Junio 2026 / edición 162

MÁS SEGURIDAD

Magazine

Revoluciona a la industria Latina

Junio 2026 / No. 162 / Año 18
Internacional / precio $60.00 MXN
www.revistamasseguridad.com.mx

www.revistamasseguridad.com.mx

Organiza

Grupo Empresarial íntegra
Soluciones en Propiedad Horizontal

EXPO SEGURIDAD

VIGILANCIA • SEGURIDAD PRIVADA • TECNOLOGÍA

El punto de encuentro de la industria de la SEGURIDAD

¡VINCÚLATE YA!

Julio 28 y 29 | 2026

ÚLTIMOS CUPOS PARA EXPOSITORES

NEOMUNDO

Informes
(+57) 318 623 5411

BUCARAMANGA | COLOMBIA

MÁS SEGURIDAD
Magazine

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
Más Seguridad Magaine

Revista Más Seguridad Año 18, No 162, Junio 2026, Publicación Mensual de **Grupo Editorial MS Global S. de R.L. de C.V.**, con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 5555272279 / +52 5528732719. **Editor responsable: Humberto Mejía Hernández.** Certificado de Reserva 04-2022-050614181900-102 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No. 11483 y Certificado de Licitud de Título No. 13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: **Grupo Mejía Impresores**, calle La Poza No. 72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel: +52 5518947067.

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

Gestor de Riesgos, Oficial de Cumplimiento, Profesional en Seguridad Corporativa, Consultor especializado en Seguridad Física, Electrónica e Investigaciones. Res. 23747 SVSP - Mindefensa

Profesional en Negocios Internacionales con énfasis en Seguridad Corporativa, Gestión de Riesgos, Cumplimiento, Transporte de Valores, Pericia Forense, Asesorías, Auditorías, Dirección y Gerencia de Empresas y Departamentos de Seguridad con alta orientación a resultados.

Oficial de Cumplimiento – externo (10 compañías: Colombia, Dubai AEU, USA, El Salvador)

Gerente General de la firma SERCOPP S.A.S.

Héctor Fabio Blandón Posada

Colombia

SUMARIO

MÁS SEGURIDAD
Magazine

Tour Internacional 2025

EXPO SEGURIDAD
VIGILANCIA • SEGURIDAD PRIVADA • TECNOLOGÍA

intersec
BUENOS AIRES

ESS+
FERIA INTERNACIONAL DE SEGURIDAD

EXPO SEGURIDAD TELECOM COSTA RICA

EXPO SEGURIDAD TELECOM EL SALVADOR

EXPO SEGURIDAD TELECOM PANAMÁ

SEGURIDADEXPO
by [illegible] CHILE

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

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 empres 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. Respaldado 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.

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

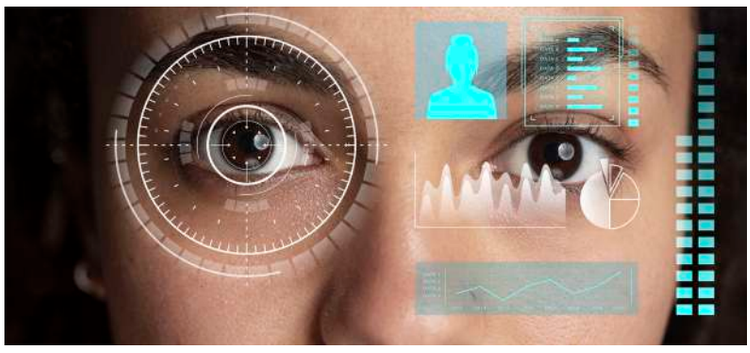
- Urgen principios de legalidad, privacidad, proporcionalidad y rendición de cuentas.
- La CURP biométrica representa una seria amenaza a los derechos humanos.

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)

salto
INSPIRED ACCESS

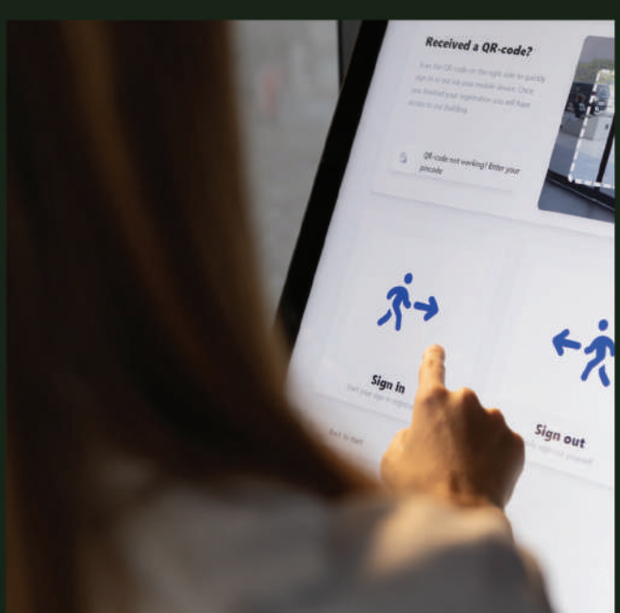
SALTO WECOSYSTEM

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

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.

TU GRUPO DE TRABAJO NECESITA CAPACITARSE EN SEGURIDAD.

Con nuestros Cursos InCompany, a la medida de tus necesidades, nosotros lo hacemos posible.

Programa los cursos que más te interese:

- Alarmas y Detección de incendios
- Alarmas y Detección de Intrusión
- Ciberseguridad para Alta Gerencia
- Control de Acceso
- Drones en Seguridad
- Evaluación de Riesgos de Seguridad
- Evaluación del Retorno de la Inversión en Seguridad
- Fundamentos de Seguridad Electrónica
- Gerencia de Proyectos
- Hacking Ético
- Integración de Sistemas de Seguridad
- Inteligencia Artificial en Seguridad
- Management 3.0
- Operadores de Cuartos de Control
- Redes IP e Inalámbricas
- Seguridad Perimetral
- Ventas para la Industria de la Seguridad
- Video Vigilancia

Si buscas un curso que no está en la lista, cuéntanos y lo estaremos coordinando para ti.

MANUELA RIVERA
Encargada de Cursos
WhatsApp: +57 304 2738724
Email: cursos@alas-la.org

CURSOS ALAS

ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

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 Mantenerte 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 Hermosillo 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.

SMART**CITY**
EXPO LATAM CONGRESS

2 - 4 JUNIO 2026
PUEBLA, MÉXICO
CENTRO EXPOSITOR
Y DE CONVENCIONES

INNOVACIÓN URBANA, PROSPERIDAD COMPARTIDA

EL EVENTO QUE REDEFINE LAS CIUDADES

Tu lugar en el futuro
te está esperando.
¡Compra tus accesos hoy!

Más de 8,500 líderes se reunirán para impulsar las decisiones que están definiendo el futuro urbano de Latinoamérica. En el marco del **Smart City Expo LATAM Congress**, la **alianza con el INAFED y el Gobierno de México para organizar el Encuentro Nacional de Alcaldes por la Innovación y la Prosperidad** se consolida en su segunda edición. Asimismo contaremos con la participación del **Departamento de Estado de EE. UU. como Institución Aliada Principal** para fortalecer la ciberseguridad, el desarrollo urbano digital y el acceso a financiamiento internacional.

CONOCIMIENTO
Acceso a las ideas que están dando forma a la política digital, movilidad y sostenibilidad.

NETWORKING
Alcaldes, gobernadores y C-levels en un mismo espacio para construir alianzas.

SOLUCIONES
Tecnologías reales que transforman la infraestructura urbana.

COLABORACIÓN ESTRATÉGICA

INSTITUCIÓN ALIADA PRINCIPAL

11ª EDICIÓN
#SCELC26

smartcityexpolatam.com

ANFITRIÓN

SEDE

ORGANIZADO POR

UN EVENTO DE

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.

HELP
RANSOMWARE

Desencriptación y recuperación total de datos tras ataques ransomware

Escanea
Evalúa y fortalece tu defensa digital

La defensa ya no es solo física. También es digital

Amenazas invisibles
que transforman nuestra vida digital

Dr. Gustavo Guzmán Hernández
LinkedIn: Gustavo Guzmán Hdez.
gguzmanh01@gmail.com
Tw @GustavoG_Kc
México
Articulista Invitado

Introducción

En las últimas décadas, la transformación digital ha revolucionado la manera en que las personas, las empresas y los gobiernos interactúan, trabajan y se comunican. Al mismo tiempo, el crecimiento acelerado de las tecnologías digitales también ha generado nuevos riesgos y amenazas que afectan directamente la seguridad, la economía y la estabilidad social. Entre estas amenazas destacan el cibercrimen y los ciberdelitos, fenómenos que han evolucionado de manera exponencial y que actualmente representan uno de los mayores desafíos globales.

Aunque ambos conceptos suelen utilizarse como sinónimos, existen diferencias importantes entre ellos. Comprender estas diferencias resulta fundamental para analizar su impacto y para desarrollar estrategias efectivas de prevención, protección y respuesta.

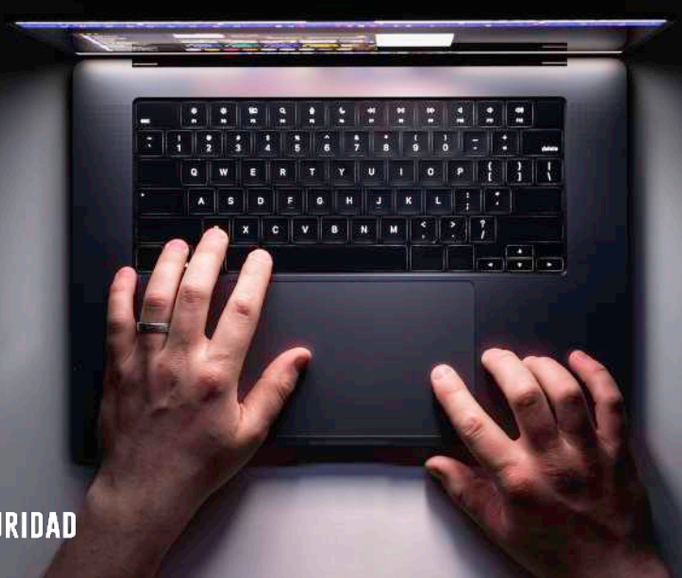
Desarrollo

El cibercrimen puede definirse como el conjunto de actividades ilícitas realizadas mediante el uso de tecnologías digitales, redes informáticas o sistemas de información, con fines económicos, políticos o estratégicos. Se trata de un fenómeno amplio que incluye operaciones complejas y organizadas, muchas veces ejecutadas por grupos criminales transnacionales o incluso actores vinculados con Estados.

Por otro lado, el ciberdelito hace referencia a una conducta específica tipificada como delito dentro del marco legal de un país. Es decir, el ciberdelito constituye la acción concreta que viola una ley penal relacionada con medios digitales. Entre los ejemplos más comunes se encuentran el fraude electrónico, el robo de identidad, el acceso ilícito a sistemas, el phishing, la distribución de malware y el ransomware.

La principal diferencia entre ambos conceptos radica en su alcance. El cibercrimen es un fenómeno general y estructural que engloba múltiples actividades criminales digitales, mientras que el ciberdelito representa una conducta específica sancionada jurídicamente. En otras palabras, el cibercrimen es el ecosistema criminal digital, y el ciberdelito es la acción particular que lo compone.

Las implicaciones del cibercrimen y los ciberdelitos son profundas y afectan a distintos sectores de la sociedad. Para la ciudadanía, estas amenazas representan riesgos como el robo de información personal, el fraude financiero, la extorsión y la pérdida de privacidad. Actualmente, millones de personas son víctimas de ataques de phishing y de robo de identidad, muchas veces sin ser conscientes de ello.



En el caso de las empresas, los impactos pueden incluir pérdidas económicas millonarias, interrupción de operaciones, daño reputacional y pérdida de confianza por parte de clientes y socios comerciales. Los ataques de ransomware han demostrado la capacidad de paralizar organizaciones enteras durante días o incluso semanas.

Para los gobiernos, el problema es aún más complejo. Los ciberataques pueden afectar infraestructura crítica, servicios públicos, sistemas financieros y plataformas gubernamentales. Además, el crecimiento de las ciberamenazas ha dado origen a nuevas formas de conflicto internacional, conocidas como ciberguerra, donde actores estatales o grupos patrocinados por gobiernos realizan operaciones ofensivas con fines geopolíticos o estratégicos.

El impacto del cibercrimen y de los ciberdelitos en nuestra vida cotidiana es enorme porque dependemos cada vez más de la tecnología. La banca digital, el comercio electrónico, las redes sociales, los servicios gubernamentales y las comunicaciones personales funcionan sobre infraestructuras digitales interconectadas. Esto significa que una vulnerabilidad tecnológica puede afectar simultáneamente a millones de personas y organizaciones.

Diversos organismos internacionales, como INTERPOL, Europol, la Agencia de Ciberseguridad y Seguridad de Infraestructura de Estados Unidos (CISA) y el Foro Económico Mundial, coinciden en que el cibercrimen representa uno de los principales riesgos globales del siglo XXI. El carácter transnacional de estas amenazas dificulta su combate, ya que los atacantes pueden operar desde cualquier parte del mundo.

Actualmente, los esfuerzos para combatir el cibercrimen involucran a gobiernos, fuerzas de seguridad, organismos internacionales, empresas privadas y centros especializados en inteligencia de amenazas. Existen unidades policiales especializadas en delitos informáticos, centros nacionales de respuesta a incidentes (CERT y CSIRT), agencias de inteligencia y organizaciones internacionales que colaboran para compartir información y coordinar acciones.

Asimismo, muchas empresas han fortalecido sus capacidades de ciberseguridad mediante el uso de tecnologías de detección, monitoreo y respuesta, así como programas de capacitación y concienciación para sus empleados.

Sin embargo, la tecnología por sí sola no es suficiente. La protección efectiva requiere una cultura de ciberseguridad. Los profesionistas y empresarios pueden reducir significativamente sus riesgos mediante acciones relativamente simples, como utilizar contraseñas robustas, implementar autenticación multifactor, mantener los sistemas actualizados, capacitar continuamente al personal y desarrollar planes de respuesta ante incidentes.

Además, resulta fundamental mantenerse informado a través de fuentes oficiales y confiables sobre amenazas emergentes y vulnerabilidades críticas. La prevención y la preparación continúan siendo las herramientas más efectivas frente a un entorno digital cada vez más complejo.

Conclusiones

El cibercrimen y los ciberdelitos son fenómenos que ya forman parte de la realidad cotidiana de personas, empresas y gobiernos. Su crecimiento responde al avance de la digitalización global y a la creciente dependencia tecnológica de las sociedades modernas.

Comprender las diferencias entre ambos conceptos permite analizar mejor sus alcances y consecuencias. Mientras el cibercrimen representa un ecosistema criminal amplio y sofisticado, los ciberdelitos constituyen las acciones específicas que afectan directamente a las víctimas.

El impacto económico, social y político de estas amenazas continuará creciendo en los próximos años. Por ello, la ciberseguridad debe entenderse no solo como un tema técnico, sino como un componente estratégico para la protección de la sociedad, la economía y la estabilidad nacional.

La colaboración internacional, el fortalecimiento institucional y la generación de una cultura de prevención serán elementos clave para enfrentar con éxito los desafíos del entorno digital.

¡Estrategia e inteligencia y riesgos, la tríada de no anticipar el ataque a Irán!

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

El contexto mundial se llama NAVI, como describí en mi último artículo en esta revista. El mundo de NAVI requiere mucha agilidad en la toma de decisiones, hecho que la nueva ISO/TS 31050, que trata con riesgos emergentes, cuenta con un marco sólido con el ciclo de inteligencia estratégica integrado con la gestión de riesgos. Por lo tanto, requiere que las empresas y los gobiernos dispongan de inteligencia, información interpretada, para la toma de decisiones.

Con la gran volatilidad de los asuntos geopolíticos, el cierre del estrecho de Ormuz por parte de Irán es, en mi opinión, consecuencia de una gran mala interpretación de Estados Unidos e Israel, cuando decidieron bombardear Irán.

El bombardeo nos enseña y, al mismo tiempo, pone de manifiesto un fallo crítico en la estrategia contemporánea: no la ausencia de inteligencia, sino la incapacidad de integrarla en escenarios adaptativos. Si profundizamos en la perspectiva de ISO/TS 31050, Riesgo Emergente, observaremos una ruptura en el ciclo de inteligencia, especialmente en los siguientes aspectos: modelado del oponente, construcción de escenarios y definición del Efecto Final Deseado (EFD).

El resultado fue la generación de efectos estratégicos contrarios a lo esperado, fortaleciendo la resiliencia de Irán y poniendo en riesgo la estabilidad mundial. En mi opinión, fue miope esperar que Irán simplemente retrocediera ante los atentados y asesinatos de sus líderes. En los conflictos contemporáneos, especialmente los asimétricos, la superioridad tecnológica e informacional no garantiza una ventaja estratégica. Se aplicó la fuerza, pero no se impuso la voluntad. Esto sugiere una paradoja central: "*cuanto mayor es la complejidad del sistema adversario, menos eficaces son los enfoques lineales basados únicamente en la superioridad militar.*"

En mi estudio del marco ISO/TS 31050, el defecto más influyente que produjo los efectos dominó fue la ausencia del estudio EFD (Efecto Final Deseado), la intención del actor, con la siguiente estructura:

1. Definir el comportamiento deseado de Irán
2. Elaboración de modelos de escenarios de reacción y consecuencias para EE.UU., Israel y el mundo.
3. Nível de resiliencia iraní.;
4. Acciones estratégicas necesarias para abordar los contextos y escenarios previstos.

Los estadounidenses se centraron únicamente en herramientas tácticas, como misiles de destrucción. Y como sabemos, las herramientas no son estrategias. La inteligencia estadounidense debería haber integrado la información con escenarios de riesgo y decisiones estratégicas. Subestimaron a los iraníes, no tuvieron en cuenta que la religión está impregnada en el pueblo iraní. Irán no es solo un estado burocrático, se presentó con un proyecto moral durante la Revolución de 1979. Integró la soberanía con la historia sagrada. Las cuestiones emocionales y sagradas han estado arraigadas en el pueblo iraní desde el 10 de octubre del año 680 d.C., cuando el nieto del profeta Mahoma, Hussein ibn Ali, fue masacrado junto con familiares y seguidores por las fuerzas del califa omeya Yazid I, tras negarse a someterse a su autoridad. Este evento se considera un momento decisivo en la historia islámica, consolidando la brecha entre musulmanes suníes y chiíes.

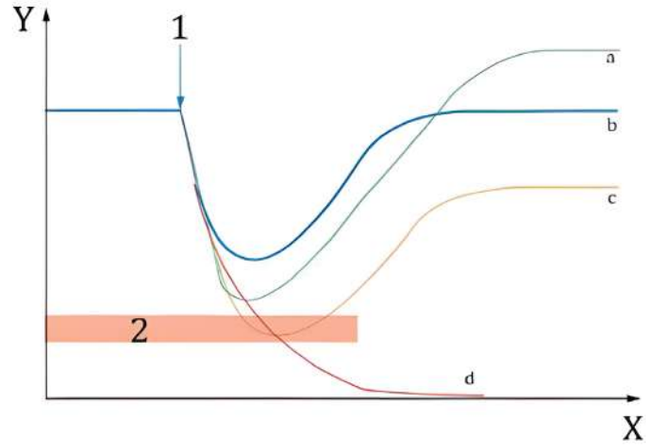
La opresión no significa derrota. El sufrimiento es estar del lado de la verdad y la muerte puede convertirse en una forma de testimonio. Por tanto, el martirio es uno de los grandes valores del islam. Lo que es devastación desde fuera en Irán se narra como testigo, resistencia y fidelidad. La dimensión teológica debería haber tenido un estudio profundo para saber a qué se enfrentaría, porque la dimensión psicológica de la guerra en Irán hace que el ataque externo sea más cohesivo internamente, la pérdida es un sacrificio legitimador además de ser una narrativa de injusticia.

Otro gran fracaso fue no haber evaluado el tipo de defensa que Irán podría haber adoptado, incluso a la vista de los ataques estadounidenses e israelíes en 2025.

Defensa del Modelo del Mosaico, con características:

1. comando descentralizado;
2. autonomía operativa;
3. continuidad incluso con pérdidas;
4. uso de proxies.

El gráfico siguiente del ISO/TS 31050 lo demuestra claramente:



Eje X: Fase temporal del escenario
Eje Y: Funcionalidad
1. Inicio
2. Prueba de Estrés de Límite
A: mejor funcionalidad que antes
B: Funcionalidad igual
C: Funcionalidad parcialmente recuperada
D: Funcionalidad perdida

Gráfico de ISO/TS 31050 muestra la respuesta a, como la mejor, porque respondió en caos, con crecimiento.

El principal defecto estratégico era la falta de aplicación estratégica de la inteligencia, la ausencia de escenarios sólidos, la subestimación de la adaptación adversarial, la falta de consideración del aprendizaje histórico y el fracaso en la lectura sociopolítica.
O Gráfico de ISO/TS 31050 muestra la respuesta a, como la mejor, porque respondió en caos, con crecimiento.

Podemos concluir:
1. La inteligencia sin escenarios no genera estrategia;
2. El adversario debe modelarse como un sistema adaptativo;
3. El Efecto Final Deseado debe guiar todas las acciones;
4. La guerra moderna es sociopolítica, no solo militar;
5. La resiliencia prevalece sobre la superioridad operativa.

La guerra contemporánea no se gana por la fuerza, sino por la capacidad de practicar ARARA: **Anticipar, Resistir, Absorber, Responder y Adaptarse**. Estados Unidos e Israel tenían superioridad táctica. Irán tenía superioridad ADAPTATIVA, RESILIENCIA. En este siglo XXI, "quien mejor se adapta, ***¡¡gana!!***".

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 periodo 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

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.

Afíliate y sé parte de nuestra comunidad.

#TÚERESASIS

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217

ASIS MÉXICO 217
$5,650 MXN

ASIS INTERNACIONAL
$130 USD

BENEFICIOS *Membresía*

- Reuniones mensuales gratuitas con conferencistas de primer nivel.
- Webinars sin costo con instructores certificados y cursos que otorgan CPE's.
- Presencia del capítulo en los mejores eventos de seguridad en México.
- Convenios con descuentos exclusivos en productos y servicios.
- Bolsa de trabajo especializada en seguridad.
- Comunidades temáticas para intercambiar conocimiento.
- Newsletter semanal con información relevante.
- Chat privado exclusivo para socios activos.
- Acceso a guías y estándares de ASIS Internacional.
- Conexión con más de 34,000 profesionales de seguridad en el mundo.

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

Linktree

El ingenio en tiempos de guerra

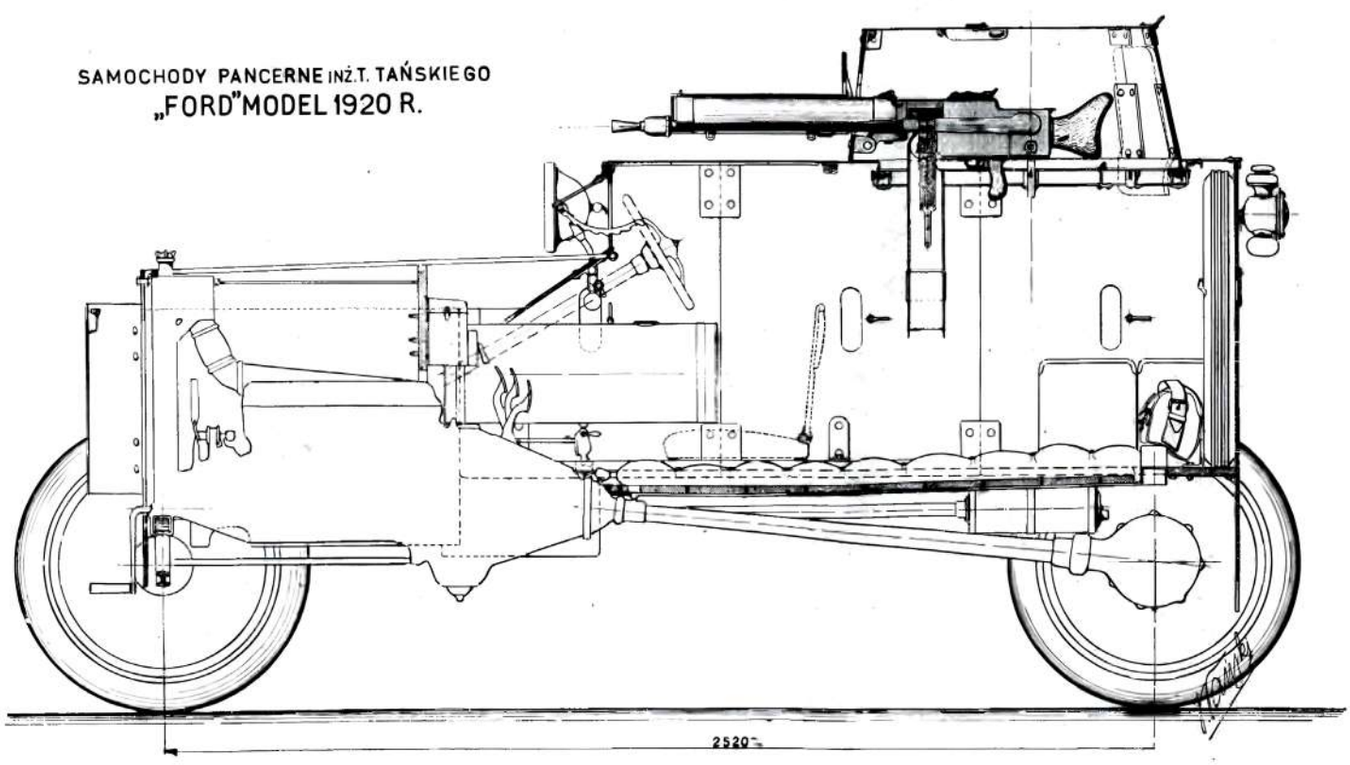
el blindado polaco FT-B con plataforma del Ford modelo T

Ricardo Guzmán
Director de operaciones en vinculo estrategas comerciales. Amplia experiencia en el ámbito del blindaje automotriz y colaborador comecial a nivel gerencial y directivo en las más importantes blindadoras de México
rguzman@vinculoec.com.mx
México

Articulista Invitado

En 1920 Polonia estaba en guerra con la Unión Soviética, los rusos habían llegado a través de Ucrania y estaban a las puestas de Varsovia. Polonia tenía la cuarta división blindada más grande del mundo en ese momento. Sin embargo, los tanques Renault FT-17 eran vehículos lentos e inadecuados para el tipo de maniobras rápidas que los polacos necesitaban para contrarrestar a los soviéticos. Esto hacia la urgente necesidad de hacerse de una flotilla de acorazados y en parte lo lograban capturando algunos vehículos de combate de otros países, pero presentando los mismos problemas de movilidad con las orugas. El pueblo polaco había utilizado el ingenio para improvisar vehículos blindados en el pasado reciente, sobre todo con el camión blindado conocido como "Tank Pilsudskiego" de 1918. Diseñado en 1920 por Tadeusz Tanski, el Ford FT-B se basaba en el chasis clásico del Ford Modelo T, ligeramente modificado. Motor Ford de 22,5 CV, 2900 cc, a gasolina, 4 cilindros en línea, 4 tiempos, refrigerado por agua, arranque con manivela.

Contaba con un bastidor rectangular de acero y suspensión con ballestas transversales semielípticas. El eje trasero se reforzó adicionalmente con largueros. La posición del depósito de combustible se cambió de transversal debajo del asiento del conductor a longitudinal, junto al conductor. Las ruedas eran de madera y las dimensiones de los neumáticos eran de 30 x 3.5 pulgadas. Tanski utilizó planchas hechas con placas de acero de trincheras alemanas, material recuperado de los campos de batalla polacos tras la primera guerra mundial y rellenó los neumáticos con pulpa de madera para protegerlos hasta cierto punto contra las balas de fusil y ametralladora. El resultado fue un pequeño vehículo blindado, con una tripulación de dos personas, armado con una ametralladora en una torreta giratoria.



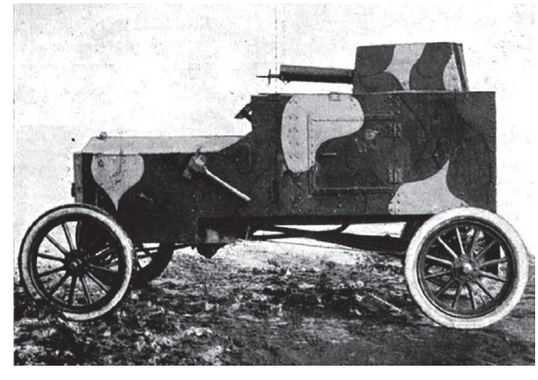
El blindaje tenía un espesor de 8 mm. En algunas publicaciones se indica que las placas superiores tenían un blindaje de 3 mm. sin embargo, según el informe de la comisión de abril de 1921, las placas superiores no estaban blindadas, sino que eran de chapa de acero común de 2 mm. La parte inferior no estaba blindada, sino hecha de tablones de madera. Se podía utilizar una cubierta blindada sobre el radiador de agua de la ametralladora con un pequeño escudo.

También había una escotilla de dos partes sobre el conductor que facilitaba la conducción en condiciones no de combate. El radiador estaba protegido con puertas blindadas. Una rueda de repuesto se transportaba en el interior a lo largo de una plancha trasera del casco. Los coches podían diferir en los detalles del blindaje, inicialmente no tenían faros, posteriormente se les instaló un único faro delante de la plancha frontal del conductor. La torreta tenía forma pentagonal, estrechándose hacia adelante, con una pequeña escotilla en una plancha superior. El blindaje protegía contra balas perforantes de fusil a 300 m y contra balas de fusil convencionales a cualquier distancia. El peso de la armadura era de aproximadamente 590 kg. El cuerpo blindado podía desmontarse de una sola pieza y estaba sostenido por una estructura de ocho puntos.

- El diseño fue aprobado de inmediato por las autoridades el 12 de junio de 1920 y el prototipo se completó en dos semanas a finales de junio. Las pruebas resultaron satisfactorias y se encargó una serie. Los Ford blindados se construyeron bajo la supervisión de Tański en la fábrica de herramientas Gerlach & Pulst en Varsovia, que ya había fabricado vagones para trenes blindados. El Ford FT-B fue el primer vehículo blindado polaco fabricado en serie produciéndose entre 16 y 17 unidades según algunas fuentes.

El coche tenía puntos débiles como las tablas del piso de madera sin protección y los mismos radios de madera en las ruedas. Sin embargo, en parte debido a que era un vehículo considerado rápido en la época, el enemigo nunca pudo aprovechar esas debilidades. Cada coche estaba tripulado por dos hombres armados con una sola metralleta alemana Maxim 05/15 de 7.92 mm. con 1250 balas, así como 25 granadas de mano. Debido a la naturaleza simple del motor Ford, los vehículos rara vez se averiaban y cuando lo hicieron, los equipos hicieron reparaciones en el campo, incluso a veces bajo el fuego mismo incluso si se requería una reparación más profunda, toda la parte blindada del coche podía levantarse del bastidor en una sola pieza. Un aspecto curioso es que el FT-B podía funcionar con combustible y aceite de mala calidad, una ventaja indispensable en condiciones de escasez de suministros en tiempos de guerra.

El Ford FT-B se desempeñó bien durante la guerra polaco-bolchevique de 1920, sobresaliendo en el combate de alta movilidad que caracterizó ese conflicto, tan diferente de la guerra de trincheras estática de la Primera Guerra Mundial. El Ford se distinguió particularmente en "La incursión en Kovel" y salvó a muchos soldados polacos durante la retirada de Ucrania hacia Varsovia. Luego apoyó el contraataque hacia el este, después de la exitosa defensa de Varsovia, conocida como el "Milagro del Vístula", donde Sikorski derrotó a los rusos haciéndolos huir en el proceso y enviando ellos retrocediendo por la frontera ucraniana y más allá. Bastantes Ford FT-B sobrevivieron hasta la década de 1920, en 1930 solo tres todavía estaban en condiciones de uso y fueron retirados en 1931, aunque algunos indicios sugieren que al menos uno sobrevivió hasta 1939.



Calidad vs cantidad, objetivo del sector de geolocalización: AMESIS

- 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.*

SERCOPP

SERVICES & CONSULT

Servicios de consultoría y personal profesional

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

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

Dg. 81i #74C-19, Bogotá, D.C. Colombia
+57 3108052421
gerenciasercopp@gmail.com

www.sercopp.com

La transformación digital que está blindando la seguridad en Latinoamérica

Bogotá, Colombia.- En un mundo donde la inmediatez y la precisión de la información definen el éxito de una operación, el sector de la seguridad privada y el transporte de carga se enfrenta a un desafío histórico: abandonar el papel y los procesos manuales para abrazar la era digital. Bajo esta premisa, Sercop, una firma de consultoría experta en gestión de riesgos de seguridad y cadena de suministro, ha desarrollado SARI, la plataforma que está redefiniendo cómo se administra el riesgo en la región.

En entrevista con Héctor Fabio Blandón, Gerente General de Sercop, se revelaron las claves detrás de este software que ya no es solo una promesa, sino una realidad tangible en Colombia y México.

De la "minuta" de papel a la gestión en la nube

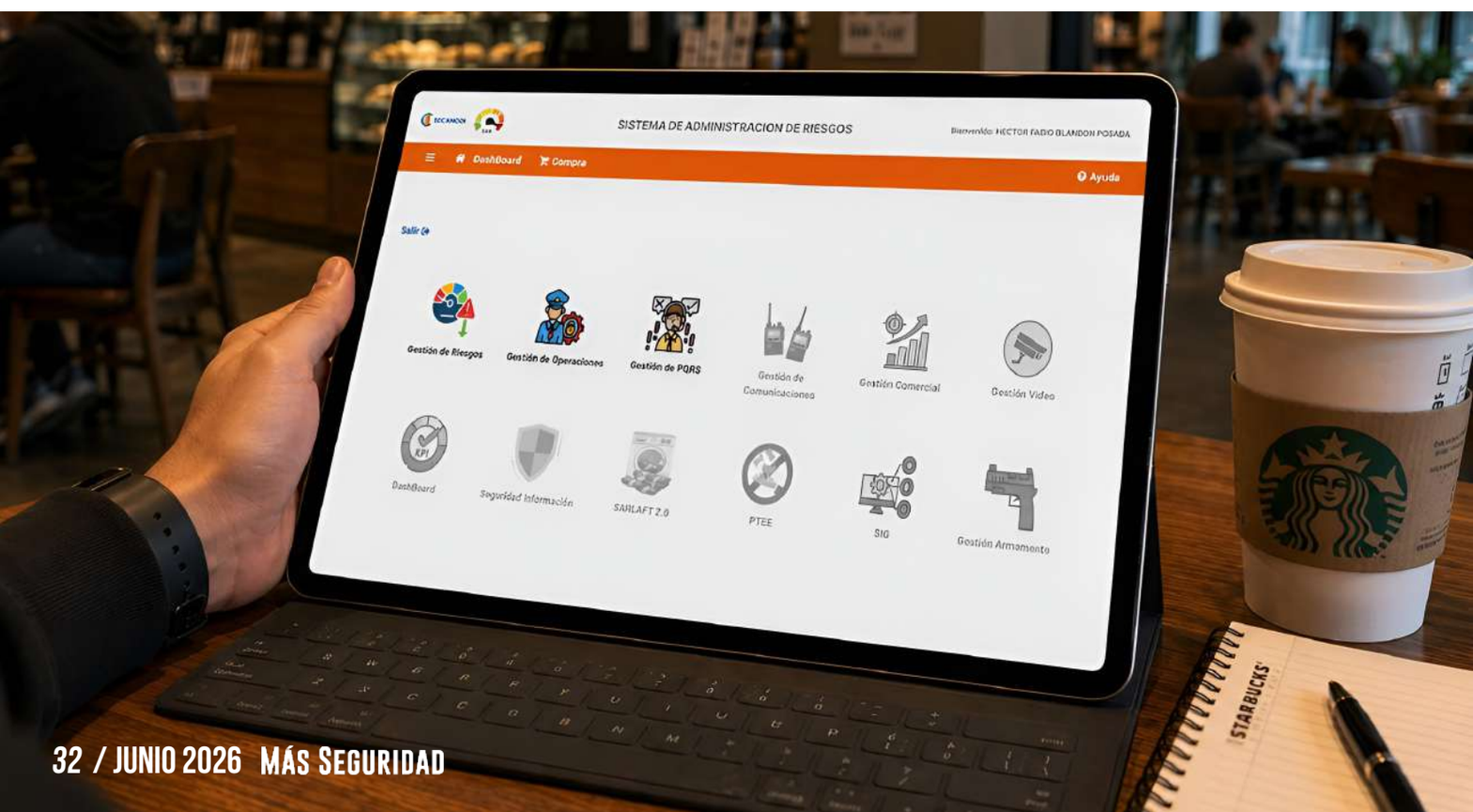
El objetivo de SARI es claro: sacar a las empresas de vigilancia y departamentos de seguridad del uso rudimentario de procesadores de texto y hojas de cálculo. Héctor Fabio explica que la oportunidad nació al observar que muchas operaciones seguían dependiendo de libros de control y minutas físicas.

"Lo que buscamos es que el reporte de operaciones, riesgos y vulnerabilidades se pueda realizar desde el mismo teléfono celular de los supervisores o guardias, teniendo la información a un solo clic y respaldada totalmente en la nube".

Las bondades que marcan la diferencia

SARI no es solo una herramienta de registro; es un aliado financiero y operativo. Entre sus beneficios más destacados se encuentran:

- **Accesibilidad total:** Es una plataforma web responsiva que funciona en cualquier equipo o teléfono móvil con datos, sin obligar a las empresas a adquirir hardware costoso de marcas específicas.
- **Modelo de costos eficiente:** A diferencia de otros softwares, SARI no cobra por número de usuarios. Ofrece un costo mensual fijo, permitiendo a los departamentos financieros presupuestar sin sorpresas, sin importar cuántos informes o empleados se gestionen.
- **Identidad de marca blanca:** Uno de los puntos más innovadores es que SARI funciona bajo un esquema de "marca blanca". La marca de Sercop desaparece para que la



Alianza internacional:

SERCOPP
SERVICES & CONSULTING

MÁS SEGURIDAD
Magazine

CON SEGURIDAD
Magazine Latam

Ya está México!

SARI

- Instalaciones
- Vehículos
- Rutas
- Rondas
- Minuta
- Novedades

LA HERRAMIENTA MÁS COMPLETA PARA LA SEGURIDAD PRIVADA

1. Licencia de uso por el termino de un año, con el IVC - imagen visual corporativa de la empresa, colores, logo. Imagen o video de fondo en el front principal o de menú.

2. Usuarios individuales ilimitados mes (3 tipos de perfil: Operador, Analista, Director).

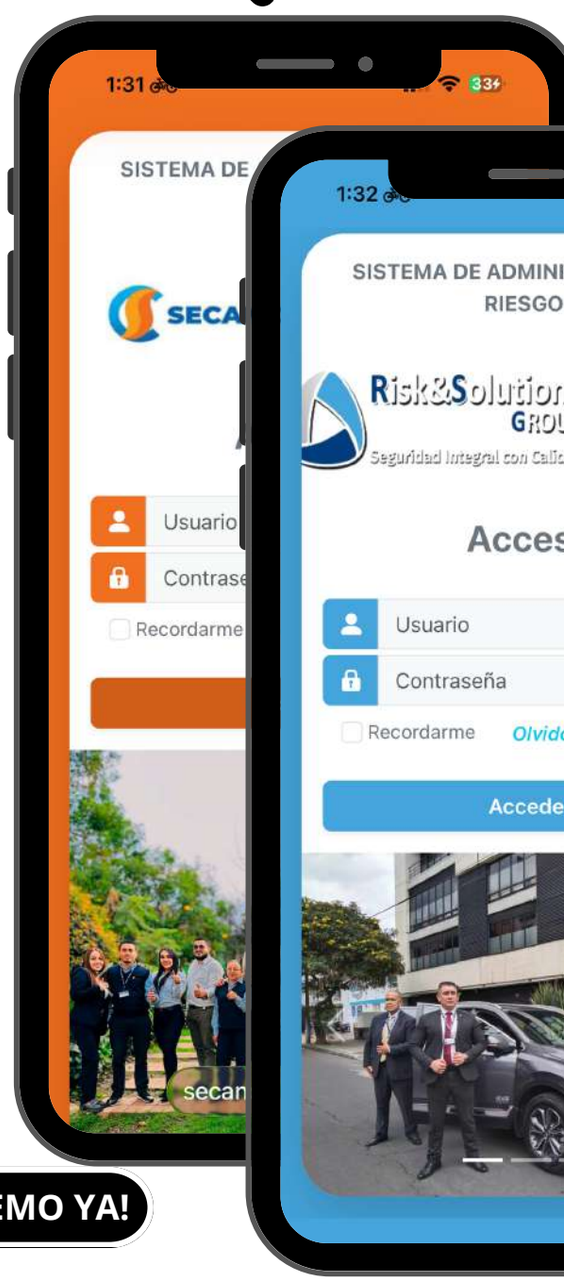
3. Capacitación y entrenamiento al personal operativo actual y nuevo del nivel Supervisores, Analistas, Coordinadores, Jefes y Directores.

4. Servidor o alojamiento dedicado para los Análisis de Riesgos e informes de la empresa, con alta redundancia y disponibilidad.

5. Certificado SSL (Secure Sockets Layer): certificado digital que autentica la identidad de sari.com.

6. Dominio con nombre de la empresa: https://empresa.sari.com.co/index.html

7. Soporte técnico de Lunes a Sábado de 08:00 a 18:00 horas y/o 24 * 7 nivel de critico de la plataforma.



SOLICITA TU DEMO YA!

08:00 A. M. - 06:00 P. M. (57) 3108052421 DG 81I #74C-19 OF. 202 - BOGOTÁ, COLOMBIA

empresa de seguridad pueda presentar la plataforma como propia, con sus colores y logotipos corporativos, ante sus clientes finales.

- **Ahorro por prevención:** Al identificar condiciones inseguras y amenazas externas en tiempo real, las empresas pueden neutralizar riesgos antes de que se conviertan en siniestros. Esto se traduce en un blindaje legal y financiero: "Si ocurre un evento, el cliente de SARI puede demostrar que informó oportunamente sobre el riesgo y recomendó planes de acción, protegiéndose de reclamaciones por pérdidas".

Casos de éxito: De la "Colombia profunda" a las grandes multinacionales

En Colombia, SARI ya ha demostrado su potencia en operaciones de gran envergadura. Héctor Fabio destaca tres casos emblemáticos:

- **1.** Secancol Limitada: Una compañía con más de 1,200 hombres que gestiona la seguridad de gigantes como GM Colmotores, el Grupo Inditex (Zara, Bershka), Grupo Éxito y Decathlon.
- **2.** Seguridad del Sur: Con otros 1,200 efectivos, esta empresa opera en la "Colombia profunda", en zonas limítrofes con Ecuador y la Amazonía, donde la gestión del riesgo es crítica y compleja.
- **3.** Risks and Solutions Group: Especializada en la protección de componentes diplomáticos y embajadas.

Expansión en México y proyección hacia Norteamérica

La llegada de SARI al mercado mexicano se consolidó en el segundo semestre de 2025. Actualmente, la plataforma ya es utilizada por cuatro empresas de seguridad privada y dos de transporte. Estas organizaciones utilizan el software para mapear riesgos en rutas de escoltaje, protección de edificios y traslado de mercancías, un factor vital para las firmas que exportan hacia Norteamérica.

Para este 2026, la proyección de Sercop en territorio mexicano es alta: un crecimiento del 200% en su cartera de clientes. Participar en Expo Seguridad, la empresa busca consolidarse como la herramienta preferida para el sector transporte y blindajes en el país.

Un mensaje para el empresario

Finalmente, Héctor Fabio enfatiza que SARI ha sido diseñado para democratizar la tecnología: "No está hecho solo para empresas grandes; está diseñado para que incluso las pequeñas puedan acceder a soluciones de alta calidad sin sacrificar su estabilidad financiera".

Con una metodología unificada y un enfoque en la calidad (ISO 9001, 28000, 27001), SARI se posiciona como el puente necesario hacia una seguridad privada más profesional, transparente y, sobre todo, rentable.

Héctor Fabio Blandón
Gerente General de Sercop

¡Únetenos!

CON SEGURIDAD
Magazine Latam

Síguenos en

Telegram e Instagram

@conseguridadmagazine

Safety & Security: Binomio con tecnología

Cómo la tecnología, la comunicación y la gestión de riesgos están transformando el papel de Safety & Security en las organizaciones

Parte 2 de 2

Samuel Hernández Martínez
Gerente de Seguridad Intramuros GALEAM
México

Articulista Invitado

En la primera parte de este artículo, mencionaba que en un entorno donde la información viaja en segundos y los riesgos evolucionan constantemente, la seguridad dejó de ser únicamente una función operativa. Hoy representa un componente estratégico para proteger a las personas, garantizar la continuidad del negocio y fortalecer la reputación de las organizaciones.

De la seguridad reactiva a la seguridad estratégica

También mencioné que, durante muchos años, en muchas organizaciones la seguridad se gestionó bajo una lógica fragmentada. Safety y Security coexistían dentro de la misma empresa, pero rara vez operaban como un sistema integrado. En muchos casos parecía más una competencia entre áreas que una estrategia común para proteger a las personas, las operaciones y la reputación de la organización.

Dicho lo anterior, surge la necesidad de decisiones basadas en información. Las operaciones modernas requieren sistemas que permitan detectar, medir, gestionar riesgos y controlar con mayor precisión. La tecnología ha permitido desarrollar herramientas que facilitan la comunicación, el análisis de incidentes y la toma de decisiones oportunas.

Lo que la pandemia nos enseñó… y lo que olvidamos

Bajo esta misma línea, no podemos hablar de evolución sin mencionar que la pandemia dejó consecuencias profundamente lamentables, pero también generó aprendizaje importante en materia de prevención que con el paso del tiempo ha comenzado a diluirse.

Uno de los temas menos discutidos ha sido el impacto en la salud mental y sus efectos en la vida laboral y personal. Factores como el estrés, fatiga o presión emocional pueden convertirse en riesgos organizacionales ante la falta de modelos de integración considerando Familia-Sociedad-Trabajo/Escuela.

Durante ese periodo también se fortalecieron hábitos positivos relacionados con la higiene, la prevención y el autocuidado. Sin embargo, muchos de estos comportamientos se han debilitado conforme la emergencia sanitaria quedó atrás. Otro aprendizaje relevante fue el valor de la *comunicación preventiva:* cuando la información sobre riesgos se comunica de forma clara y oportuna, las personas pueden tomar decisiones más responsables para protegerse a sí mismas y a los demás.

Aspectos para considerar en toda la organización

- **La fragmentación:** Considerar que son sistemas independientes puede ocasionar que se solucione el mismo problema con doble presupuesto, sin resultados favorables y con perspectivas diferentes.
- **La tecnología:** Definitivamente ayudará, sin embargo, tecnología sin cultura solo es tener información sin gestión.
- **Accountability:** Para establecer una cultura se deben tener las 3C: Estar Conscientes, estar Convencidos y estar Comprometidos.

La seguridad corporativa está viviendo una transformación profunda. Pasamos de modelos reactivos y fragmentados a enfoques cada vez más integrados donde tecnología, cultura preventiva y liderazgo convergen para fortalecer la resiliencia organizacional. En un entorno cada vez más complejo, la verdadera ventaja para las organizaciones no es evitar todos los incidentes, sino desarrollar la capacidad de anticiparlos, gestionarlos y aprender de ellos.

GRUPO ALEM

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

¡Garantizamos su tranquilidad!

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

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

Custodias: Para todo tipo de transporte de mercancías en tránsito

Rastreo satelital: Vehículos particulares, carga o flotillas

Videovigilancia: Fija, móvil y remota

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

www.grupoalem.mx

edgar.seguridad.integral@gmail.com

+52 564705 2246

Cuando el riesgo se digitaliza:

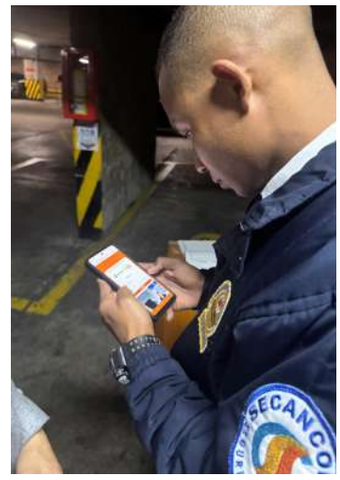
Seguridad del Sur lleva su operación a tiempo real con SARI

Pasto, Colombia. - En el sur del país, región donde la vigilancia privada protege infraestructura pública, entidades financieras, empresas y operaciones industriales, la firma Seguridad del Sur transforma uno de los procesos más sensibles de su operación: La elaboración de estudios de seguridad que cada cliente debe recibir al iniciar un servicio.

La compañía, con sede principal en Pasto, Colombia, opera desde hace más de 35 años en el suroccidente colombiano. Actualmente cuenta con más de 900 guardas al servicio, más de 110 clientes en seguridad física, además de servicios de monitoreo de alarmas, escoltas, vigilancia híbrida y soluciones tecnológicas para distintos sectores productivos.

Y fue precisamente el crecimiento de esa operación lo que obligó a revisar procesos internos de la firma: "Cuando recibo la dirección de operaciones en 2024, iniciamos la tarea de hacer los estudios de seguridad de todos nuestros clientes asociados a la empresa, bajo la norma ISO 31000", explica Milton Albeiro Montes Bedoya, coronel retirado del Ejército Colombiano, consultor en seguridad privada y director de operaciones de la compañía.

Un solo cliente podía consumir seis semanas y la metodología cumplía con todos los requisitos como ubicación del cliente, análisis delictivo del sector, visitas de campo, revisión de sistemas de seguridad y evaluación de riesgos.



Un cliente podía tener una sola razón social… pero operar en 25 o 30 ubicaciones distintas: "Ese único cliente me generaba entre 27 y 30 estudios de seguridad", relata Montes. El procedimiento manual implicaba movilizar supervisores a campo, levantar evidencias fotográficas, documentar hallazgos y regresar a oficina para redactar cada reporte bajo el modelo institucional.

"Ponía a trabajar a todos mis supervisores operativos y al mismo director de operaciones. Nos gastábamos tres semanas en trabajo de campo y otras tres semanas en oficina. Ese solo cliente me consumía seis semanas", relata.

La búsqueda de una solución

Después de cursar un diplomado en gerencia de seguridad física avanzada, el consultor en seguridad Milton Montes comenzó a evaluar herramientas tecnológicas disponibles en el mercado colombiano: "Vimos otras opciones, pero una de las primeras bondades que encontramos con SARI fue el costo de uso de la plataforma".

El segundo factor fue de tipo operativo: "Lo puedo ver de forma inmediata en mi plataforma. El supervisor hace el trabajo desde el celular, toma fotos, monta evidencias y yo puedo empezar a revisar casi al segundo".

La plataforma, además, estaba alineada con la metodología que la empresa ya utilizaba: "Está basada en normatividad colombiana, bajo ISO 31000, y cumple completamente con lo que nosotros necesitábamos".

La prueba de fuego llegó pronto con otro cliente de características similares: de 30 puestos de operación. La diferencia fue que ese mismo trabajo lo hicimos solamente en dos semanas".

Es cuando el flujo operativo cambió radicalmente, ya que los supervisores realizan levantamiento de información en campo desde dispositivos móviles, cargan fotografías, observaciones y evidencias en tiempo real. Después interviene un auditor que revisa calidad documental y finalmente el director de operaciones valida el producto final antes de entregarlo al cliente.

"Yo estoy hablando de casi más del 60% de ahorro en tiempo y en costos de hora-hombre elaborada", señala.

SARI actualmente cuenta con once operadores, cinco ciudades y más de 240 estudios dentro de la organización. Supervisores, auditores, coordinadores regionales y dirección operativa. La plataforma ya respalda operaciones distribuidas entre las ciudades de Pasto, Ipiales, Tumaco, Mocoa y Bogotá.

Solo en Pasto, la compañía tiene proyectados cerca de 180 estudios de seguridad; en Tumaco y Ipiales, alrededor de 20 en cada ciudad; en Mocoa, otros 13, además de nuevas operaciones en expansión. "Con esos números, imagínate todo el tiempo que yo perdía haciéndolo manual. Las bondades que me ha traído SARI han sido espectaculares".

Y la mejora ya empezó a reflejarse en nuevos contratos. Entre los clientes recientes de Seguridad del Sur figuran la Gobernación de Nariño y la Alcaldía de Pasto, instituciones que requieren estudios técnicos en tiempos muy cortos una vez se activan los servicios de vigilancia.

"Lo estamos poniendo como un plus dentro de la organización: tener una plataforma bien constituida bajo normatividad para entregar estudios de seguridad juiciosos y completos".

"SARI no te vende el software y te dice úselo. Vinieron, capacitaron a mi personal en teoría, en campo, hicieron evaluación y finalmente capacitaron al director de operaciones…Hoy, como se están manejando las operaciones de seguridad privada, es importante tener software como SARI. Los beneficios se notan desde el primer momento en que uno empieza a utilizar la plataforma", finaliza Milton Albeiro Montes.

Expertos en **soluciones menos lesivas**

APRINSA

100 Aprinsa

200 Aprinsa

Modelos: 100 y 200

Equipo de control electronico inteligente

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

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

@seguridad1 33 3700 7721

direccion@aprinsa.net

LATAM

PDCA en el Sistema de Gestión de Riesgos CPTED:

Trazabilidad con **ISO 22341** y **22341-2** para el Diseño de Proyectos de Seguridad

Parte 2 de 2

Dra. Mercedes Escudero Carmona

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

México

Articulista Invitada

Quintana Roo, México.- En el ámbito del diseño urbano y la gestión de riesgos socio-espaciales, la prevención del crimen mediante el diseño ambiental —conocida por su acrónimo anglosajón CPTED (Crime Prevention Through Environmental Design)— ha consolidado su posición como referente metodológico internacional. Su estandarización a través de las normas ISO 22341:2021 e ISO 22341-2:2025 dota a los profesionales de un lenguaje técnico común y de requisitos verificables para su implementación en contextos de alta diversidad urbana.

Expliqué que la mera adopción de principios CPTED no garantiza la eficacia sostenida de las intervenciones de seguridad. Para que un sistema de gestión de riesgos socio-urbano sea verdaderamente resiliente, debe integrar un mecanismo estructurado de mejora continua. El ciclo PDCA (Planificar–Hacer–Verificar–Actuar), conceptualizado por Walter Shewhart y difundido globalmente por W. Edwards Deming, constituye el andamiaje metodológico idóneo para esta finalidad.

5. Aplicación en el Diseño de Proyectos de Seguridad

5.1 FASE PLAN — DIAGNÓSTICO Y PLANIFICACIÓN ESTRATÉGICA:

Todo proyecto de seguridad basado en CPTED debe iniciarse con un diagnóstico riguroso del entorno. Este proceso, descrito en las Cláusulas 5 y 6 de ISO 22341:2021, comprende la caracterización sociodemográfica del área de intervención, el levantamiento y cartografía de incidentes delictivos históricos, la identificación de puntos calientes (hot spots) mediante análisis espacial, y la evaluación cualitativa de la percepción de seguridad de los usuarios a través de metodologías participativas.

En esta fase, el equipo de proyecto define los objetivos de seguridad CPTED en términos medibles y verificables, y elabora el plan de intervención, que debe especificar las estrategias a implementar, los recursos necesarios, los responsables, los plazos y los indicadores de éxito. El plan constituye el documento de referencia para toda la trazabilidad normativa posterior, y debe ser aprobado formalmente por la dirección conforme a Cláusula 5.3 ISO 22341.

5.2 FASE DO — IMPLEMENTACIÓN CPTED INTEGRADA AL DISEÑO:

La fase de implementación traduce los principios CPTED en decisiones concretas de diseño arquitectónico y urbano. Siguiendo las directrices de ISO 22341-2:2025 , la tipología del espacio determina la combinación y jerarquía de estrategias a aplicar. Para un espacio público de alta afluencia, la vigilancia natural y el soporte a actividades son prioritarios; para una infraestructura crítica, el control de accesos y la robustez resultan determinantes.

Es fundamental que la implementación no se limite a intervenciones físicas, sino que incorpore componentes de gestión operacional: protocolos de mantenimiento preventivo y correctivo, sistemas de reporte comunitario, coordinación con cuerpos de seguridad pública y programas de apropiación y animación del espacio. La Cláusula 8 de ISO 22341 aborda específicamente la operación y el control de estas medidas, incluyendo requisitos de documentación y competencia del personal.

5.3 FASE CHECK — AUDITORÍA Y EVALUACIÓN DEL DESEMPEÑO:

La verificación es la fase que distingue a un sistema de gestión maduro de una intervención puntual. La Cláusula 9 de ISO 22341:2021 establece los requisitos de seguimiento, medición, análisis y evaluación del desempeño del sistema CPTED. Esto se materializa a través de auditorías CPTED periódicas —ejecutadas por equipos internos o auditores externos independientes— que evalúan el estado de implementación de cada estrategia y la conformidad con los requisitos normativos.

5.4 FASE ACT — MEJORA CONTINUA Y GESTIÓN ADAPTATIVA:

El cierre del ciclo —y el inicio del siguiente— se produce cuando los hallazgos de la verificación alimentan la planificación revisada. La Cláusula 10 de ISO 22341:2021 establece que la organización debe responder a las no conformidades mediante acciones correctivas proporcionales, verificar su eficacia en plazos definidos y documentar los resultados. Más allá de la corrección reactiva, la mejora continua implica identificar oportunidades proactivas de fortalecimiento del sistema.

6. Recomendaciones para el Diseño de Proyectos:

- **Documentación trazable:** registrar cada decisión de diseño con su correspondiente cláusula normativa y evidencia de evaluación. La trazabilidad es condición de auditabilidad y de eventual certificación del sistema.

- **KPIs desde la planificación:** definir indicadores de desempeño medibles desde la fase Plan, no como añadido posterior. Cada objetivo de seguridad debe tener su métrica y línea de base asociada.

- **Auditorías mixtas:** combinar auditorías técnicas CPTED con encuestas de percepción a usuarios. La seguridad objetiva y la subjetiva son dimensiones complementarias e igualmente relevantes.

- **Gestión adaptativa:** el plan CPTED debe revisarse ante cambios significativos del entorno: nuevos usos del suelo, variaciones demográficas o evolución de patrones delictivos locales.

- **Enfoque multidisciplinario:** integrar urbanistas, arquitectos, criminólogos, trabajadores sociales y representantes comunitarios. La perspectiva integral es requisito explícito de la norma ISO 22341.

- **Seguridad en capas:** aplicar defensa en profundidad: estrategias CPTED primarias reforzadas por medidas electrónicas y organizacionales, conforme recomienda ISO 22341-2 para entornos complejos.

7. Conclusiones:

La integración del ciclo PDCA en el sistema de gestión de riesgos CPTED, sustentada en la trazabilidad formal con ISO 22341:2021 e ISO 22341-2:2025, representa una evolución sustantiva en la forma de concebir y gestionar la seguridad en el entorno socio-urbano. Esta integración supera la visión estática de la seguridad como conjunto de medidas puntuales y la eleva a un proceso de gestión continua, auditable, orientado a resultados y alineado con los más altos estándares normativos internacionales.

La norma ISO 22341 CPTED no es un fin en sí misma, sino el marco que hace posible que cada ciclo PDCA genere entornos progresivamente más seguros, más resilientes y más orientados a la calidad de vida de sus usuarios.

"La excelencia en seguridad socio-urbana no se declara; se demuestra a través de ciclos sucesivos de planificación, acción, verificación y mejora. El entorno construido es el mejor indicador de la calidad del sistema de gestión que lo gobierna."
Mercedes Escudero.

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

Articulista 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:

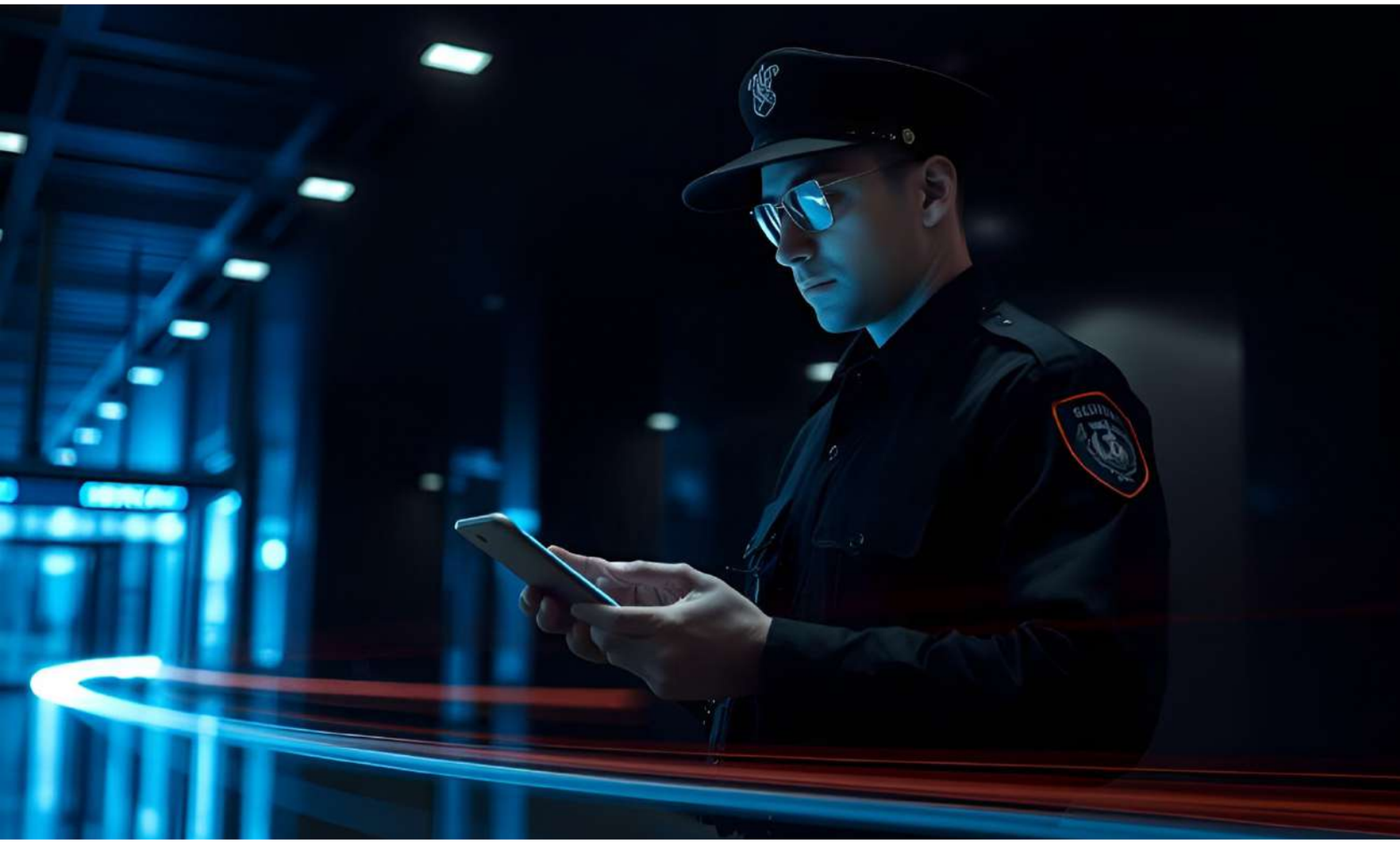
- Reducción de informalidad
- Uniformidad y coherencia normativa
- Mejor calidad técnica en el sector
- Mayor transparencia y rendición de cuentas
- Mejor integración público-privada en seguridad nacional
- Protección de derechos sociales y laborales
- Capacidad de adaptarse a nuevas amenazas tecnológicas

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 di 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-vibracionales, 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.

HIKVISION® | Guanlan

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

Protección perimetral
Impulsado por HikIA

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

ESS+®
FERIA INTERNACIONAL DE SEGURIDAD

26 AL 28 AGOSTO 2026
›CORFERIAS‹

INTEGRACIÓN DE TECNOLOGÍAS GLOBALES

ESS+ 2026 - La plataforma estratégica para fabricantes de seguridad en América Latina y el Caribe

Exhiba su tecnología donde se toman las decisiones

Acceso directo a proyectos activos en:

- Infraestructura crítica y energía
- Banca y finanzas
- Retail y centros comerciales
- Transporte y logística
- Gobierno y ciudades seguras
- Industria y data centers

ESS+ Hub para expansión comercial de América Latina y el Caribe

Contáctenos

Adriana Patricia Márquez Acosta
Directora Comercial
Correo: amarquez@securityfaircolombia.com
Teléfono: +57 310 334 1669

ORGANIZAN

IFEMA MADRID · PAFYC · corferias

Conozca más información aquí o en securityfaircolombia.com