

MÁS SEGURIDAD

Magazine



Hotelería protegida



Ene 2026 / No. 159 / Año 18



Internacional / precio \$60.00 MXN

HIKVISION®



Guanlan

To understand the nature and movement of water, one must observe its waves.



Protección perimetral Impulsado por

De 1 m a 100 km con protección precisa en cualquier entorno.

Nuestras soluciones perimetrales combinan **inteligencia artificial con tecnología avanzada** para proteger de forma precisa cualquier tipo de espacio: fábricas, puertos, granjas, residencias, fronteras y más.

Incluso bajo lluvia intensa, niebla o viento fuerte, la seguridad no se detiene.



IA con 99.9% de precisión.



Estabilidad en condiciones climáticas adversas.



Cobertura desde 1 m hasta 100 km.



Alertas inmediatas y verificación en tiempo real.



@HikvisionMx
www.hikvision.com/mx

Hikvision México
sales.mexico@hikvision.com

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

SERGIO GIOVANI REYES POZO
COORDINACIÓN DISEÑO
diseno@revistamasseguridad.com.mx

ROSA MARÍA SALAS
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

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

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

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@globaldefense.com.mx

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

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

ASISTENCIA A CLIENTES
atencion@revistamasseguridad.com.mx

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

SIGUENOS EN:

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

Revista Más Seguridad Año 18, No 159, Enero 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: PPI5-5134 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.

Protección, la medida clave para el sector hotelero en México

Una industria que prioriza tecnología, prevención y criterio humano.

La seguridad hotelera en México es un tema clave que ha llevado a la industria a intensificar sus medidas y protocolos de vigilancia. Si bien las zonas turísticas más concurridas generalmente se consideran seguras, la percepción general de inseguridad en el país sigue siendo un factor importante que los hoteles buscan mitigar.

El panorama de la industria hotelera en 2025 fue crucial para la economía del país, en donde se generan miles de millones de dólares anualmente. En respuesta a las diferentes amenazas que afectan al sector, y aunado a la creciente afluencia de turistas internacionales, estos inmuebles se han dado a la tarea de adoptar diferentes medidas de protección a lo largo del territorio nacional, para contar así con Zonas Turísticas Seguras en diversas playas y en la Ciudad de México, en ambos casos se trata de contar con una presencia de seguridad más visible para todos los visitantes, lo que impulsa a los hoteles a mejorar constantemente sus estándares.

Actualmente, las medidas de seguridad clave en hoteles que se están implementando, se robustecen con diferentes tecnologías y prácticas para garantizar la estancia de los huéspedes; esto a través de vigilancia con la implementación de sistemas de videovigilancia, cerraduras electrónicas avanzadas, lectores de pasaportes/identificaciones para un registro eficiente y credenciales de acceso para ascensores ya es común. Contar con personal capacitado de seguridad para el control de accesos hoy es un elemento fundamental. Asimismo, contar con una infraestructura adecuada, en la que se observe una buena iluminación en todas las áreas y mantener las puertas de las habitaciones cerradas son medidas básicas y efectivas.

Recordemos que los hoteles son pequeñas ciudades en movimiento constante, todo pasa al mismo tiempo: los huéspedes llegan uno tras otro, los grupos se cruzan, el personal rota en turnos apretados, los proveedores entran sin hacer ruido, el mantenimiento trabaja a deshoras y los servicios operan con una exigencia permanente.

En medio de ese ir y venir, la seguridad ya no sólo es un apoyo periférico, sino que sostiene buena parte de la reputación del hotel y marca la continuidad de su operación diaria.

Hoy, el sector de la hotelería en México, atraviesa un periodo de crecimiento. La apertura de nuevas cadenas, la presión que viven los destinos de playa y la expectativa del Mundial de 2026 obligan a revisar la manera en que se protege un hotel y cómo prevenir incidentes. En el presente, la seguridad ya no solo un conjunto de cámaras, guardias, rondines y controles de acceso. Hoy la operación exige un sistema que mantenga conectados accesos, energía, videovigilancia inteligente, credenciales, zonas de riesgo y supervisión del personal. La seguridad funciona como el soporte que sostiene la experiencia del huésped, aunque casi nunca se vea. 🌐

Los profesionales de LATAM

Licenciado en Derecho. Técnico Profesional en Administración de Recursos Humanos. Profesional de Protección Certificado (CPP), Investigador Profesional Certificado (PCI®) y Profesional de Seguridad Física (PSP®), todas estas certificaciones por ASIS International.

Miembro fundador de ASIS International, Capítulo México. Director de SIPROSI Corporativo S.A. de C.V.

Ampliamente reconocido como consultor, posee una larga y exitosa trayectoria en la preparación de profesionales en el área de la seguridad. Invitado frecuente en eventos de la industria de la seguridad en América y Europa. 🌐



Rubén Fajardo Correa
México



• Escucha —  —



NUESTRO
PODCAST

a través de Spotify



MÁS SEGURIDAD
Magazine

SUMARIO

- 5** Modelo virtual Hilvision de gemelos digitales
- 8** 7a edición del Ajax Special Event
- 13** México se suma al International Code Council (ICC)

22

Se redefine la Seguridad Hotelera en México



- 28** Llega a México Heracron, fibra de alto desempeño para blindaje
- 30** Calidad vs cantidad, objetivo del sector de geolocalización: AMESIS
- 32** Autenticidad y calidad del producto para un blindaje responsable



Aniversario No 18

Como dicen en México: oficialmente llegamos a la mayoría de edad. Sí, 18 años cumplidos ¡y contando en nuestra publicación **Más Seguridad Magazine**!

Son ya más de tres lustros en nuestro andar por los caminos de la seguridad corporativa, abriendo otros mercados en América Latina, EE.UU. y España, con nuevos clientes y lectores, haciendo alianzas con diversas organizaciones gremiales, participando en varios foros internacionales, llevando ejemplares impresos a personas y lugares que no habíamos imaginado. Son 18 años de pura adrenalina, gusto y pasión por el periodismo escrito especializado.

Hace 18 años, apoyados en un par de computadoras, una línea telefónica casera, una mesa de jardín, dos grabadoras de microcassette y una pequeña cámara fotográfica digital de 5 píxeles, iniciamos la revista (fea y colorida en diseño) "**Más Seguridad Para Todos**", nombre que con el paso de los años cambió a **Más Seguridad Magazine**, título con el que hoy nos identifican más allá de las fronteras de México, donde hacemos presencia física y directa con nuestro personal y ejemplares impresos.

A lo largo de 18 años, hemos sido testigos de infinidad de acontecimientos de la industria de la seguridad privada y de casi todos publicamos información al respecto, siempre apegados a la ética, imparcialidad y profesionalismo, lo cual nos ha distinguido al mantener como política una línea editorial que nunca ha cambiado: objetividad.

Con muchos vaivenes y sobresaltos en diversos aspectos, nos renovamos constantemente. Nos sumamos a las tendencias

digitales que permean en el sector, con aciertos y errores, pero siempre con la convicción de ofrecer información que sirva como una herramienta en la toma de decisiones. En cada edición presentamos temas de vanguardia y actualidad para el, siempre soportados por expertos, ya sean fabricantes, distribuidores, integradores, autoridades y consultores, ello con el objetivo que sea tomada como referencia al establecer proyectos, recomendar un bien o servicio, al momento de cerrar un negocio. Para eso nos esforzamos en cada publicación.

Hoy, a casi dos décadas de existencia ininterrumpida, es vasta la lista de organizaciones de México, El Salvador, Nicaragua, Brasil, Colombia, Guatemala, Perú, Chile, Argentina, Ecuador, EE.UU. o España; por mencionar algunos, con las que hemos hecho sinergias: ASIS, NFPA, AMESIS, AMBA, CNSP, ANERP, UNESPA, ASUME, FNS, AMEXSI, AMSIRIA, AIB, CNB, FEPASEP, COLADCA, ANDEVIP, ADISPO, AIMCSE, ALAS, CAESBA, CEMARA, CEMERA, APSEPBA, AMESP, CEAS, IFPO, ASOSEC, ACES, SUTCA, ASEGPRIN, AJDSE, CAPSI y ANCSI, entre otras. A todas estas agrupaciones les externamos un sincero y enorme agradecimiento por su apoyo e impulso a nuestro proyecto editorial.

Sin lugar a duda, nuestro arribo a la industria sirvió para que organizaciones y empresarios que no tenían voz pública, se les escuchara. Muchos fabricantes descubrieron en nuestras páginas otra alternativa de difusión para sus productos, mientras que usuarios finales acogieron al medio como un aliado importante al momento de informarse. A todos los involucrados en nuestro proyecto editorial les AGRADECEMOS infinitamente la confianza. 18 años y vamos por más... 📱

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



SÍGUENOS

 **Revista Más Seguridad**

 **@revmasseguridad**

 **MasSeguridadMagazine**

 **revmasseguridad**

 **Revista Más Seguridad**

 **Revista Más Seguridad**

 **Más Seguridad Magazine**

MÁS SEGURIDAD

Magazine

www.revistamasseguridad.com.mx

Futuro impulsado por modelo virtual de gemelos digitales de **HIKVISION**

- El ecosistema proporciona a las universidades una estrategia para optimizar operaciones y elevar la calidad educativa.
- Desde reducción de costos hasta la mejora de la experiencia de aprendizaje, beneficios innovadores y de gran impacto.

Las tecnologías digitales están transformando la educación superior, brindando a las instituciones una ventaja competitiva y moldeando el futuro del aprendizaje. Entre las innovaciones emergentes, destacan los gemelos digitales (réplicas virtuales de un sistema físico), que están transformando seguridad, operaciones y experiencias educativas del campus. Al integrar estos sistemas con cámaras inteligentes y tecnologías modernas para las aulas, las universidades están creando campus más inteligentes, seguros y eficientes.

"Un gemelo digital es un modelo detallado de un campus —incluyendo sus edificios, aulas e infraestructura— creado en una computadora. Aunque aún no se ha desarrollado plenamente el potencial de esta nueva tecnología, los gemelos digitales ya ofrecen diversas aplicaciones que pueden revolucionar los entornos y los resultados educativos", destaca Miguel Arrañaga, director Regional de Ventas de Hikvision México.

Comenta que los métodos tradicionales de gestión de campus se basan en cámaras anticuadas y sistemas independientes. Por ello, suelen ser inadecuados y costosos, sobre todo para universidades en crecimiento con decenas de aulas. Además, los sistemas de control de acceso que dependen de lectores de tarjetas aislados suelen complicar los procesos de seguridad. Por otro lado, las aulas convencionales con pizarras básicas y proyectores de baja resolución no consiguen captar la atención de los estudiantes y suponen una carga para los docentes.

Estos sistemas ineficientes y desconectados, dice, ya no satisfacen las demandas de un campus moderno a gran escala. Es aquí donde la tecnología de gemelos digitales puede marcar una diferencia tan significativa.

Beneficios de aplicar gemelos digitales a instituciones educativas

Los gemelos digitales conectan los entornos físicos y digitales para mejorar los servicios, entornos y procedimientos educativos. Algunos beneficios clave:

- **Permiten** la monitorización y el análisis en tiempo real de los espacios físicos. Los administradores pueden optimizar la distribución de las aulas, el equipamiento y los flujos de trabajo para ofrecer una experiencia de aprendizaje fluida desde el momento en que los estudiantes entran al campus hasta que salen. Se benefician de entornos más inteligentes y tecnológicos, lo que fomenta la participación y la eficiencia.
- **Integran** diversos sistemas de gestión, mejorando la precisión de los datos y la visibilidad operativa, lo que a su vez optimiza la prestación de servicios educativos. Esta composición proporciona una visión integral de las operaciones del campus, permitiendo a los administradores supervisar y gestionar diversos aspectos del campus, como la seguridad, el mantenimiento y la asignación de recursos, desde una plataforma centralizada. Al optimizar estos procesos, los gemelos digitales reducen las ineficiencias operativas y los costos.
- **Promueven** la responsabilidad ambiental al monitorear el uso de recursos, como energía y agua. Las universidades pueden usar la información para reducir su huella ecológica, por ejemplo, identificando ineficiencias en los sistemas de iluminación o climatización y reasignando recursos físicos para evitar el desperdicio.

"Tenemos un ejemplo claro de su uso en la Universidad Qassim de Arabia Saudita que, en colaboración con Hikvision, desarrollamos un ecosistema de gemelos digitales de realidad aumentada (RA) que abarca sus 30 edificios. Cuenta con un modelo 3D detallado con más de 6000 cámaras inteligentes. Con un panel de control intuitivo y centralizado, los administradores pueden supervisar fácilmente la distribución y las estructuras interiores, lo que garantiza un entorno más seguro para todos en el campus".

Arrañaga detalla que los educadores se han beneficiado de sistemas mejorados de programación y gestión de asistencia, lo que les permite centrarse más en la interacción estudiantil y la calidad de la enseñanza, ofreciendo una educación transfronteriza. Las aulas con tecnología avanzada promueven el aprendizaje activo y ofrecen a los estudiantes una experiencia más ágil en el campus. Para los administradores, las plataformas centralizadas simplifican las operaciones complejas, mejorando la eficiencia en áreas clave como el comedor, las residencias estudiantiles y las comunicaciones del campus.

El ecosistema de gemelos digitales ofrece a las universidades una hoja de ruta para operaciones más inteligentes y resultados educativos superiores. Desde la reducción de costos operativos hasta el enriquecimiento de las experiencias de aprendizaje, las posibilidades son inmensas.



Lanza **AXIS** COMMUNICATIONS **reporte en la industria de la videovigilancia**

- Las tecnologías de vanguardia de Pelco ofrecen un rendimiento confiable en condiciones extremas y una fácil integración con sistemas de gestión de video existentes.

La empresa mundial del sector de la videovigilancia, Axis Communications, ha publicado su último informe, “El estado de la IA en la videovigilancia”, que explora las perspectivas del sector sobre el uso de la IA en la seguridad, la protección y más allá. El informe revela los principales conocimientos críticos sobre las tecnologías de IA, su integración y las oportunidades y desafíos con respecto a la seguridad, inteligencia, inteligencia empresarial y la eficiencia operativa.

El despliegue de la IA se ha disparado en los últimos dos años, sobre todo debido al aumento de las demandas de los clientes, la mejora del conocimiento de las aplicaciones y la aparición de nuevos casos de uso.

Mats Thulin, director de soluciones de IA y análisis de Axis Communications, comentó: “La IA sigue siendo una de las tecnologías más potentes y transformadoras dentro de la industria de la videovigilancia. Esta nueva investigación revela que, si bien existen oportunidades significativas para que la IA mejore la seguridad, la eficiencia operativa y la inteligencia empresarial, debe haber un enfoque en la implementación ética y las integraciones significativas que generen valor”.

A través de entrevistas de investigación cualitativa con expertos en IA de la red global de socios de Axis, en este nuevo informe se descubrieron varias ideas temáticas sobre las tecnologías de IA.



Transición de la IA en la nube y en el borde sigue acelerándose

Los resultados de la investigación destacan que el paso de los sistemas de servidores locales a las arquitecturas híbridas continúa a buen ritmo. Este desarrollo está impulsado por la necesidad de una mayor escalabilidad, un procesamiento más rápido y un mejor uso del ancho de banda. El modelo híbrido, que combina las capacidades de procesamiento inmediato de la IA periférica en las cámaras con la escalabilidad y el almacenamiento de datos a largo plazo de la nube, se está convirtiendo en el enfoque preferido por muchos. Este equilibrio permite a las organizaciones aprovechar las fortalezas de ambas tecnologías.

Integración de diversas fuentes de datos

Los encuestados de la investigación coincidieron en que la integración de datos sensoriales adicionales, como el audio y los factores ambientales contextuales, para complementar los datos de video mejorará la conciencia situacional, proporcionará información más profunda y procesable, y ofrecerá una comprensión más completa de los eventos. En última instancia, esto revolucionará la seguridad y la protección, al tiempo que elevará las capacidades de inteligencia empresarial.



La combinación de múltiples flujos de datos permite una detección y predicción más precisas de posibles amenazas. Por ejemplo, en escenarios de emergencia, la combinación de datos visuales con análisis de audio puede permitir a los equipos de seguridad responder de forma más rápida y precisa.

Reconocimiento facial gana terreno

La investigación también destacó que el reconocimiento facial parece haberse adoptado más ampliamente en muchos países, respaldado por la introducción de nuevas regulaciones para ayudar a aclarar cómo se puede aplicar esta tecnología de manera ética y proporcionar un marco para su uso responsable.

Los expertos entrevistados predijeron que el reconocimiento facial seguirá ganando terreno a nivel mundial, pero primero debe haber una alineación con las regulaciones de privacidad y transparencia sobre cómo funciona la tecnología. Las consideraciones éticas en torno al uso del reconocimiento facial siguen siendo un foco central, especialmente en regiones con leyes de privacidad estrictas.

Ofrece **MOTOROLA SOLUTIONS** seguridad robusta para infraestructura crítica con **Pelco**

- Nuevo Portafolio innovador de dispositivos de Pelco impulsados por IA.
- Las tecnologías de vanguardia de Pelco ofrecen un rendimiento confiable en condiciones extremas y una fácil integración con sistemas de gestión de video existentes.

Chicago, EE.UU.- Motorola Solutions anunció el nuevo portafolio innovador de dispositivos impulsados por Inteligencia Artificial Pelco, diseñados específicamente para empresas que operan en algunos de los entornos más desafiantes, como petróleo y gas, o puertos. Respaldo por la profunda experiencia en ingeniería de la compañía y significativas inversiones en investigación y desarrollo, la línea de dispositivos de Pelco incluye cámaras fijas, cámaras robustas y de largo alcance, sensores inteligentes y análisis de Inteligencia Artificial (IA) que se integran fácilmente con una amplia gama de sistemas de gestión de video (VMS) de terceros.



Desde la adquisición de Pelco en 2020, Motorola Solutions ha transformado completamente la línea de cámaras, que se ha duplicado desde que la compañía trajo a casa áreas de ingeniería y diseño. Bajo una nueva y moderna marca Pelco, el portafolio reúne tecnologías de seguridad especializadas de las adquisiciones estratégicas de Videotec, IP Video y Silent Sentinel.

“Pelco proporciona a los operadores de seguridad soluciones robustas de seguridad impulsadas por IA, capaces de funcionar en una amplia gama de condiciones ambientales”, dijo Hamish Dobson, vicepresidente corporativo de Pelco. «Hemos creado Pelco con el propósito de combinar hardware resistente, detección de última generación y análisis impulsados por IA para un portafolio de dispositivos agnóstico al VMS que está impulsando estándares más altos en la seguridad de la infraestructura crítica».

Las expansiones del portafolio amplían las oportunidades de crecimiento con empresas e industrias de infraestructura crítica como el transporte, la aviación, el sector marítimo y los servicios públicos. Tales operaciones soportan rutinariamente condiciones climáticas extremas, elementos corrosivos y otras condiciones peligrosas donde las cámaras y dispositivos de seguridad estándar se dañan rápidamente.

El nuevo portafolio especializado de Pelco incluye:

- **Cámaras Anti-corrosión Espirit:** Pueden soportar los duros elementos oceánicos de los entornos marítimos.
- **Cámara fija ExSite Enhanced Thermal 2:** proporciona a sitios peligrosos como centrales eléctricas una cámara de seguridad de imágenes térmicas con certificaciones globales a prueba de explosiones.
- **Sensor Halo Smart:** un sensor inteligente todo en uno que ofrece seguridad sin video, protegiendo la privacidad mientras detecta instancias como vapeo, disparos, ruidos anormales, movimiento y palabras clave de emergencia como “ayuda”.
- **Cámaras Aeron y Jaehar** ofrecen capacidades de detección a distancias de hasta 32 kilómetros en entornos extremos asociados con los sectores militar, aviación, marítimo e infraestructura crítica.

Todos los dispositivos Pelco cuentan con el respaldo de Elevate, una plataforma de soporte de cámaras basada en la nube. Evalúa la salud de las cámaras y amplía las capacidades de detección con IA basada en la nube. Los dispositivos Pelco están diseñados para ser compatibles con sistemas Open Network Video Interface Forum (ONVIF) lo que simplifica la instalación, permite integraciones flexibles y mitiga las costosas renovaciones del sistema. Las cámaras IP de Pelco permiten el cumplimiento normativo con las reglas actuales de la Sección 889 de la Ley de Autorización de Defensa Nacional (NDAA) para la adquisición de equipos seguros. 🌐

AJAX presentó nuevas soluciones en el 7º Ajax Special Event: Atrévete a ser el primero

Ajax Systems anunció la 7ª muestra anual **Ajax Special Event: Atrévete a ser el primero**. La empresa exhibió soluciones que revolucionan el sector y abren nuevas oportunidades para los partners, profesionales y usuarios de Ajax. La presentación se retransmitió en línea el pasado 21 de noviembre de 2025 en los canales de YouTube de la empresa.



El Ajax Special Event: Atrévete a ser el primero es el evento más importante del sector. Reveló los nuevos dispositivos de protección contra incendios, de videovigilancia y de protección contra intrusiones, y las formas de combinarlos en un único sistema integrado. La presentación mostró cómo los Servicios Ajax pueden aumentar la satisfacción de los clientes y cómo el software Ajax, en constante evolución, aporta ventajas a los usuarios más experimentados y a los PRO.

Con el lema Atrévete a ser el primero, el equipo de Ajax anima al sector a enfrentarse una vez más a lo desconocido con la emoción de las nuevas innovaciones, superando retos de siempre, mejorando la experiencia tanto de los profesionales como de los usuarios y estableciendo nuevos puntos de referencia en la industria.

La presentación en línea se transmite en todo el mundo en más de 20 idiomas con locución y subtítulos. Siga el enlace para inscribirse en la presentación en línea del Ajax Special Event: Atrévete a ser el primero y mantenerse al día con las últimas noticias de la compañía. 📺



AJAX

SPECIAL EVENT

DARE TO BE FIRST
NOVEMBER 21

Redefine **HID** la integración de la seguridad física y digital

- Nueva plataforma de servicios de integración como servicio (IPaaS), concebida para desarrolladores de aplicaciones, integradores de soluciones y proveedores de software.
- HID Integration Service responde a las exigencias cada vez más complejas en la gestión de infraestructuras de seguridad.

Austin, Texas. - HID, firma mundial en soluciones confiables de gestión de acceso e identidades, anunció el lanzamiento de HID Integration Service, una plataforma que integra la seguridad física, ciberseguridad y gestión de identidades digitales.

Esta plataforma de integración como servicio (IPaaS) fue concebida para que desarrolladores de aplicaciones, integradores de soluciones y proveedores de software puedan integrar de forma ágil y sin complicaciones las soluciones esenciales de seguridad física, simplificando los procesos y mejorando la interoperabilidad de los sistemas. Al hacerlo, la plataforma busca aliviar la carga de mantenimiento y actualizaciones que conlleva la gestión y puesta en marcha de integraciones entre los sistemas de seguridad física y la ciberseguridad, generando así un ahorro de costos, operaciones más eficientes y una significativa disminución en los tiempos de implementación.

"Las organizaciones llevan mucho tiempo lidiando con integraciones inestables y complejas, además de los elevados costos que implica su mantenimiento", explicó Martin Ladstaetter, vicepresidente sénior y responsable de la división de Soluciones de Gestión de Identidad y Acceso de HID. "HID Integration Service resuelve estos problemas al proporcionar una plataforma de integración que conecta los productos de seguridad física y digital, lo que reduce el tiempo de lanzamiento al mercado para nuestros socios desarrolladores, quienes están creando una nueva generación de soluciones de seguridad con mayor velocidad, calidad, resiliencia y valor para el usuario".

HID Integration Service se enfoca directamente en los principales beneficios que buscan los responsables de la seguridad en las organizaciones al adoptar soluciones de gestión unificada —mejorar la eficiencia, simplificar la gestión y obtener un panorama completo de los procesos—, ayudándolos a:

- Reducir la complejidad operativa y los costos de mantenimiento.
- Implementar con mayor rapidez nuevas prestaciones de seguridad en soluciones adaptadas a cada sector.
- Simplificar los puntos de interacción con los sistemas de seguridad mediante experiencias de uso más ágiles y sin complicaciones.

Las siguientes son las principales características de la solución:

- Una capa unificada de integración que abarca desde conexiones punto a punto hasta integraciones con múltiples plataformas y usuarios.
- Integraciones preconfiguradas que agilizan la implementación y reducen los costos de desarrollo.
- Escalabilidad y seguridad que se adaptan a las necesidades cambiantes de su organización.

HID tiene el privilegio de contar con varios usuarios pioneros que ya están implementando la plataforma. Cada uno de ellos aporta una amplia trayectoria y sólidas funcionalidades en diversas tecnologías, mercados verticales y ámbitos de seguridad.

"Estamos entusiasmados con las nuevas posibilidades que ofrece la plataforma de integración de HID, pues creemos que fortalecerá aún más la capacidad de SwiftConnect para responder a las expectativas y necesidades cada vez más amplias de nuestros clientes en el sector inmobiliario comercial y empresarial", señaló Matt Kopel, cofundador y codirector ejecutivo de SwiftConnect. "La coincidencia de visión y dirección entre ambas compañías potenciará y amplificará los cambios corporativos que nuestros clientes desean implementar", añadió Kopel.

"Imaginamos un mundo en el que las fotografías de identificación lleguen mágicamente a su destino, sin intervención humana", afirmó Luke Rettstatt, director ejecutivo de CloudCard. "Para hacer realidad esta visión, debemos desarrollar y mantener numerosas integraciones, algo que supone una gran carga de trabajo para un equipo pequeño. HID Integration Service nos permite concentrarnos en el flujo de trabajo impulsado por IA de RemotePhoto, en lugar de destinar tiempo y recursos al desarrollo y mantenimiento de integraciones certificadas con terceros".

Esta demanda cada vez de mayor integración y eficiencia se ve reflejada en el Informe sobre el estado de la Seguridad y la Identidad de 2025. Según este estudio, el 67% de los encargados de la protección están migrando hacia soluciones basadas en software, mientras que casi tres cuartas partes de las organizaciones consideran fundamental para sus operaciones la recopilación unificada de datos. 📊

Implementar CURP biométrica traerá graves riesgos: GIDH

- Urgen principios de legalidad, privacidad, proporcionalidad y rendición de cuentas.
- La CURP biométrica representa una seria amenaza a los derechos humanos.

El Grupo Integral de Derechos Humanos (GIDH) “Lex-magister”, expresó su profunda preocupación por el rumbo que podría tomar la digitalización de la identidad ciudadana en México, particularmente con la implementación de la nueva CURP biométrica impulsada durante la presente administración federal.

Su presidente, Jesús Rey Fierro Hernández, enfatizó que “toda política pública debe sujetarse irrestrictamente a los principios fundamentales de legalidad, privacidad, proporcionalidad y rendición de cuentas. La CURP biométrica, sin un marco jurídico sólido y transparente, representa una seria amenaza a los derechos humanos de millones de personas en México”.



Fierro Hernández, doctor en derecho, denunció que este nuevo sistema de identificación —que almacenará huellas digitales, iris, fotografía facial y firma electrónica— carece de controles democráticos, supervisión autónoma y mecanismos de reparación del daño en caso de filtraciones o uso indebido, lo que abre la puerta a prácticas de vigilancia arbitraria, suplantación de identidad y violación al derecho a la privacidad.

“Nos alarma que el Estado mexicano, que no ha sido capaz de proteger sus propias plataformas institucionales, ahora pretende centralizar los datos biométricos de toda la población, sin asumir con seriedad la responsabilidad que ello implica. No existen aún garantías plenas ni marcos legales específicos para asegurar su uso lícito y protegido”, denunció.



Jesús Rey, reconocido con el Premio Nacional de Derechos Humanos 2017, recordó que durante el sexenio anterior se vulneraron las bases de datos de la Secretaría de la Defensa Nacional, así como de la Presidencia de la República, revelando la debilidad estructural en materia de ciberseguridad del Estado mexicano.

“No se puede hablar de transformación digital ni de modernización si no hay respeto absoluto por los derechos humanos. La experiencia del caso “Guacamaya” en 2022 nos deja claro que ni las Fuerzas Armadas fueron capaces de salvaguardar información crítica y de seguridad nacional”, subrayó.

Enfatizó que, bajo el actual mandato presidencial, se corre el riesgo de que las digitales gubernamentales —sin contrapesos legales— se conviertan en instrumentos de control y vigilancia ciudadana. Esto podría derivar en atropellos sistemáticos a los derechos a la intimidad, autodeterminación informativa y debido proceso.

“La defensa de los derechos humanos no puede subordinarse a la inercia tecnocrática. Es obligación del Estado proteger, no exponer, a sus ciudadanos. La administración actual tiene la responsabilidad histórica de evitar una arquitectura digital que derive en autoritarismo técnico”, advirtió el especialista.

De esta forma, el presidente del GIDH subrayó el llamado urgente a la ciudadanía a, “informarse antes de proporcionar datos biométricos en cualquier plataforma digital; exigir leyes claras, con principios de seguridad, transparencia y proporcionalidad”.

“Rechazar cualquier medida que no contemple auditorías ciudadanas y supervisión independiente. Participar activamente en procesos de consulta sobre esta materia”, dijo.

Asimismo, exhortó a los integrantes del Congreso de la Unión a detener la implementación masiva de la CURP biométrica hasta contar con una Ley Nacional de Protección de Datos Biométricos, distinta y más estricta que la Ley General de Datos Personales en Posesión de Sujetos Obligados.



Jesús Rey Fierro Hernández
presidente del Grupo Integral de
Derechos Humanos (GIDH)

18

ANIVERSARIO

MÁS SEGURIDAD

Magazine

¡Estamos de festejo y vamos por más!

Gracias México, América Latina,
EE.UU. y España por leernos un año más

#SeguridadSomosTodos

#PorTuSeguridad

Nueva serie de paneles INSPIRE de Honeywell

- Con Connected Life Safety Services (CLSS) para simplificar la instalación, el mantenimiento y el cumplimiento de normativas.

La empresa global en tecnologías de protección contra incendios y seguridad para la vida, Honeywell, presenta NOTIFIER INSPIRE, sistema de protección contra incendios todo en uno que ofrece un rendimiento fiable, monitoreo inteligente, mantenimiento simplificado e integración perfecta. El sistema se conecta a la plataforma Connected Life Safety Services (CLSS) de la firma, proporcionando información en tiempo real y aumentando la productividad de los técnicos.



Asimismo, la marca también está lanzando en México el detector de humo Self-Test, que automatiza el diagnóstico para verificar el estado del dispositivo y el cumplimiento de las normas NFPA 72, mejorando la seguridad y reduciendo la necesidad de inspecciones manuales.

Ventajas del producto:

La serie NOTIFIER Self-Test cuenta con los primeros detectores homologados por UL capaces de realizar pruebas totalmente automatizadas. Esta revolucionaria innovación está lista para transformar la forma en que se instalan, prueban y mantienen los sistemas de seguridad contra incendios.



Las pruebas de seguridad tradicionales pueden ser lentas, caras y molestas, especialmente en espacios cerrados, zonas de difícil acceso o edificios con techos altos. Estas dificultades hacen que a menudo no se comprueben los detectores, lo que pone en peligro la seguridad.

Los detectores NOTIFIER Self-Test superan estos obstáculos con una tecnología de autodiagnóstico patentada y aprobada por UL. Cada dispositivo puede generar calor y humo internamente para verificar la funcionalidad de los sensores térmicos y fotoeléctricos, a la vez que garantiza que los puntos de entrada de humo permanezcan despejados y sin obstrucciones.

Gracias a las avanzadas funciones de autodiagnóstico de NOTIFIER, incluso los sistemas en red más grandes pueden comprobarse de forma rápida y eficaz, lo que permite ahorrar tiempo, reducir costos y mejorar la seguridad general contra incendios.

“Con el lanzamiento de INSPIRE, reafirmamos nuestro compromiso de ofrecer soluciones de detección de incendios no sólo tecnológicamente avanzadas y fáciles de usar, sino también adaptadas a las necesidades locales en Latinoamérica. Este sistema además de mejorar la seguridad, garantiza una integración perfecta con la infraestructura existente, reforzando nuestra misión de proteger vidas y activos valiosos”, comenta Neove Pipper, director general de Building Automation para Latinoamérica.

Aspectos a destacar:

- Refuerza el compromiso de Honeywell con edificios más seguros e inteligentes.
- Reduce el tiempo de los técnicos in situ con diagnósticos remotos.
- Ofrece soluciones de protección contra incendios escalables y rentables.
- Respalda el cumplimiento de normativas y la eficiencia operativa en todos los mercados de Latinoamérica.

México se suma al ICC para evitar daños por incendios

- Adoptará para la industria de la construcción nacional códigos y estándares internacionales de actuación.
- En los últimos 4 años se registraron pérdidas por 34 mil millones de pesos a causa de los incendios.

Expo Fire & Safety 2025: Espacio dónde se presentaron las nuevas tecnologías para la protección contra incendio, sus tendencias y desafíos.

Guadalajara, Jalisco.- Para evitar que los incendios sigan causando graves daños y pérdidas, México, a través de la Asociación Mexicana de Rociadores Automáticos Contra Incendios (AMRACI) y el Consejo Nacional de Protección Contra Incendios (CONAPCI), se sumarán y adoptarán los códigos y estándares de actuación del International Code Council (ICC) para la seguridad y las experiencias exitosas de naciones latinoamericanas.

Para ello, directivos de estos organismos se reunieron en nuestro país para compartir información y firmar los acuerdos de colaboración correspondiente, encabezados por David Morales, vicepresidente de AMRACI; Juan José Camacho, presidente de CONAPCI; José Roig, miembro del Consejo Directivo del ICC y Víctor Espínola, director general de AMRACI y CONAPCI.

A nombre del ICC, José Roig, explicó que este organismo es la principal fuente mundial de códigos y normas modelo, así como de soluciones para la seguridad en la construcción.

Por ello, brindarán colaboración a AMRACI y CONAPCI en cuanto a la evaluación de productos, acreditación, tecnología, capacitación y certificación. Los códigos, normas y soluciones del ICC se utilizan para garantizar comunidades y edificios seguros, asequibles y sostenibles en todo el mundo.



Toda esta experiencia se sumará a los esfuerzos que lleva a cabo AMRACI y CONAPCI para prevenir las conflagraciones urbanas, las cuales han sido de más de 34 mil millones de pesos en pérdidas registradas en los últimos cuatro años, según informe de las principales instituciones de seguros del país.

De ahí la importancia de atender y prevenir ese tipo de accidentes, los cuales son los responsables del 31% de los desastres en territorio nacional y del 26.9% de la mortalidad asociada.

En la reunión, los directivos destacaron que los incendios urbanos en México se han convertido ya en un grave problema de salud pública y, a diferencia de los sismos o huracanes, se presentan con mayor frecuencia de lo que parece. Anualmente se registran más de 95 mil incendios urbanos y no urbanos. 260 al día, según el Instituto Nacional de Estadística y Geografía (INEGI).

De ahí la importancia de la 8ª edición de Expo Fire & Safety, el evento mundial en protección contra incendios en México y Latinoamérica, que

se realizó por vez primera en Guadalajara, Jalisco. Este evento abordó la alarmante problemática de incendios que azotan a diversos estados de la República impactando todos los sectores económicos y la vida de miles de personas.

Juan Camacho Gómez, presidente de CONAPCI, informó que en México en los últimos 10 años más de 6 mil personas fallecieron por exposición a fuego no controlado. Los grupos más afectados son niños y adultos mayores.

Por su parte David Morales, vicepresidente de AMRACI, comentó que la industria de protección contra incendio es uno de los sectores que tiene un impacto transversal en todas las actividades económicas y sectores industriales, comercio y turismo, y ahora en el nearshoring. Por tanto, al incidir en prácticamente todos los sectores industriales, podría representar un verdadero riesgo para la salvaguarda de la vida de las personas, continuidad de operaciones y la competitividad de una industria.

AMRACI y CONAPCI representan a más del 70% del sector de protección contra incendios en México. Son la voz de la industria con objeto de impulsar, mejorar, legislar, profesionalizar y promover la cultura de prevención y protección a través del desarrollo de normas, códigos, buenas prácticas de diseño, instalación y mantenimiento con el fin de salvar vidas y proteger propiedades promoviendo una industria ordenada que permita un crecimiento sostenible

Expo Fire & Safety 2025

Por su parte, Víctor Espínola, director de AMRACI y CONAPCI, se refirió a la realización de la Expo Fire & Safety 2025, el cual es un foro único que reunió a las personalidades y proveedores más importantes a nivel global. Permitió actualizarse con las tendencias de prevención y protección de los riesgos que demandan las distintas industrias con la llegada del nearshoring, en materias como tecnologías emergentes, uso de baterías de litio, almacenamiento, manufactura, edificios altos, centros de datos; privilegiando siempre la seguridad humana y la continuidad de operaciones.

El evento contó con una gran convocatoria nacional e internacional, en ella se dieron cita:

- 4,500 asistentes
- 400 congresistas en las Máster Class
- 25 estados de la República
- 12 países visitantes
- 8,700 metros de exhibición
- 230 stands

Asimismo, se presentó el Museo Itinerante de Prevención de la Fundación Michou & Mau; y se realizó un rally presentación del Programa de Educación Pública "Aprende a Mantenerse Seguro" para niños de primaria con participación de la SEP y DIF Jalisco.

México registra gran atraso en materia de **Protección Civil**

- Se ha avanzado en cuestión de sismos, pero aún tenemos grandes carencias en materia de prevención de incendios.
- En el primer semestre de 2025 llevamos pérdidas por 12 mil millones de pesos, y diariamente se registran en territorio nacional 260 incendios.

Guadalajara, Jalisco.- México tiene un gran atraso en materia de protección civil que se debe corregir de inmediato para evitar muertes y daños económicos. Y es que en el primer semestre de 2025 se llevan ya 12 mil millones de pesos en pérdidas por incendios.

Por ello es necesario que juntos, gobierno, industria y sociedad en general actúen y generen políticas públicas para, como en el caso de los sismos, preparar a la población para saber qué hacer en caso de incendios en casas, escuelas, oficinas, comercios y fábricas, pero sobre todo cómo prevenirlos y evitarlos, aseguró Juan José Camacho Gómez, presidente del Consejo Nacional de Protección contra Incendios (CONAPCI).

A su vez, Juan Francisco Guzmán Hernández, presidente de la Asociación Mexicana de Rociadores Automáticos Contra Incendios (AMRACI) informó que en el territorio nacional se registran al año más de 95 mil incendios urbanos y no urbanos, es decir 260 al día, según datos del INEGI.

Ambos especialistas en materia de prevención de incendios participaron en la inauguración de la 8ª Expo Fire & Safety 2025, que se llevó a cabo en octubre en la ciudad tapatía.

El presidente de AMRACI advirtió que el 31% de los desastres en México son ocasionados por los incendios, que son responsables del 26.1 por ciento de la totalidad de la mortalidad por humo y gases tóxicos.

Esto, sin duda es muestra del gran impacto que tienen los incendios, que, a diferencia de los sismos y huracanes, no reciben la misma importancia de las autoridades e incluso de la misma sociedad, a pesar de que provocan mayores daños que estos últimos.



Asimismo se dieron a conocer avances del programa "Aprende a Mantenerse Seguro" para niños de preescolar y primaria que se pretende implementar en todo el país y se llevó a cabo en "Rally de Prevención" el cual estuvo conformado por diversas actividades educativas en las que se enseñó a niños pequeños cómo actuar en casos de incendios.

Durante el mismo evento, AMRACI y CONAPCI concretaron la firma de un convenio de colaboración con la Secretaría de Educación Pública del estado de Jalisco, para aplicar en la entidad dicho programa que consiste en capacitar a los niños en qué hacer previo, durante y posteriormente a un incendio, pero, sobre todo, en cómo provenirlo y evitarlo.

Esta firma de convenio es punta de lanza en el país, al poner en marcha de manera conjunta esta prueba piloto del programa de educación en materia de prevención de incendios en niños de tercer año de educación básica, en planteles ubicados en zonas de alta vulnerabilidad.

Por su parte, Bomberos de Madrid, España donaron equipo y capacitaron a sus homólogos del estado de Jalisco sobre nuevas técnicas para la

prevención y combate de incendios urbanos; en especial mostraron nuevas formas de enseñanza a niños y jóvenes para que estén alertas y sepan cómo actuar ante siniestros de este tipo, en sus casas y escuelas.



La inauguración del evento a nombre del gobernador del estado Pablo Lemus Navarro, estuvo a cargo de la Coordinadora General Estratégica de Gestión del Territorio, Karina Herosillo Ramírez. En el acto, ambos organismos otorgaron un donativo por 100 mil pesos a la fundación Michou & Mau que encabeza su presidenta Virgina Sendel, para la atención de niños quemados.

La Expo Fire & Safety contó con la participación de diversos especialistas en materia de prevención de incendios provenientes de varios estados de la República, así como de Costa Rica, República Dominicana, Perú, Brasil, Colombia, Paraguay, Ecuador y Estados Unidos. A lo largo de 240 stands se presentaron las últimas tendencias de prevención y protección de riesgos por la llegada de tecnologías emergentes, baterías de litio, almacenamiento, manufactura, edificios altos y centros de datos, privilegiando la seguridad humana y la continuidad de operaciones. Participaron los proveedores líderes y las soluciones más avanzadas en protección pasiva, detección, alarma y supresión de conflagraciones, así como personalidades varias del sector de la prevención de incendios.

La 8ª Expo Fire & Safety, contó con el diseño y planeación de Víctor Espinola Llaguno, director de AMRACI-CONAPCI, quien logró conjuntar en un sólo lugar, (Expo Guadalajara), a los mejores y más conocidos expertos en la materia, que compartieron sus experiencias y mejores prácticas en la materia, además de contar con los expositores que trajeron lo más avanzado en equipos, herramientas y maquinarias en la prevención y combate de incendios, para evitar, en primer lugar, más víctimas por fuego. 🇲🇽

Impulsa seguridad IAAPA® en parques y atracciones

- El Mes de la Seguridad IAAPA 2025 reunió a expertos globales para reforzar el compromiso de la industria de parques y atracciones con la protección.
- Iniciativa internacional que une educación, colaboración e innovación a través de eventos virtuales y presenciales.

Cada año, más de 332 millones de personas visitan parques de diversiones, temáticos, acuáticos, centros de entretenimiento familiar, zoológicos, acuarios, entre otras atracciones en América Latina y el Caribe, de acuerdo con IAAPA la Asociación Global para la Industria de las Atracciones.

A ese total, México aporta 74.5 millones de visitantes anualmente, esta cifra no solo refleja la popularidad de esta industria, sino también el nivel de confianza que millones de visitantes depositan en ella cada año. Detrás de cada atracción, existe un compromiso inquebrantable con la seguridad mantenido por más 528 mil profesionales en la región, siguiendo estándares y protocolos de seguridad.

Mes de la Seguridad IAAPA

La oficina de IAAPA para América Latina y el Caribe presentó la edición 2025 del Mes de la Seguridad IAAPA, iniciativa internacional que une educación, colaboración e innovación a través de eventos virtuales y presenciales. El objetivo: elevar las prácticas de seguridad en parques, atracciones y centros de entretenimiento familiar, entre otros.

"En IAAPA sabemos que la seguridad es la base de las operaciones en nuestra industria. La capacitación continua es esencial para construir y mantener una fuerte cultura de seguridad que garantice experiencias memorables y seguras" señala Paulina Reyes Vicepresidente y directora ejecutiva de IAAPA América Latina, Caribe. "El Mes de la Seguridad IAAPA ofrece una oportunidad única para aprender, conectar e intercambiar ideas con profesionales de la industria en toda la región".

Durante el pasado mes de mayo, profesionales y expertos de la industria se reunieron de manera virtual y presencial para compartir buenas prácticas, explorar estrategias innovadoras y fomentar una cultura proactiva de seguridad y prevención. La oferta en línea de esta iniciativa incluyó una masterclass, un simulacro virtual, así como foros y paneles con una red global de expertos, diseñados para fortalecer las operaciones, proporcionar conocimientos y una cultura de prevención, así como herramientas prácticas para una mayor seguridad en las operaciones. Los interesados en extender la experiencia del Mes de la Seguridad, se registraron

además en un Bootcamp práctico de dos días en el parque de diversiones Mundo Petapa, en Guatemala.



Además de los eventos, los asistentes contaron con acceso a contenidos educativos grabados, materiales de apoyo descargables y herramientas digitales que les permitió implementar de inmediato lo aprendido en sus organizaciones. Para asegurar el acceso global a esta información, IAAPA utiliza tecnologías avanzadas de traducción, asegurando que los recursos educativos estén disponibles en múltiples idiomas y puedan beneficiar a la industria en todo el mundo.

Gracias a sólidos protocolos de seguridad, a la innovación constante y a un personal altamente calificado, la industria de las atracciones sigue ofreciendo experiencias seguras y memorables a millones de familias alrededor del mundo. 🌍



Certifica **HIKVISION** productos con **norma IEC 62443-4-1**

- Reforzando su compromiso con la ciberseguridad
- Al obtener esta certificación, la firma garantiza que sus soluciones sean seguras y fiables para mitigar amenazas en un mundo conectado.

Hikvision ha obtenido con éxito la certificación internacional IEC 62443-4-1 para su proceso de ciclo de vida de desarrollo de productos. Esta norma de ciberseguridad especifica los requisitos para el desarrollo seguro de productos en sistemas de control y automatización industrial, la cual subraya el compromiso de Hikvision con la ciberseguridad en todos sus procesos de investigación y desarrollo.

Durante el riguroso proceso de certificación, demostró su adhesión a prácticas de desarrollo seguras en varias áreas clave, entre ellas la identificación de requisitos de seguridad, evaluación de riesgos, diseño de seguridad y verificación de seguridad. Al integrar medidas de seguridad sólidas desde la fase de diseño inicial, Hikvision garantiza que sus productos cumplan con los altos estándares de ciberseguridad.



Hikvision se compromete a ofrecer soluciones más seguras y fiables que ayuden a las organizaciones a mitigar las amenazas cibernéticas de forma eficaz. La obtención de la certificación IEC 62443-4-1 refuerza la dedicación de la compañía a desarrollar productos seguros que cumplan con los estándares globales de ciberseguridad y protejan a sus clientes en un mundo cada vez más conectado.



La firma lleva mucho tiempo dedicada a la creación de un sistema de desarrollo seguro integral, el Hikvision Secure Development Life Cycle (HSDLC), que abarca todas las etapas, desde el análisis de requisitos, el diseño, el desarrollo y las pruebas hasta la entrega del producto. El HSDLC no solo cumple con los estándares de seguridad globales, sino que también incorpora las últimas investigaciones y tecnologías de ciberseguridad, lo que garantiza que los productos Hikvision mantengan sólidas defensas de seguridad contra amenazas cibernéticas cada vez más sofisticadas.

De cara al futuro, Hikvision seguirá fortaleciendo el desarrollo del sistema HSDLC, promoviendo la gestión de la seguridad a lo largo de todo el ciclo de vida del producto, mejorando las capacidades de I+D y prestando un mejor servicio a los mercados globales. Hikvision también explorará activamente colaboraciones con otras empresas líderes de la industria para promover las mejores prácticas en toda la cadena industrial y abordar conjuntamente los desafíos cambiantes de la ciberseguridad.



¿Qué es IEC 62443-4-1?

La IEC 62443-4-1 es una norma importante desarrollada por la Comisión Electrotécnica Internacional (IEC) para la ciberseguridad de los sistemas de control y automatización industrial. Ayuda a las organizaciones a garantizar que los sistemas de control industrial sean seguros durante sus fases de diseño, implementación y operación, protegiéndolos contra riesgos como ciberataques, violaciones de datos y fallas del sistema, al tiempo que brinda protección durante todo el ciclo de vida del producto.

La norma IEC 62443-4-1 proporciona un marco detallado y específico que aborda muchos requisitos clave de las normas de ciberseguridad, como la Directiva NIS2 de la UE. Al implementar las prácticas y directrices de la norma IEC 62443-4-1, las organizaciones mejoran significativamente su postura de seguridad y protegen eficazmente sus operaciones industriales contra las amenazas cibernéticas.



ReputationUP, expertos
en defender el activo
más frágil: **la reputación.**

REPUTATIONUP.COM

Hacia una ciberresiliencia federal en México: prioridades y desafíos



Dr. Gustavo Guzmán Hernández

LinkedIn: Gustavo Guzmán Hdez.
gguzmanh01@gmail.com
Tw @GustavoG_Kc

México

Articlista Invitado

- Un aparato burocrático fragmentado y con capacidades desiguales.
- Un marco normativo excesivo, cambiante y difícil de coordinar.
- Falta de continuidad y profesionalización administrativa.
- Pluralidad y competencia entre actores del sistema político-administrativo.
- Desbalance entre diseño de políticas y capacidades reales de ejecución.
- Reformas frecuentes pero superficiales, no integrales y sin consolidación institucional.

La acelerada digitalización de la Administración Pública Federal (APF) impulsa eficiencia y acceso ciudadano, pero también amplifica considerablemente la superficie de ataque y la dependencia de sistemas ciberfísicos interconectados. El Plan Nacional de Ciberseguridad 2025-2030 (PNC-2025-2030) presenta un portafolio de proyectos e iniciativas ambicioso, concebidas para incrementar la resiliencia cibernética del país y posicionar a México como referente regional en ciberseguridad. Desafortunadamente, la administración pública mexicana puede llegar a tener variables complejas, desde los ojos de dos grandes expertos en la materia Ricardo Uvalle y Omar Guerrero, la administración pública en México tiene diversas complejidades, su mayoría proveniente de:



Lo anterior, sin duda, deberá ser considerado en cada una de las fases y puesta en marcha de los proyectos e iniciativas del PNC 2025 -2030, ya que entre la formulación estratégica y la consecución de resultados medibles existen cuellos de botella institucionales, técnicos y sociales que requieren una respuesta disciplinada, coordinada y sostenida en el tiempo.

Partiendo de la premisa de que la ciberseguridad y la resiliencia cibernética es una responsabilidad compartida, y en harás de promover el análisis del PNC 2025-2030 e identificar los puntos donde como actores, académicos y profesionales podríamos aportar, a continuación, comparto lo que identifico como 10 puntos a considerar para alcanzar una implementación exitosa.

1. Gobernanza nacional vinculante.

La creación de un Consejo Nacional de Ciberseguridad con mandato legal permitirá resolver solapamientos, coordinar recursos y fijar responsabilidad política y técnica. La matriz RACI propuesta en el Plan debe volverse de cumplimiento obligatorio.

2. Financiamiento multianual y modelo de priorización por riesgo.

Los proyectos críticos (CSOC, IA, Cyber Range) demandan recursos sostenibles y criterios claros de asignación basados en criticidad y retorno de inversión en resiliencia.



3. Estrategia nacional de capital humano. Implementar becas, certificaciones obligatorias para roles sensibles y la Academia Virtual para cerrar la brecha de especialistas y dotar de capacidades operativas 24/7.

4. Inventario de activos e identificación de infraestructuras críticas. Un catálogo nacional permitirá priorizar protecciones, SLAs y pruebas de continuidad por impacto potencial.

5. CSOC y CSIRT operativos con KPIs: objetivos alcanzables (p. ej. CSOC operativo Q4 2026) y métricas de desempeño (MTTR, detección temprana, tiempo de remediación).

6. Programa operativo de evaluación de vulnerabilidades. Escaneo continuo, ejercicios de pentest y remediación priorizada para reducir la "ventana de exposición".

7. Cooperación pública-privada y acuerdos operativos. Formalizar MoUs con SLAs, intercambio de inteligencia y ejercicios conjuntos en Cyber Range para sincronizar capacidades.

8. Marco legal y armonización normativa. Ley de ciberdelitos, obligaciones de reporte y regulación para la protección de infraestructuras críticas deben avanzar en paralelo a las capacidades técnicas.

9. Gestión de la cadena de suministro y soberanía tecnológica. Políticas de adquisición seguras y criterios de evaluación para proveedores y modelos IA que protejan la continuidad operativa.

10. Cultura, transparencia y métricas de impacto. Campañas nacionales de

concientización, métricas de efectividad de capacitación y políticas de reporte de incidentes para restaurar confianza ciudadana.

Por otra parte, los desafíos que en este momento observo son:

- 1) **Déficit de especialistas y retención de talento:** sin un plan agresivo de formación, certificación y desarrollo de perfiles (seguridad ofensiva y defensiva), la operación del CSOC/CSIRT podría quedar comprometida.
- 2) **Coordinación efectiva en un entorno federal fragmentado:** 68 CSIRTs y múltiples actores exigen mecanismos obligatorios de integración operativa.
- 3) **Presupuesto y sostenibilidad:** la inversión debe ser previsible y ligada a KPIs de resiliencia.
- 4) **Armas tecnológicas (IA) en manos adversas:** la "weaponización" de IA necesita marcos defensivos proactivos.
- 5) **Confianza pública y gobernanza de datos:** incidentes pasados y la variabilidad en la transparencia erosionan legitimidad; la respuesta requiere transparencia controlada y métricas.



Plan Nacional de Ciberseguridad 2025–2030

Contiene los elementos que parecen ser muy prometedores; la principal variable de éxito será la calidad de la ejecución: gobernanza con mandato, recursos sostenibles, capacidades humanas, métricas y cooperación multisectorial. Retomar a un pacto operativo entre gobierno, academia e industria para convertir la visión en resiliencia tangible: el gobierno debe legislar y financiar, la academia debe producir talento y evaluación independiente, y la industria debe comprometerse con MoUs, transferir tecnología y participar en ejercicios; juntos pueden transformar la amenaza en ventaja competitiva regional. La implementación con disciplina y considerar los factores aquí comentados, podrían elevar la postura defensiva de México y servir de guía para liderar la cooperación hemisférica en ciberseguridad. 🌐

¿La computación cuántica es una realidad para la seguridad empresarial?



Antonio Celso Ribeiro Brasiliano

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

Brasil

Articulista Invitado

São Paulo, Brasil.- La computación cuántica está emergiendo como una revolución tecnológica con profundos impactos en la seguridad empresarial. Basado en los principios de la mecánica cuántica, utiliza *qubits* (bits cuánticos) capaces de operar en múltiples estados simultáneamente, permitiendo la resolución de problemas complejos exponencialmente más rápido que los sistemas clásicos.

1. Concepto central

La aplicación de la computación cuántica a la seguridad corporativa se estructura en dos grandes ejes estratégicos:

- A)** Protección contra futuras amenazas cuánticas, mediante criptografía y seguridad de la información;
- B)** Uso de la potencia cuántica para detectar, simular y responder a riesgos empresariales complejos en tiempo real.



2. Eje de protección — Quantum – Seguridad

2.1 Criptografía postcuántica.- Las computadoras cuánticas pueden en el futuro romper los algoritmos criptográficos tradicionales como RSA y ECC. Las empresas se están moviendo hacia modelos de criptografía resistente cuántica (PQC), estandarizados por NIST. Esta transición protegerá datos confidenciales, contratos y comunicaciones corporativas.

2.2 Distribución de claves cuánticas (QKD).- Basado en el entrelazamiento cuántico, QKD le permite generar claves de comunicación a prueba de manipulaciones. Cualquier intento de interceptación se detecta inmediatamente. Se utiliza en redes corporativas críticas, bancos centrales y sistemas logísticos estratégicos.

3. Eje de inteligencia — Análisis de seguridad cuántica

3.1 Detección de anomalías y ciberataques.- La capacidad de procesamiento paralelo de la computación cuántica permite detectar correlaciones sutiles en grandes volúmenes de datos, identificando ataques APT y patrones anómalos en redes críticas (IT y OT).

3.2 Simulación de riesgos interconectados.- La superposición de estados cuánticos permite simular múltiples escenarios de riesgo simultáneo. Esto permite análisis más realistas de las crisis corporativas, fallas sistémicas e interdependencia entre riesgos físicos y cibernéticos.

4. Eje de Resiliencia — Quantum optimizado para seguridad empresarial

4.1 Optimización de respuestas y contingencias.- Los algoritmos cuánticos resuelven problemas de optimización combinatoria en segundos. Sus

aplicaciones incluyen la planificación de contingencias, la evacuación en tiempo real y la asignación dinámica de recursos de seguridad.

4.2 Simulación de seguridad física y de activos.- Los modelos cuánticos permiten simular flujos de personas, activos y vulnerabilidades en instalaciones críticas como puertos, ferrocarriles y refinerías. Combinados con sensores del IoT y cámaras inteligentes, anticipan eventos de riesgo físico y cibernético.



5. El desafío de la preparación cuántica

A pesar del progreso constante en el desarrollo de hardware cuántico, incluidos los avances recientes en el diseño de chips, redes y corrección de errores, muchas empresas todavía están esperando ver cómo se ve el mercado. Esta vacilación se debe a las prioridades tecnológicas en competencia, la complejidad inherente de la computación cuántica y la incertidumbre sobre los plazos de avance. Es una estrategia arriesgada porque cuando el aprendizaje automático explotó hace una década, contratar científicos de datos y acceder al hardware se volvió casi imposible. Esto hizo que muchas empresas perdieran la ventana de oportunidad.

6. Posibles escenarios futuros para la computación cuántica

La consultora internacional Deloitte, a través de su informe "Computación cuántica en los próximos cinco años: planificación de escenarios para la resiliencia estratégica", emplea un análisis prospectivo para explorar cuatro futuros potenciales que podrían desarrollarse para 2030:

Escenario 1

Sorpresa: La computación cuántica llega antes de lo esperado, pero el ecosistema de talento sigue subdesarrollado. Los pioneros obtienen ventajas significativas, mientras que otros luchan por acceder a conocimientos limitados. Las organizaciones se enfrentan a una intensa competencia por unos pocos miles de expertos calificados en todo el mundo.

Escenario 2

Dilema: Tanto la tecnología cuántica como el desarrollo del talento avanzan lentamente. Las organizaciones cambian el enfoque a otras tecnologías, como la IA, dejando solo unos pocos profesionales en la experimentación cuántica. Estas empresas persistentes aseguran ventajas de talento y mantienen el conocimiento institucional a través de la experimentación continua.

Escenario 3

Explosión: Tanto la tecnología cuántica como los ecosistemas de talento se desarrollan rápidamente. El mercado experimenta una fiebre del oro similar al auge de la IA, con la llegada de fondos de riesgo y la proliferación de ofertas cuánticas como servicio. Las organizaciones con comités de liderazgo ejecutivo establecidos y centros de excelencia obtienen la mayor ventaja.

Escenario 4

Saltar: El ecosistema de talento se desarrolla más rápido que la tecnología. A pesar del lento avance técnico de la computación cuántica, el auge de la tecnología de IA impulsa el crecimiento de las habilidades y el talento STEM (Ciencia, Tecnología, Ingeniería y Matemáticas) en las ciencias de la información cuántica. Las habilidades STEM representan el conjunto de habilidades técnicas, analíticas y cognitivas necesarias para actuar, innovar y resolver problemas complejos en áreas científicas y tecnológicas. Los inversores invirtieron mucho en talento y salieron adelante.



Por qué las organizaciones deben actuar ahora

La computación cuántica ampliará la seguridad empresarial de dos maneras complementarias: protegiendo a las organizaciones de futuras amenazas (criptografía poscuántica y QKD) y fortaleciendo la inteligencia empresarial para abordar crisis y riesgos interconectados.

Durante los próximos 5 a 10 años, será un pilar de 'Enterprise Security 5.0', integrando inteligencia cuántica, criptografía avanzada y simulaciones de riesgos complejos. ¡Este es nuestro futuro! 🌐

Se redefine la seguridad hotelera en México

- Una industria que prioriza tecnología, prevención y criterio humano.

Beatriz Canales Hernández

Los hoteles son pequeñas ciudades en movimiento constante, es decir, todo pasa al mismo tiempo: los huéspedes llegan uno tras otro, los grupos se cruzan, el personal rota en turnos apretados, los proveedores entran sin hacer ruido, el mantenimiento trabaja a deshoras y los servicios operan con una exigencia permanente.

En medio de ese ir y venir, la seguridad ya no sólo es un apoyo periférico, sino que sostiene buena parte de la reputación del hotel y marca la continuidad de su operación diaria.

La hotelería mexicana atraviesa un período de crecimiento con luces y sombras. La apertura de nuevas cadenas, la presión que viven los destinos de playa y la expectativa del Mundial de 2026 obligan a revisar la manera en que se protege un hotel y cómo se previenen incidentes.

Para acercarnos a esa transformación, cinco empresas con enfoques distintos —Hikvision, ZKTeco, Jaguar del

Caribe, Salto WecoSystems y Dahua Technology— comparten lo que están observando desde dentro de la industria.

Durante años se pensó en la seguridad hotelera como un conjunto de cámaras, guardias, rondines y controles de acceso. Hoy la operación exige un sistema que mantenga conectados accesos, energía, videovigilancia inteligente, credenciales, zonas de riesgo y supervisión del personal. La protección funciona como una columna que sostiene la experiencia del huésped, aunque casi nunca se vea.

Hikvision explica muy bien este cambio. **Miguel Arrañaga**, director

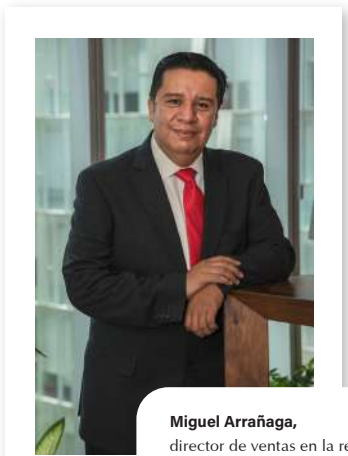


de ventas en la región Bajío, comenta que la videovigilancia ya no puede entenderse como un aparato que solo graba lo que ocurre. En sus palabras, "ya no hablamos solo de cámaras, sino de dispositivos inteligentes capaces de integrarse con plataformas que administran todo el ecosistema del hotel".



Ese tipo de integración modificó la manera en que los hoteles adoptan tecnología: lo que antes implicaba proveedores distintos, hoy puede gestionarse desde un solo sistema que unifica seguridad y operación.

La búsqueda de plataformas interoperables se volvió una constante. Los hoteles quieren sistemas estables, menos puntos débiles y una forma clara de supervisar su operación interna sin depender de soluciones sueltas.



Miguel Arrañaga,
director de ventas en la región Bajío, Hikvision.

La experiencia del huésped y la precisión operativa

Las cadenas quieren que la seguridad fluya sin estorbar. Buscan accesos simples, llaves que funcionen sin tropiezos, privacidad para el huésped y un entorno confiable. Las cerraduras inteligentes, las credenciales inalámbricas y las llaves digitales responden a esa necesidad.



Salto WecoSystems Scala trabaja justo en ese equilibrio. Su responsable de la vertical de hotelería, **Ramiro Gordillo**, comenta que los hoteles apuestan por un sistema que concentre la identidad del huésped en un solo medio. Puede ser una tarjeta, un brazalete o el teléfono. Con eso abren su habitación, usan el elevador, entran al spa, acceden a lockers o recorren áreas comunes: "La experiencia debe ser simple y a la vez completamente segura".

Cada tipo de hotel resuelve ese acceso de forma distinta. En los resorts, la pulsera es la opción más cómoda para quienes pasan el día entre la playa y los restaurantes. En los hoteles urbanos, la llave digital tiene mayor aceptación. En hoteles boutique, la tecnología debe adaptarse al diseño del edificio sin comprometer la estabilidad.



Ramiro Gordillo,
responsable de la vertical de hotelería en Salto WecoSystem.

ZKTeco observa la misma tendencia hacia la unificación. **Luis Enrique Reyes**, director de Marketing y Tecnología para Latinoamérica, comenta: "Lo que antes se resolvía comprando varias marcas, hoy se puede resolver con un solo ecosistema". En este segmento cualquier falla técnica afecta el ánimo del huésped, por lo que la integración dejó de ser un lujo.



Luis Enrique Reyes,
director de Marketing y Tecnología
para Latinoamérica, ZKTeco.



Daniel Romero,
director operativo, Jaguar
del Caribe.

El factor humano como pieza que sostiene el sistema

Se suele pensar que la tecnología terminará reemplazando la seguridad física. Sin embargo, quienes están dentro del sector no lo ven así. El guardia sigue siendo una figura indispensable.

Jaguar del Caribe expresa en la voz de su director operativo, **Daniel Romero**, quien comenta que ningún sistema sustituye la capacidad humana de interpretar lo que está ocurriendo: “La tecnología detecta, registra y alerta, pero el personal físico es quien interpreta, actúa y toma decisiones inmediatas”.

En un hotel se viven situaciones que requieren criterio: huéspedes vulnerables, incidentes en zonas aisladas, emergencias médicas, apoyos a familias, discusiones que deben calmarse con cuidado o intervenciones rápidas donde la tecnología solo alcanza a enviar una señal. Por ello, esta empresa insiste en que cada hotel debe evaluarse por separado; la geografía, el tamaño, la operación interna y el flujo de personas cambian completamente la definición del riesgo.



La Inteligencia Artificial como apoyo para anticiparse

La videovigilancia moderna ya no puede limitarse a observar, y ahora interpreta. Al respecto, **Dahua Technology** impulsa gran parte de ese avance. Su director de desarrollo de negocio en México, **Rodrigo Escamilla**, explica que la analítica les permite adelantarse a ciertos riesgos. “La Inteligencia Artificial permite ser más proactivos. Analizar patrones, detectar riesgos y responder antes de que ocurra un incidente”.

Los hoteles ya trabajan con herramientas que hace pocos años parecían lejanas. Las cámaras térmicas vigilan playas y detectan situaciones fuera de lo habitual. Las analíticas en albercas identifican caídas o ausencia de personal de rescate. El reconocimiento facial ayuda a controlar los accesos del personal y de proveedores. Los sistemas vehiculares registran placas y detectan comportamientos extraños. Los flujos en pasillos permiten mantener rutas despejadas y anticipar puntos de congestión.

Uno de los desarrollos más avanzados es el gemelo digital, un modelo virtual del hotel que permite visualizar en tiempo

real lo que ocurre en cada área. Una herramienta común en manufactura que empieza a encontrar su lugar en la hotelería.



Rodrigo Escamilla,
director de desarrollo de negocio
en México, Dahua Technology.

Plataformas estables para un hotel que no puede detenerse

La hotelería mexicana se inclina por plataformas sólidas, estables y capaces de sostener la operación durante todo el año. **Hikvision, ZKTeco, Salto WecoSystems y Dahua** coinciden en que los hoteles buscan sistemas que no dependan de infraestructura frágil ni provoquen interrupciones.



En este punto, **Salto WecoSystems** subraya algo que sus clientes mencionan con frecuencia --muchos hoteles eligen su plataforma porque funciona sin caídas. Una



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

cerradura que deja de emitir llaves, una puerta que se desconfigura o un sistema que se congela puede generar pérdidas económicas y afectar la imagen del hotel. La estabilidad técnica se vuelve parte esencial del servicio.



La lógica operativa de los hoteles apunta hacia plataformas que administren la identidad de todos los actores que entran y salen del edificio. Cada persona —empleado, huésped, proveedor o visitante— requiere permisos específicos, horarios y zonas autorizadas. Reducir la improvisación ayuda a mantener controlado un edificio que nunca descansa.

El turismo mexicano ante los próximos años

México se mantiene entre los países más visitados del mundo. La entrada de nuevas cadenas y la presión que traerá el Mundial de 2026 ponen a prueba la capacidad hotelera. Habrá más visitantes, más movimiento interno y menos margen de error.

Dahua anticipa una expansión importante en infraestructura, con más habitaciones, centros de entretenimiento y espacios que necesitarán análisis inteligente, monitoreo de eventos, control vehicular y plataformas capaces de manejar grandes volúmenes de personas. El turismo funciona cada vez más como una red que exige coordinación entre hoteles, autoridades, aeropuertos y empresas privadas.

Una seguridad que mezcla tecnología y criterio humano

Después de revisar las ideas y propuestas de estas cinco entrevistas, se confirma que el futuro inmediato de la seguridad hotelera en México dependerá de un balance preciso entre tecnología y criterio. Por ejemplo, la IA alerta, pero no interpreta emociones; las cámaras leen patrones, pero no sustituyen la interacción humana; las plataformas administran identidades, pero no pueden resolver una crisis sin la intervención de alguien preparado.

Daniel Romero, de **Jaguar del Caribe**, lo resume: “La seguridad física no ha disminuido; se ha transformado”.

Los hoteles buscan un modelo donde la tecnología amplifique el trabajo del personal y donde este use la tecnología como una extensión natural de su labor. Un equilibrio práctico y funcional.









Taking You Into A New Full-color Era with
Smart Dual Illuminators Technology

alas-la.org/cumbre-gerencial-alas

El 2026 llega con el mayor Encuentro de
Líderes de la Seguridad en LATAM - Únete a la
Cumbre Gerencial ALAS Cancún



CUMBRE
GERENCIAL
ALAS

2026



CANCÚN, MX. ABRIL 22 - 23



Llega a México Heracron: fibra para-aramida de alto desempeño para blindaje automotriz y corporal

- Esta fibra se utiliza internacionalmente con mucha frecuencia.

La industria latinoamericana del blindaje automotriz y de protección personal suma un nuevo competidor tecnológico: Heracron®, la fibra para-aramida fabricada por Kolon Industries en Corea del Sur, una de las tres empresas más importantes del mundo en aramidas para uso balístico. Su distribución en México estará a cargo de ProRescue, compañía con 10 años de experiencia en soluciones para seguridad y blindaje.

Heracron® es un material utilizado con éxito en Asia, Europa y Brasil, manteniendo en este último, el mercado de blindaje más grande del mundo, con una participación estimada entre el 30% y 35% gracias a su combinación de tenacidad, estabilidad térmica y desempeño balístico. Su llegada a México busca fortalecer la disponibilidad de materiales premium para fabricantes locales de blindaje automotriz y corporal.

Disponibilidad inmediata para el sector de blindaje premium

Los primeros embarques de láminas multicapa de 9 y 11 capas (3.0 x 1.5 m) ya se encuentran en stock en la Ciudad de México y han comenzado a utilizarse en proyectos con diferentes empresas blindadoras. Los paneles cumplen con estándares internacionales equivalentes a los niveles NIJ II y IIIA, aplicables en vehículos, chalecos, cascos y prendas de protección.

“Heracron® viene a complementar la oferta tecnológica del segmento premium, ofreciendo un material estable, confiable y con disponibilidad local”, explicó Gerardo Corona, director de ProRescue México. “El compromiso es garantizar un producto de alto desempeño, versátil, además de disponibilidad y soporte directo para los blindadores”, agregó.



Tres etapas de introducción al mercado

ProRescue considera tres fases en la expansión del material en el país:

1. Blindaje automotriz premium, donde operan más de 20 empresas especializadas.
2. Fabricantes de ropa balística, segmento en crecimiento con más de 3 participantes.

3. Productores de chalecos policiales, militares y de seguridad privada, un mercado estimado en más de 25,000 unidades año.

México, mercado estratégico para Kolon

Para Kolon Industries, México representa el segundo mercado más relevante de América, después de Brasil. “La calidad técnica del blindaje mexicano es reconocida internacionalmente, y por esa razón Heracron® tiene una oportunidad natural de desarrollo aquí”, señaló Guido Hyeon, representante comercial para el continente americano de Kolon Industries.

Hyeon explicó que Heracron® es una fibra para-aramida de alta resistencia utilizada en aplicaciones donde se requiere ligereza, estabilidad térmica y elevada resistencia a la tracción, como blindaje, cables, compuestos y protección industrial.



“En balística, Heracron ofrece una excelente relación entre desempeño y peso, lo que la ha posicionado como una alternativa sólida a otras aramidas del mercado”, afirmó.

Lanzamiento respaldado por pruebas técnicas

Los lotes iniciales en México han sido sometidos a pruebas de laboratorio y demostraciones controladas para validar el rendimiento del material en los diferentes niveles de blindaje civil. ProRescue confirmó que la cadena de suministro para fin de 2025 e inicio de 2026 está asegurada. 🇲🇽

HERACRON®

KOLON INDUSTRIES

La Aramida de Clase MUNDIAL.

"Heracron® Ofrece protección de grado profesional validada en zonas reales de conflicto y bajo normas internacionales.

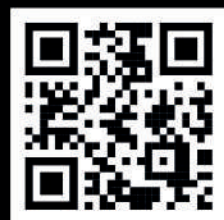
Sus filamentos creados específicamente para el blindaje, tienen mayor tenacidad, versatilidad para vehículos y silueta personal además de mayor resistencia térmica.."

La Nueva Elite del Blindaje en México.

Solicita ya tus láminas de 9 y 11 capas para niveles NIJ II y IIIA.



CONTACTO:
www.heracron.mx
www.prorescue.mx
contacto@prorescue.mx



Calidad vs cantidad, objetivo del sector de geolocalización:

- Muchas compañías están debidamente registradas, pero muy pocas son confiables y seguras.
- Es necesario prestar atención sobre todo cuando se trata de intangibles que tienen que ver seguridad y están involucrados unidades, mercancías y vidas humanas.

A pesar de que no existe un padrón real sobre el universo de compañías de localización satelital que atienden al transporte de carga, pasaje y particular, se estima que existen alrededor de 300, incluso muchas están registradas ante las secretarías de Seguridad y Protección Ciudadana (SSPC) y estatales, pero no significa que cuenten con estándares de calidad en el servicio y confiabilidad de las plataformas y procedimientos que ofrecen al mercado.

De acuerdo con datos de la SSPC, en la actualidad están registradas a nivel federal más de 3 mil empresas de seguridad privada y cientos de estas compañías ofrecen el servicio de rastreo satelital.

Raymundo Mancera Sandoval, presidente de la Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital (AMESIS), alertó que otro fenómeno adicional de la competencia desleal con las compañías "irregulares", es aquel donde muchas firmas legales de la geolocalización poseen los permisos oficiales pertinentes, pero carecen de certificados en cuanto a calidad del producto y servicio al usuario final.



"Como empresas formales y profesionales, instamos a nuestros clientes a que investiguen y clasifiquen a los proveedores confiables, ya que, aunque muchos de ellos estén autorizados por las SSP, esto no garantiza su profesionalismo ni la calidad de sus servicios". Señaló que es vital tener cuidado, especialmente cuando se trata de intangibles relacionados con un asunto tan sensible como la seguridad y que involucra a vidas humanas, unidades y mercancías.

A juicio de la AMESIS, organización con 18 años de existencia y permanencia en los sectores del transporte de carga y seguridad, muy pocas firmas llevan a cabo evaluaciones de satisfacción al cliente, de la infraestructura, experiencia, durabilidad, calidad y eficiencia de las soluciones de localización.

"Es importante señalar que, para aquellos de nosotros que nos ocupamos de proteger vehículos y mercancías en tránsito, proporcionar resultados satisfactorios es una prioridad. Es necesario que los protocolos se apliquen en segundos, que la reacción no tarde más de 20 minutos y que la resolución ocurra lo más pronto posible, ya que de esto depende si un delito se frustra", añadió el directivo.

El GPS y sus servicios ofrecidos debe ser confiable y sobre todo proteger las cuantiosas inversiones de prácticamente todos los sectores económicos, contando con el respaldo de técnicos monitoristas capacitados, centros de monitoreo para emergencias (no garajes o automonitoreo por internet) y asesores de seguridad especializados en el tema de rastreo satelital.

La inseguridad en México es considerada por la asociación como el detonante principal de la proliferación de centenares de empresas ilegales que ofrecen servicios de rastreo satelital y seguridad sin ningún tipo de regulación. Por esta razón, se considera prioritario mantener una relación con las autoridades gubernamentales en los tres niveles para cooperar eficazmente en beneficio de los usuarios finales.

Recomendaciones vs empresas irregulares

AMESIS recomienda que, para cerrarle el paso a las empresas irregulares de rastreo y localización satelital, el cliente puede contribuir si al momento de contratar el servicio exige:

- Que cuente con la autorización vigente expedida por la autoridad federal o estatal.
- Verificar si posee alguna certificación de calidad (ISO o similar).
- Asegurar el servicio mediante un contrato avalado por la PROFECO.
- Exigir una factura oficial de los trabajos contratados.
- Exigir la garantía por escrito del producto y servicio contratado.
- Preferir empresas que se manejen sobre Estándares de Competencia Laboral del CONOCER.
- Verificar si cuenta con reconocimientos vigentes de asociaciones relacionadas al sector.
- Solicitar la documentación que avale la experiencia de la empresa.
- Solicitar al menos cinco referencias comerciales para validar su servicio. 



Mantenemos la VIDA en MOVIMIENTO.



Flats Over® High performance®

Descubra por qué las mejores
blindadoras confían en Flats Over®

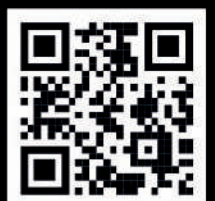
Flats Over® es un inserto runflat de grado profesional diseñado para ofrecer movilidad extendida en vehículos de seguridad y unidades blindadas. Desde 2003 ha sido el protagonista silencioso en cientos de evasiones exitosas en zonas de máximo riesgo, incluso con una o más llantas pinchadas. Gracias a su compuesto de caucho de alta resistencia y a su mecanismo de bloqueo por trinquete (ratchet), se ha consolidado como la opción premium preferida por las blindadoras en Latinoamérica.

En la práctica, **Flats Over®** opera como una mini-llanta interna que proporciona soporte estructural, tracción y control direccional tras la pérdida total de presión causada por pinchaduras o impactos balísticos.

Su geometría reforzada y su compuesto de alta resistencia permiten al vehículo mantener estabilidad y movilidad extendida hasta alcanzar una zona segura.



CONTACTO:
www.prorescue.mx
contacto@prorescue.mx



Autenticidad y calidad del producto, Puntos primordiales para blindaje responsable:



- Información y documentos clave que debe recibir el usuario.
- Más del 20% del blindaje en circulación, no cumple con los requerimientos mínimos éticos por falta de regulación o por pertenecer al “mercado negro”.
- Solo las empresas formalmente registradas y certificadas ofrecen blindajes con trazabilidad completa, documentación oficial y garantías que realmente protegen a los usuarios.

El Consejo Nacional de la Industria de la Balística (CNB) hizo un llamado a reforzar la ética, la transparencia y el cumplimiento normativo en los servicios de blindaje, ante el crecimiento del mercado informal y el incremento de familias, negocios y empresas que buscan soluciones de protección confiables.

En el caso del blindaje automotriz, el CNB advirtió que el usuario debe verificar siempre la documentación oficial del vehículo, ya que en los últimos años se han detectado casos de unidades que presumen niveles de protección inexistentes o procesos incompletos.

Ante ello, Leopoldo Cerdeira, delegado de la Comisión de Blindaje Automotriz del CNB, enfatizó la importancia de la certificación emitida por la autoridad: “Todo vehículo blindado legalmente debe contar con un certificado de blindaje y un código QR asignado por la Dirección General de Seguridad Privada. Son documentos esenciales que acreditan que el proceso fue realizado por una empresa autorizada y con materiales certificados. Validarlos es la mejor forma de evitar fraudes”.



En blindaje arquitectónico, el CNB destacó que la tendencia creciente en la protección de casas habitación ha generado la necesidad de procesos más claros y documentados. Las empresas formales deben garantizar trazabilidad completa, desde el material instalado hasta la forma en que se reforzó cada zona del inmueble.

René Rivera, presidente de la Comisión de Blindaje Arquitectónico del CNB, explicó que esta claridad permite al usuario conocer exactamente qué está comprando y qué nivel de resistencia tiene su propiedad, en algo tan particular como el blindaje en vidrios, por ejemplo: “Las familias están buscando proteger sus viviendas y requieren información confiable. Una empresa formal debe entregar una bitácora detallada de todo el proceso del blindaje, explicar cada etapa y mantener convenios de confidencialidad. La transparencia es clave para que el usuario tenga claridad y confianza”.

El blindaje corporal también enfrenta desafíos importantes debido al aumento de productos ilegales y sin procedencia verificable. El consejo señaló que muchos chalecos y placas que circulan en redes sociales o mercados informales muestran inconsistencias entre lo que se factura y lo que realmente se entrega, además de materiales usados o caducados que representan un riesgo directo. Ignacio Baca Torres, presidente de la Comisión de Blindaje Corporal del CNB, recomendó a los usuarios revisar cuidadosamente cada elemento del producto antes de comprar: “Es indispensable comparar la información técnica con la factura y con el proceso reportado por la empresa. Cuando algo no coincide o se vende por debajo del costo promedio, es casi seguro que se trata de material sin procedencia fiable, usado o caducado. Ese tipo de productos pone en riesgo la vida y no cumple con los requerimientos éticos que la industria formal sí garantiza”.

Con el propósito de orientar al público, el CNB presenta la documentación obligatoria que deben compartir al usuario final en diferente modalidad de blindaje:

Blindaje automotriz:

- Registro ante la autoridad.
- Pruebas balísticas y materiales certificados.
- Constancia de Autenticación con información del blindaje instalado y código QR verificables.
- Bitácora de materiales y puntos sensibles.
- Protocolos de instalación.
- Garantía y servicio postventa.

Blindaje arquitectónico:

- Registro formal y lineamientos de Compliance.
- Trazabilidad de materiales.
- Convenio de confidencialidad.
- Bitácora detallada del proceso.
- Certificación de resistencia.
- Probetas (opcional).

Blindaje corporal:

- Certificaciones vigentes.
- Garantía real y vida útil clara.
- Etiquetas de lote, nivel y fechas.
- Comparación entre factura, producto y proceso.
- Trazabilidad del origen.
- Prohibición total de material usado o caducado. 🚫

MÁS SEGURIDAD

Magazine

REGÍSTRATE CON EL CÓDIGO

MASSEGURIDAD

antes del 20 de febrero y obtén un **10%** de descuento en tu registro en **FASE 2**



CONGRESO NACIONAL
DEL BLINDAJE

25 Y 26 DE FEBRERO

INNOVACIÓN QUE PROTEGE

**EXPO SANTA FE
CDMX**

+18

EXPERTOS QUE HABLARÁN
SOBRE DIVERSOS TEMAS
DE BLINDAJE

+700

M2 DE EXHIBICIÓN PARA
LAS MARCAS LÍDERES EN
EL MERCADO

+170

TOMADORES DE DECISIÓN
EN TEMAS DE BLINDAJE

=

ESPACIO ÚNICO
DE NETWORKING
EN BLINDAJE



www.congresonacionaldelblindaje.com.mx

Testigos sociales en las licitaciones de vehículos blindados

- Representa un mecanismo de participación ciudadana, transparencia y rendición de cuentas, que contribuye a la transformación del actuar gubernamental.



Lic. Ricardo Guzmán
Director de operaciones en Vínculo 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

México

Articulista Invitado

Las compras y contrataciones públicas del gobierno federal implican uno de los principales rubros en que se destina el presupuesto anual, donde se destinan alrededor de 500 mil millones de pesos para la adquisición de los insumos que se requieren para que pueda operar toda la administración pública y las necesidades de la ciudadanía. En este tema, se deben incorporar principios de competencia y libre concurrencia en el diseño de los procedimientos de contratación pública, en la medida en que se logran mejores condiciones de contratación, el Estado obtiene ahorros derivados de un uso más eficiente de los recursos públicos y está en mejor capacidad de prestar servicios públicos.

De hecho, los entes gubernamentales tienen como mandato constitucional llevar a cabo procedimientos de contratación que consigan las mejores condiciones de precio, calidad, financiamiento y oportunidad para el Estado en términos del Artículo 134 Constitucional. En el logro de esas condiciones, la competencia económica y la libre concurrencia juegan un rol fundamental.

La Comisión Federal de Competencia Económica (COFECE) que fue sustituida por la Comisión Nacional Antimonopolio, publicó en el 2016 las *RECOMENDACIONES PARA PROMOVER LA COMPETENCIA Y LIBRE CONCURRENCIA EN LA CONTRATACIÓN PÚBLICA*, éstas identifican los aspectos que en materia de competencia y libre concurrencia deberían considerarse en cada una de las etapas de un procedimiento de contratación: planeación, diseño de requisitos y reglas de participación, y el desarrollo del concurso; así como aquellos que tienen un impacto transversal.

Asimismo, la Organización para la Cooperación y Desarrollo Económico (OCDE) reconoce el problema que persiste en países miembro y hace un análisis de las modalidades comunes de manipulación de licitaciones que incluyen mecanismos de reparto y distribución entre los oferentes coludidos de las utilidades extraordinarias que se obtienen como resultado del mayor precio contratado.

Por ejemplo, los competidores que aceptan no presentar ofertas o presentar una oferta perdedora podrían ser subcontratados o recibir contratos de prestación de servicios o suministro de bienes por parte del oferente ganador a fin de repartir entre ellos los frutos obtenidos ilegalmente de una licitación de mayor precio. La manipulación de licitaciones también puede incluir pagos por parte del licitador ganador a uno o más de los coludidos. Este pago de compensación se asocia también con las empresas que presentan ofertas complementarias.

Aunque la colusión en la presentación de ofertas en licitaciones puede ocurrir en cualquier sector económico, existen algunos en los que esto es más probable debido a las características específicas de la industria o del producto involucrado como es el caso de la industria del blindaje automotriz. Tales características tienden a fomentar los esfuerzos de las empresas para manipular ofertas. La OCDE identifica estas ocho características o puntos de alerta para tomar en cuenta y crear los mecanismos para reducir las posibilidades de colusión.

- 1. Número reducido de compañías.** Es más probable que se dé la manipulación de ofertas cuando sólo un número reducido de compañías proveen el bien o servicio en cuestión.
- 2. Participación baja o nula.** Cuando pocas empresas han entrado recientemente o tienen bajas probabilidades de entrar a un mercado porque la entrada es costosa, difícil o lenta, las compañías en este mercado quedan protegidas de la presión competitiva que representa la posible inclusión de nuevos participantes.
- 3. Condiciones de mercado.** Los cambios significativos en las condiciones de la demanda o la oferta tienden a desestabilizar los acuerdos en vigor para manipular licitaciones.

4. Asociaciones industriales. Las organizaciones pueden servir como mecanismos pro competitivos que son legítimos a los miembros de un sector de negocios o de servicios para fomentar la aplicación de estándares, la innovación y la competencia. No obstante, cuando se utilizan para fines ilegales y anticompetitivos, los ejecutivos de las empresas usan estas asociaciones para reunirse y ocultar sus discusiones acerca de formas y medios para llegar a un acuerdo de manipulación de licitaciones e implementarlo.

5. Ofertas repetitivas. Las compras repetidas aumentan las probabilidades de colusión. La frecuencia de presentación de ofertas ayuda a los miembros de un acuerdo de manipulación de licitaciones a asignar contratos entre ellos.

6. Productos o servicios idénticos o sencillos. Cuando los productos o servicios que venden las personas o compañías son idénticos o muy similares, resulta más fácil que las empresas lleguen a un acuerdo en torno a una estructura de precios común.

7. Pocos o nulos sustitutos. Cuando hay pocos o ningún sustituto adecuado de los productos o servicios que se está buscando adquirir, las personas o empresas que buscan manipular las licitaciones tienen la seguridad de saber que el comprador tiene pocas o ninguna opción y, por ende, es más probable que sus esfuerzos por elevar los precios tengan éxito.

8. Poco o ningún cambio tecnológico. El déficit o la carencia franca de innovación en el producto o servicio en cuestión ayuda a que las empresas lleguen a un acuerdo y lo mantengan en el tiempo.

Para el caso mexicano tenemos una excelente figura poco aprovechada que son los Testigos Sociales del Gasto Público. Los "Testigos Sociales", son personas físicas o morales que participan en los procesos de compras y contrataciones públicas, como representantes de la sociedad para vigilar la legalidad y transparencia de estos procesos. Con la finalidad de contribuir a la integridad de las compras públicas y asegurar para el Estado las mejores condiciones disponibles, así como propiciar la colaboración entre la sociedad y gobierno en el año 2004 atendiendo a los objetivos establecidos en el artículo 134 Constitucional, se institucionalizó la figura del Testigo Social en las contrataciones que realizaban las dependencias y entidades de la Administración Pública Federal.

Testigo social

Representa un mecanismo de participación ciudadana, transparencia y rendición de cuentas, que contribuye a la transformación del actuar gubernamental, además de que fortalece a las instituciones, legítima y retroalimenta los actos y decisiones de las autoridades, ya que el actuar en conjunto de la sociedad y gobierno robustece la gobernanza de la sociedad. En caso de que el Testigo Social detecte irregularidades en los procedimientos de contratación en los que participe, deberá remitir su testimonio a la autoridad competente para los efectos de la investigación administrativa correspondiente.

El compromiso ciudadano de participar en los asuntos públicos no es menor en ningún sentido, las instituciones han sentado las bases, la ciudadanía es cada vez más exigente porque el fenómeno de la corrupción está infiltrado en la vida diaria y el hartazgo colectivo por los costos que representa es una problemática que atañe a todos los sectores. Por eso este puente de colaboración entre los dos actores es fundamental para el desarrollo del control y bienestar social. 🇲🇽

+
+

¡Únetenos!

+
+

CON SEGURIDAD
Magazine Latam

Síguenos en
Telegram e Instagram

@conseguridadmagazine

+
+

Referencias y guías internacionales en seguridad patrimonial: Un aliado técnico

La selección informada y el uso responsable de estándares reconocidos permiten a las organizaciones diseñar esquemas de seguridades patrimoniales coherentes, escalables y sostenibles.



Armando García Sánchez

Gerente de Consultoría en Timur Latinoamérica.
Vicepresidente Ejecutivo de AMEXSI 2025-2026
<https://www.linkedin.com/in/armando-garcia-sanchez/>

México

Articulista Invitado

La seguridad patrimonial se ha consolidado como un componente estratégico para la continuidad operativa, la protección de las personas y la preservación de los activos físicos, tecnológicos y de información en organizaciones públicas y privadas. En un entorno cada vez más complejo —marcado por riesgos físicos, sociales, tecnológicos y reputacionales—, resulta indispensable contar con marcos de referencia claros, probados y alineados con las mejores prácticas internacionales.

Actualmente existe una vasta cantidad de normas, estándares y guías técnicas desarrolladas por organismos nacionales e internacionales que abordan la seguridad patrimonial desde distintos enfoques: gestión del riesgo, protección física, controles de acceso, seguridad electrónica, respuesta a emergencias, continuidad del negocio y resiliencia organizacional, entre otros. Esta diversidad de información, lejos de ser un obstáculo, representa una oportunidad para diseñar sistemas de seguridad más robustos, integrales y adaptables a distintos contextos, como el educativo, industrial, de servicios o institucional.

El uso de referencias internacionales reconocidas —como Normas ISO, estándares de ASIS International, lineamientos ANSI o NFPA— permite a las organizaciones estructurar sus estrategias de seguridad bajo criterios objetivos, comparables y auditables, facilitando además la alineación con procesos de calidad, cumplimiento normativo y mejora continua. Adoptar estos marcos no implica perder identidad local, sino fortalecerla mediante prácticas validadas globalmente y ajustadas a la realidad operativa de cada institución.

A continuación, se mencionan algunas (de las muchas) referencias representativas que algunas organizaciones ofrecen para consulta, la cual requiere de su adquisición (de forma electrónica o física) o del pago de alguna membresía.

- **ISO (gestión, riesgo, continuidad y operaciones de seguridad).** - www.iso.org
- **ISO 18788:2015** – Security Operations Management System (SOMS) para operaciones de seguridad privada (útil si contratas/gestionas proveedores de seguridad y quieres un sistema auditable).
- **ISO 28000:2022 (y 28000:2007)** – **Security management systems, con foco en cadena de suministro** (muy usado para proteger activos en logística, transporte, almacenes, distribución).
- **ISO 22301:2019** – **Business Continuity Management System (BCMS)** (resiliencia ante incidentes que afecten operaciones y activos críticos).
- **ISO/IEC 27001:2022** – **Seguridad de la información con controles físicos** (incluye controles de monitoreo físico y control de accesos a áreas).
- **ISO 22341:2021** - **Seguridad y resiliencia – Seguridad Protectora** – Directrices para la prevención del delito a través del diseño medioambiental CPTED.
- **ISO 22360** - **Seguridad y resiliencia - Gestión de crisis** - Conceptos, principios y marco

- **ISO 31000:2018 – Gestión del Riesgo** - Principios y directrices.

2) **ANSI/ASIS (estándares específicos de Security Management / Risk / Asset Protection).** - <https://webstore.ansi.org> ; www.asisonline.org

- **ANSI/ASIS PAP.1-2021 – Physical Asset Protection Standard (PAP)** — Marco para proteger y gestionar activos físicos: personas, propiedad e instalaciones.
- **ASIS BCM-2021 - Business Continuity Management Guideline.**
- **ASIS ESRM-2019 - Enterprise Security Risk Management Guideline.**
- **ASIS – Security Risk Assessment Standard (SRA)** - Guía estructurada para evaluación de riesgos de seguridad: amenazas, vulnerabilidades, impactos y tratamiento.
- **ANSI/ASIS/... RA.1-2015 – Risk Assessment (programa y competencias del evaluador)** (enfoque de programa de evaluación de riesgos; complementa ISO 31000).

3) **NFPA e IEC (referentes técnicos).** - www.nfpa.org

- **NFPA 730 – Guide for Premises Security** (guía integral para reducir vulnerabilidades en inmuebles).
- **NFPA 731 – Standard for the Installation of Premises Security Systems** (estándar para instalar sistemas electrónicos de seguridad en inmuebles).
- **IEC 62676 (serie) – Video Surveillance Systems for use in security applications** (requisitos/guías/partes para VSS/ CCTV).

El análisis y aplicación de estándares de seguridad patrimonial evidencian que no existe una solución única ni aislada para la protección de los activos y las personas, sino un ecosistema amplio de normas, metodologías y buenas prácticas que, correctamente integradas, elevan significativamente el nivel de madurez de cualquier organización. La gran cantidad de información disponible hoy refleja la evolución del concepto de seguridad, que ha pasado de ser reactivo y operativo a estratégico y preventivo.



Apoyarse en referencias internacionales ofrece beneficios claros: proporciona un lenguaje común, reduce la improvisación, fortalece la toma de decisiones basada en riesgo y facilita la evaluación objetiva del desempeño de los sistemas de seguridad. Además, estas referencias sirven como un respaldo técnico frente a auditorías, procesos de certificación, revisiones regulatorias y exigencias de aseguradoras o partes interesadas.

En este contexto, la selección informada y el uso responsable de estándares reconocidos permiten a las organizaciones diseñar esquemas de seguridad patrimonial coherentes, escalables y sostenibles, alineados con las mejores prácticas globales y con una clara orientación a la protección integral, la continuidad operativa y la mejora continua. 🌐



¡Garantizamos su tranquilidad!

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

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

Custodias: Para todo tipo de transporte de mercancías en tránsito



Rastreo satelital: Vehículos particulares, carga o flotillas

Videovigilancia: Fija, móvil y remota

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

www.grupoalem.mx

edgar.seguridad.integral@gmail.com



+52 564705 2246

La seguridad como pilar transversal de la sostenibilidad local: el vínculo entre la ISO 22341:2021 & ISO 22341-2: 2025 (cpted) y la ISO 18091:2019



Dra. Mercedes Escudero Carmona
Presidenta CPTED México ICA Chapter & presidenta ASIS International Capítulo 311.
México

Articulista Invitada

La sostenibilidad en el ámbito local es un concepto holístico que se cimienta en cuatro pilares: Institucional, Económico, Social y Ambiental. La aplicación efectiva de este modelo de desarrollo, a menudo guiado por la Norma ISO 18091:2019. Sistemas de gestión de la calidad — Directrices para la aplicación de la Norma ISO 9001 en el gobierno local, requiere la integración de herramientas que impacten en múltiples dimensiones simultáneamente.

En este contexto, la Norma ISO 22341:2021 (Directrices para la prevención del delito mediante el diseño ambiental, o CPTED por sus siglas en inglés) y 22341-2:2025 (Directrices para la prevención del delito mediante el diseño ambiental de instalaciones residenciales) emergen como estándares de seguridad de carácter inherentemente transversal, demostrando que la prevención del delito es un motor esencial para alcanzar los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de la Organización de Naciones Unidas (ONU).

1. ISO 18091: El marco de la gobernanza confiable y la agenda 2030:

La Norma **ISO 18091:2019** establece las directrices para la aplicación de la ISO 9001 (Gestión de la Calidad) en los gobiernos locales. Su misión fundamental es garantizar una **gestión integral de la calidad** y avanzar hacia el **Bien Común Local** mediante la alineación con los Objetivos de Desarrollo Sostenible de la Agenda 2030.

Utilizando el sistema de gestión de la calidad como el mecanismo para medir y gestionar las **Políticas Públicas** en los cuatro ejes de desarrollo: Institucional para un Buen Gobierno,

Económico Sostenible, Social Incluyente y Ambiental Sostenible. La ISO 18091 se convierte así en el sistema operativo que permite la planificación, ejecución y medición de la sostenibilidad.



Fuente: ISO 18091:2019

2. ISO 22341 (CPTED): Seguridad por diseño y transversalidad:

La ISO 22341 estandariza el enfoque de la Prevención del Delito a Través del Diseño Ambiental (CPTED), el cual busca reducir la delincuencia y el miedo al delito manipulando el entorno físico y social. Tradicionalmente centrada en principios de vigilancia natural y control de acceso, CPTED ha evolucionado hacia una tercera generación, la cual incorpora explícitamente los principios de sostenibilidad económica, ambiental y de salud.

Esta evolución es clave para su transversalidad, pues convierte la seguridad en una variable de diseño indispensable para:

- La resiliencia comunitaria.
- La revitalización de la actividad económica.
- La promoción de la cohesión social.

3. Vínculo y aportación de CPTED a los indicadores de sostenibilidad:

La aplicación sistemática de la ISO 22341, bajo el paraguas de gestión de la ISO 18091, impacta directamente en cada uno de los cuatro ejes de desarrollo sostenible presentados y de los 39 indicadores, CPTED aporta en los siguientes:

A. Desarrollo Institucional para un Buen Gobierno:

Indicador Clave	Aporte de la ISO 22341 (CPTED)
10. Seguridad pública	Es el objetivo directo. Un diseño urbano seguro optimiza los recursos policiales y de vigilancia, haciéndolos más eficientes.
9. Protección civil y resiliencia	CPTED es parte de la seguridad protectora y la gestión de riesgos socio-urbanos (alineada con ISO 31000), fortaleciendo la capacidad de la comunidad para anticipar, resistir y recuperarse de amenazas, incluido el delito.
6. Estado de derecho y derechos humanos	Fomenta el uso legítimo de los espacios públicos y reduce la necesidad de medidas de seguridad excesivamente restrictivas, promoviendo un entorno de respeto a los derechos ciudadanos.

B. Desarrollo Económico Sostenible

Indicador Clave	Aporte de la ISO 22341 (CPTED)
5. Turismo	Los espacios percibidos como seguros y atractivos son fundamentales para el desarrollo turístico. CPTED mejora la imagen del entorno, la atraktividad y la confianza del visitante.
8. Industria, comercio y consumo	La prevención del delito reduce el riesgo de vandalismo y robo, disminuyendo los costos operativos de los negocios y fomentando la revitalización de la actividad comunitaria en centros urbanos y comerciales.
8. Vivienda digna (Social, pero con impacto económico)	Un diseño CPTED incrementa el valor de la propiedad y la habitabilidad de la vivienda, vinculando el diseño seguro al crecimiento económico del barrio.

C. Desarrollo Social Incluyente:

Indicador Clave	Aporte de la ISO 22341 (CPTED)
9. Convivencia pacífica y cultura cívica	CPTED (especialmente la 2ª Generación, con enfoque social) busca la cohesión comunitaria. Los espacios diseñados para el uso social legítimo facilitan la interacción, la apropiación del espacio por parte de la comunidad y la vigilancia natural.
2. Deportes, recreación y ocio	Garantiza que los parques, plazas y áreas deportivas sean percibidos y utilizados como lugares seguros, promoviendo la buena salud y el bienestar.
5. Población vulnerable y personas con discapacidad	Un diseño de seguridad que considera la accesibilidad y la visibilidad, reduce la vulnerabilidad de estos grupos al delito y la exclusión social.

D. Desarrollo Ambiental Sostenible

Indicador Clave	Aporte de la ISO 22341 (CPTED)
3. Imagen del entorno y atractividad	El mantenimiento y el buen diseño ambiental son principios CPTED para prevenir el efecto de "ventanas rotas". Esto se traduce en un entorno limpio, cuidado y atractivo.
4. Recursos naturales, biodiversidad y ecosistemas	La Tercera Generación de CPTED alinea la seguridad con el diseño ecológico y la sostenibilidad ambiental, utilizando soluciones basadas en la naturaleza para la seguridad (ej. barreras verdes, iluminación eficiente), y asegurando que las áreas verdes sean seguras para el uso y disfrute ciudadano.
9. Acciones para el cambio climático.	El diseño resiliente ante riesgos socio-urbanos (incluido el clima extremo y el delito) es un componente integral de la ISO 22341 que contribuye a la resiliencia climática de la ciudad.

La aplicación de la ISO 18091 proporciona el sistema de gestión necesario para que un gobierno local implemente la visión holística de la sostenibilidad (Institucional, Económica, Social y Ambiental) para que mediante las políticas públicas sume a la sociedad en general y al sector privado para lograr cumplir con las metas de cada ODS. Dentro de esta estructura, las Normas ISO 22341 y 22341-2 (CPTED) se posicionan como una herramienta metodológica esencial que transforma el entorno construido para reducir el riesgo, la violencia y el miedo, el resultado es: la Co-producción de seguridad de la mano ciudadana.

La seguridad ya no es un fin en sí mismo, sino un habilitador del desarrollo sostenible. Al garantizar la convivencia pacífica, la vitalidad económica de los espacios y la calidad del entorno, CPTED demuestra su transversalidad total y se convierte en un pilar indispensable para la gestión de calidad y la consecución de los ODS de la Agenda 2030 de la ONU en el ámbito local, es decir, en cada calle de cada ciudad.

“CPTED es la arquitectura de la paz que, al diseñar seguridad que deja fuera la oportunidad del crimen e impulsa la vida social, permite que la vitalidad urbana florezca, garantizando que cada persona, sin importar su género o condición, pueda usar cada rincón seguro de la ciudad, de día y de noche”.

Mercedes Escudero Carmona.



Cuando los estándares se encuentran con el alma de la seguridad



Milagros Céspedes Álvarez
Coach PNL involucrada en el mundo de la seguridad desde hace 32 años. Fundadora y directora del Centro de Estudios de Seguridad para Latinoamérica.
www.ceslatam.com
Perú

Articlista Invitado

Lima, Perú.- Hace unos días, durante la celebración de aniversario por los 30 años del Capítulo ASIS 222 Perú, durante el último panel titulado “Gestión de Riesgos de Seguridad Empresarial – ESRM: evolución, tecnologías y aplicación”, destacados colegas compartieron sus perspectivas sobre la evolución de la seguridad corporativa desde la guía ESRM, y los estándares SRA (Security Risk Assessment), ISO 31000 e ISO 31050.

En medio de ese contexto, mientras escuchaba la exposición de cada panelista, mi mente no dejaba de reflexionar: todo suena bonito, estructurado, profesional, técnicamente sólido.... pero ¿en qué momento se involucran las personas? ¿En qué parte de estos modelos está el ser humano que piensa, decide, se equivoca, siente y finalmente ejecuta?

Esa inquietud me acompañó durante todo el panel. Y reafirmé algo que vengo sosteniendo desde hace tiempo, que más allá de los estándares, **hay un abismo entre hacer seguridad y ser parte de ella**. Podemos tener normas, políticas y procedimientos de clase mundial, pero si las personas no se sienten integradas emocionalmente al sistema, si no entienden el “para qué” de lo que hacen, ningún estándar podrá sostenerse en el tiempo.

Estándar	Qué busca	Qué le falta	El espejo humano (Neuroseguridad)
ESRM – Enterprise Security Risk Management	Vincular la seguridad con la estrategia del negocio.	Alinea procesos, pero no emociones.	Alinear la seguridad con el propósito humano, donde cada persona entienda el “para qué” de lo que protege.
SRA – Security Risk Assessment	Identificar, analizar y tratar riesgos a los activos.	Evalúa amenazas externas, no las internas del comportamiento.	Analizar riesgos cognitivos y emocionales: fatiga, impulsividad, sesgos, desmotivación, exceso de confianza.
ISO 31000 – Gestión del Riesgo	Definir principios y procesos para decisiones seguras.	Se enfoca en sistemas, no en percepciones.	Aplicar los mismos principios a la autogestión emocional y la coherencia personal.
ISO 31050 – Resiliencia Organizacional	Fomentar la capacidad de adaptación ante el cambio.	Mide continuidad, no bienestar.	Promover resiliencia emocional colectiva, donde el error sea aprendizaje y la presión, crecimiento.

De esa reflexión nace este artículo. De la necesidad de unir los marcos de gestión con la conciencia humana, de conectar los estándares con el alma de la seguridad.

Los estándares nos ayudan a estructurar la gestión, pero no siempre logran conectar con la esencia humana que los hace posibles. Revisemos brevemente su propósito y lo que, desde la Neuroseguridad, podemos complementar:

En muchas organizaciones, los procedimientos existen, pero las personas no los viven. Existe un abismo invisible, las personas no se sienten parte

del Sistema, no lo entienden ni saben cuál es su rol. Cumplen protocolos, pero sin comprensión profunda. Actúan dentro del sistema, pero sin conexión con él. Esa desconexión emocional se convierte en el mayor riesgo oculto. Un colaborador que no percibe sentido en lo que hace, que opera en automático o que siente que “no es su responsabilidad”, puede erosionar en segundos lo que costó años construir. **El desafío no está solo en diseñar políticas, sino en despertar conciencia.** Que cada persona comprenda que es parte activa del sistema de seguridad, que sus decisiones, emociones y actitudes influyen directamente en el resultado colectivo.

La Neuroseguridad surge como el puente que conecta los estándares con la realidad humana. Desde la neurociencia entendemos que el comportamiento ante el riesgo no es solo racional; está influenciado por emociones, percepciones y sesgos cognitivos.

Algunos ejemplos clave que nos hace comprender a lo que me refiero:

- La atención disminuye ante la rutina, eso genera vulnerabilidades.
- El miedo o el estrés reducen la capacidad de análisis, eso aumentan el error.
- La dopamina (hormona del placer) nos lleva a priorizar recompensas inmediatas sobre la seguridad a largo plazo.
- El liderazgo emocionalmente inteligente puede reprogramar la cultura de cumplimiento en una cultura de conciencia.

En otras palabras, **la seguridad no se impone, se inspira.**

El líder de seguridad del siglo XXI no solo debe dominar los estándares, sino entender la mente humana. Liderar desde la empatía, la autoconciencia y la confianza se ha convertido en una competencia estratégica. Las habilidades blandas, que en realidad son las más duras de construir, se vuelven esenciales:

- Escucha activa y comunicación emocional.
- Gestión del estrés y toma de decisiones bajo presión.
- Creación de entornos psicológicamente seguros.
- Liderazgo inspirador más que jerárquico.

Un estándar puede definir el proceso, pero solo el líder define la emoción que lo sostiene.

Cuando los estándares se encuentran con el alma de la seguridad, la organización deja de ser un sistema que controla y se convierte en una comunidad que cuida. Ahí es donde la seguridad trasciende el cumplimiento y se convierte en conciencia colectiva. Porque al final, la seguridad no depende de lo que hacemos, sino de quiénes somos cuando lo hacemos. 🌟

Reflexión inspirada en el panel “Gestión de Riesgos de Seguridad Empresarial – ESRM: evolución, tecnologías y aplicación”, celebrado en el 30° Aniversario de ASIS Capítulo Perú (2025).

Lima se prepara para la feria de seguridad más importante de la región: **SEGURITEC 2026**

• Reserve su stand.

Lima, Perú.- Del 27 al 29 de mayo en la ciudad capital de Lima, se llevará a cabo la 15ª versión de la Feria Internacional de Seguridad, «SEGURITEC PERÚ 2026». Este evento se ha consolidado como la plataforma de negocios más influyente entre fabricantes, distribuidores, integradores y profesionales del sector en el Perú y la región.



¿Por qué exhibir en SEGURITEC PERÚ 2026?

- 1. Negocios face to face:** SEGURITEC PERÚ reúne a +5000 visitantes de primer nivel entre directores de seguridad, gerentes de operaciones, jefes de compras, integradores, instaladores y entidades del Estado, todos en búsqueda de nuevas soluciones y proveedores confiables.
- 2. Exhibición de productos:** Su stand será el escenario perfecto para presentar las últimas tecnologías de la industria, realizar demostraciones en vivo y cerrar nuevos negocios.
- 3. Visibilidad de marca:** Su empresa aparecerá en el catálogo oficial de la feria, redes sociales, página web y comunicaciones previas al evento. Durante la feria su marca se presentará a miles de clientes, quienes están interesados en adquirir sus productos.
- 4. Congreso técnico:** Un programa de conferencias técnicas se desarrollará durante el evento teniendo como objetivo actualizar los conceptos generales de la seguridad de hoy y anunciar la más reciente tecnología disponible en el mercado internacional.

Lo invitamos a asegurar su stand y formar parte del principal punto de encuentro de la industria de la seguridad en la Región "SEGURITEC PERU 2026" 🌐

Emails de contacto:
bsanchez@thaiscorp.com
gdeltorre@thaiscorp.com



Decálogo de errores al realizar un análisis de riesgos de seguridad



Alfredo Yuncoza

Presidente del Hispanic Advisory Board de IFPO.
Director Senior de Smart Risk Consulting. Presidente del
Security College US. Presidente de Arcus Group C.A.
Email: a_yuncoza@yahoo.com
ayuncoza@gmail.com
Skype: alfredo.yuncoza
Twitter: @alfredoyuncoza

Venezuela

Articlista Invitado

Caracas, Venezuela.- En el contexto de la gestión de seguridad, el análisis de riesgos representa el fundamento esencial para una estrategia de protección eficaz. No obstante, en la práctica, incluso los equipos con mayor experiencia pueden incurrir en errores comunes que afectan negativamente la calidad de los resultados y generan decisiones poco óptimas o innecesariamente costosas. Este decálogo presenta y analiza 10 de los errores más relevantes que pueden comprometer la precisión, validez o funcionalidad de un análisis de riesgos en seguridad, acompañando cada uno con ejemplos pertinentes al entorno corporativo y operativo.

1. No definir con precisión el alcance del análisis

Uno de los errores más comunes es iniciar el análisis sin haber delimitado claramente qué se va a evaluar. Un alcance indefinido lleva a esfuerzos dispersos, pérdida de tiempo y resultados sin aplicación concreta.



Ejemplo: una empresa multinacional decide "evaluar los riesgos de seguridad física" de su sede regional, pero sin precisar si el foco está en las instalaciones críticas, los activos de información o la protección del personal. El equipo termina elaborando un informe extenso con datos inconexos que no permiten tomar decisiones operativas.

2. Basar el análisis solo en percepciones o supuestos

Otro error frecuente consiste en fundamentar el análisis en impresiones subjetivas en lugar de evidencia verificable. Las percepciones, aunque valiosas, deben contrastarse con datos objetivos, incidentes previos y fuentes confiables.

Ejemplo: un responsable de seguridad asigna una probabilidad "alta" a un ataque cibernético porque "ha escuchado de varios casos en la región", pero sin revisar estadísticas o tendencias de incidentes propios. El resultado es una priorización desbalanceada que desvía recursos de riesgos más probables o dañinos.

3. Utilizar metodologías inadecuadas o inconsistentes

El uso incorrecto o improvisado de metodologías de análisis invalida todo el proceso. Debe elegirse un marco coherente con el tipo de organización, su madurez y el contexto regulatorio.

Ejemplo: una institución financiera aplica un modelo de evaluación cualitativo que clasifica los riesgos como "bajo", "medio" o "alto", sin emplear métricas cuantitativas. Esto impide cumplir con exigencias normativas como las del Comité de Supervisión Bancaria de Basilea, que requieren estimaciones numéricas de impacto y probabilidad.

4. Ignorar los activos intangibles y humanos
El análisis suele concentrarse en activos físicos o tecnológicos, subestimando el valor de los conocimientos, reputación o relaciones institucionales.

Ejemplo: una empresa de seguridad descuida los riesgos asociados a la pérdida de personal crítico con competencias únicas. Al producirse la salida de un analista senior, la organización pierde capacidades analíticas y acceso a contactos estratégicos, generando vulnerabilidad operativa no prevista en el análisis original.

5. No integrar las amenazas emergentes ni el contexto dinámico
El riesgo es una función del tiempo. Ignorar factores emergentes o el contexto de cambio conduce a conclusiones obsoletas. El monitoreo continuo es parte esencial del análisis.

Ejemplo: un operador portuario realiza un estudio de riesgos en 2023 centrado en amenazas físicas, pero no actualiza su análisis después del incremento global del cibercrimen en sistemas de control industrial. Dos años más tarde, un incidente en su red digital paraliza operaciones durante días, evidenciando una omisión significativa.

6. Subestimar el componente humano y organizacional
Las debilidades más graves a menudo residen en el factor humano: errores, negligencia o falta de cumplimiento. No contemplar la cultura organizacional ni las variables de comportamiento distorsiona la evaluación del riesgo.

Ejemplo: una empresa identifica que la principal amenaza es el acceso no autorizado a áreas restringidas, pero ignora que muchos incidentes derivan de empleados que comparten credenciales. Sin incorporar la dimensión conductual, el análisis no logra reflejar la raíz del problema.

7. Evaluar la probabilidad o el impacto de manera arbitraria
Las escalas de evaluación suelen definirse sin criterios sólidos, generando resultados subjetivos y no comparables. La falta de trazabilidad en las ponderaciones reduce la credibilidad del análisis ante auditorías o revisiones externas.

Ejemplo: en una matriz de riesgos, dos analistas asignan diferentes niveles de probabilidad al mismo evento porque no existen parámetros definidos. Uno considera que un robo de carga es "poco probable", mientras otro lo califica como "frecuente". Esta inconsistencia impide priorizar adecuadamente los controles.

8. No vincular el análisis con decisiones y planes de tratamiento
Un análisis que no deriva en acciones concretas equivale a un ejercicio académico. Cada riesgo identificado debe generar decisiones de mitigación, aceptación, transferencia o eliminación, con responsables y plazos definidos.

Ejemplo: una empresa minera realiza un excelente diagnóstico de vulnerabilidades, pero no elabora un plan de acción posterior. Cuando ocurre un sabotaje menor, la organización no posee protocolos actualizados ni asignaciones presupuestarias para contramedidas.

9. Omitir la validación cruzada y revisión multidisciplinaria
La calidad del análisis mejora cuando se integra la visión de áreas diversas: operaciones, finanzas, tecnología, cumplimiento y recursos humanos. Analizar en solitario o sin revisión externa limita la objetividad.

Ejemplo: el departamento de seguridad física realiza el análisis sin consultar al área de TI. El resultado subestima riesgos en sistemas de acceso electrónicos que posteriormente muestran vulnerabilidades críticas no detectadas.

10. No documentar adecuadamente el proceso y sus supuestos
Todo análisis debe ser auditado y replicado. La falta de documentación o trazabilidad de datos, fuentes, criterios y decisiones invalida la integridad del proceso.

Ejemplo: una consultora externa presenta un informe de riesgos sin conservar registros de las entrevistas ni de la base de datos utilizada. Ante un cuestionamiento posterior de la dirección, resulta imposible justificar la asignación de ciertos niveles de riesgo o su evolución en el tiempo.



En conclusión, un análisis de riesgos de seguridad no es un documento estático ni una formalidad metodológica: es un proceso estratégico de apoyo a la toma de decisiones. Los errores descritos en este decálogo no solo afectan la exactitud del diagnóstico, sino que también exponen a la organización a pérdidas operativas, riesgos reputacionales y sanciones regulatorias.

El desafío para los profesionales de alto nivel en seguridad radica en mantener una disciplina técnica, una visión integral y una constante actualización frente a la evolución de amenazas. Evitar estos diez errores no garantiza la ausencia de incidentes, pero sí construye una cultura analítica más madura, trazable y alineada con los principios de gestión moderna del riesgo, donde la precisión metodológica se traduce en resiliencia organizacional. 🌐

Seguridad privada en Latinoamérica: del reglamento a la ley orgánica

“La profesionalización del sector privado de seguridad solo es posible cuando la ley se convierte en su columna vertebral institucional.”



Edison Cadena Ayala
MSC, CPO, CPOI, CSSM gerente general de
SEINNATIONAL CIA. LTDA.
Ecuador

Articulista Invitado

Quito, Ecuador.- En muchos países de Latinoamérica, la seguridad privada ha sido regulada históricamente por reglamentos, decretos o normas de rango secundario. Pero esos instrumentos suelen carecer del respaldo constitucional, estabilidad jurídica y exigencias técnicas que aporta una ley orgánica. Este salto desde regulación secundaria hacia una ley con rango superior tiene implicaciones profundas como:



- Fortalecer la gobernanza del sector
- Clarificar la relación Estado-privado
- Garantizar estándares mínimos uniformes
- Aporta legitimidad institucional.

Es fundamental darse un tiempo para analizar acerca de la trascendencia de contar con una ley orgánica de seguridad privada —o equivalentes constitucionales— en los países de la región, frente a los retos contemporáneos (criminalidad transnacional, tecnología, derechos humanos, informalidad). Comparar, exponer y revisar experiencias nacionales e internacionales representativas, para con ello plantear recomendaciones que permitan avanzar hacia marcos jurídicos más sólidos.

Una ley orgánica garantiza mayor estabilidad, participación democrática y rectoría estatal sólida. En contraste, los reglamentos son instrumentos fácilmente modificables, lo que genera inseguridad jurídica y fragmentación normativa.

La existencia de una ley orgánica aporta jerarquía normativa, define competencias, delimita responsabilidades y establece parámetros de control estatal sobre el sector.

Los retos contemporáneos actuales como el crimen organizado transnacional, la convergencia tecnológica y la informalidad del sector demandan marcos normativos de alto nivel. Una ley orgánica permite responder con mecanismos sólidos de fiscalización, trazabilidad tecnológica y respeto a derechos humanos.



Es importante considerar a países como Ecuador y Chile, quienes han dado pasos significativos con la aprobación de leyes orgánicas modernas. Otros países como México, Colombia, Costa Rica, Uruguay y Paraguay aún dependen de leyes ordinarias o reglamentos. Estos casos muestran que muchas naciones siguen operando con marcos legales robustos, pero sin el respaldo formal que implicaría una ley orgánica. Las discrepancias surgen en grados de control, estabilidad y exigencia normativa.

Cabe recalcar que esta diferencia de rango jurídico irremediablemente se traduce en niveles dispares de intervención, profesionalización y legitimidad.

Al pasar del reglamento a la ley orgánica, los beneficios esperables son varios y pueden medirse con indicadores, que beneficiarían respecto a:

- Reducción de informalidad
- Uniformidad y coherencia normativa
- Mejor calidad técnica en el sector
- Mayor transparencia y rendición de cuentas

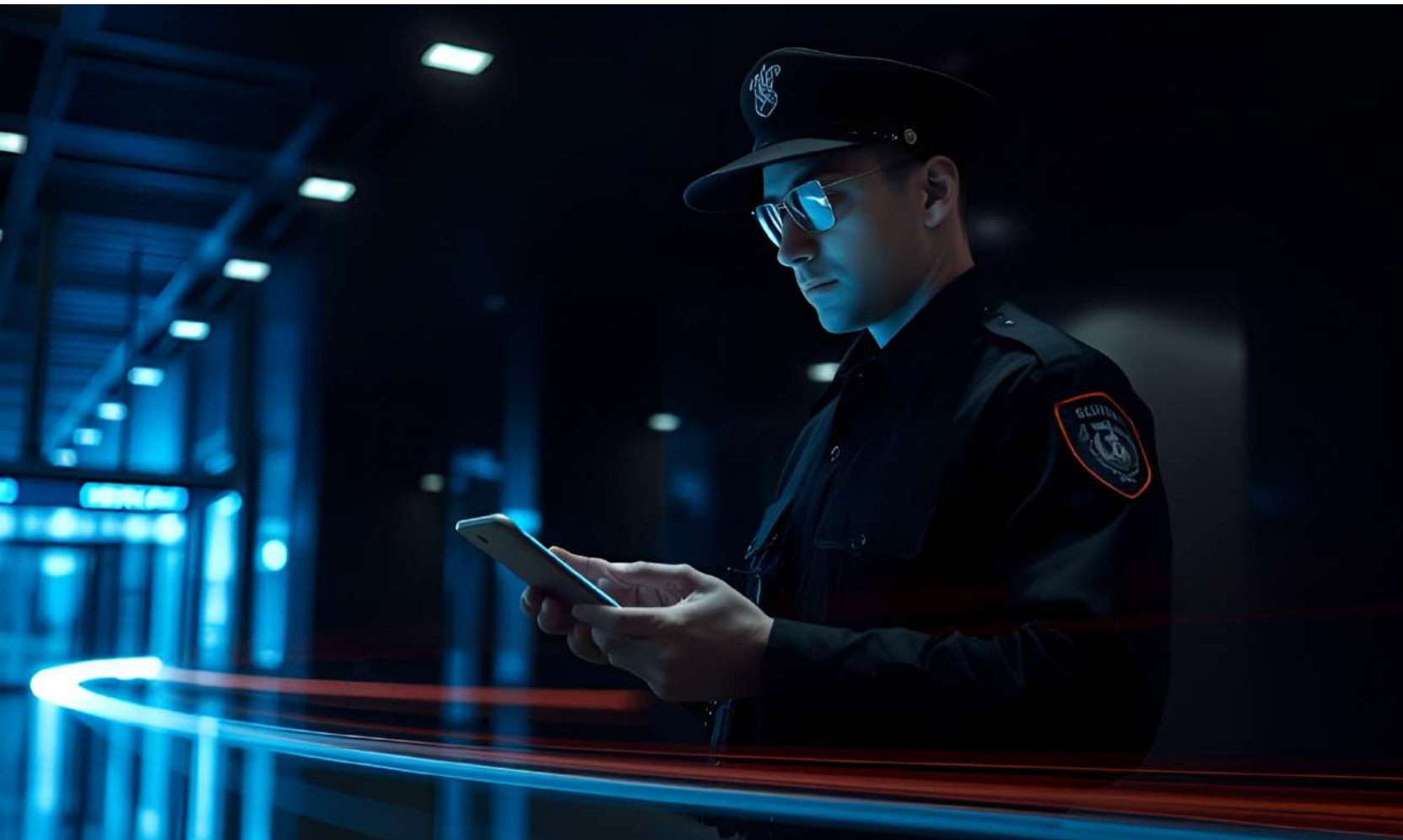
- Mejor integración público-privada en seguridad nacional
- Protección de derechos sociales y laborales
- Capacidad de adaptarse a nuevas amenazas tecnológicas

Para que estos impactos ocurran, la ley orgánica debe estar acompañada de un institucionalismo fuerte (una autoridad con recursos, independencia, sistemas de auditoría) y de voluntad política sostenida.

En resumen, me permitiría concluir manifestando que, la evolución normativa de la seguridad privada en Latinoamérica transita del predominio de reglamentos y normas secundarias hacia la adopción de leyes orgánicas robustas. Esa transformación no es mero formalismo: es el paso necesario para dotar al sector de estabilidad jurídica, capacidad técnica, coordinación institucional y legitimidad social. 🌐

Bibliografía de referencia

- Asamblea de la República del Ecuador. (2023). Ley Orgánica de Vigilancia y Seguridad Privada. Ministerio del Interior.
- Cámara de Diputados de México. (2006). Ley Federal de Seguridad Privada.
- Chile. (2024). Ley N° 21.659 sobre Seguridad Privada y Decreto 209 (2025).
- Superintendencia de Vigilancia de Colombia. (1994). Decreto 356: Estatuto de Vigilancia y Seguridad Privada.
- Congreso de Costa Rica. (2003). Ley 8395: Reguladora de los Servicios de Seguridad Privada.
- Uruguay. (2018). Ley 19.721 de regulación de la seguridad privada.
- Congreso de Paraguay. (2016). Ley 5.568 de servicios de vigilancia y transporte de valores.
- Congreso de Guatemala. (2010). Decreto 52-2010, Ley que regula los servicios de seguridad privada.
- Superintendencia de Seguridad Privada (El Salvador). (2003). Ley de los Servicios Privados de Seguridad.



Lo que no ves también te vigila

Anatomía secreta de la nueva vigilancia silenciosa



Andrea Guidugli.

Consultor Miembro Federación Periodistas de la ciudad de Madrid. Periodista y Opinador acreditado por la Federación Internacional de la Prensa de Bruselas

Italia

Articulista Invitado

La Spezia, Italia.- Una conversación, una voz, una vibración mínima: Todo basta. La vigilancia moderna ya no necesita micrófonos, solo rastros. De las salas seguras a los teléfonos de operativos, de los láseres que leen ventanas a los algoritmos que reconocen una voz entre millones: un viaje por la vigilancia que no se declara, la que no deja huellas físicas, pero sí digitales. Un territorio donde México tampoco es ajeno.

La voz que te delata

Durante años pensé que la seguridad era cuestión de prudencia. Una tarjeta SIM extranjera, un teléfono comprado en un aeropuerto remoto, una llamada hecha desde un pasillo de hotel en un país donde nadie conocía mi nombre. Creía —como tantos— que cambiar de tarjeta equivalía a cambiar de identidad. Era ingenuidad. Elegante, pero ingenua. Aquel día, en un despacho sin ventanas de una empresa del grupo —un lugar donde los técnicos de ciberseguridad hablaban en voz baja incluso estando solos— un colega se echó a reír al escuchar mis “métodos”.

Si alguien te está vigilando, no necesitan tu número. Necesitan tu voz. Una vez que la tienen, te siguen donde vayas. Cambies la SIM, el teléfono o de continente.

Me quedé callado. Él agregó, casi divertido: El error clásico del aficionado es creer que la vigilancia depende del dispositivo. En realidad, depende de ti.

Aquella frase me acompañó durante años y hoy, cuando miro el ecosistema de vigilancia mundial, me doy cuenta de que tenía demasiada razón.

No vivimos en la era de la ciberseguridad. Vivimos en la era de la ciber-percepción: donde las máquinas ya no buscan lo que haces, sino lo que eres.

Y ahí empieza esta historia.

La vigilancia que ya no necesita micrófonos: anatomía de un mundo silencioso

La vigilancia moderna ha cambiado de piel. No se basa en cables escondidos, grabadoras incrustadas en muebles o micrófonos diminutos. Eso es arqueología operativa. Hoy la vigilancia es óptica, vibratoria, algorítmica y, sobre todo, es pasiva.

No emite señales. No interfiere. No deja huellas. Solo observa.

1. Visual Intelligence (VISINT): cuando la luz escucha

El MIT lo demostró en 2014: una bolsa de patatas filmada a miles de fotogramas por segundo podía revelar conversaciones enteras. Pero ese experimento —*The Visual Microphone*— fue solo el prólogo. Desde entonces, varias unidades de inteligencia lo han llevado más lejos:

- NSA, Tailored Access Operations (TAO): integración de VISINT con SIGINT
- Unidad 8200 israelí: fusión de análisis temporal de video con captación de micro vibraciones

- GCHQ británica: análisis de ventanas a 200 metros con láseres de bajo retorno
- DEFENSA y SEMAR mexicana (información pública): uso de sensores ópticos en vigilancia urbana de alto riesgo.

Nada de esto es secreto; solo se comunica poco. Esta nueva generación de herramientas no escucha sonidos: escucha movimientos. Una cortina. Una botella de agua. Una lámpara. Una chapa metálica. Una ventana. Todo vibra cuando hablas y todo lo que vibra puede ser traducido.

2. El método Lamphone: la bombilla que delata secretos

Universidad Ben-Gurión, Israel, 2020. Demostración pública: captaron una conversación entera observando únicamente la luz de una bombilla. ¿Por qué funciona? Porque el filamento o el LED vibra y la luz vibrada contiene sonido codificado. Ese estudio está hoy en bases de datos policiales y militares internacionales. No porque sea exótico. Sino porque es operativo.

3. LDV (Laser Doppler Vibrometry): lo que revela un cristal

La técnica favorita de varias agencias: leer ventanas, detectar patrones de voz, captar discusiones de salas “seguras” que no lo son tanto. Un láser que apunta al cristal refleja micro oscilaciones que, reconstruidas, devuelven la voz. Ya no necesitas plantar un micrófono. Solo necesitas mirar el reflejo de un vidrio.

De la física a la doctrina: cómo operan los Estados

Los países que trabajan con vigilancia pasiva no improvisan. Tienen doctrinas, manuales internos, reglas de despliegue, cadenas de autorización. Aquí menciono las partes públicas, accesibles mediante fuentes abiertas:

1. Estados Unidos – Doctrine for Technical Surveillance Countermeasures (TSCM)

Manual desclasificado parcialmente, protocolo para detectar: vibraciones sospechosas, interferencias ópticas, emisiones secundarias, manipulación de ventanas, presencia de VISINT remota. Cada año se entrenan unidades específicas del FBI y del servicio diplomático.

2. Israel – SIGINT Fusion Doctrine

La Unidad 8200 integra: vibración, imagen, acústica residual, análisis de tráfico digital. No buscan pruebas directas. Buscan correlaciones y esas correlaciones valen más que una grabación clásica.

3. Francia – DGSI/DGSE

Usan VISINT en: negociaciones de rehenes, seguimiento antiterrorista, operaciones contra crimen organizado de origen saheliano. Francia fue de las primeras en integrar VISINT en operaciones urbanas en Marsella y Lyon.

4. México – DEFENSA, SEMAR, CN5I

México no se queda atrás. En 2022 y 2023, varios documentos públicos mencionan uso de sensores ópticos de largo alcance, estaciones móviles de vigilancia vibratoria, integración con plataformas de reconocimiento urbano. México tiene una ventaja: su “experiencia de frontera” con Estados Unidos ha permitido cooperación técnica constante.

El error humano: somos rastros antes que personas

Aquí entra mi anécdota personal, que ahora adquiere un peso distinto. Aquello que me dijo mi colega “necesitan tu voz, no tu teléfono” es una doctrina real. Se llama: **Speaker Identity Tracking (S.I.T.)**.

No importa qué número uses. Da igual en qué país estés. Si una agencia tiene tu firma vocal, puede detectarte cuando: llamas por VoIP, envías un mensaje de voz, hablas cerca de un dispositivo conectado, apareces en el audio de un video, incluso cuando hablas dentro de un automóvil moderno. La voz es más fuerte que tu pasaporte y más traidora que tu SIM.

Los casos reales que nunca se cuentan

Aquí es donde la historia deja de ser técnica y se vuelve humana. La vigilancia pasiva es tan poderosa como discreta. Sus éxitos no suelen aparecer en comunicados oficiales, y cuando lo hacen, se atribuyen a “trabajo de inteligencia”, una expresión que sirve para ocultar tecnologías que no conviene mencionar. Aquí van versiones ampliadas, basadas en información pública, documentos judiciales y reconstrucciones de fuentes abiertas, que permiten entrever cómo estas técnicas operan realmente.

1.- Beirut, 2019 – El eco de un vidrio

(Información cruzada de prensa libanesa, Haaretz e informes de la ONU)
Un edificio aparentemente anodino, en un barrio donde ninguna agencia occidental podía plantar un micrófono y sin embargo, una reunión de comandantes de un grupo armado fue detectada. ¿Cómo? Una cámara térmica situada a más de 300 metros captó oscilaciones irregulares en el vidrio del piso superior. No era suficiente para oír palabras, pero sí para detectar *ritmo conversacional*, intensidad, número de voces y momentos de tensión. Ese “perfil vibracional” permitió confirmar que la cúpula estaba reunida. El ataque selectivo llegó horas después. Nunca se mencionó VISINT. Solo se habló de “información precisa y oportuna”.



2.- Sonora, 2021 – Un dron contra el silencio

Arresto de un operador del CJNG tras análisis de vibración en techos refrigerados.
México, 2022 — Drones con telemetría térmica vibracional.
No fue una llamada interceptada ni un informante infiltrado. El inicio de la operación provino de un dato anómalo: la vibración térmica irregular en un techo industrial ubicado en el corredor entre Caborca y San Luis Río Colorado, Sonora, una región donde células del Cártel Jalisco Nueva Generación (CJNG) mantenían laboratorios de procesamiento y bodegas refrigeradas para el almacenamiento de droga sintética.

Los agentes federales no buscaban exactamente ese edificio. La vigilancia aérea formaba parte de un reconocimiento rutinario, usando drones multiespectrales con sensores de telemetría térmica vibracional, tecnología que combina tres matrices:

- Radiometría infrarroja** (cambios de temperatura, incluso bajo cubiertas opacas)
- Patrones de vibración estructural** (micro oscilaciones por voz, maquinaria o movimiento humano)
- Análisis de coherencia acústica residual** (traducción matemática en patrones rítmicos)

Lo que llamó la atención no fue el calor — muy común en instalaciones clandestinas — sino una frecuencia vibratoria rítmica, comparable a la cadencia del habla humana. El techo del contenedor refrigerado vibraba a entre 82 y 134 Hz durante lapsos irregulares. Esa banda de frecuencia es consistente con conversaciones masculinas en voz baja. El dron no captó palabras. Tampoco necesitaba hacerlo. Los especialistas del Centro Nacional de Fusión de Inteligencia (CN5I) detectaron algo más interesante: las vibraciones indicaban dos patrones vocales distintos, uno dominante y otro subordinado. Era, estadísticamente, una conversación de mando.

Aquello transformó el vuelo de rutina en un objetivo prioritario.

La segunda confirmación: los compresores

El análisis térmico detectó que los compresores de refrigeración se apagaban durante lapsos de 4 a 7 minutos, siempre después de las vibraciones. Los peritos concluyeron que el silencio mecánico se usaba para conversaciones sensibles, reduciendo ruido ambiental y facilitando la comunicación interna. Eso es doctrina. Doctrina criminal, pero doctrina al fin.

La fase terrestre

En menos de cuatro horas, un equipo mixto Sedena-FGR ejecutó una incursión silenciosa.

Dentro del contenedor encontraron:

- 14 kg de metanfetamina en etapa cristalina
- 1 prensa hidráulica contaminada con fentanilo
- 2 radios Kenwood modificados con cifrado casero
- 1 cuaderno con rutas en Arizona y contactos en Mexicali
- y, sobre todo, al objetivo esperado:

Eduardo “N”, alias *El Ganso*, operador logístico del CJNG, con órdenes de aprehensión por tráfico transfronterizo. En ningún boletín oficial se mencionó la tecnología utilizada.
Se emitió la versión estándar: trabajo de inteligencia, seguimiento y coordinación interinstitucional.

Pero la realidad —según dos funcionarios consultados bajo reserva— es otra: “No hubo llamadas interceptadas. No hubo soplones. Lo que habló fue el techo”.

Por qué este caso cambió protocolos internos

Tras la operación, la FGR y DEFENSA ajustaron criterios de vigilancia para bodegas refrigeradas, creando una matriz de riesgo vibracional, ahora usada en varios estados:

1.- París, 2022 – La botella que habló

(Información judicial francesa)
En un apartamento vigilado por la policía francesa, no era posible introducir micrófonos: el sospechoso desmontaba el mobiliario tras cada visita. La solución fue inesperada: una cámara térmica registró la vibración mínima de una botella de vidrio sobre la mesa. El software reconstruyó patrones térmico-vibratoriales, suficientes para confirmar órdenes, tiempos y la implicación del sospechoso. La prensa habló de “seguimiento técnico”. Nunca explicaron la botella.

2.- Kandahar, 2018 – La motocicleta delató al mensajero

(Fuentes abiertas afganas y estadounidenses)
Un reclutador talibán evitaba teléfonos, radios y reuniones en interiores. El error: hablar mientras conducía. Su motocicleta vibraba más cuando hablaba que cuando circulaba en silencio. Un dron analizó micro fluctuaciones del chasis. La vibración reveló su identidad vocal. Lo siguieron tres semanas. Arrestado sin haber pronunciado una sola palabra en un teléfono.

3. Madrid, 2020 – La impresora que los delató

(Datos de sentencia judicial)
Hubo casos europeos —como la operación en Madrid contra una red de trata, en la que la vibración térmica de una botella dejó al descubierto una reunión clandestina—, pero aquellos episodios son hoy casi prehistoria. La doctrina operativa real está naciendo en Beirut, en los túneles de Siria y en los galpones refrigerados del norte de México.

En una célula yihadista, nadie usaba móviles. Se comunicaban escribiendo mensajes y destruyéndolos. Pero una impresora vieja vibraba de forma distinta cuando había varias personas hablando alrededor. Esas vibraciones, cruzadas con cámaras de tráfico del barrio, permitieron deducir asistencia, turnos y jerarquías internas.

Estos casos no aparecen a menudo en manuales abiertos. Pero son los casos que explican por qué la vigilancia moderna ya no busca sonido. Busca patrones.

La frontera mexicana: un laboratorio silencioso

Pocos países han visto su territorio convertirse, sin anunciarlo, en un laboratorio de vigilancia pasiva. México es uno de ellos. No por un plan maestro, sino porque su geografía, su criminalidad organizada y su cooperación con Estados Unidos han creado un ecosistema operativo único.

1. Las “casas mudas” de los cárteles

En estados fronterizos, los cárteles adaptaron habitaciones enteras con materiales acústicos comprados en EE. UU. Creían haber logrado silencio total. Error: las paredes insonorizan sonido, pero no frenan vibración estructural. En 2023, una operación en Tamaulipas detectó actividad en una casa “muda” gracias a la vibración de una tubería exterior expuesta al viento. El análisis reveló movimientos internos equivalentes a conversaciones. Los agentes entraron sin haber escuchado un solo sonido.



2. Vehículos “insonorizados” que no lo son

Varios grupos criminales usan camionetas modificadas con paneles acústicos. Pero la vibración de los espejos retrovisores — captada por cámaras de tráfico mexicanas integradas a software estadounidense — permite deducir si dentro se está hablando, cuántas voces hay y si la conversación es tensa o relajada. Esto ya se usa en Nuevo León y Baja California.

3. Drones híbridos de vigilancia vibracional

Sedena y Marina han adquirido, según documentos públicos de compra, drones equipados con:

- cámaras de 120-240 fps
- sensores IR para vibración térmica
- algoritmos de correlación VISINT

Los despliegues están concentrados en Tijuana, Mexicali, Matamoros y Ciudad Juárez.

4. Intercambio técnico México–EE.UU.

En centros binacionales (como el de El Paso), agentes mexicanos reciben formación en análisis vibracional. México, a su vez, entrega datos operativos reales, imposibles de obtener en territorio estadounidense. Es cooperación pragmática: ellos tienen la tecnología; México tiene el escenario operativo.

5. Intercambio El “Efecto Migratorio”

La biometría no solo controla quién entra. Desde 2021, varios sistemas fronterizos detectan:

- nivel de estrés en la voz
- micro tensiones faciales
- vibración involuntaria del tórax

No es psicología. Es física más machine learning. Ese cruce de señales alimenta bases de riesgo que, oficialmente, no existen. La frontera mexicana es hoy un aula donde las agencias aprenden cómo vibra el crimen y cómo vibra quien intenta no dejar rastro.

El núcleo del asunto: ya no importa qué dices, sino cómo vibras

En vigilancia moderna, toda identidad es física antes que digital. No importa la contraseña, el número de teléfono o el dispositivo: la vibración es el nuevo ADN operativo.

La voz, convertida en arma de rastreo

La técnica S.I.T. (Speaker Identity Tracking) permite identificar a un individuo incluso cuando:

- usa un modulador de voz
- habla detrás de un vidrio
- está a más de 20 metros del micrófono accidental
- aparece en un video ambient noise

La firma vocal es más estable que una huella digital.

El cuerpo vibra, aunque guardes silencio

Incluso sin hablar, un individuo genera:

- vibración torácica
- micro flujos de aire
- resonancias de pasos
- presión rítmica en superficies

Un láser bien ajustado puede detectar la respiración acelerada de alguien que está nervioso detrás de una pared.

Los objetos a tu alrededor son tus enemigos

Todo delata:

- una taza de café (excelente resonador)
- una laptop (la tapa vibra con la voz del usuario)
- una mesa metálica
- un parabrisas
- una persiana barata

Cada objeto es un micrófono involuntario.

La luz también escucha

Cámaras de tráfico en ciudades como Tokio, Londres, París y CDMX pueden detectar micro variaciones lumínicas en ventanas o fachadas. No “escuchan”: reconstruyen movimiento y el movimiento es conversación.

El enemigo verdadero: la correlación

No hace falta oír tu voz. Basta correlacionar:

- vibración de objetos
- ubicación GPS
- horarios
- temperatura ambiente
- redes Wi-Fi visibles

Cada variable aislada es inocente. Juntas, construyen tu presencia.

El silencio ya no existe

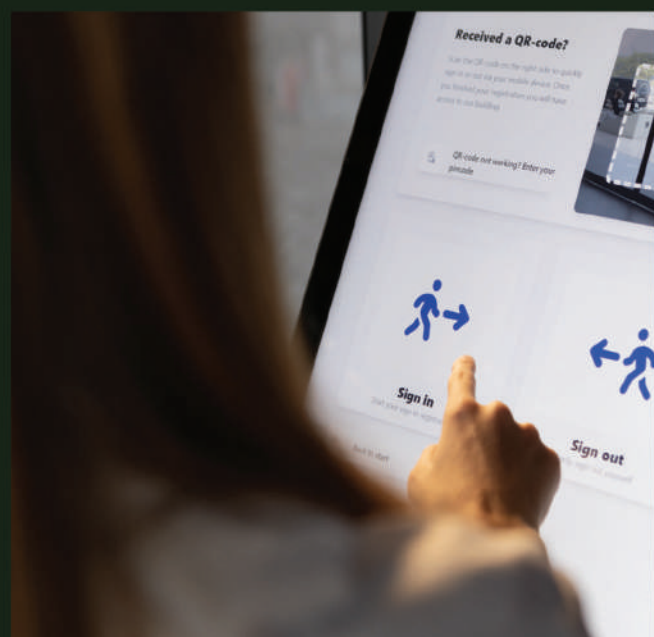
Quien crea que la vigilancia moderna funciona como en las series, micrófonos, pinchazos, hackers tecleando frenéticamente, está viendo una película antigua. Hoy la inteligencia no te busca, te percibe. No entra en tus dispositivos, entra en tus vibraciones. No quiere tu contraseña, quiere tu patrón. Y eso, si se usa bien, puede salvar vidas. Si se usa mal, puede destruir libertades. Esa es la paradoja del siglo XXI. 🌐

Impulsando un acceso más inteligente

SALTO lidera la transformación digital en la gestión de accesos e identidades, combinando tecnologías innovadoras con soluciones pensadas para cada necesidad.

Desarrollamos tecnología de vanguardia en control de accesos, gestión de identidades y cerraduras electrónicas, para ofrecer experiencias seguras, confiables y sin fricciones en todo tipo de espacios.

saltosystems.com



Datos de contacto

marketing.cala@saltosystems.com





15^{VA} FERIA INTERNACIONAL DE SEGURIDAD

MAYO
27 - 29
2026
LIMA-PERÚ



FÍSICA & ELECTRÓNICA ✓
PERSONAL (EPP) ✓
DEFENSA PERSONAL ✓
INCENDIO Y RESCATE ✓
VIGILANCIA & PROTECCIÓN ✓
POLICÍA Y SERENAZGO ✓
VIAL ✓
CIBERNÉTICA ✓
COMUNICACIONES ✓
PROTECCIÓN OCUPACIONAL ✓

¡RESERVE SU STAND HOY!

www.seguritec.thaiscorp.com

Sede



Oficialización



Prensa Asociada

MÁS SEGURIDAD
Magazine



CON SEGURIDAD
Magazine Latam

Organiza: Thais Corporation S.A.C. - thais@thaiscorp.com - [+51 989-177-352](https://www.whatsapp.com)