomas, porque el seguimiento post venta de las marcas no es el que quisiéramos a veces, porque lo haces todo mediante tickets de servicio, y te va contestando un robot, pero cada tres horas, y entonces, no hay información completa.

Hoy, con un agente especializado, lo entrenamos y enseñamos con una base de conocimiento los protocolos de comunicación estandarizados para los equipos de rastreo y su respectivo sistema para hacer las integraciones nuevas, que tarda en promedio tres horas para integrarlo y probarlo; con ello, no hay

necesidad sacar un ticket y ‘subirse’ a una plataforma a la que se debe adaptar”, refirió el directivo.

A partir de la integración de modelos de IA a los procesos diarios se ha logrado mayor eficiencia y alcanzar metas, así como ventajas tecnológicas frente a la competencia que está quedando en el rezago operativo, y se puede decir que se ha empezado a rebasar a muchos proveedores que no están usando IA.

Hoy los clientes de rastreo satelital exponen sus necesidades y un LLM específico trabaja en la solución que le resuelve realmente al usuario final, que se adapte a los requerimientos, incluso vs softwares tradicionales de tráfico y rastreo satelital, afirmó el directivo.

IA vs robo de camiones

Para la AMESIS, la IA combate el robo al transporte de carga al pasar de un simple rastreo satelital reactivo a modelos predictivos que anticipan los atracos con minutos u horas de ventaja.

La IA puede analizar grandes volúmenes de datos históricos y en tiempo real para identificar patrones y predecir posibles robos. Al detectar anomalías como desvíos de ruta, paradas no programadas o cambios bruscos de velocidad, puede alertar a las empresas de rastreo y autoridades.

- Antelación de riesgos: Los algoritmos analizan cientos de variables como el historial delictivo, el clima, los horarios y las zonas rojas para calcular la probabilidad de un asalto antes de que la unidad inicie su viaje.
- Alertas: Herramientas como asistentes virtuales pueden predecir incidentes con hasta 25 minutos de anticipación o detectar anomalías en la conducción.
- Respuesta: Nuevos sistemas extienden la capacidad de predicción entre 60 y 90 minutos al identificar reducciones de velocidad injustificadas o aperturas de puertas no autorizadas.
- Trayectos optimizados: Traza rutas y evita zonas de alto riesgo
- Comunicación automatizada: Por paros de la unidad no autorizados, se emiten de forma automática llamadas de alerta al conductor.
- Coordinación de respuestas: Alertas en tiempo real para maximizar coordinación con autoridades y prestadores de telemetría. 📡

Atentado al carruaje blindado del zar alejandro II

Los primeros vehículos civiles blindados aparecieron mucho antes que los tanques. Se puede considerar que el carruaje del Zar Alejandro II fue uno de los primeros intentos de protección blindada en carros oficiales rusos tras varios intentos de asesinato fallidos, este carruaje tirado por caballos se caracterizaba por contar con placas de acero debajo de la estructura, fue un obsequio de Napoleón III de Francia. Construidos principalmente de madera y hierro recubiertos de cuero, los zares y la nobleza poseían colecciones de carruajes suntuosos para ceremonias, incluyendo modelos cerrados y blindados como el que se utilizaba en 1881. El carruaje de Alejandro II se llamaba "Brougham" en honor al escocés Lord Brougham quien popularizó este tipo de carruajes, aunque en realidad eran fabricados en Londres por la casa Robinson&Cook. Tenía un habitáculo cerrado con dos puertas, como la sección trasera de otros coches de la época contaba con dos asientos y un asiento de caja en el frente para el conductor y un acompañante. A diferencia de otros carruajes, el Brougham tenía una ventana frontal acristalada, de modo que los ocupantes podían ver hacia adelante. Las ruedas delanteras eran capaces de hacer giros con facilidad.

La mañana del 1 de marzo de 1881, el Emperador ruso Alejandro II (1818-1881) visitó la iglesia de San Petersburgo, como solía hacer casi todos los domingos. A las 12:45, se dirigió al picadero Mikhailovsky (academia de equitación) para asistir al entrenamiento de la caballería imperial. Sin embargo, 40 minutos después, decidió marcharse para visitar a su prima, la duquesa Catalina Mijáilovna de Rusia, que vivía cerca. Este repentino cambio de planes frustró el complot terrorista para asesinarlo ese mismo día, mediante el cual habían colocado una potente bomba bajo una calle de San Petersburgo, en su ruta habitual.

De regreso de su Palacio de Invierno, un grupo de apoyo de la organización revolucionaria terrorista Narodnaya Volya ("Voluntad del Pueblo") se preparaba para el atentado tras el fallido intento durante la procesión imperial. Nikolai Rysakov, miembro de Narodnaya Volya, se acercó a la procesión y arrojó una bomba bajo las ruedas del carruaje blindado del Emperador. Algunos de sus guardias murieron. El Emperador, sin embargo, salió ileso. El incidente no le impidió persignarse y preguntar si los terroristas habían sido capturados. Desafortunadamente, desobedeció las instrucciones de su oficial de marcharse de inmediato. No estaba acostumbrado a recibir órdenes. En cambio, se detuvo para comprobar el estado de las víctimas y de su carruaje. Incluso amenazó a los terroristas con el dedo. En ese momento, otro



miembro, Ignaty Grinevitsky, le gritó al Zar, que se encontraba entre las ruinas humeantes: "¡Es demasiado pronto para dar gracias a Dios!", y detonó una segunda bomba a los pies del Emperador.

Tras disiparse el humo, Grinevitsky yacía muerto, mientras que el Emperador estaba gravemente herido. Sus hombres, a quienes se les había confiado su seguridad, no sabían qué hacer. Según un historiador, habrían detenido la hemorragia y le habrían salvado la vida si lo hubieran trasladado de urgencia al hospital militar cercano. En lugar de desobedecer las órdenes del Emperador, lo atendieron en su Palacio de Invierno, pero falleció aproximadamente 45 minutos después.

En su libro "El precio del paraíso", Lain Overton afirma que la bomba que mató a Alejandro II pesaba solo dos kilos y medio y tenía un alcance de explosión de un metro. Los atacantes se vieron obligados a elegir entre dos opciones: lanzar las bombas desde lejos y arriesgarse a fracasar, o detonarlas a muy corta distancia, matando tanto al atacante como a la víctima. La muerte del atacante era el precio del éxito, y así comenzó la era de los atentados suicidas. Tony Scotti, de la International Security Driver Association afirma que el Zar Alejandro fue efectivamente una de las primeras víctimas de un atentado a una caravana en un vehículo blindado y va más allá recordando que la premisa que funciona hoy en día habría funcionado entonces, proteger al principal y abandonar la zona de peligro. 🌐



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

Articlista Invitado



TU OPERACIÓN LOGÍSTICA SIEMPRE PROTEGIDA



GPS & RASTREO

Flota · Activos · Carga



VIDEO TELEMÁTICA

IA embarcada · Eventos



DIAGNÓSTICO SCS

OEA · C-TPAT · BASC



ANGEL GUARDIAN

Control IA/RFID



FLEETCONTROL PRO

Gestión de flota



PREVENCIÓN DE PÉRDIDAS

Robo · Fraude · Merma

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

De experiencia

+ 50,000 EQUIPOS GPS

Activos

4 PAÍSES

Méx · Col · EUA · Arg

24/7/365

Sin interrupciones

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

Más allá de la calidad: el impacto de iso 9001:2026 en la seguridad

1 de 2 partes

Cancún, México.- Introducción: Claridad metodológica ante la coyuntura normativa: El 16 de septiembre de 2026 se oficializó la publicación de la sexta edición del estándar internacional ISO 9001:2026, sucediendo formalmente a la versión de 2015. Con este hito, como suele ocurrir en los procesos de transición de estándares de la Organización Internacional de Normalización (ISO), han comenzado a circular interpretaciones apresuradas, lecturas descontextualizadas e imprecisiones sobre su alcance transversal.

Desde la perspectiva de la seguridad estratégica y la gestión integral de riesgos, es imperativo establecer los límites y el rigor técnico desde el inicio: ISO 9001:2026 no deroga, no modifica ni reemplaza el cuerpo normativo de ninguna otra norma técnica internacional.

Estándares rectores para la comunidad de seguridad y resiliencia —tales como ISO 22301 (Continuidad del Negocio), ISO 28000 (Seguridad en la Cadena de Suministro), ISO/IEC 27001 (Seguridad de la Información), ISO 18788 (Operaciones de Seguridad Privada), ISO 45001 (Seguridad y Salud en el Trabajo) y los marcos de prevención ambiental como ISO 22341 (Prevención del Delito mediante el Diseño Ambiental, CPTED)— mantienen plenamente vigentes sus cláusulas y su arquitectura técnica.

Sin embargo, el impacto de ISO 9001:2026 sobre la función de seguridad es innegable e interactúa a través de tres vías concretas:

- La Estructura Armonizada (Harmonized Structure): la adopción del marco común para normas de sistemas de gestión (HLS/HS) que perne a todas las disciplinas de control y gobernanza.
- La integración de procesos críticos: el blindaje de la cadena de valor mediante la resiliencia operativa y la mitigación de interrupciones.
- El gobierno corporativo y la cultura de cumplimiento: la formalización del comportamiento ético, la rendición de cuentas y la conciencia del riesgo/oportunidad en el entorno organizacional.

Un análisis comparativo entre la versión ISO 9001:2026(es), la NMX-CC-9001-IMNC-2015 y la histórica edición 2008 permite desglosar con precisión los verdaderos cambios

sustantivos que los líderes de seguridad deben incorporar en su radar estratégico.

Análisis técnico de los cambios estructurales:
1. Capítulo 3: Armonización conceptual y precisión taxonómica:

El capítulo 3 ahora integra 20 definiciones esenciales homologadas para los sistemas de gestión (incluyendo organización, parte interesada, alta dirección, riesgo, proceso, competencia, desempeño, auditoría y eficacia).



Para el profesional de seguridad, contar con una semántica estandarizada en el marco de la Alta Dirección elimina ambigüedades operativas y audita con mayor nitidez la interfaz entre la seguridad corporativa y los procesos sustantivos de la organización.

2. Capítulo 4: Contexto organizacional, gobernanza y enmienda climática:

El apartado 4.1 formaliza el mandato de determinar si el cambio climático constituye una cuestión pertinente para el contexto, mientras que el 4.2 subraya las expectativas de las partes interesadas al respecto.

- Impacto en seguridad: Los eventos climáticos extremos ya no pueden tratarse como contingencias aisladas; forman parte del inventario de amenazas directas a la infraestructura crítica, la cadena de suministro y la integridad de las instalaciones.
- Adicionalmente, el 4.2 introduce una exigencia de gobernanza clave: definir de forma explícita cuáles requisitos de las partes interesadas se atenderán formalmente a través del sistema, fortaleciendo el cumplimiento regulatorio, contractual y comunitario.

3. Capítulo 5: Cultura organizacional, ética y liderazgo con propósito:

El apartado 5.1.1 exige de la Alta Dirección la promoción activa de una cultura de la calidad y de comportamiento ético, separando categóricamente el pensamiento basado en riesgos del pensamiento basado en oportunidades.

Esto se articula de manera directa con:

- El apartado 7.3 (Toma de conciencia), exigiendo que el factor humano comprenda y viva esa cultura ética y preventiva.
- El apartado 7.1.4 (Ambiente para la operación de los procesos), reconociendo que los factores psicosociales, de integridad y conductuales inciden de forma determinante en la seguridad y continuidad operativa.

4. Capítulo 6 (6.1 y 6.3): La bifurcación metodológica de Riesgos vs. Oportunidades y Gestión del Cambio

El cambio modular de la norma se concentra en el apartado 6.1, que se desglosa formalmente en:

- 6.1.1 Determinación.
- 6.1.2 Acciones para abordar riesgos.
- 6.1.3 Acciones para abordar oportunidades.

A diferencia del enfoque de 2015, la edición 2026 demanda determinar, analizar y evaluar ambos conceptos por vías independientes, exigiendo acciones estrictamente proporcionales al impacto.

Nota técnica de alta relevancia para la seguridad: La nota del 6.1.2 incorpora de forma explícita los riesgos asociados a la capacidad de entregar productos y servicios conformes durante y después de una interrupción. Aunque el Anexo A aclara que no se impone una metodología formal ni un proceso documental rígido —remitiendo a las directrices de ISO 31000 como estándar guía—, esta nota conecta directamente la calidad con la continuidad del negocio (ISO 22301) y la resiliencia en la cadena de suministro (ISO 28000).

Por su parte, el apartado 6.3 (Planificación de los cambios) eleva de cuatro a siete

consideraciones clave, incorporando la comunicación del cambio, la medición de su eficacia, la revisión de resultados y la disponibilidad de recursos, incluyendo explícitamente a la información como activo estratégico.

5. Capítulos 8, 9 y 10: Continuidad operativa, evaluación y mejora continua

- Operación (Capítulo 8): El apartado 8.2.1 obliga a que la comunicación con clientes incluya planes y acciones de contingencia ante interrupciones. Asimismo, el 8.4.3 impone el deber de comunicar a proveedores externos las reglas de interacción no solo con clientes, sino con otras partes interesadas, aspecto vital en contratos de seguridad física, patrimonial y tecnológica.
- Evaluación del Desempeño (Capítulo 9): La revisión por la dirección (9.3.2) y el análisis y evaluación (9.1.3) deben evaluar por separado la eficacia de las acciones ante riesgos y ante oportunidades. Las auditorías internas (9.2.2) deben contar con



objetivos explícitos en cada ejercicio.

- Mejora (Capítulo 10): Se reorganiza la arquitectura lógica: se antepone la mejora continua (10.2) a la no conformidad y acción correctiva (10.1).

(Continuará...)

Dra. Mercedes Escudero Carmona

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

Articlista Invitado

La seguridad es irremediablemente ... maternal

Lima, Perú.- En la seguridad, afirmar que esta es maternal suena raro al principio. Pero si observamos bien, notamos que la seguridad tiene similitudes con una madre: proteger, cuidar y prever. Ese es el punto que vamos a demostrar, con ejemplos de la vida personal, social y gubernamental. Vamos a explicar cómo esas cualidades de una madre se manifiestan en la seguridad, con datos y teorías.

La Protección como Pilar Fundamental

La primera parte de la seguridad que se parece a lo maternal es la protección. Las madres cuidan a sus hijos y evitan que les pase daño. Esa misma protección forma parte de cualquier sistema de seguridad. Según Maslow (1943), la seguridad y la protección son necesidades básicas, justo después de las necesidades fisiológicas. En la sociedad, los gobiernos y las instituciones actúan como una madre al crear leyes y normas para proteger a la gente de peligros internos y externos. Ese paralelismo muestra que la seguridad se comporta como una madre.

El Cuidado como elemento esencial

Otro rasgo de una madre es el cuidado. El cuidado significa estar pendiente de lo que necesita otra persona y ayudar cuando hace falta. En la seguridad, el cuidado se ve en políticas y programas que mejoran la vida de la gente. Por ejemplo, los servicios de salud pública y los sistemas de seguridad social son ejemplos de cuidado maternal, porque buscan atender a los ciudadanos y protegerlos de la enfermedad, la pobreza y el desempleo (Giddens, 1991).

La Previsión y la planificación

La previsión también es una cualidad maternal. Una madre piensa en el futuro, prepara alimentos, revisa la casa y se asegura de que todo esté listo para lo que pueda venir. En la seguridad, la previsión se traduce en planes de contingencia, simulacros y análisis de riesgos. Los gobiernos elaboran planes de emergencia, los organismos de seguridad hacen simulacros de desastres y las empresas crean protocolos para proteger a sus empleados. Esa planificación anticipada es una forma de cuidar y proteger, igual que lo hace una madre.

En resumen, la seguridad comparte con lo maternal la protección, el cuidado y la previsión. Cuando la seguridad actúa como una madre, la gente se siente más segura, más cuidada y preparada para lo que venga.

La previsión es una cualidad maternal que resulta esencial para la seguridad. Las madres

suelen planificar y anticipar el futuro para que sus hijos tengan lo necesario y puedan crecer. De forma parecida, la seguridad necesita previsión y una planificación estratégica que reduzca los riesgos que puedan aparecer. Esa previsión se muestra en la gestión de riesgos y en la planificación de emergencias, donde las autoridades deben anticipar posibles desastres y crear planes de contingencia para reducir sus efectos. La capacidad de prever y planificar resulta clave para lograr un entorno seguro y estable (Beck, 1992).



Implicaciones sociales y políticas

El reconocer que la seguridad tiene un carácter maternal implica cambios importantes en el diseño y la ejecución de las políticas de seguridad. Al adoptar un enfoque maternal, los responsables de la política pueden dar prioridad a la protección, al cuidado y a la previsión en sus estrategias. Ese enfoque no solo mejora la efectividad de las políticas de seguridad, sino que también fomenta una cultura de empatía y de responsabilidad social. En un mundo cada vez más conectado y complejo, esas cualidades maternas pueden servir como un marco útil para enfrentar

retos de seguridad global, como el cambio climático, el terrorismo y las pandemias.

Críticas y consideraciones

Aun cuando un enfoque maternal aporta ventajas a la seguridad, existen críticas. Algunos sostienen que la idea de seguridad maternal refuerza estereotipos de género que asocian lo maternal solo a las mujeres, dejando fuera a otras personas que también pueden ser protectoras y cuidadoras. Sin embargo, si se entiende lo maternal como un conjunto de cualidades y no como un rol de género, se puede superar esa barrera y aplicar esos principios de forma inclusiva.

Mis conclusiones y convicciones

Adoptar la previsión y el cuidado maternal en la seguridad permite crear políticas más protectoras, empáticas e inclusivas.

Para terminar, la seguridad se parece mucho a la forma en que una madre cuida. La seguridad protege, cuida y piensa en el futuro. Esa forma de proteger no depende del género; es un compromiso de todos para que la comunidad esté bien. Si las políticas de seguridad toman esas cualidades de madre, serán más comprensivas y servirán mejor, creando un lugar más seguro para cada persona. Así, la seguridad, en su esencia, muestra los valores de una madre que son clave para que la sociedad

crezca y se mantenga estable.

Desde mi experiencia personal, nada impactó mi vida de forma más drástica y genuina, que recibir esa asignación tan maravillosa de ser madre y desde entonces la visión de la seguridad para mí, cambió. 🌍

Referencias

- Beck, U. (1992). "Risk Society: Towards a New Modernity". Sage Publications.
- Giddens, A. (1991). "Modernity and Self-Identity: Self and Society in the Late Modern Age". Stanford University Press.
- Maslow, A. H. (1943). "A Theory of Human Motivation". Psychological Review, 50(4), 370-396.



Laura Alcas
CEO de softguard
Presidente de la Asociación
Latinoamericana de Seguridad,
ALAS Capítulo Perú

Perú

Articulista Invitado

Escucha —|||—

NUESTRO PODCAST

a través de Spotify



Patrocinador:



MOTOROLA
SOLUTIONS



Solo será por hoy

Cuando la excepción se convierte en el verdadero sistema de seguridad

Quito, Ecuador.- Son las 06:58. La fila frente al acceso comienza a crecer. El lector biométrico tarda más de lo previsto, un vehículo espera autorización y el cambio de turno no puede detenerse. El supervisor mira el reloj. Alguien pronuncia una frase que parece razonable: «Ábrale; solo será por hoy». El guardia obedece, la operación continúa y nada ocurre. No hay intrusión, pérdida ni alarma. La excepción parece haber funcionado.

Al día siguiente, repetirla cuesta menos. Una semana después, ya no se explica. Con el tiempo, el procedimiento continúa escrito, pero la práctica real circula por otro camino. El control permanece en la política y, posiblemente, en un indicador de cumplimiento. Sin embargo, dejó de gobernar la conducta.

Diane Vaughan (2016) estudió cómo ciertas anomalías fueron aceptadas dentro de la NASA antes del desastre del Challenger. Su concepto de normalización de la desviación explica un mecanismo inquietante: si una práctica se aparta de lo previsto y no produce consecuencias inmediatas, la organización puede considerarla tolerable. No cabe equiparar una excepción de acceso con una tragedia aeroespacial; sí reconocer la misma trampa: confundir ausencia de daño con evidencia de seguridad.

En protección solemos buscar al responsable visible. Es fácil señalar al guardia que abrió o al trabajador que prestó su credencial. Es una explicación rápida, pero incompleta. Reason (2000) diferenció el enfoque centrado en culpar a la persona del enfoque sistémico, que examina sus condiciones de trabajo. Cuando seguridad exige verificar cada ingreso, operaciones exige evitar demoras y la dirección demanda ambas cosas sin resolver la contradicción, el incumplimiento deja de ser solamente individual.

Un control que funciona únicamente cuando hay poco flujo, tiempo suficiente y ninguna presión no es un control robusto. Es una condición ideal disfrazada de seguridad.

Beautement, Sasse y Wonham (2008) entrevistaron a 17 trabajadores de dos grandes organizaciones y concluyeron que cumplir una política se relaciona con los costos y beneficios percibidos. Los autores denominaron compliance budget al esfuerzo limitado que las personas pueden dedicar al cumplimiento. Stanton et al. (2016), en un estudio cualitativo con 40 participantes, encontraron que más de la mitad aludió a fatiga de seguridad, expresada en resignación, pérdida de control y minimización del

«No podemos cambiar la condición humana, pero sí las condiciones bajo las cuales las personas trabajan».
—James Reason (2000, traducción propia)

FIGURA 1

Cuando la excepción se convierte en sistema

La ausencia de incidentes no demuestra que el control sea eficaz.



UNA EXCEPCIÓN CONTROLADA DEBE TENER

- 01 Causa documentada
- 02 Responsable definida
- 03 Fecha de cierre
- 04 Control compensatorio
- 05 Cierre verificado

Medir: excepciones abiertas - venidas - nacientes - cerradas y verificadas

Fuente: elaboración propia de Edison Cordero Ayala con base en Reason (2000), Beautelement et al. (2008), Stanton et al. (2016) y Vaughan (2016).

riesgo. Ambos trabajos pertenecen a la seguridad de la información; trasladarlos directamente a la seguridad física sería incorrecto. Aun así, el mecanismo conductual merece atención: si proteger exige luchar contra el sistema de trabajo, las personas crean atajos.

Propongo llamar deuda operativa de seguridad a la acumulación de excepciones que permiten continuar hoy a cambio de debilitar la protección mañana. Surge cuando una puerta permanece abierta «por unas horas», una cámara queda pendiente hasta el siguiente mantenimiento, una credencial se comparte para ganar tiempo o un acceso temporal continúa activo sin fecha de cierre. Cada decisión puede tener una razón legítima.

El problema comienza cuando la excepción no tiene causa documentada, responsable, plazo, control compensatorio ni verificación de cierre.

Esta deuda casi nunca aparece en el presupuesto. Se reconoce en frases: «siempre lo hemos hecho así», «nunca ha pasado nada» o «después lo regularizamos». También puede medirse. La organización debería conocer cuántas excepciones mantiene abiertas, su antigüedad, cuáles vencieron, cuáles se repiten y qué porcentaje fue cerrado y verificado. Los tiempos de acceso en horas de mayor flujo, los rechazos de credenciales y las aperturas manuales ayudan a distinguir entre indisciplina y un control mal dimensionado.

La conclusión es incómoda: algunas vulnerabilidades no ingresan desde el exterior. Se construyen internamente cada vez que una solución temporal se vuelve costumbre y nadie conserva la obligación de cerrarla. Por eso, revisar documentos no basta. Hay que observar la instalación cuando aumenta la fila, llega el proveedor, falla la tecnología o la producción presiona. Allí se descubre si el sistema protege bajo condiciones reales.

El llamado a la acción es concreto. Recorra su operación y pregunte a quienes ejecutan los controles: ¿qué parte del procedimiento deben evitar para poder trabajar?, ¿qué excepción dejó de sentirse excepcional?, ¿quién tiene autoridad y plazo para cerrarla? Escuchar esas respuestas no debilita la seguridad. Permite rediseñarla antes de que el incidente revele, de la peor manera, lo que la rutina ya había normalizado. Tal vez el verdadero punto de quiebre no sea el día en que alguien atraviesa una puerta sin autorización. Tal vez ocurrió mucho antes, la primera vez que dijimos «solo será por hoy» y aceptamos que, como nada sucedió, el riesgo tampoco existía. 🌐

Referencias

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. En Proceedings of the 2008 New Security Paradigms Workshop (pp. 47–58). Association for Computing Machinery. <https://doi.org/10.1145/1595676.1595684>

Reason, J. (2000). Human error: Models and management. BMJ, 320(7237), 768–770. <https://doi.org/10.1136/bmj.320.7237.768>

Stanton, B. C., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. IT Professional, 18(5), 26–32. <https://doi.org/10.1109/MITP.2016.84>

Vaughan, D. (2016). The Challenger launch decision: Risky technology, culture, and deviance at NASA (edición ampliada). University of Chicago Press. (Trabajo original publicado en 1996)



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

Articulista Invitado

AJAX

DOMINA TU ESPACIO

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



FireProtect 2

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



Dónde comprar

www.ajax.systems

La influencia discreta de la ingeniería en seguridad

Cómo la profesionalización de la seguridad patrimonial puede convertir una función de protección en una fuente de inteligencia y valor para el negocio.

Lima, Perú.- Eran las 10:47 de la mañana y el equipo comercial seguía sin entender por qué había caído el tráfico en uno de los centros comerciales más importantes de la compañía. Un área le echaba la culpa a una campaña poco efectiva, otra dudaba de la dotación operativa y alguien más ya estaba armando promociones para atraer de nuevo a los clientes. Pasaron varios días cruzando cifras e hipótesis buscando una explicación que ya estaba disponible dentro de la propia organización, no en un reporte financiero sino en los sistemas que operan a diario detrás del negocio.

Cuando por fin se cruzaron los datos de videovigilancia, la analítica de flujo y el conteo de personas con los indicadores comerciales,

La tecnología que se instaló para proteger a las organizaciones terminó convirtiéndose, casi sin buscarlo, en una de las fuentes de información más valiosas para tomar decisiones, porque cámaras, controles de acceso, sensores y plataformas de monitoreo generan datos que dicen cómo se mueven las personas, cómo se ocupan los espacios y hacia dónde va la operación en tiempo real.

La pregunta de fondo cambió: ya no es solo cómo proteger mejor una organización, sino cómo tomar toda esa información que ya existe y convertirla en algo que ayude a decidir mejor.

Y aquí conviene aclarar una idea: el valor de la seguridad moderna no está tanto en los equipos que



apareció algo que nadie esperaba: la afluencia no había bajado; lo que había caído era la conversión. Los clientes seguían entrando, solo que pasaban menos tiempo en las zonas que por lo general concentraban la mayor parte de las ventas, y el área que detectó primero ese comportamiento no fue comercial ni marketing, sino seguridad.

Ese episodio resume algo que viene ocurriendo hace tiempo en muchas organizaciones, casi sin que nadie lo note. Durante décadas, la seguridad patrimonial se entendió como una función defensiva encargada de proteger a las personas, cuidar activos, prevenir incidentes y mantener la operación en marcha, y esa parte de la misión sigue siendo igual de importante, aunque ya se quedó corta.

se instalan, sino en los datos que producen y, sobre todo, en la capacidad de leerlos bien. Una cámara puede funcionar como un sensor de comportamiento, el conteo de personas puede mostrar patrones de circulación y permanencia, y un control de acceso puede decir bastante sobre cómo se usa realmente un espacio.

De ahí surge la necesidad de profesionalizar esta función. El especialista de hoy ya no puede quedarse solo en el manejo de plataformas, equipos o protocolos; le toca entender de analítica de datos, inteligencia artificial, continuidad de negocio, experiencia del cliente, gestión de riesgos y estrategia corporativa. Su verdadero aporte está en traducir toda esa información técnica en algo útil para la organización, y en la práctica, profesionalizar significa dejar

de administrar dispositivos y empezar a gestionar capacidades, dejar de reaccionar ante lo que ya pasó y empezar a interpretar patrones antes de que se conviertan en un problema.

Esto se nota especialmente en el retail por que pocas áreas cuentan con una infraestructura tan repartida por toda la operación, tan constante y tan pegada al día a día como seguridad, y mientras otras funciones suelen mirar hacia atrás, revisando resultados históricos. Seguridad está observando el presente: cómo entra la gente, por dónde circula, dónde se detiene y qué tendencias empiezan a asomar antes de que aparezcan en los indicadores tradicionales. Ahora bien, generar valor con esa información no significa usarla toda sin criterio; hace falta un gobierno de datos serio, privacidad, ética, ciberseguridad y un propósito legítimo detrás de cada uso, porque solo así la videovigilancia, la analítica, los controles de acceso y la inteligencia artificial dejan de funcionar como piezas sueltas y empiezan a aportar contexto y conocimiento a toda la organización.

Quizás el cambio más grande sea dejar de vernos únicamente como custodios de activos para empezar a actuar como socios estratégicos del negocio, y esto no significa que seguridad venga a reemplazar a comercial, a BI o a TI, sino que aporta una mirada distinta construida desde el

riesgo, la operación diaria y la tecnología. La integración real no ocurre cuando dos plataformas logran hablarse entre sí, sino cuando esa información conectada termina mejorando una decisión concreta.

En un entorno donde los datos pesan cada vez más, las organizaciones más competitivas no van a ser las que tengan más cámaras o más sensores, sino las que sepan leer lo que esos sistemas producen y convertirlo en decisiones que generen valor de forma sostenida.

Este cambio ya empezó y no arrancó con una cámara nueva ni con un algoritmo más sofisticado, sino que empieza cuando dejamos de preguntarnos únicamente qué pasó y comenzamos a preguntarnos qué significa eso para la organización. Porque la seguridad va a seguir protegiendo personas, activos y procesos críticos como siempre, solo que ahora, gracias a la tecnología, la analítica y la ingeniería, también puede entender lo que está pasando, anticiparse y generar valor de negocio para el negocio.



Jeff Navarro C.
Ingeniero Electrónico y especialista en Seguridad Patrimonial y Seguridad Electrónica. Líder en innovación tecnológica, gestión de riesgos y protección de activos, con enfoque en generar valor estratégico para el negocio a través de la seguridad. Miembro de la International Foundation for Protection Officers (IFPO).
Perú

Articlista Invitado



empresa pionera en integración de robótica en marketing y seguridad



Bogotá, Colombia.- Durante 25 años, Promomarka se ha posicionado en el mercado a través de proyectos de publicidad, marketing estratégico y activaciones de marca. Importante resaltar que hace más de un año la empresa dio un paso clave al incursionar en la robótica, integrando tecnología de vanguardia como parte de su negocio.

En el centro de este desarrollo está Migo, un robot humanoide capaz de interactuar con las personas, desplazarse en

diferentes entornos e integrar sensores avanzados. Promomarka ha enfocado a Migo principalmente en el ámbito comercial y de marca; sin embargo, las características físicas y tecnológicas del robot abren oportunidades para ser aprovechadas por otros sectores, entre ellos la seguridad.

Un ejemplo de ello ha sido Migo en ESS+ 2026, quien, en alianza con la **Mas Seguridad Magazine**, compartió stand en esta feria, una de las más importantes a nivel internacional de este sector, donde el robot humanoide captó la atención de la industria al demostrar cómo su tecnología de interacción y captura de datos puede integrarse con éxito en las operaciones de las empresas líderes en protección y vigilancia.

El rol de Promomarka es actuar como el aliado tecnológico que suministra e integra el robot para que las empresas especializadas del sector de la seguridad puedan implementarlo en sus operaciones.



Contáctanos:

Ernesto Celis Marín, Gestor de Innovación

Whatsapp:

+57 324 3678206 / Bogotá - Colombia

Redes:

@migo.bot

La evolución de la seguridad residencial: un horizonte de profesionalismo, disrupción y factor humano en la propiedad horizontal

Santander, Colombia.- El entorno de la gerencia y administración de PH actual exige una transformación constante, donde el verdadero profesionalismo trasciende lo académico para convertirse en una actitud vital frente al cambio. Esta mentalidad es indispensable para revolucionar uno de los sectores más estáticos, burocráticos y críticos en Colombia y Latinoamérica: la seguridad en la Propiedad Horizontal (PH).

Actualmente, el modelo tradicional de seguridad basado exclusivamente en “horas-hombre” enfrenta una severa e irreversible crisis de insostenibilidad financiera. Proyecciones de CONFEVIP advierten que para 2026, los altos costos laborales de un puesto de vigilancia de 24 horas devorarán gran parte del presupuesto de las copropiedades. A pesar de esto, se vive una “esquizofrenia corporativa”: las comunidades exigen tecnología de punta, pero se resisten ferozmente a abandonar la falsa sensación de seguridad que otorga la presencia física tradicional en la portería.

Para superar este estancamiento, es imperativo redefinir el liderazgo. Citando a Julián Ugarte, un verdadero profesional es aquel con la capacidad de resolver problemas en el mundo real. En la PH, esto significa dejar atrás las barreras manuales y mitigar vulnerabilidades integrando herramientas como la biometría, lectura automática de placas e inteligencia artificial.

Sin embargo, el eslabón que mayor resistencia genera es el personal operativo, que teme ser reemplazado por tótems o software. Recordando la fórmula de Víctor Küppers $V=(C+H) \times A$, es evidente que la actitud (A) del vigilante frente a la innovación es la clave que multiplica su valiosa experiencia en el entorno. Es deber del líder transformar ese pánico en una actitud multiplicadora mediante una transición amigable. Tal como Steve Jobs integró un asa en el iMac para hacerlo menos intimidante psicológicamente, la tecnología en la PH debe presentarse como una herramienta amigable que empodera al guarda.

Este diseño de transición requiere obligatoriamente dignificar los espacios operativos. Un vigilante no puede gestionar tecnología de punta y analizar bases de datos si está confinado en una garita obsoleta. Al modernizar su entorno, el guarda deja de ser un simple “abre-puertas” para convertirse en un analista de riesgos y gestor de convivencia, aportando inteligencia emocional y criterio humano, cualidades irremplazables por las máquinas.

El principal obstáculo directivo es la inexcusable falta de “venia”: la aversión al riesgo de asambleas y administradores que prefieren la comodidad del modelo tradicional antes que atreverse a innovar. Se necesitan líderes disruptivos, dispuestos a desafiar la burocracia del “siempre se ha hecho así”, para implementar ecosistemas tecnológicos híbridos que salven el presupuesto y protejan la vida. Como explica

Ane Agirre, liderar la arquitectura del cambio exige escuchar todas las posturas y crear una “tensión creativa” entre la vulnerabilidad actual y la tranquilidad del futuro deseado.

Finalmente, esta innovación exige un profesionalismo integral. De nada sirve la hiper-especialización técnica si se carecen de habilidades blandas como la empatía y la resolución de conflictos. La tecnología solo tiene sentido cuando es impulsada por profesionales que saben gestionar su impacto humano. En conclusión, la modernización de la seguridad en la PH es un trayecto continuo, similar a la utopía de Eduardo Galeano: sirve para seguir caminando. Solo al abrazar la disrupción y combinar un talento humano empoderado con tecnología de vanguardia, seremos imparables en la construcción de un entorno seguro y moderno. 🌐



Juan Felipe Camargo Sánchez
CEO de CION (Opciones Lógicas en
Propiedad Horizontal)
Colombia

Articlista Invitado



Alianza internacional:



MÁS SEGURIDAD
Magazine

CON SEGURIDAD
Magazine Latam

Ya está en México!



08:00 A. M. - 06:00 P. M.



(57) 3108052421



CRA 27 #82-14 OF. 202 - BOGOTÁ, COLOMBIA

SAR-IA la inteligencia que lleva a SARI de Colombia a México

1 de 2 partes

Seguridad privada, riesgo público y transporte de mercancías conectados por datos, geolocalización e inteligencia artificial.

Bogotá, Colombia.- SARI abre una nueva etapa de expansión con una propuesta tecnológica orientada al mercado mexicano de la seguridad privada y el transporte de mercancías. En el centro de esta evolución está SAR-IA, el asistente de inteligencia artificial integrado a la plataforma para apoyar la identificación, el análisis y la valoración de riesgos, transformar información de campo en conocimiento útil y fortalecer decisiones preventivas y operativas.

De la operación tradicional a una seguridad conectada

La propuesta comercial de SARI parte de una necesidad concreta del sector: disponer de metodologías prácticas para identificar, valorar, medir y monitorear riesgos, al tiempo que se digitalizan actividades que históricamente han dependido de papel, formatos físicos, radios convencionales y archivos ofimáticos.

“La tecnología no sustituye la experiencia del profesional de seguridad: la potencia con información estructurada, alertas y capacidad de análisis”.



Una plataforma pensada para la operación real

- Gestión y administración de riesgos en instalaciones y operaciones.
- Riesgo público con georreferenciación, mapas dinámicos, zonas de concentración y alertas.
- Inspecciones, rondas, novedades, control de accesos, correspondencia y minuta virtual.
- Inspección de contenedores y vehículos de carga para procesos de transporte y cadena logística.
- Información disponible para operaciones, dirección, gerencia y cliente final.
- Arquitectura en la nube, disponibilidad, SSL, ciberseguridad y soporte técnico.

Héctor Blandón: “SARI convierte la información operativa en prevención”

El gerente y cofundador de SARI explica la visión que impulsa la plataforma, el papel de SAR-IA y la manera en que la tecnología busca acompañar a las organizaciones de seguridad en su transformación digital.

¿Qué es SARI y qué problema busca resolver?

Héctor Blandón responde que SARI nació para atender una necesidad recurrente del sector de la vigilancia y la seguridad privada: contar con una herramienta que permita identificar amenazas y riesgos, registrar evidencias en campo, generar reportes inmediatos y convertir la información operativa en acciones preventivas, correctivas y de control. Indica que la plataforma fue desarrollada por ingenieros colombianos

y que su diseño busca ser práctico para vigilantes, supervisores, analistas, coordinadores, directores y gerentes.

¿Qué diferencia a SARI de una aplicación de reportes?

Blandón manifiesta que la diferencia está en la integración. SARI no se limita a capturar una novedad: articula gestión de riesgos, riesgo público, operaciones, recorridos, accesos, PQRS, activos, documentación, comunicaciones y otros módulos en un mismo ecosistema. Agrega que la información puede ser consultada por los responsables internos y por el cliente final, facilitando trazabilidad, indicadores y seguimiento en tiempo real.

¿Por qué incorporar inteligencia artificial?

volumen de información de seguridad crece rápidamente

y la organización necesita convertir datos dispersos en criterios útiles. Por eso, SAR-IA se integra a SARI como un asistente que ayuda a interpretar condiciones del entorno, antecedentes, vulnerabilidades, amenazas y factores de exposición, haciendo más ágil y estructurada la construcción de conceptos de riesgo.

¿SAR-IA reemplaza al analista o al responsable de seguridad?

Blandón aclara que no. SAR-IA complementa el análisis humano y está concebida como una capa de apoyo. El criterio profesional, la validación de la información, la priorización de los controles y la decisión final permanecen bajo responsabilidad de los equipos de seguridad y gestión del riesgo.

Inteligencia artificial aplicada a la identificación y valoración de riesgos



¿Qué hace SAR-IA?

- Interpreta información registrada en SARI.
- Relaciona variables operativas, geográficas y contextuales.
- Apoya la determinación de niveles de criticidad.
- Ayuda a priorizar situaciones que requieren atención.
- Genera criterios, alertas y recomendaciones para apoyar decisiones.
- Fortalece la documentación y trazabilidad del análisis.

“SAR-IA convierte la información disponible en SARI en conocimiento útil para anticipar riesgos y adoptar decisiones más oportunas, documentadas y basadas en información.”

Riesgo público como capa de contexto

SARI Riesgo Público integra georreferenciación, mapas dinámicos, zonas de concentración de eventos, alertas e información sobre hechos de seguridad. A través del análisis de variables como delincuencia, alteraciones de orden público, emergencias, condiciones sociales, eventos naturales y noticias relevantes, la plataforma busca facilitar una lectura visual del nivel de exposición al riesgo. SAR-IA puede apoyarse en esta información para complementar la interpretación del entorno y orientar controles preventivos.

(Continuará...)



Héctor Blandón,
gerente y
cofundador de
SARI

ESS+ 2026

cerró edición marcada por la integración tecnológica y oportunidades para la industria

Bogotá, Colombia.- La Feria Internacional de Seguridad ESS+ concluyó su edición 2026 donde la tecnología, el conocimiento especializado y las necesidades reales de las organizaciones se encontraron en un mismo escenario.

Bajo el concepto “Integración de Tecnologías Globales”, la feria presentó soluciones para la protección de personas, activos, información, operaciones e infraestructura. La muestra permitió conocer avances en seguridad electrónica, protección industrial, prevención de incendios y tecnologías que hoy se articulan para responder a riesgos cada vez más complejos e interconectados.

La presencia de profesionales de telecomunicaciones, tecnología, seguridad pública, privada e industrial, comercio, construcción, logística, educación, gobierno, energía, infraestructura y salud



Durante tres días, la feria reunió en Corferias soluciones, conocimiento y profesionales de distintos sectores alrededor de los nuevos desafíos de la seguridad.

confirmó el alcance transversal de la seguridad. Una misma solución pudo ser analizada desde distintas necesidades, aplicaciones y mercados.

Una audiencia que llegó a conocer, evaluar y decidir

Más que protagonizar el cierre, las cifras ayudan a entender el perfil de quienes recorrieron la feria. El 62,9 % de los visitantes señaló que asistió para actualizarse en nuevas tecnologías y tendencias o buscar productos y servicios. Además, el 76,5 % participa directamente en las decisiones de compra o influye en la recomendación de soluciones.

El interés comercial también estuvo presente en la agenda de los asistentes. Las demostraciones, reuniones y espacios de relacionamiento facilitaron el contacto entre empresas expositoras, compradores, integradores, distribuidores y responsables de proyectos que llegaron a ESS+ con necesidades concretas. Un punto de encuentro con alcance nacional e internacional

ESS+ recibió profesionales de Bogotá y de diferentes regiones de Colombia, junto con visitantes procedentes de mercados de América, Europa y Asia. Esta diversidad amplió las posibilidades de intercambio, permitió identificar nuevas aplicaciones para las soluciones exhibidas y fortaleció la proyección internacional de la feria.

La edición 2026 dejó como resultado una industria que avanza hacia una visión más integrada de la seguridad, en la que la innovación adquiere valor cuando responde a los desafíos operativos de empresas, ciudades e infraestructuras.

La Feria Internacional de Seguridad ESS+ agradece a las empresas expositoras, visitantes, aliados, conferencistas y profesionales que hicieron parte de esta edición. Su participación continúa consolidando a ESS+ como referente para la industria y como una plataforma para presentar innovación, compartir conocimiento y generar nuevas oportunidades de negocio. 🌐



Protección ejecutiva en Family Offices: inteligencia antes que presencia

Buenos Aires Argentina. – Hay una imagen que domina el imaginario sobre la protección ejecutiva: el hombre de traje oscuro, auricular colocado, lentes oscuros, abriendo camino entre la multitud. Es una imagen poderosa, pero incompleta y para quien administra el patrimonio y la seguridad de una familia, puede ser también engañosa.

Durante años trabajé del lado operativo de esa imagen. Con el tiempo entendí algo que cambió por completo mi forma de entender el oficio: un protector ejecutivo no viste de traje por estética. Viste de traje porque su función principal no es reaccionar frente al peligro, sino no generarlo integrarse al entorno, pasar inadvertido, permitir que la persona que protege se mueva con normalidad en un mundo que, para una familia patrimonial, rara vez lo es. El uniforme táctico anuncia una amenaza. El traje la administra en silencio.

Esa misma lógica es la que debería regir la forma en que un family office piensa la seguridad de las familias que representa. La mayoría de los family offices, cuando evalúan seguridad, hacen la pregunta equivocada primero: ¿cuánta gente, qué vehículos, qué presupuesto? Es una pregunta legítima, pero llega tarde. La pregunta que debería hacerse antes es otra: ¿qué decisiones se están tomando sobre la exposición de esta familia, con qué información, y con cuánta anticipación?

Un esquema de protección sin inteligencia previa tiende a ser reactivo; responde a lo que ya ocurrió o a lo evidente. La mitigación de riesgo, en cambio, se ocupa de lo que todavía no pasó, pero es previsible, si alguien se toma el trabajo de leerlo a tiempo.

La exposición de una familia de gran patrimonio neto ya no se limita al mundo físico. Un itinerario de vuelo filtrado, una agenda familiar sincronizada sin protocolo de acceso, o el dispositivo de un hijo adolescente comprometido pueden generar una exposición real física, reputacional o financiera mucho antes de que ocurra cualquier incidente visible.

A esto se suma un vector que muchas veces queda fuera del radar: el propio personal que gestiona el día a día de la familia asistentes, choferes, staff doméstico que maneja información sensible que muchas veces no está incluido en los protocolos de seguridad que sí se aplican a los principales.

Mitigar riesgo, entonces, no es una cuestión de reforzar el

perímetro. Es una cuestión de mapear correctamente dónde está la información sensible y quién tiene acceso a ella, mucho antes de pensar en cualquier despliegue físico.

El otro error frecuente es tratar la seguridad como una contratación puntual; se activa ante un evento, un viaje, una amenaza concreta en lugar de integrarla como una función continua de gobierno familiar, con la misma seriedad con la que se trata la sucesión patrimonial o el cumplimiento normativo.

Esto implica tres cambios prácticos para un family office:

- **Primero**, incorporar la evaluación de riesgo a la mesa donde se toman otras decisiones estratégicas de la familia no como un compartimento aislado a cargo exclusivamente de “el área de seguridad”.
- **Segundo**, adoptar una cadencia de revisión periódica del entorno geopolítico, digital, social en lugar de esperar a que un evento puntual dispare la reacción.
- **Tercero**, y quizás el más difícil culturalmente: aceptar que el éxito en esta materia rara vez es visible. En el modelo reactivo, el éxito se mide por la ausencia de incidentes. En el modelo de gobernanza, se mide por la calidad

de las decisiones anticipadas muchas de las cuales nunca podrán demostrarse públicamente, porque lo que se evita no deja rastro.

Vuelvo a la imagen inicial del oficial de protección con traje porque resume bien la idea de fondo: la protección sería no se anuncia, se integra. No se mide en la cantidad de personas desplegadas, sino en la calidad del criterio que hay detrás de cada decisión. Para un Family Office, proteger no debería significar simplemente reaccionar ante el riesgo, sino incorporarlo a la calidad de las decisiones que toma la familia. Intelligence before presence. 🌐



Gustavo Merani CPO
GSGM Security Consulting
www.gsgmconsulting.com

Argentina

Articlista Invitado

El deterioro de la convivencia

Durante décadas, Chile fue considerado uno de los países más seguros de América Latina. Sin embargo, el incremento sostenido de las incivildades, la pérdida del respeto por las normas de convivencia y el deterioro progresivo del espacio público comenzaron a revelar un fenómeno mucho más profundo. Comprender esas primeras señales resulta fundamental para entender cómo una sociedad puede iniciar el camino hacia formas de criminalidad cada vez más complejas.

Santiago, Chile.- Las incivildades representan aquellas conductas que, sin constituir necesariamente delitos graves, vulneran las reglas básicas que permiten la vida en comunidad. Su efecto no radica únicamente en el daño material que producen, sino en el mensaje que transmiten: las normas pueden incumplirse sin consecuencias. Cuando esa percepción comienza a instalarse, disminuye la capacidad de autorregulación de la sociedad y aumenta la tolerancia frente a comportamientos cada vez más transgresores. Poco a poco, la ciudadanía modifica su conducta, deja de utilizar determinados espacios públicos, reduce su interacción comunitaria y comienza a aceptar el deterioro como parte de la vida cotidiana.

Desde la criminología, distintas investigaciones han sostenido que el deterioro persistente del espacio público puede favorecer procesos de escalamiento delictual cuando no existe una intervención oportuna del Estado y de la comunidad. No se trata de afirmar una relación automática entre una incivildad y un delito grave, sino de comprender que el abandono sostenido del entorno reduce la cohesión social, debilita la confianza en las instituciones y genera condiciones que pueden

ser aprovechadas por organizaciones criminales. En otras palabras, el crimen organizado no necesita crear el desorden; le basta con instalarse donde el desorden ya ha sido aceptado.

Diversas ciudades del mundo han comprendido que recuperar el espacio público constituye una verdadera política de seguridad. La experiencia desarrollada en ciudades como Nueva York durante la década de 1990, así como programas implementados posteriormente en Singapur, Tokio y diversas ciudades europeas, demostró que la intervención temprana sobre el deterioro urbano, la recuperación de espacios públicos, la fiscalización permanente y el fortalecimiento de la convivencia ciudadana contribuyen significativamente a reducir factores de riesgo asociados al desarrollo de fenómenos criminales más complejos.

La cooperación policial internacional también ha permitido observar un patrón común: las organizaciones criminales buscan instalarse preferentemente en territorios donde el control institucional es débil, la autoridad pierde legitimidad y la comunidad comienza a normalizar situaciones de ilegalidad cotidiana. En distintas regiones del mundo, el crimen organizado ha demostrado una enorme capacidad para identificar estos espacios de vulnerabilidad e incorporarlos gradualmente a sus áreas de influencia. La experiencia





internacional enseña que la mejor estrategia contra el crimen organizado comienza mucho antes de que aparezca el crimen organizado.

Durante los últimos años, Chile ha observado cómo numerosos espacios públicos comenzaron a deteriorarse simultáneamente con el incremento de otros fenómenos de mayor gravedad. Las incivildades dejaron de percibirse como simples problemas municipales para transformarse en señales tempranas de procesos más amplios de pérdida de control territorial. Muchos barrios comenzaron a experimentar una disminución del uso legítimo de plazas, parques y espacios comunes. El comercio ambulante ilegal ocupó sectores estratégicos de diversas ciudades. Las denuncias por ruidos molestos, vandalismo y daños aumentaron, mientras la percepción de inseguridad crecía incluso en lugares donde la delincuencia violenta aún era relativamente baja.

La principal lección que ofrece la experiencia chilena es que las incivildades no deben analizarse de manera aislada. Forman parte de un ecosistema mucho más amplio donde el deterioro de la convivencia facilita posteriormente la aparición de economías ilegales, ocupaciones irregulares, extorsiones, violencia organizada y, finalmente, estructuras criminales capaces de disputar espacios de poder al propio Estado.

El desafío pendiente

Chile ha impulsado importantes iniciativas para fortalecer la seguridad pública, recuperar espacios urbanos y modernizar sus instituciones. Sin embargo, el mayor desafío continúa siendo incorporar una visión verdaderamente preventiva que considere las incivildades como un problema estratégico y no simplemente como infracciones menores. La seguridad comienza mucho antes de la actuación policial. Comienza en la capacidad de una sociedad para preservar sus normas de convivencia, proteger sus espacios comunes y fortalecer permanentemente la cultura de la legalidad. Ello exige fortalecer el trabajo coordinado entre municipios, policías, establecimientos educacionales, organizaciones sociales y ciudadanía; mejorar los sistemas de fiscalización; recuperar oportunamente los espacios públicos deteriorados; promover una formación ciudadana orientada al respeto de las normas y desarrollar políticas de intervención temprana capaces de actuar antes de que el deterioro evolucione hacia formas de criminalidad mucho más complejas.

Las grandes amenazas rara vez aparecen sin anunciarse, siempre dejan señales. La diferencia entre una sociedad que logra contener el avance del crimen y otra que termina conviviendo con él depende, muchas veces, de su capacidad para reconocer esas señales cuando todavía parecen insignificantes. 🇨🇱



Richard Biernay Arriagada / Consultor Senior
Especialista en Seguridad Pública y Gobernanza territorial
Es Ingeniero Civil Industrial, Relacionador Público, Magister en Didáctica para la Educación Superior y Oficial Superior en retiro de la Policía de Investigaciones de Chile (PDI). Fue Jefe de Interpol Chile, Jefe del Laboratorio de Criminalística Central, Jefe de la Prefectura Colchagua y Cardenal Caro y Agregado Policial de Chile en Emiratos Árabes Unidos. Fue Premio Nacional de Relaciones Públicas de Chile 2021, actualmente se desempeña como consultor senior y académico en materias de seguridad, comunicación estratégica y gobernanza institucional. Correo: biernay@gmail.com

Chile

Articulista Invitado

Repetiremos la fórmula para la edición 2027 de Expo Seguridad Bucaramanga

Santander, Colombia. - Rotundo fue el éxito de la primera edición de Expo Seguridad Bucaramanga 2026, feria que por dos días consecutivos fue el escenario para la muestra tecnológica y conferencias impartidas por expertos. Más de mil 200 personas se dieron cita. **México** fue el país invitado de honor y **Más Seguridad Magazine** el encargado de inaugurar dicho foro.

De acuerdo con Mauricio Espinoza Gualdrón, director ejecutivo del Grupo Empresarial Integra, empresa organizadora de Expo Seguridad Bucaramanga, desde el primer día de actividades se vio un aforo interesante de usuarios finales, integradores, distribuidores, gerentes y directores de seguridad de diversas verticales, pues en esta ciudad colombiana, nunca se había organizado un foro tan especializado. “Las personas estaban interesadas en todo lo que tiene que ver con el tema tecnológico, domótica, robótica y por supuesto todos los avances en seguridad y vigilancia privada”, acotó.

Importante resaltar que la feria inició con 33 empresas expositoras, lo que habla de la buena respuesta del sector ante un evento que se realizó por primera vez, ello por su logística y organización, estructura académica y talleres prácticos.

Respecto al ciclo de conferencias impartidas por expertas y expertos de Bucaramanga, Medellín, Bogotá y Cali, Espinoza Gualdrón aseveró que se hizo una selección a través de una convocatoria donde se evaluaron los temas y su impacto en el sector con tendencias en seguridad electrónica, inteligencia artificial (IA), robótica, drones o ciberseguridad.

Fue una exposición, -afirmó el directivo- enfocada a la tecnología, todo lo que viene de la mano con la IA, hoy el guarda de seguridad habitual que conocemos no va a quedar relegado, pero sí va a pasar a unas tareas totalmente diferentes y alternas. Vimos tendencias en control de acceso personal con reconocimiento facial o vehicular con chips. La oferta fue con nuevas oportunidades de negocio y mejores costos.

Expo Seguridad Bucaramanga fue posible gracias al trabajo de un equipo de 40 personas que durante 11 meses crearon desde cero el evento, sin embargo, Grupo Empresarial Integra, posee amplia experiencia en la organización de relevantes foros como el Gran Salón de la Propiedad Horizontal, feria enfocada en este nicho de negocios.

Ante los resultados alentadores ya se planea la versión 2027 en Bucaramanga, incluso se estima hacer itinerante el evento en 2 o 3 ciudades más de Colombia; la primera de ellas sería entre los meses de abril o mayo próximos, con la novedad de abrir a otros nichos de la industria como sistemas contra incendios, alarmas y safety.

¿Cuál sería también la expectativa en números? En cuanto a expositores, crecer un 50% y alcanzar los 2 mil visitantes por día, así como abrir la temática de las conferencias a otros nichos de la industria



con ponentes nacionales e internacionales.

Respecto al perfil del expositor se espera que en 2027 se repita la fórmula de mayoristas, y se sumen fabricantes de forma directa. “Yo creo que podemos trabajar de manera conjunta las dos alternativas. Hay interés de otros fabricantes porque no alcanzaron a sumarse este año porque ya habíamos cerrado o vienen de otros países, hay algunas intenciones de gente de Panamá, de Venezuela y Perú”, refirió Mauricio Espinoza.

Respecto al perfil del visitante, afirmó que fue transversal, pues hubo propietarios, administradores y expertos que están enfocados en propiedad horizontal, todo

lo que tiene que ver con residencial, comercial, empresarial, de grandes empresas, marcas de transporte o de comercialización, jefes de seguridad, clientes finales, quienes hacen la recompra de las grandes marcas y se encargan de distribuir dentro y fuera del país.

Para cerrar, afirmó que el despliegue en redes sociales fue crucial para alcanzar el éxito de la primera muestra, tarea que se repetirá en 2027, además que se reforzará la presencia en medios de información locales y especializados internacionales como Más Seguridad Magazine, que se convirtió en la revista oficial de este evento. 📰



Mauricio Espinoza Gualdrón, director ejecutivo del Grupo Empresarial Integra



**EXPO 2026
NAVAL®**

XIV EXHIBICIÓN Y CONGRESO INTERNACIONAL NAVAL Y
MARÍTIMO PORTUARIO PARA LATINOAMÉRICA

1-3 DICIEMBRE

ESPACIO RIESCO

AV. EL SALTO 5000, HUECHURABA

SOMOS LA FERIA DE NEGOCIOS PARA LA INDUSTRIA NAVAL LATINOAMERICANA



ORGANIZA



PATROCINA



WWW.EXPONAVAL.CL

Exponaval



info@exponaval.cl



+56 9 4481 6922

Hik-IA Encoding

Ahorras hasta 50% de almacenamiento,
enfócate en los objetos clave

Ahorro
promedio
30% a **50%** ↓
de almacenamiento



Codificación estándar, y
alta compatibilidad

Preserva los detalles
en alta definición de los
objetos clave

Disponible en DeepinView(X), ColorVu 3.0, PowerX DVR
y dispositivos de seguridad con inteligencia integrada.



@HikvisionMex



@HikvisionMx

Hikvision México
www.hikvision.com/mx
sales.mexico@hikvision.com