MÁS SEGURIDAD

Magazine

Tendencias que definen el blindaje

(Segunda parte)

Edición 161 | Año 18 | Abril 2026

Precio internacional / $60.00 MX

¿Eres profesional de seguridad privada y aún no formas parte de **ASIS Capítulo México 217**?

Afíliate y sé parte

de nuestra comunidad.

ASIS INTERNATIONAL™
MEMBRESÍA INTERNACIONAL
130 USD

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217
MEMBRESÍA CAPÍTULO MÉXICO
$5,650 MXN

ASIS INTERNATIONAL™ | CAPÍTULO MÉXICO 217
RENOVACIÓN CAPÍTULO MÉXICO
$4,687.50 MXN

¡Qué esperas!

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

TE VEMOS EN
EXPO SEGURIDAD MÉXICO
2 - 4 JUNIO 2026
STAND 1337

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

DG CREATIVE
DISEÑO Y DESARROLLO VISUAL

TERESA RAMÍREZ OJEDA
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

SARA LUCÍA 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

VIRGINIA HERRERA MONTIEL
ADMINISTRACIÓN Y CONTABILIDAD
contabilidad@revistamasseguridad.com.mx

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

ASISTENCIA A CLIENTES
atencion@revistamasseguridad.com.mx

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

SIGUENOS EN:

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

Revista Más Seguridad Año 18, No 161, Abril 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.

El blindaje en México:
profesionalización e innovación

Hace un par de meses se llevó a cabo en la Ciudad de México la tercera edición del Congreso Nacional del Blindaje, foro que reunió a autoridades civiles y militares, fabricantes y especialistas del sector, justo en un momento de alta demanda de protección en el país. A tres años desde su nacimiento, el encuentro, organizado por el Consejo Nacional de la Industria Balística (CNB) ha creado un espacio técnico donde la discusión gira alrededor de regulación, tecnología y profesionalización del sector.

El presidente del CNB, Gadi Mokotov, fijó su postura en el sector: “El blindaje es mucho más que la tecnología, es un compromiso con la vida, la seguridad y la integridad de quienes enfrentamos los riesgos todos los días”. El objetivo del evento: elevar estándares y cerrar el paso a la informalidad.

Uno de los temas centrales fue la preocupación sobre la presencia de productos que se comercializan como blindaje sin cumplir especificaciones técnicas ni certificaciones, por ello se registra una fuerte competencia desleal con “productos milagro” que ofrecen una manufactura que sin lugar a dudas no es blindaje.

El riesgo, explicó Gadi Mokotov, no es comercial sino humano y expone la vida del usuario final. Organizaciones como el CNB o las asociaciones Mexicana de Blindadores de Automotores (AMBA) e Intercontinental de Blindadores (AIB), que encabezan Esteban Hernández y Gabriel Hernández, respectivamente; hacen sinergias y trabajos coordinados con autoridades para fortalecer la regulación, tanto para blindadores como para fabricantes de materia prima. La intención es formalizar un mercado que, aunque crece, aún enfrenta brechas normativas.

En México el blindaje automotriz, corporal y arquitectónico sigue encabezando la demanda de protección. De acuerdo con Mokotov, el producto más solicitado es el blindaje automotriz para uso civil, seguido del producto para uso gubernamental y táctico, y tercero para transporte de carga.

El avance tecnológico del parque automotor introduce nuevos y diversos retos al sector. Vehículos eléctricos, híbridos, sistemas computarizados y sensores obligan a replantear procesos tradicionales; es decir, se requiere mucho más ingeniería y tecnología y “no solo un blindador más de la vieja guardia”.

Las certificaciones y pruebas balísticas hasta amenazas aéreas vinculadas con narcotráfico y guerra asimétrica, son asignaturas pendientes en el sector, mientras que el blindaje arquitectónico permea como una respuesta a entornos de alta violencia.

El mercado mexicano mantiene una expectativa de expansión cercana al 15% anual, cifra similar a la registrada en 2025. El Mundial de Fútbol de 2026 generará demanda temporal, principalmente en renta de vehículos blindados.

Independientemente de la coyuntura deportiva, la dinámica del sector responde más a factores como percepción de riesgo, inversión pública en seguridad y crecimiento de infraestructura logística.

La industria avanza con una visión responsable que integra calidad, legalidad y cooperación entre los sectores público y privado, con la intención de apuntalar estándares técnicos mientras se depura el mercado que está en expansión bajo el dominio de tres ejes: profesionalización, cumplimiento normativo y actualización tecnológica.

Además de ser una actividad con talleres especializados, el blindaje en México involucra ingeniería avanzada, pruebas balísticas certificadas y coordinación con instancias gubernamentales, aunque la discusión se extiende a temas como sostenibilidad y confianza del usuario.

Ramiro Díaz Carreño
Colombia

Doctorando en Estudios Políticos por la Universidad Externado de Colombia. Maestría en Estrategia y Geopolítica por la Escuela Superior de Guerra de las FFMM. Especialización en Administración de la Seguridad por la Universidad Militar Nueva Granada. Profesional en Ciencias Militares, Escuela Militar de Cadetes. Certificado Internacional de Seguridad CPP por ASIS International. Y en Operaciones de Seguridad CPO por IFPO. Miembro del Consejo Consultivo Latino de IFPO.

Más de 30 años de experiencia profesional en consultoría, asesoría e investigaciones para la prevención y control del fraude, consultoría y asesoría de seguridad corporativa para empresas locales y multinacionales, análisis y evaluación de información de interés para el desarrollo de las operaciones de las empresas clientes, planeamiento y desarrollo de investigaciones corporativas y gerenciamiento de incidentes, y de crisis, desarrollo e implementación de los planes de continuidad de negocio y recuperación del desastre, manejo de relaciones y coordinación de apoyos con las autoridades de cada región.

Docente universitario para los posgrados en Administración de Seguridad de la Universidad Militar Nueva Granada y la Escuela de Posgrados de la Policía Nacional.

Sumario

@MatadorMejia

Humberto Mejía / DSE, CPSI

México bárbaro

Sí, leíste bien: **México bárbaro**, que es el título de varios artículos publicados en The American Magazine, una popular revista estadounidense, firmados por el periodista John Kenneth Turner en 1909. Hoy nuestro amado, saqueado y dividido país es visto a nivel mundial con este vergonzoso título gracias a los altísimos niveles de inseguridad y violencia que permean.

Aún cuando la "prensa a modo" se empeñe en replicar las versiones oficiales de que "todo está bien, que los niveles de inseguridad bajaron o que la seguridad está garantizada", para quienes trabajamos en la industria de la protección, leemos, nos informamos y nos distinguimos del resto la población por ello, sabemos que se trata de una falacia.

Desde hace poco más de 3 sexenios (Calderon Hinojosa, Peña Nieto, López Obrador y Sheinbaum Pardo) los ojos del mundo están puestos en México, principalmente por la ola de violencia ascendente que vivimos. Hoy, más que nunca nos miran por la cercana competencia del Mundial de Fútbol que aquí se desarrollará. El fanatismo a millones no les deja ver este antecedente y ni les preocupa.

En días pasados, tras los lamentables hechos ocurridos en la zona arqueológica de Teotihuacán donde un turista extranjero fue asesinado y otros tantos resultaron heridos, el titular de la Secretaría de Seguridad y Protección Ciudadana (SSPC) del gobierno federal, Omar Hamid García Harfuch, aseguró que "la seguridad para el Mundial de Fútbol está garantizada". Yo reitero: lo cierto es que esta aseveración huele, sabe y se distingue por lo que es: una mentira.

Sin embargo, esta falacia se tiene que repetir hasta el cansancio para no ahuyentar al turismo nacional e internacional que generará una brutal derrama económica para estadios, hoteles, restaurantes, transportes, souvenirs, estacionamientos, etc., y todo eso para el gobierno en sus tres niveles es un "apetitoso bocado" que se traducirá en impuestos. Sólo recordemos que el próximo año hay elecciones intermedias en México y para que el gobierno federal siga siendo mayoría en el Congreso requiere votos y mucho dinero para su cuestionado (y hasta odiado) partido Morena.

Sin duda, un reducido porcentaje de visitantes por el Mundial tiene la protección asegurada, pues serán los que podrán alquilar vehículos blindados y equipados con dispositivos de telemetría, escoltas y guardias privados, incluso podrán adquirir ropa balística. El turista promedio (sobre todo el nacional) seguirá moviéndose en transporte público, a pie incluso, comerá en restaurantes comunes, puestos callejeros o mercados, se hospedará en hoteles del nivel intermedio y económicos, y portará efectivo o tarjetas de crédito y débito. Ese amplio sector es el más vulnerable ante esa "bestia" denominada delincuencia.

No soy pesimista o anti-fútbol. Entiendo la importancia de la derrama económica para el país, pero no cierro los ojos ante la brutal pesadilla que vivimos millones de mexicanos por la corrupción y avaricia de cientos de funcionarios que se han coludido con la delincuencia, al punto que la han dejado crecer y hasta casi gobernar al que llaman "Estado fallido".

¿De qué hablo? De los "levantones" y ejecuciones diarias y casi en cualquier estado de la República Mexicana, ya sea de personas ligadas al crimen o ajenas a ello, de los actos delictivos cometidos al ciudadano a pie, los asaltos en las vialidades del país, el cobro de piso, la extorsión telefónica, el secuestro, el narco menudeo y un largo etc. etc. etc. Hay una tarea pendiente que alguien del gobierno no está haciendo y millones de ciudadanos lo sabemos. Es cuanto...

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

La participación femenina en seguridad tecnológica gana terreno en México

• El desarrollo de talento femenino impulsa la adopción tecnológica; por ello, Mujeres Hikvision continuará con cursos durante el año y su expansión a distintas ciudades para fortalecer la especialización y el alcance del programa en la industria.

La industria tecnológica en México enfrenta un reto estructural: incrementar la participación femenina en áreas técnicas y de liderazgo. En un sector donde la innovación avanza a gran velocidad, impulsar talento diverso no solo responde a una agenda de inclusión, sino a una necesidad real de competitividad y crecimiento.

Bajo este contexto, Hikvision México lanzó la cuarta edición de su programa “Mujeres Hikvision”, una iniciativa que busca abrir más espacios de formación y desarrollo para féminas dentro de la industria de la videoseguridad y soluciones inteligentes.

A diferencia de otros segmentos tecnológicos, la seguridad electrónica ha tenido una menor representación femenina, particularmente en áreas técnicas. Este panorama ha limitado el acceso a oportunidades de especialización y crecimiento profesional, lo que vuelve aún más relevante la creación de programas enfocados en cerrar esta brecha.

En este sentido, “Mujeres Hikvision” se ha posicionado como una plataforma que integra formación técnica, fortalecimiento de capacidades y creación de redes profesionales. Con el paso de sus ediciones, el programa ha evolucionado hacia un enfoque más integral, orientado no solo a la especialización, sino también a fomentar confianza y presencia activa de las mujeres dentro del ecosistema tecnológico.

“En Hikvision entendemos que impulsar la presencia femenina en el sector tecnológico trasciende la inclusión; representa una oportunidad para enriquecer a la industria con nuevas perspectivas y talento. A través de este programa, buscamos abrir espacios que les permitan crecer, especializarse y asumir un papel más relevante en el mercado”, señala Fran Sánchez, Marcom director de Hikvision México.

Como parte de esta edición, se llevó a cabo el curso presencial “Tendencias de Seguridad para Verticales de Negocio”, una de las sesiones iniciales de la serie prevista a lo largo del año. Impartido por Jackie Cruzprieto, el curso abordó temas como la operación en la nube, el uso de datos para la toma de decisiones y el impacto de la reforma laboral en la tecnología.

Durante la sesión, participó Jorge Jaramillo, de Grupo Valoran —empresa especializada en el desarrollo de infraestructura, parques industriales y servicios—, quien compartió la perspectiva operativa sobre los retos actuales en seguridad. En su intervención, destacó tres ejes clave: el uso de inteligencia artificial y analíticas avanzadas para la identificación de eventos críticos, la capacitación del personal en herramientas y protocolos, y la colaboración con autoridades para garantizar implementaciones alineadas al marco legal.

Este enfoque se alinea con la estrategia de capacitación del canal, donde la formación continua es clave para el crecimiento del mercado. En particular, los cursos dirigidos a mujeres complementan los programas tradicionales al generar entornos de aprendizaje más accesibles, fortaleciendo su participación en áreas como ventas, diseño de proyectos y marketing tecnológico.

“El desarrollo de talento femenino también tiene un impacto directo en la adopción tecnológica. A medida que más mujeres se especializan en estas soluciones, se fortalece la capacidad del canal para comunicar valor, entender mejor al usuario final y acelerar la implementación de nuevas tecnologías en el mercado. Como parte de la iniciativa Mujeres Hikvision, se continuarán realizando cursos durante este año para acercar estas oportunidades de formación y desarrollo profesional a más mujeres del sector”, comenta Paulina Lordméndez, Brand Communications & Content Lead de Hikvision México.

El impacto del programa va más allá del aprendizaje técnico. La posibilidad de conectar con otras mujeres del sector, compartir experiencias y generar redes profesionales se convierte en un elemento clave para fortalecer la confianza y consolidar trayectorias dentro de una industria en constante evolución.

Con iniciativas como Mujeres Hikvision, la conversación deja de centrarse únicamente en tecnología y se amplía hacia el desarrollo de talento, donde la diversidad se posiciona como un motor para la innovación y el crecimiento sostenido de la industria. Además, se contempla la realización de más cursos sobre estos temas, acercando estas oportunidades a un número cada vez mayor de mujeres dentro de la industria a nivel nacional.

Inteligencia Artificial en videovigilancia

impulsa el consumo y redefine la experiencia del público en estadios

Luis Mariano Vega, gerente de ventas del Área Sur de Latinoamérica de Axis Communications

La videovigilancia con Inteligencia Artificial dejó de ser solo un sistema de seguridad para convertirse en una poderosa herramienta de marketing deportivo y experiencia del usuario. Hoy, estadios, conciertos y eventos masivos utilizan cámaras inteligentes no solo para vigilar, sino para entender cómo se comporta el público.

Un ejemplo de esto es el próximo Mundial de fútbol, en donde, de acuerdo a datos del C5 de la Ciudad de México, la CDMX se ha convertido en la ciudad más videovigilada de todo el Mundial de Fútbol, al contar con un total de 114 mil 500 cámaras instaladas por toda la ciudad. Esto, no solo garantiza la seguridad de los aficionados, sino que, en ciertos entornos, también permite optimizar espacios, mejorar la logística y diseñar estrategias que aumentan el consumo y la satisfacción de los asistentes.

Mejorando la experiencia del aficionado

Uno de los cambios más visibles está en la experiencia del espectador en estadios. Gracias al análisis en tiempo real, los organizadores pueden identificar zonas congestionadas, mejorar el acceso a servicios y reducir filas.

La personalización del servicio es otro de los grandes avances. Las cámaras con analítica permiten conocer hábitos de consumo, preferencias y comportamientos del público. Con estos datos, los organizadores pueden ofrecer promociones específicas según el perfil de los asistentes, desde familias hasta fanáticos de un equipo. Esta segmentación mejora la conexión con la audiencia y aumenta el retorno de inversión (ROI), convirtiendo la información en una ventaja competitiva.

Más allá de la experiencia: seguridad garantizada

Pero más allá del negocio, la protección en eventos masivos sigue siendo el eje central. Incidentes recientes en grandes competencias deportivas han evidenciado la necesidad de contar con sistemas avanzados de control de acceso, monitoreo y respuesta inmediata. La videovigilancia inteligente permite detectar riesgos antes de que escalen, enviar alertas en tiempo real y actuar con mayor rapidez, fortaleciendo la confianza del público y garantizando entornos más seguros.

Por si fuera poco, toda la información recolectada permite ubicar publicidad en puntos clave, logrando campañas más efectivas. Así, la tecnología no solo ordena el evento, también convierte cada recorrido del usuario en una oportunidad de negocio.

En un contexto marcado por grandes citas como torneos internacionales y espectáculos multitudinarios, la tecnología se consolida como aliada clave. La combinación de inteligencia artificial, análisis de datos y videovigilancia no solo protege a los asistentes, sino que redefine la forma en que se viven estos eventos. Hoy, las cámaras ya no solo observan: también ayudan a entender, conectar y transformar cada experiencia en una oportunidad de crecimiento.

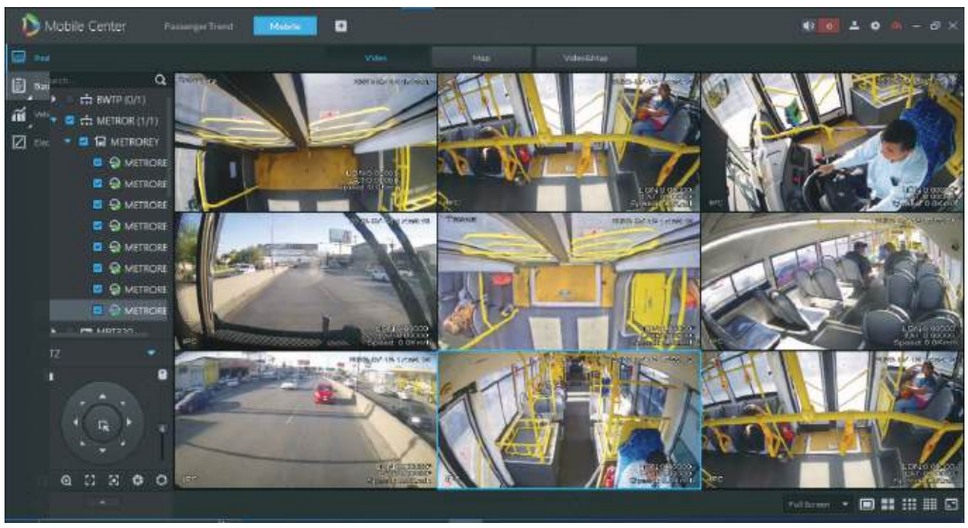
Dahua Technology impulsa digitalización del transporte público

con soluciones inteligentes de monitoreo y analítica de pasajeros en México

La modernización del transporte público es uno de los principales retos para las ciudades en crecimiento, donde la eficiencia operativa, la seguridad de los usuarios y la optimización de rutas son factores clave para mejorar la movilidad urbana.

En este contexto, Dahua Technology implementó una solución tecnológica de monitoreo y analítica de pasajeros en una de las zonas metropolitanas más dinámicas del norte del país, contribuyendo a fortalecer la gestión del transporte público y mejorar la experiencia de movilidad de miles de usuarios.

El proyecto forma parte de un programa de modernización del sistema de transporte urbano que contempla la incorporación de nuevas unidades y la adopción de tecnologías inteligentes para optimizar la operación de la red de autobuses. Como resultado de esta implementación, la tecnología de Dahua fue desplegada en 2,200 autobuses del sistema de transporte, logrando una reducción del 25 % en el tiempo promedio de espera de los usuarios y una disminución del 20 % en incidentes o irregularidades operativas, reflejando un impacto directo en la eficiencia y seguridad del servicio.



Tecnología para una gestión del transporte basada en datos

Uno de los principales retos identificados en el sistema de transporte era la falta de datos confiables para la planificación de rutas, lo que generaba ineficiencias en la cobertura del servicio y limitaba la capacidad de optimizar la asignación de unidades.

Para abordar este desafío, el proyecto incorporó cámaras inteligentes de conteo de pasajeros instaladas en las puertas de los autobuses, capaces de registrar con alta precisión los movimientos de ascenso y descenso de usuarios.

La solución desarrollada permite:

- Contabilizar pasajeros que suben y bajan en cada puerta del vehículo
- Generar reportes de flujo de pasajeros por ruta, parada y unidad
- Analizar patrones de movilidad en diferentes horarios
- Optimizar decisiones operativas basadas en datos reales

Gracias a la analítica avanzada implementada, el sistema alcanza niveles de precisión superiores al 95 % en el conteo de pasajeros, incluso en escenarios complejos como vehículos con alta ocupación o flujos simultáneos de entrada y salida.

Supervisión operativa y transparencia en la gestión del servicio

Además de mejorar la planificación del transporte, el proyecto incorporó videovigilancia y terminales inteligentes a bordo de las unidades, permitiendo fortalecer la supervisión operativa del sistema.

Entre las funcionalidades implementadas destacan:

- Comunicación y posicionamiento en tiempo real de las unidades
- Monitoreo de video en vivo desde el centro de control
- Registro y almacenamiento de video y datos operativos
- Alertas de seguridad y eventos críticos
- Integración de botones de pánico para atención de emergencias

Esta infraestructura tecnológica permite generar mayor transparencia en la operación del servicio, reducir irregularidades en los procesos de pago y fortalecer la supervisión de las unidades en circulación.

Conectividad con centros de monitoreo para mayor seguridad

Como parte del proyecto, la flota de transporte equipada con tecnología Dahua fue integrada a un centro de monitoreo de seguridad, permitiendo la transmisión en tiempo real de ubicación, video y eventos de alarma.

Esta integración fortalece las capacidades de supervisión del sistema de transporte público, contribuyendo a mejorar la seguridad de operadores y pasajeros, así como la capacidad de respuesta ante incidentes.

Undécima edición de Smart City

Expo LATAM Congress 2026

El evento (congreso y expo) de innovación urbana más relevante de América Latina presentó su undécima edición en la Ciudad de México, destacando una agenda fortalecida por alianzas estratégicas, participación internacional de alto nivel y una creciente demanda de empresas y gobiernos por impulsar ciudades más inteligentes y sostenibles.

En esta edición, sobresalen dos hitos de gran impacto, por un lado el Encuentro Nacional de Alcaldes impulsado por Instituto Nacional para el Federalismo y el Desarrollo Municipal (INAFED) del gobierno de México, así como la participación estratégica del gobierno de Estados Unidos, a través del Departamento de Estado y empresas norteamericanas con soluciones urbanas y de financiación, todo esto, reflejando el gran interés público y privado para integrarse a esta plataforma de innovación y desarrollo de ciudades inteligentes y sostenibles.

Organizado por Fira Barcelona International y PRONUS Events, en conjunto con los gobiernos estatal y municipal de Puebla como anfitriones, las secretarías de Gobernación y de Economía del gobierno Federal y el Consejo Coordinador Empresarial como aliados estratégicos, el Congreso consolida su posición como el principal punto de encuentro de empresas y gobiernos (B2G/Business to Government) en la región. Asimismo, como cada año, se celebrarán los LATAM Smart City Awards, un sello de excelencia internacional, que ha reconocido a más de 100 proyectos que han transformado la región en los últimos años.

Por otro lado, en esta edición de Smart City cuenta con una cantidad considerable de aliados y participación estratégica. Se anunció la segunda edición del Encuentro Nacional de Alcaldes por la Innovación y la Prosperidad Compartida, impulsado por el Instituto Nacional para el Federalismo y el Desarrollo Municipal (INAFED) del gobierno de México, el cual, buscará promover la modernización, la innovación y el desarrollo económico local.

Al respecto Armando Quintero Martínez, Coordinador General del INAFED, manifestó su compromiso de “realizar un esfuerzo grande para lograr la mayor presencia municipalista en la historia del congreso, con el objetivo de reunir a más de 300 presidentes municipales”, comentó que su objetivo principal es que los gobiernos locales den un salto cualitativo al aprovechar la ciencia contemporánea y las nuevas tecnologías para cumplir con sus responsabilidades.

La directora del evento, Fabiola Vega, aseguró que los gobiernos locales son el motor de la transformación, y que, “este espacio será clave para dialogar, compartir soluciones y generar alianzas frente a los retos de movilidad, cambio climático y desigualdad en nuestros territorios”.

En esta edición 2026 del Smart City Expo LATAM Congress (SCELC), se espera la participación de más de mil ciudades nacionales e internacionales, 300 alcaldes, 220 instituciones y empresas, 320 ponentes, entre los que se podrán encontrar Keynotes destacados a nivel internacional, 8,500 asistentes, más de 80 medios de comunicación, en una superficie de 15,000 m2 dentro del Centro Expositor y de Convenciones de Puebla.

Durante la presentación, el representante del gobierno del Estado de Puebla, Marco Antonio Molina, destacó la visión del gobernador Alejandro Armenta de incentivar encuentros de talla internacional, “este evento coloca a Puebla en el mapa global de las ciudades inteligentes y la consolida como un referente nacional al promover soluciones que integran tecnología movilidad, sostenibilidad y participación ciudadana”.

Por su parte, Jaime Oropeza Casas, Secretario de Economía y Turismo de la ciudad de Puebla, destacó que la entidad se convertirá en el epicentro de Latinoamérica para la discusión sobre el futuro de las ciudades, subrayando “la importancia de diseñar políticas públicas centradas en el ciudadano como lo ha hecho el alcalde de Puebla José Chedraui”.

SMARTCITY
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

INAFED · Gobierno de México

INSTITUCIÓN ALIADA PRINCIPAL

11ª EDICIÓN
#SCELC26

smartcityexpolatam.com

ANFITRIÓN

PUEBLA Gobierno del Estado 2024 - 2030 | Pensar en Grande | POR AMOR A PUEBLA

SEDE

Puebla Gobierno de la Ciudad | La Capital Imparable

ORGANIZADO POR

PRONUS eventos

UN EVENTO DE

SMARTCITY EXPO WORLD CONGRESS | Fira Barcelona International

Tecnología Biométrica

Principal aliado del sector financiero frente a los 400,000 delitos cibernéticos que se cometen al día en México.

Las denuncias por fraude cibernético en México crecen anualmente, evidenciando un problema a gran escala donde los delincuentes explotan la desinformación para el robo de identidad. Las cifras son contundentes: hasta julio de 2025, más de 13 millones de mexicanos habían sido víctimas de fraudes digitales. Según la Academia Mexicana de Ciberseguridad y Derecho Digital, se cometen más de 400,000 delitos cibernéticos al día, con un promedio de un ataque cada 39 segundos.

Por su parte, la Condusef reportó 3.3 millones de reclamaciones en el sector financiero durante el primer semestre de 2025, subrayando el impacto devastador en el patrimonio de las familias mexicanas.

Nueva regulación obligatoria

Para frenar el robo de identidad y el uso delictivo de cuentas bancarias, a partir del 1 de julio de 2026, cualquier persona que realice depósitos o retiros en efectivo iguales o superiores a $140,000 pesos deberá identificarse obligatoriamente mediante al menos un dato biométrico. Esta normativa, impulsada por la ABM y la CNBV, busca fortalecer el sistema financiero con una barrera prácticamente infalsificable: los rasgos faciales y dactilares únicos.

Identy.io: Aliado estratégico en autenticación

En este contexto, Identy.io se posiciona como el socio estratégico para implementar verificación biométrica robusta. Sus soluciones permiten validar la identidad de forma segura y privada, reduciendo drásticamente la suplantación sin afectar la experiencia del usuario.

Accesibilidad total: La tecnología de Identy.io utiliza la cámara del celular (biometría dactilar, facial y de palma) sin requerir hardware adicional. Funciona incluso en dispositivos de gama baja y en zonas de poca cobertura, permitiendo a los bancos escalar sus procesos a poblaciones con menor infraestructura.

Seguridad multimodal: Al combinar múltiples factores en un solo flujo, la validación se realiza directamente en el dispositivo del usuario. Esto evita el envío de datos sensibles a servidores externos, minimizando riesgos de filtraciones.

Combatiendo el fraude Impulsado por IA

El uso de Inteligencia Artificial ha sofisticado las estafas mediante la creación de identidades falsas y deepfakes. Para contrarrestar esto, Identy.io incorpora capacidades avanzadas de detección de vida pasiva (passive liveness). Mediante el análisis de micro-expresiones y texturas de la piel en tiempo real, el sistema distingue entre un humano auténtico y un fraude generado por IA de manera no intrusiva.

Estándares internacionales y confianza

Más que un requisito operativo, la identidad es hoy un factor clave de retención y confianza. Las soluciones de Identy.io están validadas bajo los estándares más rigurosos del sector, como NIST PFT III y NIST ISO/IEC 30107-3 Nivel 2 (PAD). Estas certificaciones garantizan su eficacia contra ataques de suplantación complejos, incluyendo máscaras y videos manipulados.

Con este enfoque, bancos y fintechs pueden implementar controles que cumplen con las normativas internacionales más exigentes, blindando el ecosistema financiero y protegiendo a los ciudadanos.

AJAX gana ocho premios

Red Dot Awards

Ajax Systems, el mayor fabricante europeo de sistemas de seguridad, ha reafirmado su liderazgo mundial al obtener ocho premios Red Dot Design Awards. Este es el tercer año consecutivo que la empresa recibe este prestigioso sello de calidad alemán, destacando por su capacidad para fusionar innovación tecnológica, funcionalidad superior y estética de vanguardia.

Valentine Hrytsenko, CMO de Ajax Systems, subrayó que este logro es testimonio de un ADN donde la belleza y la ingeniería convergen en cada etapa del producto, desde el software hasta el marketing.

Innovación en Detección de Incendios (Categoría Industrial)
La nueva línea EN54, diseñada para entornos comerciales y municipales, fue una de las grandes protagonistas:

EN54 Fire Hub Jeweller: Un panel de control (ECI) con pantalla táctil e interfaz intuitiva. Su conectividad inalámbrica permite un despliegue rápido y una gestión unificada que admite intrusión (Grado 2), video y automatización.

Sirenas y DAV EN54 FireProtect: Dispositivos certificados que emiten alertas sonoras y visuales en menos de tres segundos tras una alarma.

EN54 I/O Module (2X2): Módulo de integración que permite automatizar reacciones ante emergencias, vinculando portones, ascensores y sistemas de climatización de terceros al ecosistema Ajax.

Evolución en videovigilancia y gestión de datos
Ajax ha transformado su oferta de video, logrando premios en las categorías de cámaras y tecnologías de la información:

Cámaras Superior (TurretCam y BulletCam HLVF): Equipadas con objetivos P-Iris para evitar desenfoques por destellos y visión nocturna de alta fidelidad. Su IA integrada distingue entre personas, mascotas y vehículos con precisión quirúrgica, ofreciendo además audio bidireccional nativo.

BulletCam HL: Destaca por su iluminación híbrida (IR y luz blanca), garantizando grabaciones nítidas en oscuridad total y una integración fluida con los dispositivos de intrusión a través de una única app.

Serie NVR H y Superior NVR H2D: Los grabadores de video de Ajax ofrecen una monitorización flexible con salida HDMI para visualización local sin internet. La serie Superior H2D eleva el estándar con capacidad para dos discos duros sustituibles en caliente (hasta 48 TB) y decodificación 4K, permitiendo gestionar cámaras IP de terceros con análisis de IA centralizado.

El Sello Red Dot: Un estándar de calidad
Desde 1954, el Red Dot Design Award evalúa productos bajo criterios estrictos de funcionalidad y estética. Para Ajax, estos ocho galardones validan su estrategia de ofrecer soluciones que no solo protegen, sino que mejoran la experiencia del usuario profesional y final.

Gestión de llaves y equipos bajo control: Traka

• El secreto detrás de la operación segura en el sector minero.

En la minería de alto volumen, todo acceso y equipamiento debería estar bajo un estricto control. Sin embargo, las operaciones mineras no son lugares de trabajo convencionales, sino en grandes complejos que funcionan como una verdadera ciudad: cuentan con dormitorios, flotillas de transporte, servicios, comedores, oficinas, seguridad, infraestructura crítica, plantas de proceso, maquinaria pesada y sistemas de operación que requieren administración constante.

Es así como la asignación de llaves y la entrega de equipamiento técnico, de seguridad física, industrial y de protección personal no son procesos secundarios, son operaciones que sostienen la continuidad operativa de la mina y cuidan del bienestar de los trabajadores.

En ese sentido, sistemas automatizados de gestión de llaves y activos como gabinetes electrónicos, casilleros inteligentes y plataformas de administración, surgen como soluciones para documentar cada acceso, garantizar que solo el personal certificado opere maquinaria de alto riesgo y asegurar que los equipos de comunicación y de seguridad personal estén disponibles en condiciones óptimas.

Control de llaves y acceso operativo

En entornos mineros de gran escala, la incorporación de tecnología en la gestión de accesos y llaves, además de aportar orden y eficiencia, también representa una medida directa de protección para los trabajadores.

Al establecer controles precisos sobre quién puede ingresar o activar cada recurso, se reducen riesgos operativos y se previenen situaciones que, en muchos casos, podrían derivar en accidentes graves. La digitalización de estos procesos asegura que la protección esté integrada desde el primer punto de contacto con la operación.

En ese sentido, un armario inteligente no solo organiza llaves, sino que también ayuda a definir quién puede operar cada vehículo o instalación crítica, por ejemplo. La gestión de llaves se extiende desde autobuses de transporte hasta los tractocamiones mineros y retroexcavadoras, donde se exige certificaciones específicas. El sistema asegura que únicamente personal autorizado retire la llave correspondiente y que cada movimiento quede registrado.

El funcionamiento es sencillo y seguro. El trabajador se identifica con su credencial en el gabinete, el sistema valida si cuenta con los permisos adecuados, certifica el proceso haciendo mandatorio el reconocimiento de las políticas de la empresa, incluyendo la de seguridad personal, propósito de la operación, anotaciones de bitácora, y, en caso afirmativo, libera solo la llave asignada. Cada apertura queda registrada con hora, usuario y equipo vinculado, y si fuera el caso que el vehículo estuviera en mantenimiento o bloqueado por protocolo de seguridad, la llave permanece inaccesible; de esta manera, el gabinete actúa como filtro operativo y documental.

Una práctica común es reemplazar los cilindros de encendido de la maquinaria pesada, permitiendo la implementación de llaves maestras. Así la operación se ve mejorada, al contar con llaves de alta seguridad, controladas electrónicamente, accesibles solo a los usuarios programados y se reduce riesgos de robo, uso indebido y fallas operativas.

En el ámbito de planta física, los armarios inteligentes pueden administrar las llaves de las subestaciones eléctricas, cuartos mecánicos y otros accesos sensibles, mientras que en emergencias concentran las llaves críticas de seguridad, donde el cumplimiento normativo y la protección de vidas son prioritarios.

Finalmente, cabe señalar que la administración de llaves en los dormitorios constituye un aspecto importante también, en un complejo minero, cada acceso a habitaciones, áreas comunes y espacios de descanso debería estar regulado con la misma rigurosidad que los equipos de trabajo. La trazabilidad de quién entra y quién sale de los dormitorios garantiza orden y disciplina, protege la integridad de los trabajadores y previene incidentes derivados de accesos indebidos.

Gestión automatizada de equipos de protección y comunicación

Dentro de la operación minera, los casilleros inteligentes aseguran que cada trabajador reciba equipos de comunicación y protección personal en condiciones óptimas y verificadas. Radios, baterías, detectores de gases y mascarillas de oxígeno, tabletas, celulares y otros equipos de protección personal son recursos indispensables para enfrentar entornos de alto riesgo, y su administración no puede quedar al azar.

El acceso a estos equipos se realiza, de igual manera, mediante una credencial, el sistema valida la identidad del trabajador y libera el compartimento asignado. Al retirar un radio, por ejemplo, el casillero puede tener integrada una base de carga, y si el dispositivo presenta fallas, el usuario puede devolver el equipo, marcar la falla como crítica dentro del sistema, inhibiendo su uso para otros usuarios, bloqueándolo y registra la incidencia para activar el proceso de mantenimiento, evitando que un operador descienda a la mina con un radio inservible o sin batería, situación que en una emergencia puede ser mortal.

En el caso de detectores de gases y mascarillas de oxígeno, el casillero garantiza que cada trabajador lleve consigo el equipo de protección personal requerido antes de ingresar a las áreas de operación, ya sean subterráneas o a cielo abierto. El registro digital documenta quién retiró el dispositivo, en qué momento y bajo qué turno, permitiendo a los supervisores verificar que nadie acceda a la operación sin los elementos de seguridad necesarios.

Estos casilleros transforman cada entrega en un registro verificable y cada restricción en un mecanismo de seguridad colectiva. La rutina de retirar un radio, una batería o una mascarilla queda documentada y se convierte en evidencia de que el trabajador cuenta con el equipo necesario para operar en condiciones seguras. Así, la administración de dispositivos se integra al sistema de protección general de la mina y fortalece la disciplina operativa frente a riesgos invisibles como gases tóxicos o fallas de comunicación.

Integración operativa, control de accesos y mantenimiento en tiempo real

La implementación de armarios y casilleros inteligentes alcanza su máximo valor cuando se conectan a una plataforma de gestión centralizada como TrakaWeb. En minería, esta integración permite que las credenciales de los trabajadores, los registros de recursos humanos y los sistemas de control de acceso existentes puedan integrarse para hacer una operación unificada.

El trabajador se identifica con su credencial y, de manera automática, el sistema valida si está autorizado para retirar una llave, un radio o un detector de gases, evitando la duplicación de registros y asegurando que cada acceso quede vinculado al perfil laboral del empleado.

Esta plataforma también puede ayudar a gestionar el bloqueo de equipos en mantenimiento, al restringir la llave correspondiente y evita que el equipo sea energizado por error. Esta práctica de seguridad industrial se conoce como Lockout / Tagout (LOTO).

Lockout / Tagout consiste en cortar la energía del equipo en mantenimiento, asegurar los interruptores, generalmente con un candado, para que no puedan activarse, etiquetar los interruptores y verificar que no hay fuentes de energía activa, antes de dar mantenimiento a los equipos. Cuando varias cuadrillas ejecutan mantenimiento, múltiples candados son usados para bloquear un interruptor, y es hasta que todos los candados son retirados, por cada uno de sus respectivos supervisores, que puede volver en operación el equipo.

Gestionar el acceso a estas llaves puede salvar vidas y su aplicación es decisiva: la maquinaria pesada, las subestaciones eléctricas, los cuartos mecánicos, sistemas de aire comprimido, bandas transportadoras, equipos hidráulicos, entre otros, permanecen inactivos hasta que el personal autorizado concluye sus labores. El protocolo se basa en dos acciones complementarias: el bloqueo físico, que impide la activación del equipo, y el etiquetado visible, que advierte a todos los trabajadores que la máquina está fuera de servicio.

En este contexto, las llaves actúan como el mecanismo que mantiene un equipo fuera de operación hasta que la cuadrilla de mantenimiento concluye su trabajo. En otras palabras, una gestión adecuada de llaves es parte fundamental de la correcta aplicación del protocolo.

Cumplir con LOTO reduce de forma comprobada el riesgo de atrapamientos, electrocuciones y quemaduras, y asegura que la reactivación de los equipos solo ocurra bajo condiciones verificadas. Además, aporta trazabilidad completa, evidencia documental para auditorías y un mayor nivel de seguridad operativa en cada etapa.

Finalmente, los encargados pueden supervisar todos los gabinetes y casilleros distribuidos en distintas minas o áreas de operación mediante el software de administración, lo que les permite verificar si los radios entregados están en uso, comprobar el estado de las baterías y confirmar que los equipos de protección personal hayan sido retirados antes de iniciar la jornada laboral.

La plataforma convierte la gestión de llaves y dispositivos en un sistema coordinado que enlaza credenciales, procesos y seguridad operativa en tiempo real.

Por último, esta gestión operativa es amplificada cuando la plataforma TrakaWeb es integrada a los sistemas corporativos de seguridad y la gestión de los usuarios se centraliza a nivel global y los armarios de llaves y casilleros inteligentes se vuelven una extensión del sistema de seguridad.

Solo los trabajadores y contratistas con credencial corporativa pueden acceder a los gabinetes y solo pueden tomar las llaves y equipos asignados a través de un solo sistema. Detrás de escena, TrakaWEB mapea los permisos de acceso de la plataforma de seguridad, sincroniza los usuarios y credenciales autorizados y reporta todos los eventos generados hacia la plataforma de seguridad corporativa.

De manera preventiva, los gabinetes son la primera línea de control para su operación y, de manera correctiva, permite obtener la información para actuar ante una emergencia, como un incendio, una evacuación. No solamente la plataforma de seguridad puede asegurar que un empleado está en su área de trabajo, si también que cuenta con su equipo de protección personal y de comunicación, listo para trabajar de manera seguridad y a tiempo.

La gestión de llaves y dispositivos en minería no es una rutina aislada de cada trabajador, sino parte de una estrategia colectiva que sostiene la operación completa. El registro de accesos, la validación de credenciales y la administración de equipos de seguridad personal conforman un sistema que responde a exigencias normativas y a protocolos de seguridad. Cada interacción queda documentada y se convierte en evidencia verificable, facilitando a la empresa demostrar cumplimiento y, al mismo tiempo, reducir riesgos operativos.

Diego Cota, gerente regional de Ventas en Traka

HID y Sharry impulsan

el primer proyecto de credenciales en Wallet de Buró Property para edificios corporativos en América Latina

HID, empresa mundial en soluciones de identificación segura, anunció la implementación de su tecnología HID Mobile Access en el primer proyecto de la región que habilita credenciales móviles directamente en Apple Wallet y Google Wallet para edificios corporativos.

El proyecto consistió en la creación de un ecosistema de acceso digital en tres de los complejos corporativos más emblemáticos de Buró Property en la Ciudad de México: Puerta Polanco, DEK Polanco e In Situ Santa Fe. Gracias a esta implementación, miles de usuarios, visitantes e inquilinos pueden ingresar a torniquetes, elevadores y estacionamientos usando únicamente el teléfono móvil o reloj inteligente.

Del acceso tradicional a la experiencia digital

Previamente, el acceso en estos edificios se gestionaba mediante tarjetas plásticas y procesos manuales, lo que implicaba una ardua gestión administrativa para la emisión, reposición y desactivación de credenciales.

"Identificamos que los hábitos de los usuarios están cambiando: hoy la mayoría utiliza su celular o incluso un reloj inteligente para gestionar su día a día. Por eso, incorporar credenciales móviles en Wallet fue el paso natural para ofrecer una experiencia más ágil y segura, sin dejar de brindar alternativas a quienes prefieren mantener la tarjeta física", indicó Salomón Shabot, director general de Buró Property.

Para responder a este desafío, Buró Property desplegó una solución que combina la tecnología de HID Mobile Access con la plataforma de acceso inteligente de Sharry, creando un ecosistema de acceso unificado en torniquetes, elevadores, estacionamientos y áreas comunes mediante una credencial alojada de forma segura en Apple Wallet o Google Wallet, según el dispositivo del visitante.

Uno de los principales diferenciadores del proyecto es su enfoque en la experiencia del usuario. El sistema elimina la necesidad de descargar aplicaciones dedicadas, ya que las credenciales se vinculan directamente a la billetera digital del dispositivo. Esto simplifica la adopción, reduce fricciones y mantiene altos estándares de seguridad.

"Poder incluir nuestras credenciales en las Wallets a través de Sharry significa ofrecer una experiencia más limpia, en donde el usuario no debe tener un aplicativo instalado, lo que se traduce en mayor comodidad y autonomía para ellos", Alejandro Espinosa, director comercial de Soluciones de Control de Acceso Físico de HID en México.

"Para el usuario, la experiencia es simple: basta con acercar su teléfono o reloj inteligente al lector de HID, bien sea independiente o integrado al torniquete, botonera del elevador o boletera del acceso vehicular para obtener acceso inmediato y gracias a la tecnología de HID, las credenciales son plenamente compatibles con los lectores de los edificios, haciendo posible que todo funcione de manera unificada", señaló Carlos Vázquez, representante de desarrollo empresarial para Sharry.

Infraestructura preparada para el futuro

Los tres edificios están equipados con los lectores HID® Signo™ y iCLASS SE, diseñados para operar tanto con dispositivos móviles como con credenciales físicas, capacidad que facilita una transición gradual de tecnología bajo un modelo híbrido sin interrumpir las operaciones existentes.

La solución se basa en la tecnología de credenciales digitales HID® Seos®, una arquitectura basada en software y gestionada en la nube que ofrece seguridad avanzada y un cifrado robusto. A su vez, la plataforma en la nube HID Origo, facilita la integración con sistemas de terceros, como el control de acceso C-CURE de Johnson Controls, los estacionamientos de Skidata operados por Deprisa y los elevadores de Schindler.

IR Systems actuó como integrador principal del proyecto, garantizando que todos los componentes funcionen de manera conjunta bajo un mismo esquema digital. El resultado fue un sistema híbrido, escalable y preparado para evolucionar hacia una digitalización total del acceso.

Resultados e impacto

En Puerta Polanco, los usuarios ya han comenzado a migrar al uso de Wallet, con el objetivo de alcanzar —en los próximos años— una adopción del 100 % entre las más de 5,500 personas que ingresan cada día al edificio. En DEK Polanco, la transición avanza hacia la digitalización completa, mientras que en In Situ Santa Fe se habilitó un modelo híbrido que combina credenciales móviles para usuarios fijos y códigos QR para visitantes, garantizando accesos diferenciados y ágiles.

Esta iniciativa de Buró Property y HID, pionera en América Latina, marca un precedente al demostrar que la digitalización del acceso puede integrarse de manera segura y eficiente, ofreciendo a los administradores y usuarios un modelo operativo más ágil, sustentable y preparado para los desafíos del futuro.

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

CyberUP Institute construye la mayor Cyber Arena de Europa y prepara su despliegue en Latinoamérica para reforzar la seguridad IT y OT

Hay un momento, en toda organización, en el que la tecnología deja de ser suficiente.

No ocurre durante una auditoría. Tampoco en un comité de riesgos. Ocurre en silencio, en el instante exacto en el que un sistema falla, una alerta no se interpreta a tiempo y la operación —real— comienza a verse comprometida.

Es en ese punto donde muchas estructuras descubren su verdadera vulnerabilidad: no la falta de herramientas, sino la falta de preparación.

Durante años, la ciberseguridad se ha construido sobre capas de software, protocolos y normativas. Sin embargo, en sectores críticos —energía, utilities, transporte o infraestructuras estratégicas— el problema es otro: los sistemas no pueden detenerse, los errores no son simulables… y las consecuencias no son digitales, sino físicas.

En este nuevo escenario, emerge un concepto que está redefiniendo la preparación global: la Cyber Arena.

Y en el centro de este cambio, una organización europea ha dado un paso más allá: CyberUP Institute, parte del ecosistema tecnológico de ReputationUP, especializada en el desarrollo de infraestructuras avanzadas de ciberseguridad orientadas a la preparación real de organizaciones, gobiernos y sectores críticos.

La Cyber Arena: donde se entrena lo que no se puede permitir fallar

A diferencia de los entornos tradicionales de formación, una Cyber Arena no enseña. Expone. Presiona. Simula. Obliga a decidir.

Se trata de una infraestructura avanzada capaz de replicar con precisión entornos IT y, especialmente, OT (Operational Technology), integrando sistemas reales como SCADA, PLC o redes industriales dentro de escenarios de ataque completamente controlados.

En estos entornos, los equipos no aprenden desde la teoría, sino enfrentándose a situaciones que reproducen con fidelidad una crisis real sobre infraestructuras críticas.

Pero el verdadero cambio no está en la tecnología. Está en lo que ocurre dentro.

Operadores que deben identificar anomalías en tiempo real. Ingenieros que enfrentan fallos bajo presión operativa. Equipos de respuesta que deben contener un incidente sin margen de error. Directivos que toman decisiones con impacto inmediato en la continuidad del servicio.

No es formación. Es preparación operativa.

"La ciberseguridad no falla por falta de tecnología. Falla cuando las personas no han sido entrenadas para decidir bajo presión." — ***Andrea Baggio CEA EMEA de ReputationUP.***

Andrea Baggio, CEO en Europa

CyberUP Institute: de la formación a la infraestructura

Lo que diferencia a CyberUP Institute no es la capacidad de enseñar ciberseguridad. Es su capacidad de diseñar, construir e implementar entornos completos donde la ciberseguridad se entrena como una disciplina operativa real.

Su modelo —denominado *CyberGround*— no es un simple "cyber range". Es una arquitectura integral concebida como una infraestructura en capas, donde cada nivel cumple una función crítica dentro del entrenamiento.

Desde la base tecnológica hasta la ejecución estratégica, la Cyber Arena se construye sobre cinco pilares interconectados:

- **Infraestructura:** hardware, software y entornos seguros que permiten replicar sistemas reales
- **Integración y personalización:** adaptación completa a los sistemas y operaciones específicas de cada organización
- **Tecnología propietaria:** herramientas avanzadas de gestión, simulación y evaluación del rendimiento en tiempo real
- **Desarrollo de escenarios:** creación de ejercicios basados en amenazas reales y dinámicas del sector
- **Programas de formación:** entrenamiento progresivo adaptado a todos los niveles, desde técnicos hasta alta dirección

Este enfoque transforma la Cyber Arena en algo más que un entorno de simulación. La convierte en una réplica funcional de la organización.

Esto permite algo que hasta ahora era prácticamente imposible: reproducir el comportamiento real de una empresa frente a un ataque, sin poner en riesgo su operación.

"Las organizaciones invierten millones en proteger sistemas que nunca han sido realmente puestos a prueba. La Cyber Arena cambia eso: convierte la teoría en experiencia." — ***Andrea Baggio***

El verdadero gap: lo que no se entrena, falla

En sectores como el energético, el problema no es la falta de inversión en ciberseguridad. Es la falta de entrenamiento en condiciones reales.

Las infraestructuras críticas operan bajo restricciones únicas: no pueden actualizarse con frecuencia, requieren disponibilidad continua y cualquier error tiene impacto inmediato sobre millones de usuarios .

Esto genera un vacío estructural:

- Sistemas protegidos, pero equipos no preparados
- Protocolos definidos, pero no interiorizados
- Tecnología avanzada, pero decisiones humanas no entrenadas

La **Cyber Arena** nace precisamente para cerrar ese gap.

Porque permite repetir, ajustar y perfeccionar escenarios sin ningún riesgo operativo real, creando un aprendizaje iterativo basado en experiencia, no en teoría.

Una infraestructura estratégica para países y sectores críticos

Lo que comenzó como una solución técnica se está consolidando como un modelo estratégico.

La capacidad de desarrollar Cyber Arenas a gran escala —como la más grande de Europa— abre una nueva dimensión en la ciberseguridad nacional e internacional.

No se trata solo de formar profesionales.

Se trata de:

- Elevar el nivel de preparación de sectores críticos
- Fortalecer la resiliencia de infraestructuras nacionales
- Alinear organizaciones con estándares regulatorios cada vez más exigentes
- Crear culturas de seguridad compartidas dentro de grandes sistemas operativos

En este contexto, la posibilidad de replicar este modelo en otras regiones —especialmente en Latinoamérica— adquiere un valor estratégico evidente.

Porque permite a gobiernos y grandes organizaciones pasar de la reacción a la preparación estructurada.

Más allá de la tecnología: una cultura de anticipación

Uno de los impactos menos visibles —pero más profundos— de una Cyber Arena es cultural.

Cuando una organización implementa este tipo de infraestructura, envía un mensaje claro:

La seguridad no es una hipótesis. Es una práctica.

Esto transforma comportamientos:

- Mejora la comunicación entre equipos IT y OT
- Reduce el riesgo humano mediante formación experiencial
- Fomenta la detección temprana de anomalías
- Atrae talento especializado que busca entornos avanzados

Como señalan los propios modelos operativos, la Cyber Arena no solo identifica vulnerabilidades técnicas, sino también fallos en procesos, coordinación y toma de decisiones, antes de que estos se manifiesten en un incidente real .

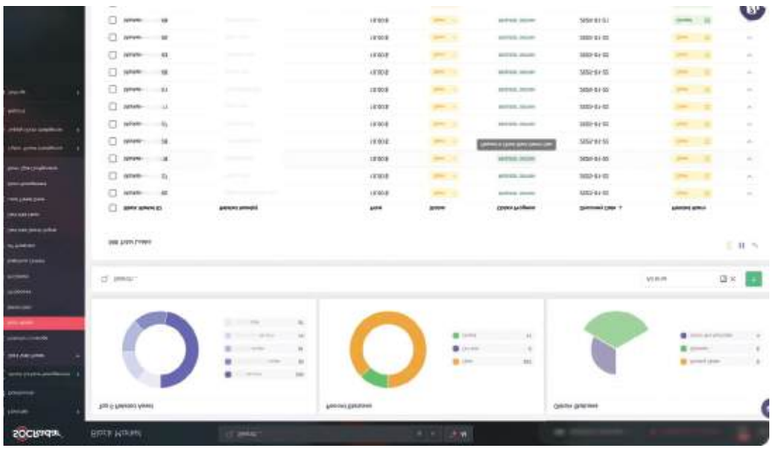
El futuro de la ciberseguridad no se construye, se entrena

Durante años, la pregunta fue: ¿cómo proteger mejor los sistemas?

Hoy, la pregunta es otra: **¿están las personas preparadas cuando los sistemas fallan?**

Hoy, los ataques son cada vez más sofisticados y las infraestructuras más interdependientes, la ventaja competitiva —y estratégica— ya no reside únicamente en la tecnología. Reside en la capacidad de respuesta. Y esa capacidad no se improvisa. Se entrena.

HD Latinoamérica pacta alianza con SOCRadar



La sinergia permite al canal ofrecer una solución para anticipar riesgos antes de que impacten la operación de negocio de sus clientes.

El mayorista mexicano con presencia regional anuncia alianza comercial con SOCRadar, proveedor de la principal plataforma especializada en Extended Threat Intelligence para dar visibilidad temprana sobre riesgos externos, credenciales expuestas, phishing, dark web, superficie de ataque y riesgo de terceros.

La colaboración llega en un contexto crítico: México y otros países de Latinoamérica se encuentran entre los más afectados por intentos de phishing y distribución de malware. En los últimos 12 meses se registraron 286 millones de bloqueos de intentos de phishing en la región, y más del 27% de las empresas sufrió algún tipo de ataque.

Los datos públicos de SOCRadar (Threat Landscape Report) confirman que los riesgos en la región incluyen exposición de credenciales y datos en la dark web. El reto no es solo que haya ataques, sino que muchas organizaciones no tienen visibilidad previa de su exposición externa, lo que permite que los ciberdelincuentes encuentren vectores sin ser detectados.

"Esta alianza une la experiencia regional de HD Latinoamérica con la plataforma de Extended Threat Intelligence de SOCRadar, que brinda visibilidad temprana sobre riesgos externos y credenciales expuestas", señaló Fausto Escobar, CEO de HD Latinoamérica.

La plataforma de Inteligencia de Amenazas Extendida (XTI) de SOCRadar aprovecha la IA y el aprendizaje automático para optimizar la detección de amenazas y proporcionar inteligencia práctica que ayuda a las empresas a defenderse proactivamente contra ciberataques, a través de sus diferentes módulos: Dark Web Monitoring, Threat Intelligence, Attack Surface Management, Brand Protection, Supply Chain Intelligence.

SOCRadar protege: datos valiosos, alta exposición digital, riesgo reputacional y dependencia de terceros.

Beneficios de la alianza:

1. Nueva línea de ingresos recurrentes: Los módulos de Threat Intelligence, Dark Web Monitoring y Attack Surface Management permiten modelos de suscripción, servicios administrados y consultoría continua, no solo venta puntual de licencias.
2. Diferenciación comercial real: El canal deja de competir únicamente en endpoint o firewall y pasa a ofrecer visibilidad externa y reducción de exposición digital, elevando la conversación a nivel CISO y comité ejecutivo
3. Cross-selling natural con portafolio actual: SOCRadar complementa soluciones de las soluciones ofertadas y cumplimiento normativo ya presentes en el ecosistema del canal.
4. Mayor ticket promedio por cliente: Al abordar exposición de marca, terceros y credenciales, se amplía el alcance del proyecto más allá del perímetro tradicional.
5. Posicionamiento estratégico ante clientes enterprise y gobierno: La inteligencia externa fortalece propuestas en sectores regulados, donde la anticipación y monitoreo continuo son diferenciadores clave.

Mercados estratégicos: Finanzas, eCommerce, retail, educación, salud, gobierno, manufactura

Finalmente, Iker Alonso, gerente comercial para México y Latinoamérica, comentó: "Hemos trabajado con HD Latinoamérica desde hace tiempo y nos sentimos muy honrados de hacer este anuncio oficial. Queremos que el canal sepa que cuenta con un aliado confiable con el que puede crecer y fortalecer su negocio".

Tejidos Digitales y Humanos en México (2026)

Nazly Borrero Vásquez
Consultora y Asesora en Gobernanza y Ciberseguridad, PCI.
México

Articulista Invitada

Un viaje jurídico por la protección de datos personales

En un país donde la tecnología permea cada aspecto de la vida —desde la educación, el trabajo y la salud, hasta la forma en que nos relacionamos con el Estado y con los demás— la forma en que se recolecta, procesa, protege o vulnera la información de cada persona ya no es un asunto técnico: es un asunto profundamente humano, social y jurídico. En 2026, México navega por un momento histórico en materia de protección de datos personales. Esta reflexión propone un abordaje jurídico que va más allá de los códigos, destacando cómo las leyes conviven con experiencias concretas de personas, familias y sistemas judiciales.

El latido de una Ley: ¿Qué significa proteger datos personales hoy?

La protección de datos personales ya no es un concepto abstracto guardado en una gaveta académica. Hoy, tocar el tema es tocar lo que define nuestra identidad, dignidad, privacidad y autonomía en un mundo digitalizado.

Desde el 21 de marzo de 2025, entró en vigor una nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México, que vino a sustituir el marco de 2010. Esta reforma surgió en el contexto de una reestructuración de la administración pública y de la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

(INAI), cuyas funciones ahora recaen en la Secretaría de Anticorrupción y Buen Gobierno.

Biometría: Entre identidad e identificación permanente

Los datos biométricos como huellas digitales, reconocimiento facial, geometría de la mano o incluso patrones de voz son un campo donde convergen seguridad, conveniencia y vulnerabilidad. Jurídicamente, la Ley ya los ubica en la esfera de los datos sensibles, aquellos que pueden afectar gravemente la esfera íntima de una persona si son mal utilizados.

Este reconocimiento legal no es decorativo. Las sanciones por el uso indebido de datos biométricos pueden ser altísimas, con multas que van desde millones hasta más de 70 millones de pesos cuando se trata de información sensible mal protegida.

La legislación mexicana contempla expresamente que, con respecto a menores de edad, debe privilegiarse siempre su protección integral, en términos de su privacidad, datos sensibles e integridad personal. Esto implica, por ejemplo:

La Ley en el banquillo forense: Evidencia digital en procesos judiciales

Una dimensión esencial de la protección de datos es su impacto en la práctica forense y judicial. Los profesionales del derecho, peritos y forenses saben que no toda evidencia digital es igual: estamos hablando de huellas que pueden reconstruir una cadena de acciones, interacciones humanas y momentos vitales.

Los juicios del siglo XXI casi siempre incluyen elementos digitales: mensajes, ubicaciones, accesos, fotos, biometría, metadatos… pero cada uno de estos elementos contiene datos personales que involucran derechos fundamentales.

El reto para los operadores jurídico-forenses es doble:

- Garantizar la integridad probatoria, sin violar principios constitucionales sobre privacidad y acceso a la información.
- Resguardar la dignidad de las personas, incluso cuando son investigadas, víctimas o testigos.

La protección de datos no puede verse como un obstáculo técnico para la justicia: cuando los peritos extraen evidencia de un dispositivo móvil, por ejemplo, deben aplicar criterios estrictos de pertinencia, proporcionalidad y legalidad, asegurando que solo lo estrictamente necesario sea analizado, conservado y presentado. Esto implica que, para los operadores judiciales, la cadena de custodia digital no es solo un proceso técnico: es parte de la garantía de justicia con mirada ética y humana.

El Rol de la autoridad y la sociedad: más allá de la Ley

En 2026, el entramado jurídico para la protección de datos en México es una construcción en movimiento. La transición de funciones del INAI a la Secretaría de Anticorrupción y Buen Gobierno representa un cambio estructural con implicaciones profundas para la supervisión y protección efectiva de los derechos de las personas.

Organizaciones de la sociedad civil, tribunales y órganos de derechos humanos siguen participando activamente en debates sobre cómo garantizar que los derechos no se queden en el papel, sino que se traduzcan en prácticas respetuosas de la dignidad humana. Por ejemplo, el Tribunal Electoral del Poder Judicial de la Federación ha abordado cómo la protección de datos afecta de manera diferencial a sectores vulnerables como mujeres, niñas y niños, lo cual subraya la importancia de miradas interdisciplinarias y de género.

La protección de datos no es un destino: es un camino continuo donde el derecho, la tecnología y la humanidad convergen para dar sentido a nuestra vida en comunidad. En ese camino, cada profesional jurídico es guardián de algo más que datos: es guardián de la confianza social, la dignidad de las personas y la justicia que merece ser realmente humana.

La seguridad empresarial

necesita saber cómo manejar el mundo NAVI

Dr. Antonio Celso Ribeiro Brasiliano
PhD: Doctor en Filosofía de las Ciencias de la Seguridad Internacional.
Universidad de Cambridge, Inglaterra.
Presidente de Brasiliano INTERISK.
abrasiliano@brasiliano.com.br
Brasil

Articulista Invitada

¡Sabes, tienes que saber usar el nuevo marco ISO/TS 31050!

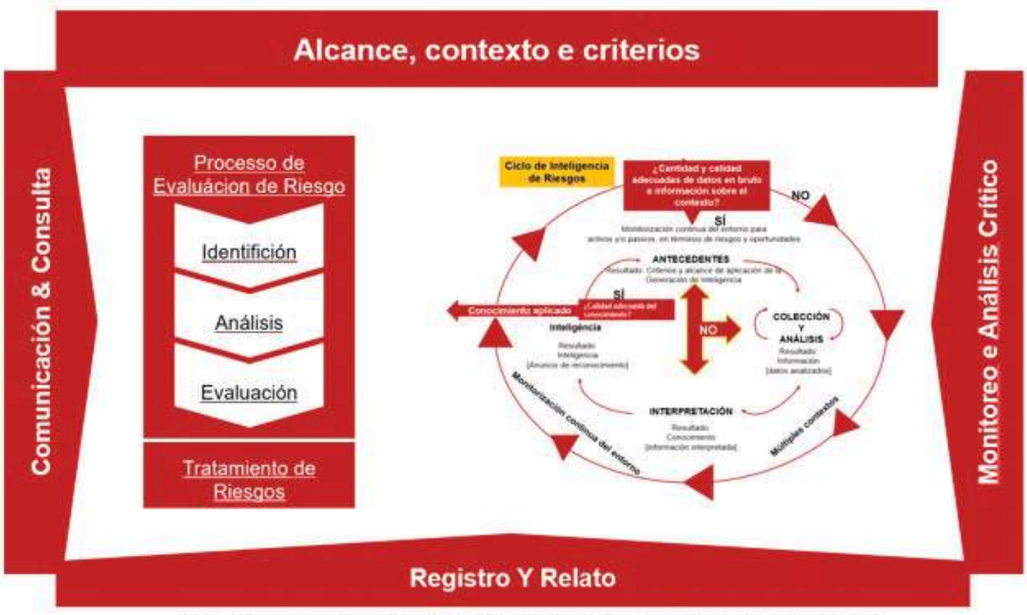
São Paulo, Brasil.- La dinámica del mercado sigue siendo un entorno volátil y muy incierto. Entonces, ¿cómo puede la seguridad empresarial afrontar riesgos y amenazas emergentes, que pueden surgir exponencialmente?

Ya hemos experimentado un mundo llamado VUCA – Volátil, Incierto, Complejo y Ambiguo, desde los años 90 hasta la pandemia de Covid-19. En la pandemia entramos en el mundo BANI – donde no podíamos ser frágiles, tuvimos que tomar decisiones muy rápidas, pero sin ansiedad, no lineales, exponenciales y el mundo era incomprensible y tuvimos que saber cómo lidiar con todo esto.

La pandemia ha sido controlada y el mundo VUCA y BANI no han desaparecido, pero son insuficientes para entender el mundo en el que vivimos ahora. Hemos pasado de un único vector: la disrupción tecnológica, a las actuales disrupciones multidimensionales, interconectadas y sistémicas. Este nuevo entorno fue designado por la consultora internacional E&Y, del mundo NAVI, que presenta las siguientes características:

1. No lineal - N
El crimen organizado está lleno de cambios no lineales, desde el estallido de estructuras faccionales hasta empresas criminales internacionales, pasando por algunos casos en políticas gubernamentales. El reto central para los líderes de seguridad empresarial es reinventar modelos y prácticas operativas que se diseñaron para un mundo lineal. Necesitamos cambiar nuestra mentalidad, pensar de forma amplia, con numerosas variables ocurriendo al mismo tiempo.

2. Acelerado - A
El cambio se está acelerando. Por ejemplo, la IA en la seguridad empresarial avanza a un ritmo sin precedentes, batiendo récords en la velocidad de adopción por parte de los usuarios



Nuevo marco ISO 31050: Riesgos emergentes

en el lanzamiento y en el ritmo acelerado de nuevas funciones. Otras tecnologías que mejoran a un ritmo rápido van desde la robótica y la tecnología de baterías hasta tecnologías de energías renovables como la eólica y la solar. El cambio climático se está acelerando en varios frentes, desde la tasa de deshielo de las capas de hielo hasta la frecuencia y el coste de los desastres naturales.

Pasamos de un cambio en 10 años a uno literalmente de la noche a la mañana, esto se acelera, el mundo con cambios simultáneos, lo que nos lleva a seguir y monitorizar todos estos cambios.

3. Volátil - V

La política se está realineando y polarizando cada vez más, aumentando la probabilidad de cambios significativos, lo que afecta a la línea de seguridad empresarial. Para los líderes empresariales y de seguridad gubernamental, navegar por este espacio volátil es mucho más complicado. Más que nunca, la seguridad empresarial debe demostrar que los servicios están mejorando, aumentando la resiliencia operativa y estratégica, con el impulso hacia la innovación.

Esta volatilidad tiene implicaciones para todas las iniciativas de seguridad empresarial, desde los recursos tecnológicos, sus procesos y la mano de obra. Esta tríada debe estar sincronizada. Se están rompiendo muchos paradigmas en la seguridad empresarial.

4. Interconectados – Interconectividad – I

El mundo de NAVI es aquel en el que las tendencias están más interconectadas, lo que significa que los choques exógenos pueden desencadenar cascadas de impactos, que a menudo culminan en resultados inesperados. Tenemos que saber qué riesgos son los que impulsan, cuáles son los que dejan al medio ambiente incierto y cuáles dependen. Este conocimiento es fundamental para ver el futuro.

Estas interconexiones suponen un desafío para los líderes de seguridad empresarial, ya que requieren contar con un marco sólido, metodologías de interconectividad de riesgos y saber cómo prospectar lo que puede desencadenar una cascada de impactos indirectos que culminan en una gran interrupción en su negocio. Para afrontar estos retos y prosperar en un mundo NAVI, las áreas de seguridad empresarial necesitan un enfoque de dos frentes: utilizar planificación de escenarios interconectada con inteligencia de negocio y la visión de riesgos a medio y corto plazo, para amenazas y riesgos que puedan afectar a procesos empresariales críticos.

Para ello, nuestra recomendación es utilizar el Marco ISO/TS 31050, que se publicó mundialmente en octubre de 2023. Describe que los escenarios prospectivos, la inteligencia y la gestión de riesgos deben formar parte de un único proceso, como se muestra en la figura siguiente:

Es un proceso muy avanzado y hecho para hoy. Fundamental para el área de Seguridad Corporativa. En próximos artículos detallaré el proceso anterior, con el uso de la Plataforma.

El año de la resiliencia: ¿qué demandará de los CISOs el 2026?

Riesgo impulsado por la Inteligencia Artificial, disrupciones geopolíticas y continuas ciber presiones, están impulsando a los CISOs a repensar la resiliencia, la gobernanza y la continuidad del negocio.

Recientemente, Fortinet publicó “Las predicciones de los CISO para 2026”, que señalan las tendencias que están marcando el año, incluyendo la rápida adopción de la Inteligencia Artificial (IA) a través de toda la función del negocio, la creciente tensión geopolítica, la presión regulatoria y la continua industrialización del cibercrimen. La conclusión fue clara: la superficie de ataque se está expandiendo más rápido que lo que los modelos tradicionales de seguridad se pueden adaptar.

Mientras que estas predicciones explican lo que viene, los CISOs tendrán que decidir cómo afrontar estos retos en un ambiente en donde la IA acelera ambos: innovación y riesgo. De acuerdo con la mirada global de ciberseguridad del Foro Económico Mundial (GCO) 2025, 72% de las organizaciones reportó un incremento en ciber riesgos el año pasado. El 2026, ese riesgo será incrementado por sistemas de IA tomando decisiones a velocidad de máquina, usualmente fuera de los flujos tradicionales de seguridad. La resiliencia ya no es solo un producto secundario de seguridad. Debe ser un principio organizador.

De CISO a director de resiliencia

El límite entre riesgo de TI y riesgo de negocio ha colapsado, acelerado por la integración profunda de IA a las operaciones, toma de decisiones y fidelización del cliente. Los sistemas de IA ahora influencian cadenas de suministro, controles financieros, decisiones de contratación e interacciones con cliente, usualmente con mínima intervención humana.

Como resultado, los CISOs ya no son solamente responsables de asegurar sistemas. Son responsables de asegurar que los procesos de negocio impulsados por IA continúen confiables, disponibles y controlables bajo estrés. En la práctica, los CISOs han empezado a operar como directores de resiliencia.

Esta evolución refleja la realidad. La IA incremente la velocidad, escala y dependencia. En ese ambiente, cuando una falla ocurre, se propaga más rápido y más lejos. Con esto en mente, en 2026 los CISOs deberán asumir que las disrupciones involucrarán componentes impulsados por IA, ya sea por modelos comprometidos, datos infectados, agentes manipulados o mal uso de la automatización. El éxito será medido por qué tan bien las organizaciones absorben y contienen esas fallas.

¿Qué estuvieron escuchando los CISOs en el Foro Económico Mundial y por qué el 2026 es diferente?

Las discusiones dentro de la reunión anual de Foro Económico Mundial han llevado decisivamente la IA más allá de una discusión puramente tecnológica. Es ahora tratada como riesgo de gobernanza o problema de resiliencia, con implicaciones directas en estabilidad económica, infraestructura nacional y confianza global. Las conversaciones han incrementado el foco en la exposición sistémica: la concentración de las capacidades de IA, la dependencia a modelos compartidos, la dependencia de datos interfronterizo y el riesgo de falla en cascada cuando los sistemas altamente conectados y automatizados se comportan de un modo no esperado.

Fortinet participó en estas discusiones, incluyendo la Reunión Anual de Davos, de la mano de líderes gubernamentales, ejecutivos de la industria y profesionales de la seguridad, porque lo que sucede en estos foros influye en cómo el riesgo es entendido y manejado a nivel global. La ciberseguridad ya no es entendida solamente como un problema empresarial, sino como una responsabilidad compartida que involucra al sector público y al privado. Para los CISOs, estas conversaciones importan porque influencian la dirección regulatoria, expectativas ejecutivas y los estándares por los cuales la resiliencia será juzgada.

Este cambio está también reflejado en los modelos de gobernanza organizacional. Los CISO están ganando acceso directo al liderazgo ejecutivo porque ahora las juntas directivas reconocen que los riesgos relacionados a la IA no pueden ser delegados a equipos aislados. En lugar de eso, las decisiones sobre el despliegue de IA, acceso a datos, automatización y control de estructuras tienen impacto directo en la continuidad operacional, exposición regulatoria y la reputación corporativa.

Para los CISOs, la implicación es clara. En 2026, la planeación de resiliencia debe considerar explícitamente la escala, velocidad y opacidad impulsadas por IA. La cuestión no es si la IA será utilizada, sino si está siendo desplegada de un modo seguro, transparente y alineado con la tolerancia al riesgo organizacional. Las discusiones que ocurrieron de Davos reforzaron que esto ya no es sólo una preocupación teórica, es una responsabilidad a nivel liderazgo.

Cinco estrategias que los CISO deben adoptar en 2026

1: Construir para la continuidad de negocio en una empresa impulsada por IA.

La disrupción a gran escala no es hipotética. La IA incrementa tanto la posibilidad como el alcance de una falla. Debido a esto, la planeación de continuidad del negocio deberá evolucionar de acuerdo con ello. Para empezar, los CISO deberán redefinir el Mínimo Viable de Negocio de la organización, tomando en cuenta las dependencias a IA. ¿Qué sistemas impulsados por IA son indispensables para seguir operando? ¿Qué decisiones automatizadas deberán ser pausadas o eliminadas durante un incidente? ¿Qué pasa si un modelo, configuración de datos o agente se convierte en poco confiable o queda indispuesto?

La resiliencia en 2026 significa comprender no sólo como los sistemas fallan, sino como la IA amplifica esas fallas. Los planes tradicionales de continuidad, rara vez toman en cuenta el comportamiento de la IA bajo estrés y eso debe cambiar. Adicional a ello, los simulacros deben incluir ahora escenarios de falla de IA, canales de datos corruptos y acciones autónomas que requieran una rápida intervención humana.

2: Tratar a la IA como una capacidad de alto riesgo.

La IA está siendo cada vez más integrada en toda la empresa, a menudo fuera de la visibilidad de seguridad tradicional. Los equipos de marketing utilizan herramientas generativas. Los desarrolladores integran modelos externos. Las unidades de negocio implementan la automatización para acelerar las decisiones. Cada uno de estos factores conlleva riesgos.

Los sistemas de IA pueden filtrar datos confidenciales, ser manipulados mediante órdenes de adversarios o ser obligados a adoptar comportamientos inseguros mediante la inyección inmediata. Además, la IA agéntica introduce una complejidad adicional, ya que los agentes autónomos interactúan con otros sistemas e identidades sin supervisión humana directa.

En 2026, los CISOs deberán tratar la IA como una capacidad de alto riesgo que exige una gobernanza explícita. Esto incluye definir la propiedad, aplicar controles de acceso, proteger los datos de entrenamiento e inferencia, y supervisar el comportamiento de la IA en producción. La IA debe estar sujeta al mismo escrutinio que cualquier sistema capaz de impactar significativamente el negocio.

3: Reforzar controles de identidad para humanos, máquinas y agentes de IA.

La identidad se ha convertido en el plano de control de los entornos modernos y la IA está acelerando la complejidad de dichos entornos. Las “Predicciones CISO 2026” destacaron la identidad no humana como una fuente creciente de riesgo sistémico. Una sola identidad de máquina o agente comprometida puede propagarse por entornos en segundos. Hoy, las identidades no humanas ya superan en número a los usuarios humanos en muchas organizaciones. Los agentes de IA añaden una nueva capa al autenticar, consultar sistemas y tomar medidas a gran escala.

En una empresa impulsada por IA, la vulneración de la identidad no es solo un incidente de seguridad. Es una falla de resiliencia. Los CISOs deben garantizar que los controles de identidad sean consistentes entre usuarios, máquinas, APIs y agentes de IA, con verificación continua y aplicación de privilegios mínimos. Al mismo tiempo, la gobernanza de la identidad también debe asumir la automatización, escalabilidad y velocidad.

4: Reforzar la colaboración al tiempo que la IA borra los límites tradicionales.

La IA disuelve las fronteras organizacionales tradicionales. Las decisiones que antes tomaban las personas ahora se distribuyen entre sistemas, equipos y flujos de trabajo automatizados. Durante los incidentes, esta complejidad puede ralentizar la respuesta si las funciones y responsabilidades no están claras.

Ninguna organización puede desarrollar resiliencia ante la IA de forma aislada. En cambio, la resiliencia depende de la colaboración. Para lograrlo, los CISOs deben alinear los liderazgos de seguridad, TI, ciencia de datos, legal, riesgo y ejecutivo con supuestos compartidos sobre los riesgos y la respuesta ante la IA. Y externamente, la colaboración con colegas, socios y organizaciones del sector público se vuelve aún más crucial a medida que las amenazas impulsadas por la IA se expanden globalmente.

5: Asumir la disrupción acelerada por IA y mantenerse adaptativo.

La IA acorta los plazos. Los atacantes se adaptan más rápido. Los errores se propagan con mayor rapidez. Las expectativas regulatorias evolucionan con mayor rapidez. En este entorno, la mentalidad adecuada es asumir una disrupción acelerada por la IA.

Esta mentalidad prioriza las pruebas continuas, la reevaluación periódica de los casos de uso de la IA y la rápida retroalimentación entre los equipos de seguridad y de negocio. Las organizaciones resilientes consideran la adaptación como una disciplina continua, no como una revisión anual.

La resiliencia como líderes es imperativa en la era de la IA

El rol del CISO nunca ha sido tan amplio ni trascendental. En 2026, los CISOs eficaces serán aquellos que entiendan la IA no solo como una tecnología, sino como una fuerza que transforma el riesgo, la gobernanza y la continuidad.

La resiliencia favorecerá a los líderes que se preparen para la disrupción impulsada por la IA, pongan a prueba sus suposiciones y garanticen que sus organizaciones puedan seguir operando cuando los sistemas automatizados fallen. Esa es la labor del CISO moderno.

Carl Windsor, Chief Information Security Officer (CISO) de Fortinet

Tendencias que definen el mercado del blindaje en México

Parte 2 de 2

En la primera parte de este artículo, se mencionó del impacto que actualmente los niveles de inseguridad en México han aumentado en el último año a lo largo y ancho del territorio nacional, así como para los habitantes de zonas federales y urbanas.

Por ello, la situación ha desencadenado una mayor demanda de los diferentes tipos de blindajes (automotriz, táctico y corporal) en sus diferentes niveles. Hoy, la industria del blindaje en nuestro país enfrenta un impacto de la inseguridad del sector, esto debido a la práctica desleal de empresas "patito" que abaratan los procesos de blindaje, lo que afecta de manera directa a las blindadoras establecidas.

En esta segunda entrega estimado lector, ofrecemos información de los diferentes tipos de blindaje, y como la industria establecida provee de datos valiosos ante esta problemática que inseguridad general en la que vivimos.

Blindaje táctico

- "Monstruos", el reflejo del mercado clandestino

Acerca del mercado del blindaje de vehículos tácticos en México, Gadi Mokotov pronosticó que se espera un crecimiento de entre 15 y 20% en ventas, y las organizaciones

- La mayoría de las ventas de blindaje corporal se van al sector gobierno, como la secretaría de la Defensa Nacional, de Marina, entre otras, señala la AIB.
- De un 100% de que lo que se produce de blindaje táctico en México, alrededor del 90% se queda en el mercado local.

que más están comprando este tipo de acorazado son los gobiernos estatales y federal.

Evidenció que actualmente en este tipo de blindaje —enfocado al gobierno— existe un "hueco" en el marco normativo y debido a eso se están fabricando muchos camiones de forma clandestina denominados "monstruos", con materiales que se consiguen de forma ilegal y cuyas unidades las emplea la delincuencia organizada para atacar a las autoridades.

Mokotov reconoció que es muy difícil cerrar de forma hermética ese "hueco" y que se dejen de producir este tipo de unidades, pero consideró que con mayor regulación tanto para proveedores, fabricantes y para quienes importan los materiales, se podría reducir la fabricación.

Cuestionado de qué tan grande es este mercado clandestino, Gadi Mokotov respondió que en el Consejo Nacional de la Industria de la Balística (CNB) no cuentan con cifras, pero "podemos ver que las autoridades a cada rato decomisan unidades o encuentran talleres, pero siguen circulando y los siguen fabricando. En redes sociales se ven caravanas de estas unidades, sí es muy común en México, desgraciadamente", expresó.

En cuanto a las innovaciones tecnológicas del blindaje táctico, el presidente del CNB refirió que actualmente la tecnología que se está incorporando a México es anti drones, ya que cada vez se están viendo más ataques con estos vehículos aéreos y con diferentes tipos de explosivos que atentan contra la seguridad de las fuerzas del orden.

Gadi Mokotov contextualizó que las unidades tácticas se usan para diferentes modalidades, desde el traslado de reos, operativos especiales de los grupos tácticos de las policías y fiscalías, hasta en los retenes que se llevan a cabo en el país.

• Centroamérica, destino de exportación

De acuerdo con datos del CNB, México exporta vehículos tácticos principalmente a Centroamérica, a países como El Salvador, Guatemala y Ecuador. Sin embargo, no existen cifras oficiales de cuánto es lo que se envía, sino únicamente se cuenta con los datos de las ventas de cada empresa blindadora.

"México es referencia en la fabricación de vehículos tácticos a pesar de que no hay muchos fabricantes de este tipo de unidades… No es tan común o tan grande este mercado como otros países que tienen mayor exportación como Estados Unidos y Canadá, quienes son los principales fabricantes de tácticos", y también se está exportando a Europa, afirmó Gadi Mokotov.

No obstante, reconoció que a nivel mundial México todavía no es referencia. Resaltó que en el país no existen muchas empresas dedicadas al blindaje táctico de forma continua y no todas pertenecen al Consejo, e indicó que, a diferencia de los vehículos ejecutivos, el proceso de blindado de los tácticos requiere mayor desarrollo y capacidad.

El presidente del CNB calculó que de un 100% de que lo que se produce de blindaje táctico en México, alrededor del 90% se queda en el mercado local y del 10% es lo que se exporta. "Es aún poco, no es un número que tenga sustento, no hay un estudio o una base de datos que sea exacta, es aproximada la cifra", aclaró.

Tres elementos sustanciales de un buen blindado:

1. Resistencia balística específica. Un blindado no es simplemente contra armas largas o cortas, sino que tiene que agrupar la resistencia balística para un determinado número de proyectiles, que tienen una forma y una estructura a nivel de ese proyectil y poseen una determinada velocidad.
2. Movilidad extendida. Significa cómo ese vehículo va a salir de la zona de riesgo una vez que ha sido impactado o se encuentra tácticamente bloqueado, ahí es donde juegan un papel importante los insertos y los neumáticos runflats.
3. Originalidad funcional. Es decir, que el vehículo debería preservar el mayor número de capacidades mecánicas y electrónicas, posterior al proceso de blindaje.

Fuente: ProRescue México

Blindaje corporal

• ¿Cuánto crece el mercado?

Gabriel Hernández Baca, presidente de la Asociación Intercontinental de Blindadores (AIB), manifestó que este mercado de protección corporal para las fuerzas policiacas está creciendo gracias a que el gobierno federal está incentivando programas de actualización de equipamiento.

La mayoría de las ventas de este blindaje se van al sector gobierno: la secretarías de la Defensa Nacional, y de Marina, Estatales de Seguridad y Direcciones de Seguridad de diversos municipios, quienes tienen su propia policía, informó Hernández Baca.

Estimó que alrededor del 90% o más del blindaje corporal se va a este sector.

Hernández Baca detalló que actualmente se observa un incremento del mercado de prendas balísticas y para este año se espera un crecimiento del 5%, específicamente en este segmento.

Por su parte, Gadi Mokotov complementó que para este 2026 se prevé un incremento en ventas de alrededor del 10% en blindaje corporal, sobre todo enel segmento de chalecos,

Gadi Mokotov, presidente del CNB.

Gabriel Hernández Baca, presidente de la AIB.

pues dijo que éstos tienen caducidad y cada cierto tiempo las corporaciones policiacas y necesitan cambiarlos.

Gabriel Hernández Baca enfatizó que los países en donde el blindaje corporal mexicano tiene mayor penetración son Ecuador, Perú, El Salvador y Guatemala; además se exporta de manera importante a Europa y a Norteamérica.

El titular de la AIB hizo una comparación del crecimiento que ha adquirido el blindaje corporal en Latinoamérica e Hispanoamérica. De Latinoamérica, afirmó que Brasil se menciona aparte, “es un mercado muy grande por sí solo y muy proteccionista en el cual ni les podemos vender y ellos tampoco salen a vendernos a nosotros, pero hablando del mercado hispanoparlante, México es líder en protección corporal y no dudo que también en blindaje automotriz”.

No obstante, consideró que en el territorio mexicano aún falta mayor cultura y conciencia de la gente para reconocer que actividades económicas como las de empresarios, comerciantes, carniceros, vendedores de frutas y verduras u otros tipos de microempresarios están expuestos a riesgos y que sí les puede ser útil contar con protección corporal.

Ejemplificó que hay casos de médicos y abogados en México que por su profesión han salvado su vida gracias a alguna prenda blindada. Sin embargo, evidenció que el personal de algunas casas de cambio no cuenta con chalecos antibalas y es sujeto de altos riesgos.

• Productos más ligeros contra más amenazas

En cuanto a las innovaciones en los materiales, Gadi Mokotov consideró que, a diferencia de la electrónica, los fabricantes no lanzan desarrollos todos los años o cada mes. Afirmó que las blindadoras siempre buscan materiales balísticos que sean más resistentes, menos pesados y más delgados, así como telas transparentes, pues consideran que la duración de la jornada del uniformado y el calor pueden afectar su operación, si no cuentan con chalecos más ligeros.

Por su parte, Gabriel Hernández documentó que, gracias a la combinación de diversos materiales más innovadores como aramidas, polietilenos y cerámicas para rangos de muy alto performance, los fabricantes han podido reducir el peso de los chalecos hasta 40% en los diferentes niveles, lo cual, apuntó, son muy buenas noticias para las corporaciones.

Para uso ejecutivo, Gabriel Hernández desglosó que se han mejorado las camisetas y los chalecos para la protección corporal, pero destacó que lo más nuevo —y cuya demanda está en ascenso— es toda la línea de portafolios y mochilas blindadas. El usuario que los compra es aquel que quizá no tiene acceso al blindaje vehicular, por lo que busca mantenerse seguro para que, en caso de un atentado, pueda utilizar estos productos como un escudo, indicó.

> En 2023 y 2024, las empresas asociadas a la AMBA registraron crecimientos históricos cercanos al 20%, en parte gracias a que se sumaron un par de compañías más. Para el cierre de 2026 esperan crecer cerca de 10%

La demanda de estos productos se ha elevado en Tamaulipas y Sinaloa, por la guerra contra el narcotráfico. “Pero también ha aumentado su compra en Veracruz y Michoacán, así como en estados del sureste como Chiapas y Tabasco, incluso en la zona hotelera de la Riviera Maya, en donde se han incrementado los niveles de criminalidad”, explicó.

Gabriel Hernández abundó que hay innovaciones en cascos balísticos para fuerzas tanto policiacas como militares, y afirmó que México

es de los pocos países que cuenta con una de las fábricas más modernas de cascos balísticos que les permiten a las corporaciones tener un producto de la mejor calidad, más ligero y que protege contra una mayor cantidad de amenazas.

• Venta de chalecos a “mitad de precio” en Mercado Libre

De acuerdo con el CNB, entre los productos irregulares más frecuentes en el mercado informal se encuentran los chalecos. Al respecto, Gadi Mokotov aseguró que este tema afecta a toda la industria y no es exclusivo solo de los chalecos, sino también de los vehículos.

En estos casos hay “empresas que no están registradas ante las autoridades, que ingresan al país productos chinos o del Oriente de baja calidad, no certificados o que prometen milagros, como con los materiales balísticos que ofrecen cierta resistencia que no coincide con la realidad. Además de la ilegalidad, los “productos milagrosos” ostentan precios que están por debajo del mercado y confunden al cliente y éste, que busca precio, va por ellos pensando que va a tener una protección balística y en realidad no la va a tener”, denunció Mokotov.

Gabriel Hernández reveló que en México existe una gran cantidad de talleres clandestinos que fabrican chalecos sin ninguna certeza de que funcionen de manera adecuada, que no cuentan con certificaciones, con el respaldo de los seguros de responsabilidad civil, ni con registros de las autoridades. Adicional a eso, hay un mercado de productos remanufacturados, ya sea robados o que por caducidad deja de utilizar una corporación, alguna empresa o persona, y los venden como nuevos, alertó.

“Esto nos impacta a la industria por los precios que se manejan. En plataformas como Mercado Libre se pueden encontrar los chalecos hasta la mitad del precio, sí es una situación que compromete porque pone en crisis la credibilidad y honestidad de la vertical de ofrecer precios justos… No se oferta un producto nuevo o garantizado, (pero) el tema es cómo fue construido, con cuántas capas y de qué material está hecho, bajo qué procesos y normas de calidad fue ensamblado para garantizar que sí va a cumplir contra los niveles de amenaza para los que fue hecho”, enfatizó Gabriel Hernández.

El directivo del CNB advirtió a los clientes de la industria del blindaje, especialmente del corporal y vehicular, que no existen “productos milagro” y que cuando adquieran uno, que se oferta a la mitad de precio o menos, que investiguen si es real para no ponerse en riesgo. El “mercado negro” para el tema balístico ronda entre el 35%, confirmó Gadi Mokotov.

Finalmente, Gabriel Hernández recalcó que “es importante que el mercado internacional conozca que México —así como ya es una potencia en la fabricación de autos— en el nicho de blindaje estamos a nivel de las primeras potencias del mundo, tenemos la misma o en algunos casos mejor tecnología, que pueden utilizar tanto los servidores públicos, policías, soldados o personas que requieran proteger su vida”.

Retos del blindaje de vehículos eléctricos:

1. Hacerlos más ligeros. Por el peso de las baterías, las unidades híbridas y eléctricas tienen menos capacidad de carga y, si son más pesadas, consumen más energía y tienen menor autonomía.
2. Seguridad del personal. Debido a que las baterías tienen alta tensión y pueden generar problemas en la integridad del empleado, las blindadoras deben trabajar de la mano de las agencias automotrices en la desconexión y reconexión de estos vehículos.
3. Cuidado de la electrónica. Son baterías sensibles y muy costosas, incluso una de éstas puede costar la mitad de lo que vale el coche, por lo que los blindadores deben tener mucho cuidado en no hacer un corto circuito en el proceso del blindaje y en las soldaduras, a fin de no afectar la parte electrónica.

Fuente: AMBA

GRUPO INDUMIL expande presencia en el sector del blindaje internacional

Grupo Indumil con tres décadas en la industria del blindaje, hoy marca un referente como líder del sector, al englobar diferentes verticales en la protección de personas a través de sus líneas de negocios: **Armor Life Lab, Diamond Glass y Global Armor Blindajes**.

Durante 30 años, la empresa ha consolidado una trayectoria basada en el desarrollo tecnológico que contribuye a la protección de personas, instituciones y organizaciones que operan en contextos donde la seguridad resulta un factor crítico.

Desde su fundación, el Grupo ha construido un modelo empresarial que integra investigación tecnológica, manufactura especializada y presencia en mercados nacionales e internacionales. Esa evolución ha permitido a la compañía posicionarse como un actor relevante en la industria del blindaje en México y América Latina.

El principio que guía a la organización se puede resumir en **“hacer las cosas bien”**, ya que para el Grupo esta idea se traduce en un enfoque integral que abarca desde la concepción del producto hasta los procesos industriales, el cumplimiento regulatorio, la relación con colaboradores y la responsabilidad ambiental. La empresa sostiene que la formalidad empresarial, el desarrollo tecnológico y la calidad del producto deben formar parte de un mismo ecosistema de trabajo.

El desarrollo balístico es el ADN de este negocio; es decir, este concepto define la base tecnológica de la compañía y se refiere al proceso mediante el cual se investigan materiales, se prueban combinaciones y se desarrollan soluciones que permiten crear sistemas de protección cada vez más eficientes.

Según explica la dirección de la empresa, el objetivo consiste en combinar materiales y tecnologías para lograr productos capaces de ofrecer protección efectiva, bajo peso, durabilidad y un costo competitivo.

Durante la inauguración de su nueva planta industrial, el director general de Grupo Indumil, José Eduardo Llanos, explicó el enfoque tecnológico. “El desarrollo balístico consiste en combinar materiales para lograr soluciones que protejan, que sean livianas, que tengan un costo razonable y que mantengan durabilidad”. Esta filosofía de ingeniería aplicada ha permitido a la compañía evolucionar constantemente en el diseño de productos balísticos y ampliar su portafolio de soluciones.

La expansión de Grupo Indumil

Esta se refleja en la inversión destinada a su nueva infraestructura. La empresa inauguró una planta en el parque industrial Plataforma Logística Hidalgo (PLATAH), en Villa de Tezontepec, resultado de una inversión aproximada de 160 millones de pesos, orientada a fortalecer su capacidad de producción de blindaje automotriz, vidrio balístico y protección corporal en un mismo complejo industrial. Dicha inauguración representa uno de los hitos más importantes en su historia. Esta integración permite a la compañía operar bajo un esquema que articula diferentes segmentos de la seguridad.

ALL ARMOR LIFE LAB®

División especializada en protección corporal, ha desarrollado una línea de productos que incluye chalecos balísticos, cascos de protección, escudos tácticos y equipamiento antimotines. Estas soluciones están diseñadas para atender las necesidades de corporaciones policiales, defensa y organizaciones que requieren equipamiento especializado para operar en entornos de riesgo.

John Valbuena, director de Armor Life Lab, explicó que la nueva planta permite incrementar significativamente la capacidad de producción de la empresa: “Nuestra nueva factoría tiene la capacidad de producir 10 mil chalecos

mensuales en un turno de 8 horas, una capacidad que permite atender proyectos de gran escala y responder con rapidez a contratos institucionales y licitaciones internacionales".

DIAMOND GLASS®

La firma especializada en el desarrollo de vidrio balístico. Este tipo de tecnología se utiliza tanto en vehículos blindados como en proyectos arquitectónicos, incluyendo instalaciones estratégicas y edificios corporativos que requieren sistemas de protección reforzada.

La fabricación de vidrio balístico implica procesos de ingeniería complejos que combinan materiales laminados y estructuras diseñadas para resistir impactos de proyectiles sin comprometer la visibilidad ni la integridad del sistema.

El director de Diamond Glass, Germán Padilla, destacó que el desarrollo de estas soluciones implica la participación de equipos multidisciplinarios de ingeniería y diseño: "Detrás de cada metro de vidrio blindado que producimos hay ciencia, ingeniería y talento humano".

GLOBAL ARMOR® BLINDAJES

Es la unidad enfocada en el blindaje automotriz. Este segmento ha adquirido relevancia en el mercado mexicano debido a la creciente demanda de protección ejecutiva por parte de empresas, organizaciones internacionales y clientes corporativos. El blindaje vehicular permite transformar automotores convencionales en unidades capaces de resistir ataques balísticos, integrando sistemas de protección sin comprometer la funcionalidad de la unidad.

Al respecto, Carolina Hoyos, directora de Global Armor, señaló: "Esta planta representa tecnología de punta y soluciones integrales de blindaje para México y Latinoamérica". Subrayó que la instalación fue diseñada para incorporar tecnología avanzada y procesos industriales que permitan mantener estándares elevados de calidad y personalización en los productos.

En términos de mercado, el blindaje automotriz continúa como una solución relevante para la protección de ejecutivos y corporaciones. De acuerdo con información proporcionada por la empresa, un blindaje automotriz Nivel III —uno de los más utilizados para protección urbana— tiene actualmente un costo aproximado de 800 mil pesos más IVA.

Uno de los aspectos que distingue el modelo empresarial de Grupo Indumil es la integración de sus distintas áreas de negocio. La empresa opera bajo un esquema que combina ventas directas al cliente final en el caso del blindaje automotriz, suministro a empresas y proyectos industriales en el caso del vidrio balístico, y comercialización mediante distribuidores en el segmento de protección personal. Este modelo permite ampliar la cobertura comercial del grupo y atender mercados diversos.

Actualmente la empresa cuenta con una red de distribuidores que opera en distintas regiones del país. A través ésta, los productos de Armor Life Lab se comercializan en 22 de los 32 estados de México. Este esquema de distribución facilita la participación de la compañía en procesos de adquisición de gobiernos estatales y municipales, mientras que las ventas a instituciones federales como la secretarías de la Defensa Nacional y de Marina se realizan de manera directa.

La presencia internacional constituye otro componente relevante del crecimiento de la empresa. Grupo Indumil ha participado en proyectos de seguridad en diversos países de América Latina y Europa. Entre los contratos mencionados por la empresa se encuentran proyectos de suministro de chalecos balísticos para Guatemala, Honduras y Perú, además de ventas realizadas a clientes en España, Inglaterra, Colombia y El Salvador.

La compañía también incursiona en ferias internacionales de seguridad y defensa. Uno de los eventos más relevantes en los que ha participado recientemente es Milipol, en París Francia, una de las exposiciones globales más importantes para proveedores de tecnología policial y soluciones de seguridad.

El contexto geopolítico también ha generado oportunidades para fabricantes regionales de tecnología de seguridad. De acuerdo con la dirección de la empresa, Estados Unidos ha dependido históricamente de proveedores asiáticos para diversos componentes de la industria balística. Sin embargo, las tensiones comerciales y los cambios en las cadenas de suministro están impulsando a compradores internacionales a buscar nuevos proveedores en América del Norte.

Para la firma, el objetivo es continuar desarrollando tecnología de protección desde México, fortalecer su presencia en mercados internacionales y contribuir al desarrollo de una industria balística regional capaz de competir en el escenario global.

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 Bladén, Gerente General de Sercop, se desvelaron 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 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 Blandón destaca tres casos emblemáticos:

1. Secancol Limitada: Una compañía con más de 1,200 hombres que gestiona la seguridad de gigantes como GM Colmotores, 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: crecimiento del 200% en su cartera de clientes. Participar en expo México 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.

Alianza internacional:

SERCOPP

MÁS SEGURIDAD Magazine

CON SEGURIDAD Magazine Latam

Ya está en 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

Safety & Security: binomio con tecnología

Mtro. Samuel Hernández Martínez.
Gerente de Seguridad Intramuros GALEAM
Socio Amexsi
https://www.linkedin.com/in/mtro-samuel-h-68941624/
México

Articulista Invitado

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

Parte 1 de 2

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

Durante varios 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.

A muchos profesionales nos tocó vivir la etapa del "no pasa nada" o "siempre se hizo así". Era una cultura donde abundaban las condiciones y actos inseguros, mientras los procesos formales de seguridad existían principalmente para cumplir requisitos regulatorios. Las comisiones de seguridad e higiene generaban reportes que pocas veces se convertían en aprendizaje organizacional, y las investigaciones de incidentes terminaban enfocadas en encontrar responsables más que en identificar las causas que realmente originaban los eventos.

En ese contexto también era común escuchar frases como: "eso no es mi problema". Para algunos equipos de Security su responsabilidad se limitaba a los controles de acceso o a la vigilancia patrimonial, mientras que Safety se concentraba exclusivamente en los accidentes laborales. La realidad es que ambas funciones operaban como silos, cuando en esencia siempre han formado parte del mismo sistema de protección.

Sentadas estas bases, la pregunta relevante hoy es inevitable: ¿Qué fue lo que cambió? ¿Realmente cambió algo?

Tres transformaciones que modificaron la seguridad corporativa

En los últimos años, tres factores han transformado profundamente la forma en que las organizaciones entienden y gestionan la seguridad.

1. La integración de las áreas y la tecnología

La integración de las áreas como una sola, jugando el mismo rol más la tecnología, nos dan un gran paso y profesionalización para la toma de decisiones: saber dónde se puede ir el dinero, dónde ajustar, dónde podemos corregir.

Sin embargo, esto por sí solo no funciona; por esto es necesario integrar un término al cual conocemos como accountability, que significa hacerse cargo de las propias acciones, decisiones y resultados, asumiendo las consecuencias y comprometiéndose a rendir cuentas de forma proactiva y transparente e implica dejar de poner excusas, ser consciente del impacto propio y tener la capacidad y el compromiso de explicar y justificar los actos ante otros o ante uno mismo, buscando soluciones y mejora continua.

2. La comunicación inmediata

Hoy cualquier persona con un teléfono móvil puede registrar y difundir un incidente en cuestión de minutos. Lo que antes permanecía dentro de una operación, hoy puede convertirse rápidamente en un tema mediático. Esto obliga a las organizaciones a responder con mayor rapidez, transparencia y capacidad de gestión.

3. El acceso a mejores prácticas globales

La disponibilidad de información y estándares internacionales ha elevado las expectativas sobre la gestión de la seguridad. Sin embargo, también podemos observar desinformación: personas que creen que por ver un video en redes sociales (reels, tik toks, threads) ya están entrenados, y esto es letal.

Continuara...

“Seguridad con causa” es la apuesta social de **Iniciativa Chapultepec Seguridad por México**

Se llevó a cabo la toma de protesta de la nueva mesa directiva de Iniciativa Chapultepec Seguridad por México, que marcó el inicio formal de la presidencia de Naim Escalante, quien asumió el cargo para encabezar una agenda centrada en la unidad del sector, la profesionalización y una estrategia de acción social.

El acto respondió a una pregunta que no podría considerarse retórica ¿qué puede hacer una organización civil del ámbito de la seguridad en un país atravesado por violencia, desapariciones y vulnerabilidad infantil?

Representantes de asociaciones, empresarios del sector, académicos y miembros de la sociedad civil escuchaban atentos el mensaje del nuevo presidente. Habló con tono firme, consciente de que el sector de la seguridad en México enfrenta una presión constante y una exigencia pública cada vez mayor.

“Seguridad con causa” será el lema de esta nueva etapa. El presidente delineó tres principios rectores: unidad, profesionalización y responsabilidad social. La unidad, dijo, implica coordinación real entre asociaciones, empresas, instituciones y autoridades. La profesionalización exige capacitación constante y apego a la normatividad. La responsabilidad social, sin embargo, fue el eje que marcó el tono de la jornada: la seguridad no se agota en protocolos, se mide por su impacto en la vida de las personas.

Con esa premisa se anunciaron cinco acciones concretas:

La primera, Red de Búsqueda “Hasta Encontrarte”, tiene como propósito acompañar a familias que buscan a personas desaparecidas. El proyecto gestionará recursos para cubrir hospedaje, alimentación y transporte durante las jornadas de búsqueda. Se realizará con el acompañamiento de Elizabeth Martínez y la organización Familias Unidas por una Causa. A la iniciativa se suman Mayra Jazmín Granado Núñez y Denise Meade, quienes participarán en la elaboración de protocolos de atención y acompañamiento para víctimas indirectas de desaparición.

El segundo proyecto, Dignidad sin Muros, se llevará a cabo en mayo y contempla la entrega de al menos 150 paquetes de higiene personal para madres en situación de vulnerabilidad dentro de centros penitenciarios. La consigna es sencilla pero importante: la dignidad no debe perderse en ningún contexto.

En agosto se desarrollará Semillas de Futuro, programa que entregará 150 paquetes de útiles escolares bajo la convicción de que la educación es una herramienta de prevención del delito. Más adelante, el proyecto Navidad con Dignidad buscará reunir 150 despensas para familias que enfrentan violencia y crisis social.

El quinto eje, Cultura de la Legalidad, estará a cargo de Gisela Hernández, quien encabezará en julio la Semana de la Legalidad, con el objetivo de promover el respeto a la ley y fortalecer la corresponsabilidad ciudadana.

Escalante subrayó que los recursos recaudados serán canalizados a través de Familias Unidas A.C., que emitirá recibos deducibles ante la Secretaría de Hacienda. La tesorera Luz Elena Gifar y el secretario Alejandro Rojo supervisarán la transparencia del proceso. A partir de abril, se informará mensualmente el avance de cada iniciativa.

Uno de los momentos más significativos de la ceremonia fue la participación de Denise Meade, fundadora y presidenta de la Fundación Renacer para la Prevención y Atención del Abuso Sexual Infantil. Recordó que México ocupa el primer lugar en abuso sexual infantil entre los países de la OCDE y advirtió la ausencia de programas sólidos de prevención gubernamental. Su fundación trabaja en prevención primaria, secundaria y terciaria, que incluye intervención forense y atención terapéutica a víctimas.

El acto también incluyó la entrega de reconocimientos a Héctor Romero Sánchez, presidente saliente (2023–2024); a Armando Zúñiga, cuyo reconocimiento fue recibido por el Sergio Eduardo Loyola; a Héctor Javier Ramírez Pérez, Vicerrector de la Universidad Panamericana; y a Bernardo Gómez del Campo, reconocido como fundador y líder moral de la iniciativa.

Al concluir, la fotografía grupal selló el relevo institucional; sin embargo, quedó en el aire la pregunta: si estas cinco acciones logran traducirse en resultados medibles, la seguridad habrá dado un paso fuera del discurso técnico para colocarse en el terreno de la corresponsabilidad social. Esa es, al menos, la apuesta de esta nueva presidencia.


Naim Escalante, presidente

PDCA en el Sistema de Gestión de Riesgos CPTED:

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

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

Parte 1 de 2

Quintana Roo, México.- 1. Introducción: 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.

Sin embargo, 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.

> "La seguridad no se diseña una sola vez; se gestiona continuamente. El ciclo PDCA transforma los principios estáticos de CPTED en un sistema vivo, adaptable a la evolución del entorno urbano y sus riesgos emergentes."
>
> Mercedes Escudero

2. Fundamentos: CPTED y el Marco Normativo ISO 22341

2.1 CPTED como Metodología de Gestión de Riesgos

La norma ISO 22341:2021 —Security and resilience — Protective security — Guidelines for crime prevention through environmental design— es el primer estándar internacional que sistematiza los principios CPTED, proporcionando un marco de orientación para gobiernos, planificadores urbanos, arquitectos, ingenieros de seguridad y gestores de riesgo. Establece directrices para la evaluación del entorno, la identificación de riesgos, el diseño de medidas preventivas y la revisión de su eficacia.

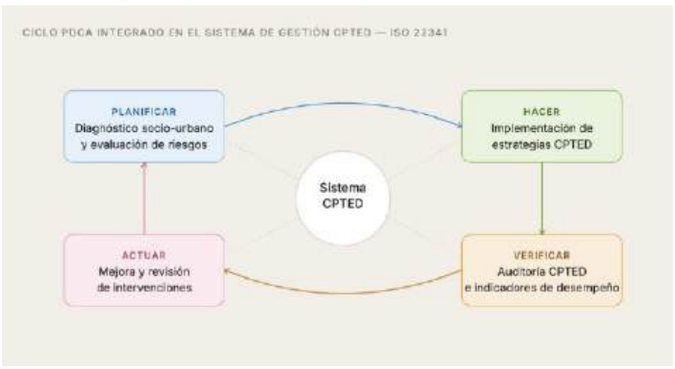
El informe técnico ISO 22341-2:2025 amplía y complementa la norma base con orientaciones específicas para diferentes tipologías de entorno —espacios públicos, infraestructuras críticas, entornos residenciales, comerciales, hospitalarios y de transporte— desarrollando casos de uso y criterios de aplicación más detallados, incluyendo los principios de la denominada "segunda generación CPTED".

2.2 los seis principios CPTED según ISO 22341:2021

1. Vigilancia natural: maximizar las líneas de visión de usuarios legítimos para facilitar la observación del entorno y disuadir comportamientos delictivos. La norma vincula este principio al diseño de iluminación, distribución de usos y control estratégico de la vegetación. (Cláusula 7.2)
2. Control de acceso: gestionar los flujos de entrada y salida mediante elementos físicos y perceptuales —barreras, señalización, configuración espacial— para distinguir entre zonas públicas, semipúblicas y privadas, orientando el movimiento de personas. (Cláusula 7.3)
3. Refuerzo territorial: crear una expresión física del sentido de propiedad e identidad que disuada a los potenciales agresores. Incluye el uso de materiales, paisajismo y señalética que comuniquen cuidado activo y pertenencia comunitaria. (Cláusula 7.4)
4. Mantenimiento y gestión de imagen: preservar el entorno en condiciones que transmitan orden y cuidado, reduciendo señales de abandono que puedan atraer conductas antisociales según la "teoría de las ventanas rotas". (Cláusula 7.5)
5. Soporte a la actividad: fomentar usos y actividades que generen presencia de usuarios legítimos en los espacios, aumentando la vigilancia natural informal y el sentido de comunidad y pertenencia. (Cláusula 7.6)
6. Capacidad de Umbral: fortalecer la resiliencia del entorno ante el crimen organizado, el terrorismo y formas sofisticadas de delincuencia, integrando capas de seguridad complementarias y consideraciones de cohesión social. (ISO 22341-2)

3. El Ciclo PDCA Aplicado a la Gestión de Riesgos CPTED:

El ciclo PDCA estructura el proceso de gestión en cuatro fases iterativas que generan una espiral ascendente de mejora. Su fortaleza reside en que cada ciclo completado proporciona información más precisa y contextualizada para el siguiente, generando un aprendizaje organizacional acumulativo. Aplicado al sistema de gestión de riesgos CPTED, cada fase adquiere un contenido técnico específico alineado con los requisitos normativos.



PLAN FASE 1 Planificar	Diagnóstico socio-espacial, evaluación de amenazas y vulnerabilidades del entorno, identificación de activos a proteger y definición de objetivos CPTED medibles. Incluye análisis de datos delictivos georeferenciados y elaboración de la matriz de riesgos. Alineado con las Cláusulas 5 y 6 de ISO 22341:2021.
DO FASE 2 Hacer	Implementación de estrategias CPTED: intervenciones de diseño urbano, iluminación preventiva, señalética, control de accesos físicos y paisajismo. Capacitación de actores comunitarios y gestores del espacio. Vinculado a las Cláusulas 7 y 8 de ISO 22341:2021 e ISO 22341-2:2025.
CHECK FASE 3 Verificar	Auditorías CPTED periódicas, medición de KPIs de seguridad, análisis comparativo de incidencias antes/después de la intervención, y encuestas de percepción de seguridad a usuarios. Corresponde a la Cláusula 9 de ISO 22341:2021 sobre evaluación del desempeño.
ACT FASE 4 Actuar	Revisión crítica de resultados, identificación de no conformidades y oportunidades de mejora. Actualización del plan CPTED, modificación de intervenciones ineficaces y estandarización de buenas prácticas. Sustentado en la Cláusula 10 de ISO 22341:2021 sobre mejora continua.

4. Trazabilidad con ISO 22341 e ISO 22341-2

La integración del ciclo PDCA con el marco normativo CPTED no es meramente conceptual; existe una correspondencia estructural entre las fases del ciclo y las cláusulas de ambos estándares que permite establecer una trazabilidad formal, verificable y auditable.

Fase PDCA	Actividad de gestión CPTED	ISO 22341:2021	ISO 22341-2
PLAN	Análisis del contexto socio-urbano y del entorno de amenaza	Cláusula 5 — Contexto de la organización	3 — Evaluación por tipología
PLAN	Evaluación de riesgos: amenazas, vulnerabilidades y activos	Cláusula 6 — Planificación y evaluación de riesgos	4 — Metodología CPTED
DO	Diseño e implementación de estrategias de vigilancia natural	Cláusula 7.2 — Vigilancia natural	5.1 — Aplicaciones por tipología
DO	Diseño de control de accesos y refuerzo territorial	Cláusulas 7.3–7.4	5.2–5.3 — Espacios e infraestr.
DO	Implementación de mantenimiento activo y soporte a actividades	Cláusulas 7.5–7.6	5.4 — Gestión operacional
DO	Integración de medidas de segunda generación CPTED y robustez	Cláusula 8 — Operación y control	2 — Segunda generación CPTED
CHECK	Auditoría CPTED y medición de indicadores de desempeño (KPIs)	Cláusula 9.1 — Seguimiento y medición	6 — Herramientas y KPIs
CHECK	Revisión por la dirección y análisis de brechas normativas	Cláusula 9.3 — Revisión por la dirección	6.3 — Procesos de revisión
ACT	Tratamiento de no conformidades y acciones correctivas	Cláusula 10.1 — No conformidades	7.1 — Gestión de mejoras
ACT	Mejora continua y actualización del plan CPTED	Cláusula 10.2 — Mejora continua	7.2 — Ciclos de actualización

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.

Continuará...

Gestión del cambio y Neurociencias

Cintia Gutiérrez
Especialista en Seguridad física y Patrimonial.
Argentina

Articulista Invitada

La biología del cuidado: Por qué las soft skills son la tecnología más avanzada en seguridad.

Buenos Aires, Argentina.- A pesar de las inversiones millonarias en barreras físicas y protocolos, la accidentabilidad en muchas industrias ha alcanzado una meseta persistente. La respuesta no está en añadir más sensores, sino en entender el "software" biológico que toma las decisiones: el cerebro del trabajador y el liderazgo que lo influencia.

Cualquier gerente de planta o especialista en HSE ha experimentado la misma frustración: una organización con certificaciones ISO, procedimientos impecables y equipos de protección de última generación, pero que sigue registrando incidentes por "errores de juicio". Tradicionalmente, la industria ha etiquetado estos eventos como negligencia, falta de actitud o simplemente la fatalidad del "factor humano". Sin embargo, la neurociencia moderna nos ofrece una perspectiva disruptiva que obliga a replantear nuestras estrategias: el error humano suele ser, en realidad, un acierto biológico mal aplicado al entorno industrial.

Estamos intentando gestionar la seguridad del siglo XXI con un cerebro que evolucionó hace miles de años para la supervivencia en la sabana, no para operar puentes grúa o manejar sustancias químicas bajo presión. El desfase entre nuestra biología y nuestro entorno operativo es el verdadero agujero negro de la seguridad industrial.

La economía del cerebro: El origen del atajo

El cerebro humano es una de las máquinas más ineficientes desde el punto de vista energético si se lo compara con cualquier procesador moderno. Representa apenas el 2% del peso corporal, pero consume el 20% de la energía total del organismo. Para sobrevivir evolutivamente, este órgano ha desarrollado una obsesión por la eficiencia, creando "atajos cognitivos" o heurísticas para ahorrar glucosa y procesar la información de manera ultrarrápida.

En el entorno industrial, esta eficiencia biológica se traduce en la automatización de tareas. El cerebro busca patrones. Cuando un operario realiza una maniobra riesgosa por primera vez y no ocurre un accidente, su cerebro no registra una falla, sino un éxito de ahorro: se hizo el trabajo en menos tiempo y con menos esfuerzo mental.

El sistema de recompensa, mediado por la dopamina, refuerza esta conducta. El riesgo se convierte en un hábito ciego antes de que el supervisor más atento pueda detectarlo. El desafío del liderazgo actual, por tanto, no es vigilar la mano que ejecuta, sino comprender los disparadores neurológicos que preceden a la acción. No se trata de "corregir a la persona", sino de reentrenar la percepción del riesgo en un cerebro que, por naturaleza, prefiere la comodidad de lo conocido.

El costo invisible del liderazgo autoritario

Uno de los descubrimientos más críticos para la seguridad industrial contemporánea es el impacto del estrés y el estilo de mando en la toma de decisiones. Durante décadas, el liderazgo basado en el "mando y control" fue la norma. Sin embargo, hoy sabemos que la presión constante por la producción y el miedo al castigo generan un entorno de alta toxicidad química en el equipo que sabotea cualquier protocolo de seguridad.

Bajo estrés percibido, el organismo libera cortisol y adrenalina. Estas sustancias activan la amígdala (el centro de reacción emocional y de supervivencia) y "desconectan" virtualmente la comunicación con la corteza prefrontal. Esta última es la zona del cerebro encargada de las funciones ejecutivas: el pensamiento analítico, la previsión de consecuencias a largo plazo y, fundamentalmente, el cumplimiento de normas complejas.

Un trabajador operando bajo una presión extrema o un liderazgo intimidante no es un trabajador más rápido; es un trabajador biológicamente incapacitado para evaluar riesgos. En este estado, se produce lo que la psicología cognitiva llama "visión de túnel": el foco se estrecha tanto en el objetivo inmediato (terminar la tarea, evitar el regaño) que el cerebro ignora los estímulos periféricos, que es precisamente donde suelen aparecer las señales de peligro. La prioridad cerebral pasa de "trabajar seguro" a "sobrevivir a la amenaza", la cual, irónicamente, suele estar personificada en su propio supervisor.

"Un líder que gestiona desde el miedo no está dirigiendo personas, está activando sistemas de defensa biológica que bloquean la capacidad crítica de evaluar riesgos".

Soft Skills: Los nuevos sensores de precisión en la industria

Para romper la meseta de accidentabilidad y alcanzar la anhelada "Cultura de Seguridad Interdependiente", las organizaciones deben entender que las habilidades blandas (soft skills) no son complementos opcionales o "habilidades tiernas" de relaciones públicas. Son, en rigor, herramientas

técnicas de alta precisión para la gestión de riesgos que actúan sobre el sistema operativo humano.

1. Escucha activa como diagnóstico operativo

En seguridad, la escucha activa no es un acto de cortesía, es una técnica de recolección de datos críticos. Un líder entrenado no solo escucha las palabras, sino que detecta en la comunicación no verbal y en el clima del equipo los signos de fatiga cognitiva. La fatiga es el precursor silencioso del error. Un cerebro cansado toma las mismas decisiones que un cerebro bajo los efectos del alcohol.

Cuando un supervisor desarrolla la habilidad de escuchar “entre líneas”, puede identificar una distracción emocional o una saturación mental en un colaborador antes de que se traduzca en un dedo atrapado o una caída a nivel.

2. Comunicación asertiva y reducción del ruido Cognitivo

El cerebro tiene horror al vacío. Ante una instrucción ambigua o incompleta, el cerebro no se detiene a preguntar en la mayoría de los casos; llena los vacíos de información con suposiciones basadas en experiencias previas. Una instrucción imprecisa es, biológicamente, una invitación al error.

La comunicación asertiva y clara reduce la carga cognitiva del trabajador. Al eliminar la ambigüedad, el líder permite que el operario mantenga sus recursos mentales enfocados exclusivamente en los puntos críticos de control de la tarea. Menos dudas significan menos atajos y, por ende, menos accidentes.

3. Seguridad psicológica: El lubricante del sistema

La neuroplasticidad demuestra que el aprendizaje y la atención plena (mindfulness) solo ocurren en entornos de seguridad psicológica. Si existe temor al reporte, si el error es penalizado sistemáticamente en lugar de ser analizado como una falla del sistema, la organización pierde su activo más valioso: la información sobre los “casi-accidentes”.

Estos eventos son las señales de advertencia que el sistema envía antes del colapso. Un líder con soft skills desarrolladas fomenta un entorno donde el trabajador se siente seguro para levantar la mano y decir “no sé cómo hacer esto” o “casi me accidento”. Esa información es la que permite corregir el proceso antes de que la sangre llegue al río.

La neuroplasticidad aplicada: Reconfigurando la cultura

La buena noticia es que el cerebro es plástico. Esto significa que la cultura de seguridad no es algo estático, sino algo que se construye y se refuerza físicamente en las conexiones neuronales de los trabajadores a través de la repetición y el liderazgo positivo.

Cuando un líder utiliza el reconocimiento en lugar del castigo, activa el circuito de recompensa del trabajador, vinculando la seguridad con una sensación de bienestar y estatus. Esto genera una adherencia a los protocolos mucho más profunda y duradera que la que se obtiene mediante la vigilancia externa. El objetivo final es que el trabajador elija la opción segura no porque alguien lo mira, sino porque su cerebro ha sido condicionado para entender que la seguridad es el único camino eficiente.

La inversión necesaria en el capital neurocognitivo

La madurez de un sistema de gestión de seguridad hoy se mide por la calidad y la profundidad de las interacciones humanas en la línea de fuego. Las empresas que continúan priorizando exclusivamente la inversión en activos físicos —fierros, cámaras y sensores—, postergando el desarrollo de competencias conductuales en sus mandos medios, están dejando el factor más crítico del riesgo al azar de la biología primitiva.

Resulta imperativo que la alta dirección de las compañías industriales reconozca que el entrenamiento en soft skills y neurociencias aplicadas es, en realidad, la actualización más crítica que pueden hacer al “sistema operativo” de la compañía. Una organización que no entiende cómo funciona la mente de su gente está condenada a repetir los mismos accidentes, sin importar cuántos millones gaste en tecnología de protección.

La optimización del presupuesto de prevención debe, por tanto, equilibrar la adquisición de tecnología física con el fortalecimiento del capital neurocognitivo de la organización. Debemos pasar de una seguridad reactiva y punitiva a una seguridad proactiva y biológicamente informada. Al final del día, la prevención más robusta no reside en la resistencia de un material o en la dureza de un casco, sino en la solidez de una cultura de liderazgo capaz de gestionar la complejidad y la fragilidad del factor humano.

SIA, Women In Security Forum 2026

Un espacio seguro para las mujeres de la industria de la seguridad.

SIA, Security Industry Associaton, llevó a cabo la segunda edición de su encuentro con mujeres del sector de la seguridad y la tecnología. Este año, la intención principal fue reunir a estas expertas en los sectores mencionados, y compartir en un espacio seguro experiencias, pero sobre todo para seguir formando comunidad con el propósito de trabajar en estos espacios que brinda la industria para las mujeres.

Kenia Caballero, directora de SIA Capítulo México, hizo hincapié al tiempo que las mujeres invirtieron al estar presentes, ya que el tiempo es uno de los activos más escasos, asimismo resaltó el compromiso que tienen con su crecimiento profesional, pero sobre todo de fortalecer esta comunidad de mujeres.

"Quiero empezar agradeciendo a quienes hicieron posible este desayuno, a nuestras embajadoras y por supuesto nuestros patrocinadores: Axis Communications, Hanwua Vision, Jhonson Control, HID y Milestone. Nada de esto sería posible sin el apoyo de las embajadoras y de ustedes como comunidad," refirió. Recordemos que SIA es un catalizador de éxito para las empresas, para las personas de esta industria de la seguridad que ofrece información e influencia y que a través de sus recursos busca profesionalizar a la industria.

En este encuentro de mujeres, se resaltó la presencia de la invitada especial, la Maestra Sayuri Herrera Román, luchadora social y trabajadora de la Fiscalía General de la República; una mujer con el rol visible y la lucha contra los feminicidios, lo cual es un recordatorio de que la seguridad no solo es tecnología, no es solo negocio, es sistema y es colaboración.

La plática de la invitada especial giró en torno a su experiencia profesional que le llevaron a desarrollar

líneas de investigación y de apoyo a mujeres que fueron violentadas durante su servicio. Asimismo, compartió los retos que esto le ha llevado en su vida y obviamente cómo ha logrado superarlos a lo largo del tiempo, sobre todo por las personas que ha tenido que ayudar.

Con un cierre emotivo, la directora de SIA, así como las diferentes embajadoras, de las diferentes marcas patrocinadoras, ofrecieron un reconocimiento realizado por manos artesanas a la Maestra Herrera, haciendo mención de que se quedaban con el corazón lleno, ya que se sentía en el ambiente la comunidad presente en cada una de las participantes en este encuentro de seguridad y tecnología impartido en el marco del Día Internacional de la Mujer.

Entre la percepción y la realidad

Edison Cadena Ayala
Gerente de SEINNATIONAL CIA. LTDA.
Presidente de AIMCSE Ecuador
Ecuador

Articulista Invitado

El riesgo de gobernar la seguridad desde lo simbólico

Quito, Ecuador.- La seguridad que más se ve no siempre es la que más protege. En América Latina, esta afirmación deja de ser una provocación para convertirse en un diagnóstico incómodo: estamos gestionando, cada vez con mayor frecuencia, la percepción del riesgo en lugar del riesgo mismo.

El despliegue de operativos visibles, tecnología instalada sin integración y controles que priorizan la presencia por encima de la efectividad responde a una lógica que la literatura denomina política simbólica (Edelman, 1964). No se trata de ausencia de acción, sino de una acción orientada a demostrar control más que a ejercerlo. Este desplazamiento es crítico, porque introduce una distorsión estructural en la toma de decisiones: se invierte donde se observa, no donde se necesita.

La evidencia regional es contundente. América Latina concentra aproximadamente el 33% de los homicidios globales con menos del 9% de la población mundial (BID, 2023; UNODC, 2023). Sin embargo, la percepción de inseguridad suele superar los niveles reales de victimización, generando presión para implementar medidas inmediatas, visibles y políticamente rentables, pero de bajo impacto sostenido. Así, la seguridad comienza a operar como narrativa.

Desde un enfoque técnico, esto representa un quiebre con principios fundamentales de gestión del riesgo establecidos en ISO 31000 y el modelo ESRM: identificar activos críticos, analizar amenazas, evaluar vulnerabilidades y diseñar controles integrados bajo defensa en profundidad. Cuando estos elementos se sustituyen por medidas aisladas, la organización —o el Estado— pierde capacidad de anticipación y se vuelve reactivo.

El error de fondo es conceptual y operativo: confundir acción con resultado, presencia con control y actividad con eficacia. Sin métricas, sin indicadores y sin evaluación posterior, la seguridad deja de ser medible y se transforma en una construcción discursiva. En ese contexto, los riesgos no desaparecen; se desplazan, se adaptan y, en muchos casos, se fortalecen.

Esto tiene consecuencias directas: una falsa sensación de control, asignación ineficiente de recursos y, eventualmente, pérdida de confianza institucional. La seguridad simbólica puede tranquilizar en el corto plazo, pero erosiona en el mediano.

El desafío no es eliminar lo visible, sino subordinarlo a lo estructural. La visibilidad debe ser el resultado de una arquitectura de seguridad coherente, no su sustituto. Gobernar la seguridad implica tomar decisiones incómodas, basadas en evidencia, incluso cuando no son inmediatamente visibles.

Porque al final, la diferencia no está en cuánto se hace, sino en cuánto se reduce el riesgo.

"Cuando la seguridad se diseña para ser vista, pierde su capacidad de anticipar. Pero cuando se diseña para gestionar el riesgo, incluso lo invisible protege". Anónimo.

Fuentes consultadas:
Interamericano de Desarrollo. (2023). Seguridad ciudadana en América L Caribe: desafíos y tendencias.
Edelman, M. (1964). The symbolic uses of politics. University of Illinois Press.
International Organization for Standardization. (2018). ISO 31000: Risk man
Guidelines.
ASIS International. (2019). Enterprise Security Risk Management Guideline.
United Nations Office on Drugs and Crime. (2023). Global study on homicide.

Bogotá, Colombia.- Abrir puertas y establecer puentes en la labor que hacemos todos a diario y desde hace 11 años en la Comunidad COLADCA | COLADCA Internacional, permite tener innumerables conversaciones para analizar e implementar acciones que mitiguen y/o controlen los riesgos, cada organización tiene un contexto muy particular, a continuación, uno de ellos como insumo a nuestro proyecto #RepensandoLaSeguridad.

Todo comienza cuando visité una empresa y me encontré con el alucinante mensaje en su recepción que decía: “El mayor riesgo es no asumir ningún riesgo”, fueron pocos los minutos y no me aguante preguntarle al director de riesgos ¿cuál es su apetito de riesgo?, me puedes explicar si el mensaje que acabo de ver ¿refleja la misma instrucción para todas las áreas de la organización?

A lo cual me explicó lo siguiente:
“La nueva junta directiva, luego del análisis de riesgos que presenté, y posterior a varias mesas de trabajo en que se priorizaron y establecieron las metas del 2026, consideró que luego del proceso de evaluación de riesgos, algunas áreas debían asumirlos para poder garantizar su continuidad”, fue muy enfático en que, “NO todos los riesgos se asumían y que NO era una directriz para todas las áreas”, además, dejó claro que “las directivas en años anteriores, explícitamente habían prohibido asumir riesgos” pero que eso cambiaría de ahora en adelante, que la política era “Asumir controladamente”.

Entre muchos aspectos, lo que principalmente me motivó a escribir este artículo, fue lo siguiente:

Es respetable y responsable que la alta dirección de la organización, CEO, gerentes o la denominación que se establezca, no quiera o no desee enfrentar riesgos para el cumplimiento de los objetivos trazados, pero usando ejemplos; si el objetivo es exportar a X país para lograr la expansión a nuevos mercados y no se asumen los riesgos (financieros y estratégicos) no se cumplirá la misión, visión y objetivos institucionales; es lo mismo que, no querer conectar una organización con tienda virtual, marketplace y sitio online a la internet, porque “la materialización del cibercrimen y los ciberdelitos es elevada y estaríamos en riesgo”.

Mi posición y con todo el respeto a los colegas que defienden otra, es que “el riesgo NO se puede eliminar”, algunas personas y cursos de capacitación enseñan lo contrario, pero basta con estudiar un poco más el término de “fuente de riesgo”, para entender que falta mayor explicación de los términos y definiciones de la Gestión del Riesgo.

Ambos difieren totalmente el uno del otro, y en particular, del concepto “a eliminar… El riesgo”, desde allí partiremos en la conversación.

RIESGO
Efecto de la incertidumbre sobre los objetivos.

FUENTE DE RIESGO
Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.

Riesgo creado y responsabilidad derivada
Si bien, cuando se asumen riesgos, habría según la actividad, el contexto de la organización y muchos

aspectos más, unas consecuencias posibles o probables de ocurrencia, igualmente surgen responsabilidades.

La teoría de asumir los riesgos (también conocida como teoría de la asunción del riesgo o assumption of risk en inglés) es un principio que aparece también en el campo del Derecho y su esencia es la siguiente:

Una persona o entidad que conoce un riesgo y decide voluntariamente enfrentarlo, acepta las posibles consecuencias derivadas de él.

Hablemos de Derecho y citemos el "riesgo creado":

La Jurisprudencia trae al escenario propuesto, al responsable de la consecuencia mencionada, esta nos habla del poder que tiene el responsable de evitar el daño, "dominio que la persona u organización tenía o, al menos, habría debido normalmente tener, de su actividad, así como de los hombres o de las cosas por las que el responde".

Entonces, Derecho y Riesgos van de la mano, en particular al observar en el esquema de la mencionada formulación, se prescindiría "del análisis de la culpa como elemento para atribuir aquella y siendo una manifestación de responsabilidad objetiva, algunos consideran, que se basa en la inobservancia de normas de cautela, antes que en una valoración del actuar de la persona y de sus perfiles subjetivos, de ahí que no se recurra a la culpabilidad como criterio de imputación".

La identificación, análisis y gestión de los riesgos de seguridad

En 2024 se publicó el articulo denominado "Security Risks Between Analysis and Assumptions" en español "Riesgos de seguridad, entre análisis y suposiciones" de Carmen-María MOISE, PhD e Irina TĂTARU, PhD, este explicaba que:

"La identificación, el análisis y la gestión de los riesgos de seguridad representan un verdadero desafío para cualquier Estado, especialmente en el contexto geoestratégico actual. Todos ellos forman parte del proceso de gestión de riesgos y no pueden basarse en suposiciones, sino que requieren un enfoque especializado por parte de expertos en la materia. Ningún Estado desarrollado puede permitirse el lujo de dejar los riesgos de seguridad al azar, ya que esto podría poner en peligro su propia existencia como Estado soberano e independiente".

Pero quisiera hacer énfasis en el apartado que cita de forma especial y en el entorno de seguridad actual "la falta de un análisis de riesgos adecuado puede debilitar la capacidad administrativa para responder a nuevas formas de amenazas a la seguridad, tanto regionales como internacionales". Lo cual amplía las responsabilidades del líder o gerente de riesgos, más en la obtención de la "mejor información disponible" para la toma de decisiones informadas, y principalmente para poder asumir el riesgo "real".

Análisis de Riesgos

Acá tenemos problemas, en muchos espacios se entiende que un "estudio de seguridad" es lo mismo que un "análisis de riesgos".

Sin el análisis, las organizaciones de todo

tipo, gobiernos y hasta los seres humanos "no podremos adoptar las medidas apropiadas ni las acciones necesarias para proteger intereses ante vulnerabilidades de cualquier tipo".

Por ello surge y se fortalece la necesidad de un "análisis minucioso y exhaustivo" el cual facilitará la reducción de la exposición a diferentes tipos de riesgos, minimizando así los efectos negativos derivados de la posible materialización de los riesgos de seguridad identificados.

Las autoras del artículo, concluyen muy claramente que "la identificación de riesgos es solo una etapa inicial en el complejo proceso de gestión de riesgos". Esto personalmente me muestra la importancia de la profesión, pero me hace lamentar que por más de 11 años no habíamos identificado un programa de formación especializado para el Gerenciamiento Global de Riesgos, por eso fue necesario que presentaremos nuestra propuesta y se denominó: #WORLDRISKMANAGEMENT.

Notas a resaltar y que explica la norma ISO 31000:

El proceso de la gestión del riesgo "debería" ser una parte integral de la gestión y de la toma de decisiones y se "debería" integrar en la estructura, las operaciones y los procesos de la organización. Explica que este "puede" aplicarse a nivel estratégico, operacional, de programa o de proyecto.

Puede haber muchas aplicaciones del proceso de la gestión del riesgo dentro de la organización, pero hace un llamado a la "adaptación" para lograr objetivos, y apropiadas a los contextos externo e interno en los cuales se aplican.

A lo largo del proceso de la gestión del riesgo "se debería" considerar la naturaleza dinámica y variable del comportamiento humano y de la cultura, como también es importante tener en cuenta que, aunque el proceso de la gestión del riesgo se presenta frecuentemente como secuencial, "en la práctica es iteractivo".

Aristides Contreras Fernández
Presidente Global COLADCA, Comunidad Internacional en Gestión de Riesgos y Seguridad
Colombia

Articulista Invitada

El papel vital de la sociedad civil en el Día Internacional contra la Delincuencia Organizada Transnacional

Rafael Eduardo Bernal Cáceres
Presidente Fundación COLADCA
Vicepresidente Comunidad COLADCA
Comunidad Internacional en Gestión de Riesgos y Seguridad

Colombia

Articulista Invitada

Bogotá, Colombia.- El pasado 15 de noviembre se celebró el Día Internacional para la Prevención y la Lucha contra todas las Formas de Delincuencia Organizada Transnacional, muy bien lo expresó la Sra. Ghada Waly, directora ejecutiva de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), al destacar que: “Los desafíos de la delincuencia organizada son cada vez mayores, pero también lo son las oportunidades de cooperación contra esta amenaza”.

Hablar del crimen organizado en nuestra región se ha vuelto algo diario y común, Colombia permanece en el centro de la conversación, “consolidado como el principal país productor de cocaína en el mundo” igualmente, como el lugar en el que “diferentes grupos criminales han logrado abrirse paso en el narcotráfico a través de alianzas con mafias en todo el mundo.” (Insight Crime, 2024).

El crimen organizado en la región se enfoca en múltiples economías ilícitas, desde la producción, distribución y tráfico de drogas (sustancias controladas), como minería ilegal, tráfico de migrantes, trata de personas y armas, lavado de activos, contrabando, extorsión, cibercrimen y muchas más.

Acorde con el Banco Mundial (2024), el crimen organizado plantea numerosos desafíos para nuestra región: No solo para el bienestar de los ciudadanos, sino también para el crecimiento económico: se cita la incertidumbre, la extorsión e inseguridad, los gastos improductivos en seguridad pública, el aumento en las víctimas de la violencia, los delitos a activos, el narcotráfico, la minería ilegal y los delitos contra la flora y fauna, las comunidades que viven bajo el dominio del crimen organizado, la infiltración en las instituciones estatales, lo cual debilita la calidad de los gobiernos y la provisión de servicios esenciales.

Sociedad civil como parte de la solución

El 12 de diciembre de 2024, 18 países de América Latina y el Caribe lanzaron una alianza regional para abordar el crimen organizado con apoyo del Banco Interamericano de Desarrollo (BID), esta iniciativa incluye a gobiernos, organizaciones multilaterales, sociedad civil y otros actores interesados, lo cual subraya un amplio compromiso para mejorar la seguridad en la región.

Se debe resaltar el papel y la importancia que se le dió a la sociedad civil en esta alianza, como socia para impulsar avances y, además, para brindar ayuda en labores de los gobiernos.

En la integración y reconocimiento de la sociedad civil como actor fundamental en la lucha contra el crimen organizado se observan avances y un gran fortalecimiento, es evidente y como lo afirma Daniel Kempken (2024), "se necesita una tríada de instituciones estatales fuertes con articulación de la sociedad civil y apoyo internacional como elementos mínimos para combatir el crimen organizado".

Naciones Unidas, cita a la sociedad civil como el "tercer sector" de la sociedad, junto con el gobierno y las empresas, por ello ha generado espacios como el Sistema Integrado de Organizaciones de la Sociedad Civil (iCSO) y a las organizaciones no gubernamentales, se les considera entidades de carácter consultivo que tienen acceso al Consejo Económico y Social de la ONU (ECOSOC).

¿Entonces cómo aportar? ¿Cómo vincularnos como parte de la sociedad civil?

UNTOC, Convención de las Naciones contra la Delincuencia Organizada Trasnacional y sus protocolos

Conocida como la "Convención de Palermo" por haberse suscrito en diciembre de 2000 en Palermo, Italia, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, es el instrumento global con que la comunidad internacional, demostró la voluntad política de abordar "Un problema mundial con una reacción mundial", y además, la oportunidad para que los sectores de la sociedad civil, cooperen como parte de las organizaciones no gubernamentales, con otras organizaciones pertinentes y con los Estados Parte de la Convención.

Desde COLADCA, la Comunidad Internacional en Gestión de Riesgos y Seguridad, nos vinculamos y fuimos aprobados por la Unidad de la Sociedad Civil (CSU, por sus siglas en inglés) de UNODC, como una Organización de la Sociedad Civil y partes relevantes no gubernamentales en la lucha contra el Crimen Organizado Transnacional, llevar el gremio, la industria y la profesión de la gestión de riesgos y la seguridad "Al siguiente nivel", requiere que nuestra voz y voto alcance un horizonte global, COLADCA, como un Ecosistema de múltiples partes interesadas, práctica y apoya la mejora continua de la seguridad con participación internacional.

Resaltamos, además que "Una red solo se puede luchar con la articulación y acuerdo de otras redes en el mismo propósito", por eso a la fecha, hacemos parte del proyecto de UNODC titulado "creación de capacidad de la sociedad civil para participar en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC), su mecanismo de revisión y actividades relacionadas".

Gracias a la vinculación como actores representantes de la sociedad civil, nuestros vinculados, investigadores y aliados estrategicos, en la temática de "Crimen Organizado", han podido participar en varias convocatorias a los cursos y formación especializada en la aplicación de la convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, como también en 2024, tuvimos el honor con Aristides Contreras, presidente de COLADCA, ser parte presencialmente del 12º período de sesiones de la Conferencia de las Partes, principal foro político mundial para abordar la Delincuencia Organizada Transnacional a nivel global.

El evento logró un número récord de mil 400 participantes de 131 estados, 15 organizaciones intergubernamentales y 212 organizaciones no gubernamentales se reunieron en la Conferencia, que concluyó tras cinco días de debates centrados en la implementación y el fortalecimiento de medidas para combatir la delincuencia organizada transnacional, incluidas sus formas nuevas y emergentes.

COLADCA tuvo la oportunidad de generar alianzas estrategicas con diferentes gobiernos y organizaciones de la sociedad civil a nivel global, lo cual reafirmó nuestro proposito y compromiso para colaborar en un mundo con más riesgos.

¿Qué sigue como partes relevantes de la sociedad civil?

Invitamos cordialmente a conmemorar el Día Internacional contra la Delincuencia Organizada Transnacional (TOC), que se celebra anualmente el 15 de noviembre, las Naciones Unidas realiza un evento de alto nivel cada año., si requiere más información déjelo saber en: vinculados@coladca.com

Nuestra conversación en COLADCA es activa, contamos con diferentes proyectos para seguir #RepensandoLaSeguridad y será un gusto contar con sus aportes.

#StopOrganizedCrime |
¡Bienvenidos a COLADCA!

Día Internacional contra la Delincuencia Organizada Transnacional

Félix Uribe
Profesional de la Ciberseguridad y la Privacidad; profesor asociado adjunto en la Universidad de Maryland Global Campus, presidente de Capítulo COLADCA en Estados Unidos de América.
https://www.linkedin.com/in/felixuribe/

EUA

Articulista Invitado

No hace mucho tiempo, las tecnologías emergentes se servían a la carta: una innovación a la vez, cuidadosamente probada, adoptada e integrada en la sociedad antes de que llegara la siguiente. Hoy, sin embargo, ya no elegimos de un menú ordenado de opciones individuales. Actualmente nos encontramos ante un vasto bufé tecnológico, donde la Inteligencia Artificial (IA), la Computación Cuántica, el Internet de las Cosas (IoT), el Big Data, los Sistemas Autónomos y el Blockchain, entre otras, se sirven simultáneamente y, cada vez con mayor frecuencia, se combinan en un mismo plato.

La IA se mezcla con el Big Data para potenciar el análisis predictivo; el Blockchain se fusiona con el IoT para reforzar la seguridad de las cadenas de suministro; y los vehículos autónomos dependen de sensores y aprendizaje automático para navegar por su entorno. Cada combinación revela nuevos sabores tecnológicos: algunos exquisitos y prometedores, otros difíciles de digerir. El bufé se sirve en una mesa concurrida donde cada plato ofrece oportunidades e incertidumbres, y las combinaciones pueden ser tan transformadoras como los ingredientes individuales.

Inteligencia Artificial

La Inteligencia Artificial (IA) ocupa hoy un lugar central en el vasto banquete tecnológico. Entre otras cosas, la IA impulsa pronósticos financieros, habilita vehículos autónomos, mejora la ciberseguridad, personaliza el aprendizaje en la educación y detecta fraudes en cuentas bancarias.

Por otro lado, la IA puede ser alimentada con datos incompletos o discriminatorios, que pueden profundizar desigualdades y condicionar decisiones tan sensibles como la contratación laboral, la asignación de viviendas o las sentencias judiciales. La expansión de la vigilancia impulsada por IA amenaza con normalizar el monitoreo constante, ya sea mediante cámaras con reconocimiento facial o el rastro digital que dejamos en las redes sociales, desgastando, poco a poco, la esencia misma de la privacidad.

Por su parte, la automatización está desplazando tanto a trabajadores manuales como a profesionales del derecho, el periodismo o las finanzas, generando inquietudes sobre un futuro laboral incierto y una sociedad cada vez más desigual. A ello se suma el impacto ambiental. Para entrenar y operar modelos de IA, se requieren enormes cantidades de energía, contribuyendo a la contaminación y las emisiones de carbono. Por ello, es prudente acompañar este plato con guarniciones “éticas” para asegurarnos de que lo que consumimos nutra, en lugar de dañar, nuestra salud tecnológica y humana.

Computación cuántica

Busca revolucionar la resolución de problemas, realizando cálculos a velocidades muy superiores a las de las supercomputadoras actuales. Gracias a su capacidad para procesar múltiples estados simultáneamente, promete revolucionar las simulaciones complejas, resolver desafíos de optimización, fortalecer o redefinir la criptografía y acelerar el descubrimiento de nuevos materiales y fármacos. Los beneficios son enormes, pero los riesgos son igualmente altos.

Esta tecnología representa una seria amenaza para la ciberseguridad, ya que podría volver obsoletos los métodos de cifrado actuales, comprometiendo las comunicaciones seguras, los sistemas financieros y los secretos gubernamentales. Por ello, los investigadores se apresuran a desarrollar soluciones de criptografía poscuántica, con el objetivo de garantizar la protección de la información en un futuro donde las computadoras cuánticas sean una realidad cotidiana.

En muchos sentidos, la computación cuántica es como un plato lleno de ingredientes exóticos, “lleno de potencial, pero misterioso y no completamente comprendido por los expertos”, pero depende de cómo se utilice y quién la controle.

Internet de las cosas (IoT)

Es una red inmensa que crece sin cesar, entrelazando el mundo físico y digital. Desde electrodomésticos inteligentes hasta fábricas, hospitales y sistemas de transporte. Estos dispositivos crean redes inteligentes que convierten la vida cotidiana en una red de interacciones basadas en datos.

Sin embargo, cuanto más dispositivos añadimos a este ecosistema conectado, más vulnerabilidades creamos. Cada sensor, cámara o electrodoméstico puede convertirse en un punto de entrada para los atacantes, creando debilidades que son difíciles de detectar y defender. Sin estándares universales de seguridad e interoperabilidad, el panorama del IoT es un mosaico de enlaces frágiles, donde un dispositivo comprometido puede amenazar redes enteras.

Los riesgos son reales y crecientes, desde monitores de bebés secuestrados, hasta vigilancia hasta redes eléctricas

vulnerables a ciberataques; el IoT desprende un aroma de comodidad y eficiencia difícil de resistir, pero "La conveniencia sin seguridad es una receta para el desastre digital".

Big Data

Es como un tazón desbordante en el centro del bufé: vasto, tentador y aparentemente infinito. Cada segundo acumula millones de migas digitales, cuando se analizan, estos enormes conjuntos de datos revelan patrones invisibles a simple vista, anticipan tendencias y guían decisiones más precisas.

Cuando se gestiona correctamente, el Big Data se convierte en un recurso valioso, lleno de información que puede impulsar la innovación y el progreso. No obstante, la misma abundancia del Big Data también lo hace riesgoso. Sin fuertes controles de privacidad, este festín de información puede convertirse rápidamente en una herramienta de vigilancia.

La forma en que se sazona y se sirve es importante, "con transparencia, responsabilidad y salvaguardas éticas, el Big Data puede empoderar a la sociedad"; sin ellas, se puede convertir en un plato muy peligroso para comer.

Sistemas Autónomos

Son los camareros robóticos del bufé: ya no obedecen órdenes, sino que deciden por sí mismos. Desde coches que se conducen solos hasta drones que entregan paquetes y robots que asumen tareas peligrosas.

Sin embargo, los riesgos son tan complejos como la propia tecnología. Las limitaciones técnicas significan que los coches autónomos luchan con condiciones impredecibles, mal tiempo, conductores humanos erráticos o diseños de carreteras inusuales. Los dilemas éticos también son importantes y más allá de los desafíos de codificación, se encuentra un laberinto regulatorio.

Blockchain

Es el postre del bufé del que todos han oído hablar, pero pocos comprenden su receta. Más allá de ser la base de criptomonedas como Bitcoin o Ethereum. En esencia, el blockchain es un libro de contabilidad distribuido, un recetario compartido donde cada entrada es verificada, tiene un sello de tiempo y es casi imposible de cambiar. Su encanto radica en esa promesa de confianza sin intermediarios y de transparencia servida en cada bocado.

Pero, al igual que un plato dulce, demasiado de él puede empalagar el gusto. La energía necesaria para operar el blockchain es enorme, lo que genera preocupaciones ambientales. La volatilidad en los mercados de criptomonedas ha provocado burbujas especulativas que benefician a unos pocos, mientras desestabilizan a muchos. Aunque tiene fama de ser seguro, no es inmune a las estafas, el fraude y las implementaciones defectuosas.

En conclusión, el bufé tecnológico está abierto y los platos varían cada día, cada uno tiene el poder de cambiar las economías, las sociedades e incluso cómo nos vemos a nosotros mismos. Pero, como cualquier festín, comer demasiado rápido corre el riesgo de ahogarse e ignorar los ingredientes puede provocar alergia. Para disfrutar de este festín, necesitamos equilibrio. Principios éticos como guarniciones, regulación como vajilla y el juicio humano como el chef que prepara los platos. En última instancia, el futuro de este bufé depende no solo de lo que se sirve, sino de cuán sabiamente elegimos comer.

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

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

SEGURITEC PERU

15VA FERIA INTERNACIONAL DE SEGURIDAD

MAYO
27 - 29
2026
LIMA-PERÚ

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

¡RESERVE SU STAND HOY!

www.seguritec.thaiscorp.com

Sede

Centro de Exposiciones Jockey

Oficialización

PERÚ Ministerio de Comercio Exterior y Turismo

APROSEC ASOCIACIÓN PRO SEGURIDAD CIUDADANA

Prensa Asociada

MÁS SEGURIDAD Magazine · GLOBAL DEFENSE MAGAZINE · CON SEGURIDAD Magazine Latam

Organiza: Thais Corporation S.A.C. - thais@thaiscorp.com - +51 989-177-352