

SEGUR[🌎]LATAM

REVISTA DE SEGURIDAD INTEGRAL Nº 31 SEGUNDO CUATRIMESTRE 2025



SEGUR[🌎]LATAM

ESPECIAL SEGURIDAD EN LA LOGÍSTICA Y EL 'RETAIL'

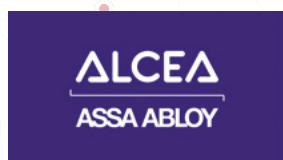


CDMX noviembre de 2025

VII Congreso Mexicano de Protección de Infraestructuras Críticas

Organiza **SEGURILATAM**

Patrocina



SOLICITAR INSCRIPCIÓN

PATROCINA EL EVENTO

De la logística y el 'retail' a las infraestructuras críticas

El pasado mes de julio, el Senado mexicano dio luz verde a un paquete legislativo que aporta un nuevo enfoque a la seguridad pública en el país. Entre las diferentes normas impulsadas cabe destacar la Ley General del Sistema Nacional de Seguridad Pública, que incorpora formalmente la Estrategia Nacional de Seguridad 2024-2030, concebida para anticiparse al delito mediante un enfoque preventivo, la profesionalización de los cuerpos policiales y una inteligencia estratégica reforzada. Asimismo, este nuevo marco regula la coordinación entre Federación, estados y municipios, fomenta la certificación continua y los estándares éticos de los cuerpos policiales e incorpora a la Guardia Nacional, que ha pasado a formar parte de la estructura militar de la Secretaría de la Defensa Nacional (Sedena).

De igual manera, en este número abordamos los desafíos que persisten en la seguridad de sectores fundamentales como la logística y el *retail*. En el ámbito logístico, la protección del transporte de carga sigue siendo una asignatura pendiente en México. Ante esta situación, la colaboración entre las fuerzas del orden, los operadores logísticos y los proveedores de seguridad es clave para revertir esta preocupante situación.

Por su parte, el sector del *retail* vive una transformación en sus prioridades de seguridad. Si bien la vigilancia física y el control de pérdidas continúan siendo esenciales en tiendas y centros comerciales, la digitalización ha traído consigo nuevas amenazas. El comercio electrónico ha expuesto al sector a delitos cibernéticos como el *phishing*, el robo de identidad, el fraude con tarjetas y el acceso indebido a datos sensibles. Por ello, las empresas del *retail* deben ampliar sus estrategias de protección integrando medidas de ciberseguridad y soluciones tecnológicas que garanticen una experiencia de compra segura para los consumidores.

Otro de los temas que abordamos con especial atención en este número es la prevención y protección contra incendios. Esta materia, a menudo tratada de forma secundaria, resulta vital en entornos como almacenes logísticos, centros de distribución y establecimientos comerciales. Las instalaciones deben contar con sistemas actualizados de detección temprana, planes de evacuación eficaces y mantenimiento periódico de los equipos contra incendios. La inversión en este ámbito protege activos y vidas humanas, y, además, garantiza la continuidad operativa en caso de emergencia.

Por otra parte, como ya es tradición, este número de *Segurilatam* se publica días antes de la celebración de la Feria Internacional de Seguridad ESS+ de Bogotá, una de las grandes citas del sector en América Latina. Este año, la feria pondrá el acento en tecnologías punteras como la inteligencia artificial aplicada a la seguridad, soluciones para la movilidad segura, la protección de espacios educativos y hospitalarios, y, de forma muy destacada, la protección de las infraestructuras críticas. Este enfoque responde a una necesidad creciente en la región: blindar los servicios esenciales ante amenazas cada vez más sofisticadas.

Precisamente, en línea con dicha prioridad, me complace anunciar que *Segurilatam* organizará, el próximo mes de noviembre en la CDMX, el VII Congreso Mexicano de Protección de Infraestructuras Críticas (PIC). Este evento, de carácter exclusivo y aforo limitado, reunirá a destacados expertos para debatir sobre la seguridad de las IC durante el Mundial de Fútbol de 2026 en México. Un acontecimiento que exigirá garantizar la operatividad de las infraestructuras que sostienen los servicios esenciales, desde el suministro eléctrico y las telecomunicaciones hasta el transporte, la salud o la alimentación. ¡Allí nos vemos! **S**



Javier Borredá
Director de Segurilatam

“ El VII
Congreso
Mexicano
PIC pondrá
el foco en el
Mundial de
Fútbol
2026 ”



Sumario



10



12



18



46



58



92

10 **Entrevista**
Yahiro Sánchez, director corporativo de Prevención de Pérdidas en Liverpool.

12 **Entrevista**
Enrique Arellano, Corporate Security Manager en Mercedes-Benz México.

18 **Entrevista**
Gerardo Ortega, director de Seguridad Corporativa en Grupo Roca.

26 **Entrevista**
Verónica Torres Landa, directora general de la Asociación Mexicana de Empresas de Seguridad Privada.

44 **Entrevista**
Concha Martínez Cano, directora ejecutiva de Lannaccess en Latinoamérica.

46 **Artículo**
Giovanni Yancoli, gerente HSEQ en Transportes Santa María SpA.

54 **Artículo**
Comexa. Prevención y protección contra incendios: clave en la seguridad integral.

58 **Entrevista**
Sargento Carlos Ramírez, Cuerpo Oficial de Bomberos de Bogotá.

66 **Producto**
José Luis Calderón González, director de NOLETAL, agente autorizado de BYRNA en México.

68 **Artículo**
Víctor Hugo Manzanilla Rangel, Managing Director de ALCEA en México.



70

Artículo

Juan Carlos Fúnez, responsable de Tecnología de la Información (IT) en Casmar.

80

Seguridad Corporativa

Curso Superior en Contrainteligencia y Seguridad de la Fundación Borredá.

84

Crónica

II Congreso Mexicano de Directores de Seguridad organizado por *Segurilatam* en la CDMX.

92

Entrevista

Patricia Acosta, directora de la Feria Internacional de Seguridad ESS+.

94

Eventos

Avance del VII Congreso Mexicano de Protección de Infraestructuras Críticas (PIC).

STAFF

Director

Javier Borredá: javier.borreda@borrmart.es

Redacción Segurilatam:

Bernardo Valadés

Redacción Seguridad Laboral Latam:

Jaime Sáez de la Llave

Departamento comercial

México:

Javier Borredá: javier.borreda@borrmart.es

Gabriela Soto: gabriela.soto@borrmart.es

Colombia

Marcela Linares: comercial.co@borrmart.es

Perú

Pedro Pleguezuelos: segurilatam.peru@borrmart.es

Ecuador

Paloma Melendo: segurilatam.ecuador@borrmart.es

Argentina

Yolanda Duro Blázquez: yolanda.duro@borrmart.es

Chile

Antonio C. Borredá: segurilatam.chile@borrmart.es

Caribe

Yolanda Duro Blázquez: segurilatam.caribe@borrmart.es

Centroamérica

Javier Borredá: segurilatam.centro@borrmart.es

Diseño y maquetación

Macarena Fdez. López

Área Web

Laura Borredá García y Natividad Benítez

Fotografía: Getty Images

Fotomecánica e Impresión:

COMECO GRÁFICO S.L.U.

EDITA: BORRMART, S.A.

Presidenta

Ana Borredá

Presidente Honorífico

Francisco Javier Borredá Martín

Directora general

Ana Borredá

Central

Don Ramón de la Cruz, 68. 28001 Madrid.

Tel.: +34 91 402 96 07. www.segurilatam.com.

E-mail: segurilatam@borrmart.es.

ISSN: 2530-5794

ISSN versión electrónica: 2530-8556

Depósito Legal: M-5449-2016.



MÉXICO: CRECE EL EMPLEO EN LA SEGURIDAD PRIVADA

El empleo en la seguridad privada ha crecido un 37% en México en la última década, superando así la media nacional (25,4%), ha comunicado la asociación AMESP. En cuanto al salario medio en el sector, se ha incrementado un 12,4% entre diciembre de 2023 y febrero 2025, lo cual refleja una tendencia positiva en las condiciones laborales de los trabajadores de la industria de la seguridad privada.

CHILE: COMITÉ DE COORDINACIÓN NACIONAL DE FRONTERAS

Con el objetivo de resguardar las zonas limítrofes con una mayor coordinación interinstitucional, el ministro del Interior de Chile, Álvaro Elizalde, ha anunciado la creación de un comité de Coordinación Nacional de Fronteras encargado de integrar, identificar y manejar las capacidades y necesidades de las instituciones que operan o tienen competencias en la frontera del país. La creación de este comité se enmarca en la estrategia integral del Gobierno para fortalecer la presencia del Estado en la frontera y enfrentar de forma decidida la migración irregular y el crimen organizado.

‘ÍNDICE DE PAZ MÉXICO 2025’: LA PAZ Y LA SEGURIDAD, ASIGNATURAS PENDIENTES EN EL PAÍS

El *Índice de Paz México 2025*, elaborado por el Instituto para la Economía y la Paz (IEP), pone de manifiesto que la paz y la seguridad continúan siendo asignaturas pendientes en el país. De manera especial, preocupa que en los últimos años se haya incrementado el número de homicidios, delitos cometidos con armas de fuego y crímenes de la delincuencia organizada.



Los estados más pacíficos de México son Yucatán, Tlaxcala, Durango, Chiapas y Nayarit. Y los más violentos, Colima, Guanajuato, Morelos, Baja California y Quintana Roo. La percepción ciudadana sigue siendo alarmante: el 73,6% de la población considera inseguro el estado en el que vive. Además, el 54% identifica el crimen y la violencia como la mayor amenaza para su vida cotidiana, situando a México con la tercera tasa más alta del mundo en esta categoría.

PERÚ Y ESPAÑA FORTALECEN LA COOPERACIÓN PARA COMBATIR EL CRIMEN TRANSNACIONAL

En el marco del encuentro EL PACCTO 2.0 celebrado en Lima, el ministro del Interior del Perú, Carlos Malaver, y su homólogo de España, Fernando Grande-Marlaska, reafirmaron el compromiso de fortalecer la cooperación bilateral en la lucha contra el crimen transnacional. Esta iniciativa se desarrolla dentro del convenio de colaboración suscrito entre ambos países desde 2019 y busca responder con firmeza a los desafíos que plantea la criminalidad organizada.



Malaver destacó que el EL PACCTO 2.0, un programa financiado por la Unión Europea, representa un esfuerzo estratégico de cooperación internacional ante uno de los mayores retos compartidos por los Estados: el crimen transnacional. Por su parte, Grande-Marlaska subrayó la importancia de contar con instrumentos eficaces para el intercambio de inteligencia y la ejecución de operativos conjuntos.

LA FUERZA PÚBLICA COLOMBIANA REFORZARÁ SU CAPACITACIÓN CON EL APOYO DE LA OTAN

La Fuerza Pública colombiana busca consolidarse como un referente en seguridad y defensa. Para ello, entre otras iniciativas, reforzará sus procesos de capacitación y educación con el apoyo de la Organización del Tratado del Atlántico Norte (OTAN) tras una visita técnica de delegados de Eslovenia, Italia, España y Polonia. Esta colaboración se enmarca en el Programa de Asociación Personalizado (ITPP) y el Programa de Mejora de la Educación de Defensa (DEEP) vigentes entre Colombia y la OTAN.

Edsson Arturo Aristizabal, director de Desarrollo de la Fuerza Pública colombiana, ha explicado que la OTAN colaborará con la revisión de las mallas curriculares y el diseño de objetos virtuales de aprendizaje. "El contexto del conflicto en el país requiere que los uniformados adquieran nuevas competencias", ha afirmado.



NACE EL DEPARTAMENTO FEDERAL DE INVESTIGACIONES, EJE DE LA NUEVA POLICÍA FEDERAL ARGENTINA

En un acto encabezado por el presidente de la nación, Javier Milei, y la ministra de Seguridad, Patricia Bullrich, se presentó la transformación estructural de la Policía Federal Argentina (PFA). A través del Decreto 383/2025, publicado en el Boletín Oficial, se aprobó el nuevo estatuto que redefine su misión, centrando sus esfuerzos en delitos federales complejos. En el corazón de esta reforma policial se encuentra la creación del Departamento Federal de Investigaciones (DFI), eje central de la nueva estrategia de seguridad nacional.

Inspirada en modelos como el Buró Federal de Investigaciones (FBI) de Estados Unidos, la Policía Federal de Brasil y la Policía Nacional de España, esta nueva PFA aspira a convertirse en una fuerza profesional y eficiente frente al crimen transnacional. El Departamento Federal de Investigaciones será el bastión principal contra el narcotráfico, la corrupción y la trata de personas.



ESPAÑA Y PARAGUAY, EJEMPLO DE TRABAJO CONJUNTO

Gracias al trabajo entre la Policía Nacional del Paraguay y la Policía Nacional de España, esta última ha podido desarticular una organización criminal especializada en robos en viviendas. Uno de los elementos fundamentales del éxito de esta operación, llevada a cabo en la Comunidad de Madrid, ha sido la comunicación entre ambos cuerpos policiales. En España, los agentes constataron que la organización mantenía una comunicación interna basada en alias y el uso del guaraní, lo que dificultaba su rastreo y requería información aportada por Paraguay.

URUGUAY LANZA LOS ENCUENTROS POR SEGURIDAD

El ministro del interior de Uruguay, Carlos Negro, ha presentado los Encuentros por Seguridad, una instancia clave en el proceso de elaboración del Plan Nacional de Seguridad Pública 2025-2035. La misma contará con la participación de partidos políticos con representación parlamentaria, organismos de los tres poderes del Estado, gobiernos subnacionales, academia, expertos, organizaciones sociales, sindicatos, el sector privado y organismos internacionales para buscar consensos en materia de seguridad pública.





Tendencias en la logística y el 'retail': opinan los expertos en seguridad

■ Por Redacción.

La seguridad logística y en el *retail* ha entrado en una era marcada por la digitalización acelerada, las tecnologías predictivas y una visión más amplia de los riesgos. En declaraciones a *Segurilatam*, directores de seguridad de grandes empresas y representantes de asociaciones coinciden en que los retos ya no se limitan al robo físico o la custodia de mercancías. Ahora, conceptos como sostenibilidad, inteligencia artificial (IA), ciberseguridad o colaboración público-privada son imprescindibles para entender el presente y futuro de la seguridad.

Luis J. Rodríguez (CHEP)

En el caso de Luis J. Rodríguez, director de Protección de Activos y Seguridad para Latinoamérica en CHEP, advierte que los retos en la seguridad logística exigen un enfoque innovador. "Vivimos en un mundo cada vez más globalizado y conectado con un movimiento de mercancías sin precedentes. Este escenario requiere tecnologías como IA, plataformas de alertas, GPS y dispositivos IoT conectados a Bluetooth que actúen con decisiones preprogramadas. Todo estará más automatizado", opina. Y añade que "veremos más empresas y gobiernos priorizando la sostenibilidad. La economía circular y la reducción de emisiones serán elementos estructurales en las políticas de seguridad del futuro".

José Luis Saavedra (GCP)

Desde el sector papelerero, José Luis Saavedra, gerente de Seguridad Patri-



monial en Grupo Corporativo Papelera (GCP), considera que las tecnologías disruptivas modificarán profundamente el trabajo del área. "El uso de *big data*, IoT y gemelos digitales aportará visibilidad en tiempo real y capacidad para anticiparse a problemas. El futuro pasa por combinar IA y experiencia humana", señala. En ese sentido, Saavedra prevé una transformación del rol tradicional de los responsables de seguridad. "Habrá una mayor integración tecnológica y un fuerte enfoque en prácticas sostenibles", comenta.

Gerardo Ortega (Grupo Roca)

Gerardo Ortega, director de Seguridad Corporativa en Grupo Roca, coincide en que la tecnología dejará de ser un so-

porte para convertirse en el centro de la estrategia de seguridad logística y en el *retail*. "La analítica de datos, la automatización y la ciberseguridad avanzada marcarán el camino. Los riesgos como ciberataques o interrupciones en la cadena exigirán una gestión dinámica y transversal. En Grupo Roca entendemos la seguridad como un habilitador del crecimiento sostenible", destaca.

Yahiro Sánchez (Liverpool)

En el sector del *retail*, Yahiro Sánchez, director corporativo de Prevención de Pérdidas en Liverpool, señala que el entorno cambiante obligará a adoptar tecnologías cada vez más sofisticadas. "La protección de la cadena de suministro y de las transacciones *online* será esen-

cial. La IA, el IoT y la gestión avanzada de datos serán herramientas imprescindibles”, sostiene. Asimismo, considera que “la colaboración público-privada nos permitirá optimizar recursos, acelerar decisiones y mejorar la prevención a través del intercambio de inteligencia entre sectores”.

Enrique Arellano (Mercedes-Benz México)

Por su parte, Enrique Arellano, Corporate Security Manager en Mercedes-Benz México, apunta que la industria automotriz ya vive una transformación en la forma de proteger su cadena logística. “La seguridad logística está dejando de ser reactiva para convertirse en proactiva gracias a la IA, la trazabilidad en tiempo real y la analítica avanzada”, argumenta. Y resalta también la urgencia de reforzar la ciberseguridad. “La frontera entre lo físico y lo digital se ha difuminado. No se puede pensar en protección sin contemplar los riesgos tecnológicos. Además, la sostenibilidad se posiciona como un eje clave que exigirá rediseñar procesos con eficiencia energética y control de emisiones”, concluye.

José Luis Sánchez, director de Seguridad Corporativa

Una mirada especialmente disruptiva es la de José Luis Sánchez, director de Seguridad Corporativa, quien afirma que “el que siga operando como hace diez años va a ser tragado por su propia inercia. El futuro de la seguridad agroindustrial será digital, predictivo, colaborativo y resiliente”. Según Sánchez, el nuevo modelo implicará una digitalización total –con sensores, *blockchain* y accesos biométricos–, inteligencia predictiva basada en algoritmos, alianzas institucionales y protocolos compartidos, así como una ética digital sólida. “Ya no se trata sólo de evitar incidentes, sino de

recuperarse rápido y aprender de ellos. La resiliencia será la nueva métrica de éxito”, observa.

Verónica Torres Landa (AMESP)

Por lo que respecta a las asociaciones, Verónica Torres Landa, directora general de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), advierte que el avance del comercio electrónico ha traído consigo nuevos riesgos: robos en centros de distribución, fraudes en línea y suplantación de identidad. Para ella, el futuro de la seguridad logística y

está revolucionando la seguridad en el *retail*. Las tiendas físicas y las plataformas *online* deben compartir un modelo de protección integral”, propone.

Vanessa Cure Anturi (Asosec)

Por último, Vanessa Cure Anturi, directora ejecutiva de la Asociación Colombiana de Seguridad (Asosec), apunta que “la transformación digital ha hecho que la seguridad se centre cada vez más en datos, automatización y análisis de riesgos en tiempo real”. Para la representante gremial, el talento humano deberá adap-

Las empresas que comprendan el nuevo enfoque de seguridad serán más competitivas en un entorno cada vez más dinámico

en el *retail* pasa por “la integración entre talento humano capacitado, automatización y modelos predictivos respaldados por tecnologías robustas”. De igual manera, Torres Landa subraya el papel de la ciberseguridad. “Además de las instalaciones físicas, debemos proteger los datos de los procesos, los clientes y las operaciones. Desde AMESP promovemos la profesionalización continua y el uso ético de la tecnología, alineados siempre con la legalidad y los derechos humanos”, explica.

Nicolás Botero-Páramo Gaviria (FedeSeguridad)

En Colombia, Nicolás Botero-Páramo Gaviria, presidente ejecutivo de FedeSeguridad, destaca la creciente fusión entre vigilancia física y soluciones digitales. “El uso de IA, drones, cámaras con reconocimiento facial y análisis predictivo

tarse a entornos híbridos complejos. “La seguridad privada no sólo evitará pérdidas, sino que, además, protegerá toda la cadena de valor, desde la tienda física hasta la última milla”, indica.

Nuevo paradigma

La seguridad logística y en el *retail* se encuentra en un punto de inflexión. Tecnologías como la inteligencia artificial, el IoT o los sistemas predictivos están cambiando el paradigma, mientras que la sostenibilidad y la ciberseguridad emergen como prioridades estratégicas. El futuro exigirá integración tecnológica, alianzas multi-sectoriales, profesionalización del talento y una capacidad operativa orientada a la anticipación y la resiliencia. Las empresas que comprendan este enfoque de la seguridad no sólo protegerán sus activos, sino que ganarán ventaja competitiva en un entorno cada vez más dinámico. **S**

**Yahiro Sánchez**

Director Corporativo de Prevención de Pérdidas
en Liverpool

“El sector del ‘retail’ enfrenta un entorno de seguridad complejo y en constante evolución”

» Por Bernardo Valadés.

Con más de 20 años de trayectoria profesional en Liverpool, la cadena de almacenes departamentales de mayor cobertura en México, Yahiro Sánchez considera que “el sector del ‘retail’ enfrenta un entorno de seguridad complejo y en constante evolución”. En su opinión, para protegerse eficazmente es esencial una política integral que contemple la capacitación del personal, una sólida gestión de riesgos, una robusta ciberseguridad y tecnologías avanzadas.

Liverpool cuenta con una presencia muy amplia en México y un canal de *e-commerce* en constante crecimiento. ¿Cuáles son los principales retos en materia de seguridad y prevención de pérdidas?

Los principales retos en una operación tan extensa y multicanal como la nuestra son la complejidad de la logística, la gestión de inventarios, la seguridad de la información y la protección contra fraudes *online*.

Bajo su punto de vista, ¿cuáles son las amenazas internas y externas que afectan a la seguridad en el sector del *retail* en México?

En el sector del *retail* identificamos amenazas internas clave como la falta de personal capacitado en seguridad, así como la ausencia de protocolos en algunas empresas para la gestión de riesgos internos. La ciberseguridad también es una preocupación importante, ya que el sector minorista es vulnerable a ataques cibernéticos que pueden comprometer datos personales de clientes o interrumpir sistemas de pago.

En cuanto a las amenazas externas, el aumento de la delincuencia, incluyendo robos, asaltos y la delincuencia organizada, representa una amenaza constante. Los robos de productos y el fraude con tarjetas bancarias son problemas comunes que afectan las ganancias. Además, la ciberdelincuencia, a través de ataques como *ransomware* o *phishing*, puede causar pérdidas financieras y dañar la reputación de las empresas. También debemos considerar los cambios en el mercado, como la competencia *online* y la expansión del comercio electrónico, que pueden aumentar la vulnerabilidad de las tiendas físicas, y la amenaza de desastres naturales a la infraestructura y las operaciones.

En conclusión, el sector del *retail* en nuestro país enfrenta un entorno de seguridad complejo y en constante evolución. Para protegerse eficazmente, es crucial implementar medidas de seguridad integrales que abarquen la capacitación del personal, una sólida gestión de riesgos, una robusta ciberseguridad y la adopción de tecnologías avanzadas.

¿Cuál es el enfoque del área de Seguridad de Liverpool? ¿Cómo se coordina la seguridad en tienda física con la logística y el entorno digital?

Actualmente, los recursos se enfocan en la prevención y la protección de la salud y la seguridad de los empleados. Esto incluye la identificación de riesgos, la evaluación de peligros a través de análisis de riesgos, la implementación de medidas de control y la supervisión continua de la seguridad en el lugar de trabajo a través de programas de capacitación y protocolos de emergencia.

La seguridad en tiendas físicas se coordina con la logística y el entorno digital mediante la implementación de sistemas integrados que protejan tanto los bienes físicos como los datos digitales. Esto implica proteger tanto el espacio físico de la tienda como la información que fluye a través de sus canales digitales, como el comercio electrónico o la gestión de inventario. Una tienda que implementa medidas de seguridad efectivas mejora su reputación y la confianza de los clientes.

En resumen, la seguridad en las tiendas físicas, la logística y el entorno digital está conectada y requiere una coordinación efectiva para proteger los bienes, la información y la reputación de la empresa.

¿Qué papel desempeñan la tecnología y la innovación, como videovigilancia

inteligente, analítica de datos, IA, etc., en la estrategia de seguridad de Liverpool?

En nuestra empresa integramos la tecnología y la innovación como pilares fundamentales en la estrategia de la organización tanto para proteger sus operaciones como para mejorar continuamente la experiencia del cliente. Utilizamos herramientas que nos permiten anticipar incidentes y responder rápidamente a problemas potenciales y hemos implementado inteligencia artificial (IA) para optimizar procesos clave como la gestión de inventarios y la experiencia de búsqueda.

Sin ninguna duda, la tecnología y la innovación son componentes esen-

Los puntos más vulnerables a riesgos o fallas que podrían comprometer la integridad de los productos, la información o la cadena de suministro son el aprovisionamiento y la colaboración de proveedores, los procesos de almacenamiento y el manejo de materiales, el transporte y la distribución, la gestión de riesgos y la respuesta a crisis.

La formación y concienciación del personal suelen ser claves para el éxito de cualquier estrategia de seguridad. ¿Qué acciones lleva a cabo Liverpool en este sentido?

Implementamos diversas acciones para la formación y concienciación de nuestro personal en materia de seguridad.

“La seguridad en las tiendas físicas, la logística y el entorno digital está conectada y requiere una coordinación efectiva para proteger bienes, información y reputación”

ciales de la estrategia de seguridad de Liverpool, permitiéndonos proteger nuestras operaciones, enriquecer la experiencia del cliente y mantenernos a la vanguardia en el sector del *retail*. En este sentido, las tecnologías que han resultado más eficientes son aquellas que nos han brindado *data*; de ellas, la IA nos ha aportado un mayor alcance y resultados eficientes en la toma de decisiones.

En el ámbito de la logística, ¿cuáles son los puntos más críticos en la cadena de suministro desde el punto de vista de la seguridad? ¿Cómo se protegen frente a incidentes como robos de mercancía en tránsito o intrusiones en centros de distribución?

Nuestro objetivo es que todos los colaboradores no sólo conozcan las medidas de seguridad, sino que, además, las interioricen y las apliquen en su día a día tanto en situaciones rutinarias como en emergencias.

Entre nuestras iniciativas clave en materia de formación y capacitación, cabe destacar las siguientes: capacitación del personal en protocolos de emergencia, simulacros de seguridad, cultura de prevención y cuidado, y desarrollo de talento. En resumen, en nuestra empresa abordamos la seguridad desde múltiples frentes, buscando una interiorización completa de las medidas por parte de nuestro personal, lo que nos permite proteger eficazmente nuestras operaciones y asegurar el bienestar de todos. **S**

**Enrique Arellano**

Corporate Security Manager en Mercedes-Benz México

“Los retos de seguridad de la cadena logística del sector automotriz requieren un modelo de prevención integral”

■ Por Bernardo Valadés.

Con una amplia experiencia en el ámbito de la seguridad, Enrique Arellano desempeña el cargo de gerente de Seguridad y Protección Corporativa en Mercedes-Benz México desde hace casi cuatro años. Al preguntarle sobre los desafíos de seguridad de la cadena logística del sector automotriz, responde que es importante “avanzar hacia un modelo de prevención integral que incorpore una cultura de seguridad en todos los niveles de la operación logística”.

¿Cuáles son los principales desafíos de seguridad a los que se enfrenta la cadena logística del sector automotriz?

Las autopartes son vulnerables frente a los mercados informales debido a su facilidad de redistribución y reventa. Por su parte, los vehículos terminados son objetivo de robo total, ya sea para su desmantelamiento o incluso para su exportación ilegal. Estos riesgos se agravan aún más por la colusión interna en sectores públicos y privados, el uso de tecnología ilegal para bloquear señales GPS y la falta de infraestructura y presencia de cuerpos de seguridad en tramos carreteros estratégicos.

Otro factor crítico es la falsificación de documentos. La suplantación de órdenes de carga o la manipulación de destinos mediante documentos físicos o digitales apócrifos puede derivar en pérdidas millonarias si no se detecta a tiempo.

Además, la ciberseguridad se ha convertido en un frente decisivo para la protección logística. El hackeo de plataformas de rastreo, el acceso no autorizado a herramientas de bloqueo de señal y la manipulación remota de datos logísticos forman parte de un patrón más amplio que exige una verdadera convergencia entre las estrategias de ciberseguridad y seguridad física.

Una vulnerabilidad recurrente sigue siendo la subcontratación de servicios de transporte sin controles rigurosos. Existen operadores logísticos que aún carecen de protocolos de seguridad patrimonial, capacitación especializada en seguridad, filtros de contratación adecuados y procesos de auditoría continua. En muchos casos, también se observa una ausencia de canales claros para la denuncia de actos delictivos, lo cual incrementa tanto la exposición como el riesgo para la carga y el personal involucrado.

Por lo expuesto, desde la perspectiva de la seguridad corporativa, ¿qué debe hacerse al respecto?

El camino hacia adelante exige avanzar hacia un modelo de prevención integral. Un modelo que incorpore una cultura de seguridad en todos los niveles de la operación logística. Esto implica realizar análisis de riesgo exhaustivos, implementar tecnologías avanzadas de rastreo, establecer monitoreo en tiempo real, conocer en profundidad y supervisar los procesos operativos, y auditar de forma continua los perfiles de confianza involucrados en la cadena logística.

Igualmente, es importante construir redes sólidas de colaboración entre entidades públicas y privadas. Sólo a través de la inteligencia compartida, la acción coordinada y la confianza mutua será posible reducir los incidentes, minimizar las discrepancias y fortalecer la resiliencia del sector ante un entorno de amenazas en constante evolución.

¿Cómo valora la relación entre la industria automotriz y las autoridades de México en materia de seguridad logística?

La relación entre las autoridades mexicanas y los diversos sectores industriales, no sólo la industria automotriz, siempre debe basarse en el apoyo mutuo, la comunicación abierta y la resolución proactiva de problemas, particularmente cuando se trata de abordar los desafíos de infraestructura. Esta colaboración también debe extenderse a los esfuerzos de desarrollo cultural en las regiones afectadas por el saqueo y la inseguridad social, al tiempo que debe estar anclada en el respeto mutuo que fortalezca la cadena logística frente a la actividad criminal.

Si estos elementos se debilitan o se alteran, la continuidad operativa de la industria automotriz y el desarrollo económico regional podrían verse se-

riamente afectados por una serie de amenazas criminales. A pesar de que las autoridades en México están implementando programas para apoyar a diversas cámaras y sectores de la industria con estrategias de seguridad, los sectores público y federal aún enfrentan un reto importante: gestionar la inmensa diver-

En estos casos, la prioridad es actuar de manera inmediata pero siempre alineados con las políticas internas, la normativa nacional y los estándares corporativos. Esta sinergia no sólo fortalece la respuesta operativa, sino que garantiza una gestión ética, transparente y segura ante cualquier riesgo.

“Seguridad Corporativa y Compliance colaboran en procesos clave como evaluación de proveedores, controles de acceso, investigaciones internas, protección de datos personales...”

sidad y complejidad de las operaciones logísticas diarias en todo el país.

Para ello, es esencial seguir colaborando con el sector público. Las iniciativas privadas no sólo deben reforzar la seguridad operativa, sino también garantizar que sus esfuerzos estén alineados y respaldados por un compromiso público y federal sostenido. Sólo a través de este esfuerzo equilibrado y coordinado se pueden construir realmente los cimientos de una cadena de suministro resiliente y segura.

¿Qué sinergias existen en Mercedes-Benz entre las áreas de Seguridad y Compliance? ¿En qué casos trabajan de forma coordinada?

Seguridad Corporativa y Compliance colaboran de forma estrecha en procesos clave como la evaluación de proveedores, controles de acceso, investigaciones internas y la protección de datos personales. También trabajamos coordinadamente en la prevención de lavado de dinero y en situaciones de contingencia, donde ambos equipos participamos activamente como parte del Comité de Crisis.

¿Qué aprendizajes del mundo del retail ha trasladado con éxito al entorno logístico-industrial en términos de gestión de riesgos y protección de activos?

Es una excelente pregunta. Si tomamos el enfoque *retail* de prevención de pérdidas, esta naturaleza filosófica de seguridad también puede aplicarse y trabajarla para que se pueda calcar en conjunto hacia las operaciones de almacenaje, distribución y ventas de la industria automotriz, ya que podemos trasladar de manera óptima aplicando métricas que permitan conocer el flujo operacional y cuáles son las mermas de las operaciones en los CEDI y manufactura. La acción de prevención en esquemas de distribución, sumando la tecnología por medio de analíticos e infraestructura que nos ayuden a saber con más exactitud y menor tiempo las áreas de oportunidad de la operación, es parte del esquema de seguridad que se fortalece con la aplicación de auditorías internas que te permitan conocer las debilidades y proponer planes de mejora ante las áreas responsables y proveeduría, pero siempre con una estrecha colaboración y comunicación desde el enfoque preventivo. **S**

**José Luis Sánchez**

Director de Seguridad Corporativa

“Una visión integral es indispensable para proteger la logística en la industria cárnica”

» Por Bernardo Valadés.

Experto en seguridad corporativa en el sector cárnico, con José Luis Sánchez se puede platicar durante horas. De hecho, esta entrevista debería ser mucho más extensa teniendo en cuenta sus respuestas a las preguntas planteadas. En cualquier caso, queda patente que es un profesional comprometido que va más allá de las medidas de seguridad física, como lo demuestra su preocupación por la reputación empresarial o la relación con las comunidades locales.

La industria cárnica opera en un sector estratégico como el agroalimentario, con operaciones de cría, procesamiento, distribución y exportación. ¿Cuáles son los principales riesgos de seguridad logística que enfrentan actualmente en esta cadena de valor tan especializada?

Buena pregunta. Cuando hablamos de seguridad logística en una empresa agroalimentaria con operaciones completas, de la granja al embarque internacional, en estados como Puebla y Veracruz, uno tiene que pensar como ajedrecista y ranchero a la vez. En esas zonas del país, los principales riesgos de seguridad logística en la agroindustria son el robo y asalto en tránsito, la corrupción y colusión en puntos de control, el sabotaje interno o fuga de información, la contaminación o manipulación de productos, las crisis climáticas, los bloqueos sociales, las amenazas cibernéticas en sistemas de logística, la interferencia política y el crimen organizado.

Ante todo esto se necesita una visión integral que contemple desde blindar la logística tecnológicamente hasta tener inteligencia operativa de las rutas y actores clave. No se trata de reaccionar a cada robo, sino de anticiparlos con mapas de calor, protocolos de crisis y mucha capacitación.

La producción y distribución de carne implica cumplir estrictos protocolos de calidad, sanidad y trazabilidad. ¿Qué papel desempeña el área de Seguridad Corporativa en la protección de estos procesos, especialmente en el transporte de animales y productos cárnicos?

Literalmente y en sentido estratégico, este es un tema de peso pesado. Cuando hablamos del transporte de animales vivos y productos cárnicos, el área de

ALWIN la solución de gestión de seguridad

ALCEA

ASSA ABLOY



ALWIN: Control total y seguridad continua.

Tu infraestructura crítica, gestionada desde una sola plataforma, innovación con el respaldo de la máxima tecnología.



Mira el video explicativo ALWIN

Optimiza la gestión de entradas y salidas con **ALWIN**. Trazabilidad total, seguridad avanzada y flexibilidad para adaptarse a cualquier entorno. Simplifica procesos. Refuerza la seguridad. Toma el control.



Tu acceso seguro, rápido y sin límites:
GATEWAY, conectando tu mundo.

ALCEA GATEWAY es la plataforma que permite conectar y gestionar todos tus sistemas de seguridad con automatización de forma centralizada, ofreciéndote control, monitoreo en tiempo real de accesos, alarmas y procesos industriales.



Descarga el brochure
GATEWAY

Te esperamos en el stand 308A de ESS
alceaglobal.es



Seguridad Corporativa no es sólo un acompañante del negocio. Además, es un actor crítico para que todo funcione bien y, sobre todo, para que nadie termine con una demanda, una alerta sanitaria o un escándalo en la prensa.

Al respecto, el rol estratégico del área de Seguridad Corporativa se basa en ser custodios del valor biológico y reputacional, gestores del riesgo sanitario y criminal, arquitectos de la trazabilidad confiable, formadores del factor humano confiable y garantes de continuidad en crisis.

En materia de seguridad, en este rubro es importante tener un protocolo de bioseguridad en transporte primario; asegurar la doble verificación de sellos, firmas y GPS antes de cada salida; hacer ins-

teligencia y coordinación milimétrica. Exportar no es sólo enviar producto, es enviar reputación, cumplimiento y confianza en un contenedor refrigerado. Para hacerlo con garantías hay que considerar las regulaciones internacionales y de cada país, los riesgos operativos y logísticos, unas medidas clave de seguridad y cumplimiento, la protección de la información, la ciberseguridad y, por último, la sensibilización y el control humano.

En resumen, exportar no es sólo un tema de comercio, sino de soberanía, credibilidad y supervivencia para la empresa. Por ello, un área de Seguridad Corporativa no puede ser espectadora. Tiene que ser protagonista, garante y estratega.

puntos de control documentados y un centro de monitoreo remoto con rondas virtuales. En cuanto a las rutas de transporte, deben implementarse estrategias efectivas como alternancia de rutas y horarios, escoltas rurales encubiertas o acompañamientos civiles y control comunitario indirecto. Sobre esto último, una comunidad bien tratada es la mejor alarma temprana.

En definitiva, la seguridad física en zonas rurales se construye con respeto, tecnología adaptada, inteligencia humana y presencia real. Es un equilibrio delicado entre firmeza operativa y cercanía comunitaria.

En un contexto en el que el robo al transporte, la intrusión en instalaciones o incluso el sabotaje a productos pueden generar graves perjuicios, ¿qué tecnologías, protocolos o prácticas destacan como parte de su estrategia preventiva?

En lo referente a la prevención, se necesita visión, tecnología y estrategia. Para el transporte, soluciones como GPS de nueva generación con geocercas dinámicas, cajas refrigeradas con sensores múltiples y cámaras vehiculares duales son muy útiles para prevenir. Por lo que respecta a las instalaciones, un perímetro inteligente con sensores de movimiento por microondas o infrarrojo, analíticos de vídeo y plataformas de integración (VMS) son muy útiles.

De igual manera, es importante contar con protocolos de control como entradas con validación biométrica o QR con vencimiento, bitácoras digitales, rondas inteligentes y listas de verificación de liberación de carga con firma digital y física. Y a todo ello debe sumarse una buena cultura organizacional, inteligencia preventiva y tecnologías emergentes como drones, IA en videovigilancia y *blockchain* para trazabilidad. **S**

“En la exportación de productos, un área de Seguridad Corporativa no puede ser espectadora. Tiene que ser protagonista, garante y estratega”

pecciones aleatorias con control de temperatura, presencia de contaminantes y documentos; diseñar bitácoras digitales con foto, hora, temperatura y firma por cada parada; entrenar a operadores en sanidad, ética y primeros auxilios animales; y contar con listas de verificación validadas por Calidad, Producción y Legal.

Cuando se exporta a países como Estados Unidos, Canadá, Japón, China y Corea del Sur, ¿cómo se gestiona la seguridad en los envíos internacionales? ¿Qué retos se enfrentan en cuanto a regulaciones, cumplimiento y protección durante la cadena logística?

Este es un terreno de alta complejidad y de altísimo riesgo si no se gestiona con

Muchas operaciones se desarrollan en zonas rurales o alejadas de los centros urbanos. ¿Cómo gestionan la seguridad física en instalaciones productivas, rutas de transporte y comunidades aledañas? ¿Qué desafíos particulares conlleva este entorno?

Estas son las preguntas que dividen a los que sólo piensan en cámaras de video-vigilancia y los que entendemos que la seguridad en zonas rurales es un acto de convivencia estratégica, no sólo vigilancia. Yo siempre digo que la seguridad no se impone en el campo, se teje. Y hay que hacerlo con confianza, respeto, firmeza...

En el caso de las instalaciones productivas, es fundamental una protección perimetral activa, guardias con perfil mixto,



SISTEMAS ELECTRÓNICOS DE SEGURIDAD

- Control de Acceso
 Project Management
 Domótica
 - Sistemas de Alarmas
 Centro de Monitoreo
 Sistemas CCTV
 Detección y Extinción de Incendio



ASOCIACIÓN
LATINOAMERICANA
DE SEGURIDAD



CONSEJO NACIONAL
CNSP
EMPRESAS DE CALIDAD



COPARMEX



Asociación Mexicana de Empresas de Seguridad Privada A.C.



INSTITUTO MEXICANO DEL COMERCIO INTERNET Y ENTORNOS A.C.



Registro de Prestadoras de Servicios
Especializados y Otras Especializadas



AMERICAN CHAMBER
MEXICO



NFPA
INTERNATIONAL

Totalmente conectado a ti



comexa_seguridad



comexa



ComexaSeguridad

www.comexa.com.mx • ventas@comexa.com.mx

Ignacio Zaragoza 73 • Col. Barrio Santa Catarina • Coyoacán 04010 • CDMX

55 1539 9215 | 55 5685 7830 | 55 5685 7837 • 800 2 COMEXA • 55 4555 7484

**Gerardo Ortega**

Director de Seguridad Corporativa en Grupo Roca

“La gestión integral del riesgo es central en nuestra estrategia de seguridad”

■ Por Bernardo Valadés.

Gerardo Ortega, director de Seguridad Corporativa en Grupo Roca, detalla cómo la compañía afronta los retos de seguridad industrial y logística en México. Desde la protección de la cadena de suministro hasta la coordinación con las autoridades de seguridad pública, Ortega subraya la importancia de “una estrategia integral diseñada bajo un enfoque transversal e interdepartamental”, afirma en esta entrevista concedida a ‘Segurilatam’.

¿Cuáles son los retos de seguridad que enfrentan en sus centros operativos, desde la producción hasta el almacenamiento y distribución de sus productos?

Entre los principales desafíos se encuentran la protección de la cadena de suministro, especialmente en rutas críticas y nodos vulnerables a robos o sabotajes; la gestión de accesos en plantas y almacenes, asegurando la trazabilidad de personas y vehículos; la seguridad patrimonial, a través de sistemas de videovigilancia, alarmas y controles perimetrales; y el cumplimiento de normas nacionales e internacionales que garanticen la integridad de nuestros colaboradores y la continuidad operativa.

Para hacer frente a estos retos, hemos implementado procesos estructurados y auditables, alineados con normas y certificaciones reconocidas como el programa CTPAT. Contamos con una matriz de riesgos que nos permite anticipar amenazas, aplicamos medidas preventivas y correctivas, y promovemos la capacitación continua del personal, fortaleciendo una cultura organizacional basada en la prevención, la disciplina operativa y la mejora continua.

¿Cómo protegen las rutas para prevenir robos y garantizar la trazabilidad de la mercancía durante su traslado a clientes o distribuidores?

El transporte seguro es un eslabón clave en nuestra cadena de valor. Hemos desarrollado un sistema integral de seguridad que incluye el uso de tecnología de punta, con unidades equipadas con geolocalización GPS, sensores de apertura de puertas y botón de pánico. Toda la actividad es monitoreada desde nuestro Centro de Monitoreo Corporativo, que opera 24/7 y tiene capacidad de respuesta inmediata ante cualquier desviación, parada no autorizada o incidente.

Además, realizamos una planeación estratégica de rutas basada en análisis de riesgo, evitando zonas con alta incidencia delictiva y definiendo ventanas de tránsito seguras. Toda la trazabilidad del traslado, desde la salida de planta hasta la entrega, es registrada y auditada. También mantenemos coordinación con autoridades de seguridad y trabajamos con terceros confiables. Este sistema de gestión se revisa y mejora continuamente conforme a los estándares internacionales.

to en zonas sensibles. También contamos con medidas de seguridad perimetral como cercado, sensores de intrusión y rondines electrónicos. Este ecosistema tecnológico y operativo nos permite mitigar riesgos de forma eficaz y garantizar un entorno seguro.

¿Cómo es la relación del departamento de Seguridad con las autoridades de seguridad pública?

La colaboración con autoridades es un pilar fundamental de nuestra estrategia

La gestión integral del riesgo es central en nuestra estrategia de seguridad porque entendemos que los riesgos no sólo afectan a lo físico, sino también a la continuidad operativa, la reputación, el cumplimiento normativo y la protección de activos digitales y humanos. Nuestra estrategia está diseñada bajo un enfoque transversal e interdepartamental.

Trabajamos de forma continua con áreas como TI, para abordar la ciberseguridad; Capital Humano, para fomentar cultura preventiva; Legal y Compliance, para garantizar el cumplimiento normativo; Finanzas, para evaluar el impacto económico de los riesgos; y Dirección General, para alinear los objetivos estratégicos. Esta integración nos permite tener políticas de seguridad sólidas, adaptables y alineadas con los procesos de producción, logística, distribución y talento.

“La colaboración con las autoridades de seguridad pública es un pilar fundamental de nuestra estrategia de seguridad integral”

¿Qué protocolos o tecnologías aplican para garantizar un entorno seguro en sus plantas y almacenes?

Nuestras instalaciones requieren un enfoque especializado. Por eso hemos definido protocolos diferenciados por unidad de negocio con base en los riesgos propios de cada operación. Contamos con control de accesos automatizado mediante *software* especializado, lo que nos permite registrar ingresos, aplicar restricciones por niveles de autorización y actuar rápidamente ante anomalías.

Hemos instalado un sistema integral de videovigilancia con cámaras de alta definición que cubren accesos, perímetros y zonas críticas. Toda esta actividad se supervisa desde nuestro Centro de Monitoreo Corporativo, que detecta eventos no autorizados y activa respuestas inmediatas. Para la gestión de contratistas, aplicamos procedimientos específicos que incluyen capacitación, entrega de equipos de protección y acompañamien-

to de seguridad integral. Mantenemos una relación estrecha y permanente con instituciones de seguridad pública a todos los niveles, lo que nos permite actuar coordinadamente en la prevención y atención de incidentes. Participamos en mesas de trabajo, redes empresariales, operativos conjuntos y simulacros que fortalecen la cooperación institucional.

Entre las acciones destacan los protocolos de notificación inmediata, el intercambio de información preventiva sobre zonas de riesgo y patrones delictivos, la participación en programas de prevención del delito y la gestión de refuerzos para rutas de transporte críticas. Esta colaboración ha sido clave para reducir riesgos, aumentar la percepción de seguridad y asegurar la continuidad operativa.

¿Cómo se alinean las políticas de seguridad con otras áreas como producción, logística o recursos humanos?

¿Qué iniciativas de formación, cultura de seguridad o protocolos de actuación promueven internamente para implicar a los equipos en la protección del entorno laboral?

Estamos convencidos de que la seguridad comienza con las personas. Por eso desarrollamos programas de capacitación y sensibilización adaptados a cada unidad de negocio dirigidos a todos los niveles operativos y administrativos. Incluyen formación periódica en seguridad patrimonial, higiene y protección ejecutiva, así como simulacros y talleres basados en análisis de riesgos específicos.

Difundimos protocolos de actuación homologados y organizamos campañas internas para fomentar una cultura de corresponsabilidad. El objetivo es que cada colaborador entienda su rol como parte activa en la protección del entorno laboral y de los activos críticos de la organización. **S**

**José Luis Saavedra**

Gerente de Seguridad Patrimonial en
Grupo Corporativo Papelera (GCP)

“Seguridad Patrimonial trabaja estrechamente con otras áreas del grupo y las autoridades locales”

» Por Bernardo Valadés.

José Luis Saavedra se encuentra al frente de Grupo Corporativo Papelera (GCP), empresa mexicana dedicada a la fabricación de productos de papel tisú. En esta entrevista, detalla cuáles son los desafíos a los que se enfrenta su departamento y aborda cuestiones como la protección del transporte y el almacenamiento, la preparación para enfrentar situaciones críticas o emergencias logísticas, la cooperación con otras áreas y las autoridades locales, etc.

GCP cuenta con una sólida presencia industrial y comercial tanto en México como en Estados Unidos. ¿Cuáles son los principales desafíos de seguridad patrimonial a los que se enfrenta el grupo actualmente?

La presencia de GCP en dos de los más grandes mercados de América es un gran logro y compromiso. En cuanto a los retos del área de Seguridad Patrimonial, enfrentamos desafíos entre los que podemos mencionar: la continua protección contra ciberataques y robo de información y datos; posibilidad de vandalismo e intrusión a cualquiera de nuestras instalaciones y propiedades; la seguridad de nuestros directivos y personal; la gestión de riesgos; y la prevención de la corrupción y el soborno. Para lograr prevenir y mitigar todo lo anterior implementamos medidas de seguridad suficientes y necesarias, además de mantener una capacitación constante a todo nuestro personal para poder responder de manera efectiva a estas amenazas.

La protección de la cadena de suministro es clave, sobre todo cuando se manejan grandes volúmenes de papel tisú y productos terminados. ¿Qué medidas implementa el área de Seguridad Patrimonial para proteger el transporte y almacenamiento de estos productos?

Desarrollamos e implementamos diversas medidas. Trabajamos de manera estrecha con nuestras áreas de Logística y Transporte para cuando es necesario planificar rutas de traslado seguras y nuestras flotas de vehículos propios están equipadas con dispositivos de seguimiento y rastreo que nos permiten el monitoreo en tiempo real, además de que todas nuestras cajas salen con sellos numerados que nos facilitan identificar cualquier posible apertura durante su traslado. Nuestras instalaciones de

almacenamiento cuentan con protocolos de seguridad que posibilitan tener un control estricto de entradas y salidas de personal y transporte complementadas con cámaras de videovigilancia y control de acceso de características biométricas para el control de nuestro personal en dichas instalaciones. Todo esto, sumado a la sensibilización que generan los líderes de las áreas operativas y de Logística, nos ayuda a responder de manera eficiente a cualquier incidente cuando se llega a presentar.

cas están aplicando en las plantas de producción para prevenir incidentes, intrusiones o pérdidas materiales?

En nuestras plantas de producción vinculamos de manera eficiente el uso de la tecnología con la concientización de nuestros colaboradores para prevenir incidentes a nivel operativo. Nuestra área de SHE mantiene una continua supervisión del cumplimiento de las reglas de seguridad al interior de nuestras instalaciones, además de mantener un continuo programa de sensibilización en

9001...). ¿Cómo influye esta cultura de cumplimiento y mejora continua en las políticas y procedimientos del área de Seguridad Patrimonial?

Contar con una cultura de sustentabilidad como empresa, y saber que se debe colaborar en la continuidad de certificaciones como FSC, SMETA e ISO, tiene un impacto significativo en el desarrollo, implementación, cumplimiento y mejora continua de las políticas y procedimientos de Seguridad Patrimonial.

Nuestro enfoque como empresa en la responsabilidad social y el cuidado del medio ambiente se refleja en la gestión de riesgos y la búsqueda continua de la seguridad integral. La concientización y capacitación sobre la importancia de la seguridad son fundamentales dentro de nuestra empresa y como área de Seguridad Patrimonial trabajamos y ajustamos nuestros procesos, buscando con los principios antes mencionados.

“El área de Seguridad Patrimonial juega un papel fundamental en la continuidad de negocio y la resiliencia operativa de la empresa”

En el caso de EEUU, ¿qué medidas han considerado en materia de seguridad logística para cumplir con los estándares del país y minimizar riesgos?

En EEUU consideramos varias medidas de seguridad y logística para cumplir con los estándares locales y minimizar los riesgos. Para cumplir con las regulaciones federales y estatales como la Ley de Seguridad de la Cadena de Suministro, procuramos que nuestros socios de negocio en los temas logísticos cuenten con certificación C-TPAT. Igualmente, la vinculación con las diversas asociaciones locales de transportistas y con las áreas de seguridad de nuestros clientes, así como una estrecha vinculación con las autoridades, es fundamental para garantizar la seguridad de nuestros productos.

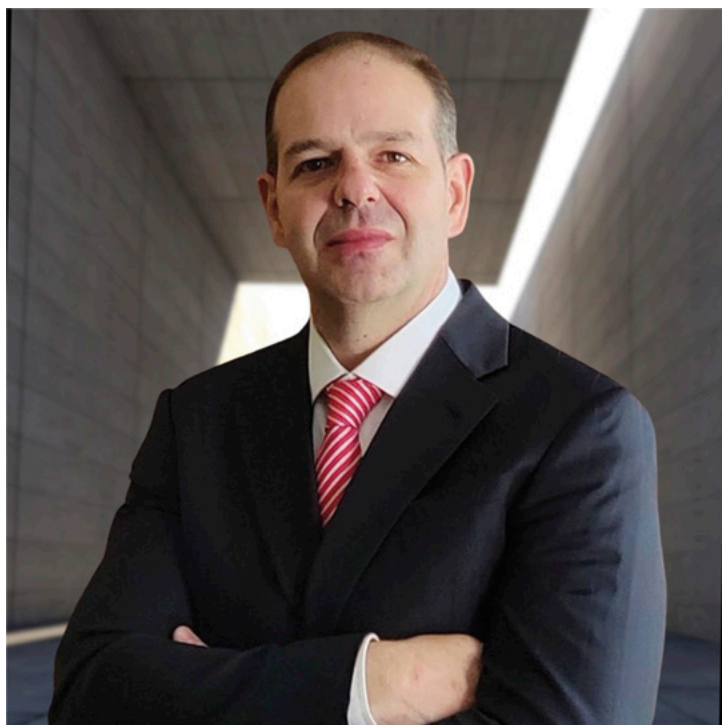
Las instalaciones industriales requieren una protección rigurosa. ¿Qué tecnologías, protocolos o buenas prácticas

cuanto a riesgos laborales. Nuestra área de Calidad evalúa de manera continua el cumplimiento de las buenas prácticas de fabricación para garantizar que nuestros productos cumplan con los más altos estándares de calidad. Y el área de Seguridad Patrimonial se apoya en el uso de sistemas electrónicos de seguridad (CCTV) con complementos de IA (analíticos) que nos permiten identificar tendencias y patrones de riesgo, sin olvidar la continua capacitación del personal del área. La medida de prevención para minimizar los intentos de sustracciones de nuestros productos parte de la directriz marcada por la alta dirección y consiste en la promoción y reafirmación por parte del área de Capital Humano de los valores de GCP: confianza, responsabilidad, integridad, lealtad, respeto y honestidad.

La empresa está comprometida con la sostenibilidad y cuenta con diversas certificaciones (FSC, SMETA, ISO

¿Qué papel juega la seguridad patrimonial en la continuidad del negocio y la resiliencia operativa de una empresa como GCP?

Sin duda alguna, el área de Seguridad Patrimonial juega un papel fundamental en la continuidad de negocio y la resiliencia operativa de la empresa. Nos enfocamos en proteger nuestros activos y garantizar que nuestras operaciones se realicen de manera segura y sin interrupciones, estamos preparados para enfrentar situaciones críticas o emergencias logísticas gracias a nuestros planes de emergencia, capacitación regular y simulacros. Pero todo esto no podría ser posible sin la estrecha coordinación que mantenemos con las demás áreas de la empresa y las autoridades locales de los lugares donde se ubican nuestras plantas. Esto nos permite una respuesta efectiva y eficaz ante situaciones de emergencia. **S**

**Luis J. Rodríguez**

Director de Protección de Activos y Seguridad para Latam en CHEP

“La tecnología es indispensable para servir mejor a los clientes y, al mismo tiempo, minimizar las pérdidas”

■ Por Bernardo Valadés.

CHEP es una empresa mexicana especializada en ‘pallets’ y contenedores automotrices. Y de proteger sus activos y velar por su seguridad se encarga Luis J. Rodríguez, con una destacada trayectoria en firmas de bebidas, ‘retail’ y logística. Este profesional ha atendido a ‘Segurilatam’ para hablar de los retos de seguridad en la cadena de suministro, la protección de ‘pallets’ y contenedores frente a pérdidas, robos o mal uso, el papel de la tecnología en la seguridad, etc.

Con su amplia experiencia en sectores como bebidas, *retail* y, actualmente, logística, ¿cuáles diría que son los principales retos en materia de seguridad dentro de la cadena de suministro hoy en día?

Sin lugar a duda, los retos son muchos, especialmente en una región como Latinoamérica. Uno de los principales retos es asegurar que las mercancías se transporten de un lugar a otro y que, además de en buen estado, lleguen completas y no sufran mermas debido a lo que en el sector se conoce como pérdida desconocida. Otro reto grande es evitar que los bloqueos carreteros, de vías férreas y de los puertos, que también han presentado mucha mayor incidencia recientemente en distintos países de América Latina, afecten el tiempo de entrega y seguridad de la mercancía.

Esto sólo se puede lograr con una actualización constante, teniendo contacto con las autoridades y contando con información de inteligencia confiable para contactar con Logística de cara a que se ajusten o pospongan las rutas.

CHEP opera con soluciones reutilizables y en un entorno logístico global. ¿Qué medidas específicas han implementado para proteger activos tan estratégicos como los *pallets* y contenedores frente a pérdidas, robos o mal uso?

Esta es una tarea muy compleja, ya que, a diferencia de otras industrias donde el activo está bajo tu resguardo, en nuestro caso, la mayor parte del tiempo no está en nuestro poder, sino en el de nuestros clientes y distribuidores.

Hemos implementado soluciones tecnológicas, plataformas web y, sobre todo, un acercamiento muy continuo con nuestros clientes, y los clientes de nuestros clientes, para acompañarlos en

Protección Segura sin Riesgo Letal



NOLETAL: Soluciones no letales para proteger y servir en México.

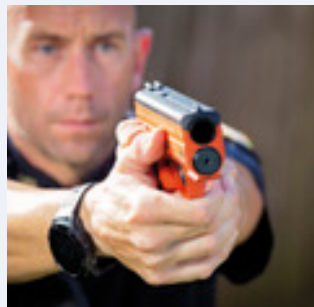
NOLETAL, distribuidor autorizado de **Byrna México**, entiende las necesidades y desafíos únicos de quienes protegen infraestructuras críticas y operan en el sector de **seguridad privada** en México. En un entorno marcado por alta violencia, falta de respeto a la autoridad y estrictas regulaciones, los **lanzadores Byrna** son herramientas seguras, efectivas y legalmente compatibles, ideales para empresas de seguridad privada y cuerpos de seguridad pública.

Beneficios Clave:

- Respuesta **efectiva y segura** en alto riesgo
- Compatible con **regulaciones** mexicanas
- Alcance de hasta **28 metros**
- **Capacitación y certificación** incluidas
- Efecto disuasorio con **bajo riesgo operativo**
- **Menos trámites** y carga regulatoria
- Certeza de uso **sin consecuencias fatales**

Di No a la Violencia Letal. Sí al Control sin Lesiones Permanentes.

Solicite una **demonstración** para ver de primera mano cómo nuestros **lanzadores no letales** pueden fortalecer sus **operaciones de seguridad en situaciones reales**.



Ofrecemos una gama de opciones, desde lanzadores compactos tipo pistola hasta modelos tipo escopeta y subametralladora, cada uno diseñado para adaptarse a las exigencias de **protección en situaciones críticas**. Con un alcance de hasta 28 metros, **alta precisión y un potente efecto disuasorio**, los lanzadores Byrna protegen infraestructuras estratégicas, instalaciones críticas y VIPs de manera confiable. Además, en **NOLETAL** brindamos **capacitación y certificación** para que los equipos de seguridad operen de manera ética, eficaz y en conformidad con la regulación mexicana.

DESCUBRE NUESTROS LANZADORES:



BYRNA LE



TMC ELITE



ESCOPEA P2P



el manejo y devolución de nuestros activos, de modo que regresen a nuestras plantas para su revisión y reparación, y puedan volver al circuito CHEP. Nuestro equipo de campo está continuamente visitando clientes y rastreando posibles transferencias que fueron registradas en nuestros sistemas con el fin de recuperar los *pallets*.

¿Cómo se equilibra la eficiencia operativa con la seguridad en un entorno donde el volumen y la rotación de activos son tan elevados como en CHEP?

Como en cualquier negocio, tenemos que buscar el equilibrio entre eficiencia y coste operativo para no afectar los balances financieros de la empresa. Continuamente se evalúan las métricas para que los recursos se utilicen de la manera más eficiente posible.

Desde su perspectiva, ¿qué papel juega la tecnología (IoT, trazabilidad, analítica de datos...) en la evolución de la protección de activos en logística? ¿CHEP está apostando por alguna innovación concreta?

El tren de la tecnología es muy importante y quien no se suba a él se va a quedar atrás. Es más, me atrevería a decir que quien no la usa ahora, ya se ha quedado atrás. De forma continua, CHEP está analizando e implementando tecnología que nos permita servir mejor a nuestros clientes y, al mismo tiempo, minimizar las pérdidas. Algunos proyectos aún son confidenciales porque están en desarrollo y no los puedo comentar.

Pero, en general, el uso del rastreo de nuestros transportes, el disponer de una base de datos de nuestros operadores de transporte que se conecta con muchas otras empresas a través de un tercero, las geocercas en las rutas y las alertas de detención del transporte, entre otras, son tecnologías de uso diario



y constante. Seguramente, en muy poco tiempo veremos mucha innovación en este campo debido a la IA y al IoT.

Con operaciones en múltiples países y culturas, ¿cómo se gestionan los estándares de seguridad y prevención en una región tan diversa como América Latina?

Es una excelente pregunta, ya que esto no es fácil. Además de la cultura, las situaciones de los países y sus problemáticas muchas veces son muy distintas. Lo que hacemos nosotros es partir de un estándar que ya tiene resultados comprobados en uno o dos países, generalmente los más grandes en cuanto a mercado, e intentar implementar el mismo estándar en otro país que está ingresando a nuestro negocio. Nuestro equipo local evalúa el desempeño de este estándar y comienza a identificar qué es lo que hay que cambiar y por qué.

Una vez que ejecutamos este proceso en todos los países, elaboramos un procedimiento estándar general para toda la región y, posteriormente, hacemos estándares particulares que abarcan

sólo algunos conceptos puntuales para cada país. Esto, por supuesto, tiene que contemplar las regulaciones y las leyes de cada país.

¿Qué principios considera fundamentales para liderar equipos de seguridad eficaces y resilientes?

Siempre debemos dar ejemplo a nuestros colaboradores, estar muy cerca de ellos y escucharlos. Los que más saben son las personas de tu equipo, las personas que están en campo, que dan la cara al cliente y que conocen el detalle del día a día. Personalmente, cuando quiero hacer un cambio a un proceso o a la forma en que realizamos algo actualmente, hablo con mi equipo sobre la propuesta y le pido su opinión sincera. Si eres un líder cercano y estás abierto a escuchar crítica constructiva, el equipo te dará su opinión real del asunto.

Y nunca hay que olvidar que líder es aquel o aquella a quien siguen por convicción y no por obligación, y eso se ve a simple vista. Como líder, no solamente eres el jefe; eres un integrante más del equipo. **S**

HACEMOS DEL MUNDO UN LUGAR MÁS SEGURO



ASISte a una de nuestras
Reuniones Mensuales
y conoce de primera mano
el valor que **ASIS** te aporta.

ASIS International es una comunidad global de más de 34,000 profesionales de la seguridad, en todas las industrias y etapas de su carrera.

BENEFICIOS DE LA MEMBRESÍA:

Oportunidades de intercambio de conocimiento, recursos valiosos y conexiones entre pares.
Expande tu experiencia y desarrolla tu carrera, sin importar tu nivel profesional (precios afiliación)
Haz crecer tu experiencia uniéndote a nuestras Comunidades
— **incluido en tu membresía ASIS.**



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

¡Qué esperas!

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





Verónica Torres Landa

Directora general de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP)

“El sector del ‘retail’ requiere servicios de seguridad privada flexibles, especiales y dinámicos”

■ Por Gabriela Soto y Bernardo Valadés.

El sector del ‘retail’ es muy importante y tiene un gran aliado en la industria de la seguridad privada. Esta última, explica Verónica Torres Landa, directora general de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP), va más allá de los guardias intramuros y contribuye a la protección de sus clientes con tecnología, rastreo vehicular, GPS, prevención de pérdidas, contención y análisis de riesgos, respuesta ante incidentes y supervisión tanto presencial como remota.

¿Qué importancia tiene el sector del *retail* para la industria de la seguridad privada en México?

Es un sector muy importante que conlleva una alta rotación de personal, afluencia de clientes de forma masiva, traslado de valores y una seguridad perimetral y logística en su cadena de suministro muy compleja y especial, lo que provoca generar análisis de riesgo específicos para proporcionar servicios de seguridad flexibles, pero, sobre todo, especiales y dinámicos.

La industria de la seguridad privada aporta valor con guardias intramuros, tecnología (controles de acceso, CCTV, monitoreo, cámaras, etc.), rastreo vehicular, GPS en productos, vehículos y personal, prevención de pérdidas, la contención de riesgos, la elaboración de protocolos de respuesta ante incidentes, la supervisión presencial y remota, y el análisis de riesgos. Todo esto ha hecho que los servicios de seguridad privada y su industria logren que el comercio al por menor tenga continuidad operativa y sea eficaz y eficiente.

¿Cuál es el perfil profesional y la formación que reciben los guardias de seguridad privada que operan en entornos comerciales?

Son profesionales que reciben capacitación específica como atención al cliente, detección de comportamientos sospechosos, derechos humanos, control de accesos, gestión de crisis y primeros auxilios. En AMESP promovemos estándares y competencias para su formación y este personal debe tener habilidades específicas para el sector del *retail*.

¿Qué papel desempeña la seguridad privada en la detección y disuasión de hurtos, tanto internos como externos, en los puntos de venta?

El papel de las empresas de AMESP que prestan servicios al *retail* es imprescindible toda vez que inicia con un análisis de riesgos y una revisión del histórico de incidencias para implementar los procesos necesarios como vigilancia intramuros, perimetral y encubierta en su caso, uso de tecnología de detección en tiempo real, prevención y disuasión. Es uno de los servicios más demandados. Por ello, la seguridad privada ha evolucionado significativamente.

Los hurtos, robos, rapiñas, etc., pueden provenir tanto del interior como del exterior. De ahí que sea necesario un servicio integral. La presencia de los guardias intramuros es altamente disuasorio con la intención de reducir los actos ilícitos. Ante un incidente, el personal está capacitado para actuar dentro del marco legal, resguardando la cadena de custodia como auxiliares de seguridad pública y reportando conforme a consignas establecidas con el cliente.

Además de la vigilancia física en tiendas, ¿qué otros servicios prestan las empresas de seguridad privada al sector del *retail*, por ejemplo, en materia de logística, protección de mercancías o gestión de riesgos?

Como comentaba anteriormente, la seguridad privada para el *retail* va mucho más allá del guardia intramuros. Brindamos servicios que abarcan toda la cadena operativa: custodia de mercancías, implementación de tecnología (cámaras, sistemas de posicionamiento global GPS, controles de acceso...), monitoreo de unidades de transporte, procesos logísticos, gestión de crisis y sistemas de control interno.

Se llevan a cabo análisis de riesgo para hacer mapas de calor y generar estrategias para que se conozcan los servicios públicos con que se cuenta para apoyo ante incidentes, determinamos áreas de

oportunidad en tiendas, almacenes o centros de distribución y diseñamos planes de contingencia ante hurtos/robos, vandalismo, farderos, rapiñas, bloqueos o protestas y situaciones generadas por la naturaleza, como inundaciones, temblores, explosiones, etc. AMESP cuenta incluso con empresas especializadas en inteligencia y seguridad corporativa que dan al cliente la posibilidad de generar estrategias operativas para su ejecución.

¿Qué soluciones tecnológicas están implementando las empresas de seguridad privada en colaboración con cadenas de *retail* para mejorar la seguridad en tiendas, almacenes, centros de distribución y transporte de mercancías?

Las empresas de seguridad privada han incorporado herramientas como controles de acceso con inteligencia artificial (IA), videoanalítica, cámaras con reconocimiento facial, sistemas de conteo de personas y plataformas integradas de monitoreo y rastreo.

Las empresas afiliadas a AMESP poseen soporte tecnológico para cubrir las necesidades del cliente, activar protocolos y disuadir incidentes. Por ejemplo, mediante análisis y con el uso de CCTV con tecnología de punta pueden detectar comportamientos atípicos de personas dentro y fuera del inmueble o en carreteras y solicitar apoyo de autoridades para evitar conflicto o ataque, y lograr evitar que presuntos delincuentes realicen un ilícito. Cuentan con drones para vigilan-

cia perimetral en grandes almacenes o centros de distribución y pueden implementar rastreo con sistemas de posicionamiento global GPS para transporte de insumos o reparto en cadena.

AMESP ha ayudado a poner al día a las empresas de *retail* en materia de tecnologías que se presentan en el mercado para que las puedan integrar a sus procesos o sistemas propios, generando sinergias que fortalecen la reducción de pérdidas y la disminución de incidencias.

¿Cómo se coordina la seguridad privada con las autoridades en situaciones de emergencia o delitos en entornos comerciales y qué protocolos existen para asegurar una respuesta eficaz?

“La industria de la seguridad privada aporta valor al sector del ‘retail’ en México con una amplia oferta de soluciones”

Uno de los éxitos más grande que tiene la industria de la seguridad privada es la vinculación estratégica con las autoridades de los tres niveles de gobierno para atender la problemática ante hechos delictivos o presunción de actos que atenten contra la seguridad de las personas.

En México, las empresas de seguridad privada actúan como auxiliares de la seguridad pública y su acción inmediata es preservar la zona donde se cometió el delito o supuesto incidente y el inicio de la cadena de custodia. Por eso, la comunicación con las autoridades debe ser inmediata, directa y con protocolos preestablecidos. Y nuestra asociación cuenta con esa coordinación interinstitucional. **S**



Nicolás Botero-Páramo Gaviria

Presidente ejecutivo de FedeseSeguridad

“La seguridad privada contribuye a que el comercio minorista sea más seguro y eficiente”

■ Por Marcela Linares Vásquez y Bernardo Valadés.

Nicolás Botero-Páramo Gaviria, presidente ejecutivo de la asociación FedeseSeguridad, analiza el papel que desempeña la seguridad privada en la industria del ‘retail’. En esta entrevista, destaca cómo la colaboración entre los usuarios y las empresas del sector de la seguridad privada permite afrontar desafíos como la prevención de pérdidas en puntos de venta y la protección logística. Además, se pronuncia sobre las tendencias que marcarán esa relación.

¿Qué importancia tiene el sector del *retail* para la seguridad privada en Colombia y cómo contribuye esta última al funcionamiento del comercio minorista?

El sector del *retail* es uno de los principales usuarios de los servicios de seguridad privada y requiere esquemas de protección integrales. La seguridad privada contribuye a un comercio minorista más seguro y eficiente mediante la protección de activos, la reducción de pérdidas y la mejora de la rentabilidad. Además, fomenta entornos de compra más seguros que incrementan la confianza de los clientes y fortalecen la fidelización. Y en grandes superficies, garantiza la continuidad operativa y protege tanto a trabajadores como a visitantes.

Gracias a los sistemas de videovigilancia y control de acceso, es posible una supervisión constante y respuestas rápidas ante incidentes, así como un mejor seguimiento de indicadores de seguridad. También es fundamental la elaboración de informes que permitan comprender y documentar los delitos. Finalmente, la seguridad privada aporta eficiencia operativa, permitiendo que los negocios funcionen con mayor tranquilidad.

¿Cuál es el perfil profesional y la formación de los guardas en el *retail*?

Los guardas deben contar con un perfil profesional específico adecuado a las exigencias del *retail*. Su labor no se limita a vigilar, sino que implica también la atención al cliente, la prevención de riesgos y el aporte a una experiencia de compra segura. Entre sus competencias destacan la vigilancia, el control de acceso, el manejo de situaciones de riesgo y la capacidad para interactuar con los clientes. Trabajan en espacios como centros comerciales, supermercados y tiendas de gran afluencia.

Además, deben dominar habilidades como la comunicación efectiva, la resolución de conflictos y el conocimiento de las normativas de seguridad. En cuanto a su formación, reciben cursos sobre legislación, protocolos de emergencia y uso de tecnologías. También se entrenan en estrategias para evitar fraudes y robos. En el *retail*, su función se adapta especialmente a las necesidades del entorno: su presencia debe ser disuasoria, pero también cercana; deben gestionar multitudes en temporadas altas y colaborar con el personal del comercio para identificar riesgos.

¿Qué papel desempeña la seguridad privada en la prevención de pérdidas en los puntos de venta?

En el caso de las amenazas externas, se trabaja en la identificación de estructuras delincuenciales en coordinación con las autoridades y se realiza una vigilancia activa desde el acceso a los establecimientos. La tecnología juega un papel fundamental, con sistemas electrónicos que detectan intentos de robo y cámaras con inteligencia artificial (IA) que identifican comportamientos inusuales. Para controlar el hurto interno, se aplican auditorías periódicas, controles discretos sobre los empleados y protocolos de supervisión. A ello se suman estrategias de disuasión como la presencia visible de seguridad, el uso de botones de pánico, sistemas de geolocalización y la capacitación tanto del personal de vigilancia como de los empleados, incluyendo formación específica en perfilamiento para caracterizar posibles infractores.

¿Qué otros servicios prestan las empresas de seguridad al *retail*?

En el ámbito logístico, ofrecen monitoreo satelital de vehículos de carga y control de acceso en bodegas con sistemas automatizados. También implementan video-

vigilancia avanzada y realizan auditorías para detectar vulnerabilidades. En la gestión de riesgos, proporcionan consultoría especializada, integran alarmas y sensores, y diseñan planes de emergencia para incidentes como robos o incendios. Todo ello se orienta a una protección integral de las mercancías, desde el transporte hasta el punto de venta.

¿Qué tipo de soluciones tecnológicas están implementando para mejorar la seguridad en tiendas y almacenes?

Entre ellas se incluyen cámaras con análisis de comportamiento, reconocimiento facial y monitoreo en tiempo real desde centros de control. En el ámbito del control de acceso, se utilizan sistemas

de 1994. Para garantizar la seguridad, se utilizan vehículos blindados con tecnología avanzada y monitoreo GPS, se diseñan rutas seguras y se entrena al personal en manejo de crisis. Desde los centros de control, se supervisa constantemente el desarrollo del trayecto para detectar cualquier anomalía.

¿Cómo se coordina la seguridad privada con las autoridades públicas?

La coordinación se realiza a través de iniciativas como la Red de Tiendas Seguras, promovida por la Policía Nacional, que facilita la comunicación entre comerciantes y autoridades. Las empresas de seguridad establecen canales directos con los organismos públicos y

“Hoy no se trata sólo de vigilar, sino de atender al cliente, anticipar riesgos y contribuir a una experiencia de compra segura”

biométricos, cerraduras electrónicas y listas de verificación para gestionar entradas. Para el transporte de mercancías, se emplean sistemas de rastreo satelital y protocolos de respuesta ante incidentes. Asimismo, la integración de plataformas de análisis de datos permite detectar patrones de riesgo y mejorar las estrategias de seguridad, mientras que la automatización de auditorías ayuda a prevenir errores y fraudes.

¿Cuáles son los principales desafíos en el traslado de valores?

El traslado de valores representa un desafío crítico. Las rutas son vulnerables a ataques, especialmente durante la carga y descarga. Además, deben cumplirse estrictas normativas, como el Decreto 356

participan en programas de formación conjunta. En caso de incidentes, se activan sistemas de alerta conectados con la Policía, se aplican procedimientos de evacuación y se intercambia información sobre los hechos para mejorar las estrategias de prevención.

¿Qué tendencias observa en la relación entre el *retail* y la seguridad privada?

Se prevé un uso creciente de la IA para anticipar riesgos. Los algoritmos de análisis predictivo, el empleo de drones para el monitoreo, las cámaras con reconocimiento facial y el refuerzo de la ciberseguridad están redefiniendo la protección del *retail*. Todo apunta a una integración cada vez más fuerte entre vigilancia física y soluciones digitales. **S**



Vanessa Cure Anturi

Directora ejecutiva de la Asociación Colombiana de Seguridad (Asosec)

“Al actuar como elemento disuasorio, la seguridad privada es fundamental en la prevención de pérdidas”

■ Por Marcela Linares Vásquez y Bernardo Valadés.

“La presencia estratégica de las empresas de seguridad privada en puntos críticos, combinada con procedimientos de control y observación, permite anticiparse a comportamientos sospechosos y actuar con oportunidad ante posibles eventos de pérdida”, comenta Vanessa Cure Anturi, directora ejecutiva de la Asociación Colombiana de Seguridad (Asosec), al destacar el papel que desempeña este sector en la protección de la industria del ‘retail’.

¿Qué importancia tiene el sector del *retail* para la industria de la seguridad privada en Colombia?

Es un aliado estratégico, ya que representa un entorno dinámico con alto flujo de personas, mercancías y transacciones que requiere protección constante. Su operación eficiente depende, en gran medida, de contar con servicios de vigilancia especializados que prevengan riesgos y generen confianza en clientes, colaboradores y proveedores.

La seguridad privada contribuye al funcionamiento seguro del comercio minorista mediante acciones preventivas, control de accesos, gestión de incidentes y apoyo logístico, permitiendo que las operaciones se desarrollen sin interrupciones. Además, fortalece la percepción de orden y respaldo en los puntos de venta, lo que incide directamente en la experiencia del consumidor y en la rentabilidad del negocio.

¿Cuál es el perfil profesional y la formación que reciben los guardas de seguridad privada que operan en entornos comerciales?

Deben contar con formación integral que combine habilidades técnicas en vigilancia con competencias en atención al cliente, manejo de conflictos y prevención de pérdidas. Esta preparación, reglamentada por la Supervigilancia, es clave para enfrentar los retos específicos del *retail*, donde la seguridad convive con la experiencia del consumidor.

Su labor se adapta a las particularidades del comercio minorista al desempeñar funciones preventivas, disuasivas y operativas, siendo muchas veces la primera imagen del establecimiento. Por ello, su perfil debe ser proactivo, comunicativo y orientado al servicio, con capacidad para actuar con criterio ante situaciones de riesgo o emergencias.



◆ Experiencia ◆ Tecnología ◆ Seguridad



**AÑOS
DESDE 1995**



Grupo IPS, líderes en seguridad privada.

grupoipsmexico.com



¿Qué papel desempeña la seguridad privada en la detección y disuasión de hurtos, tanto internos como externos, en los puntos de venta?

Las empresas de seguridad privada cumplen un rol fundamental en la prevención de pérdidas al actuar como un elemento disuasorio. Su presencia estratégica en puntos críticos, combinada con procedimientos de control y observación, permite anticiparse a comportamientos sospechosos y actuar con oportunidad ante posibles eventos de pérdida.

Además, muchas empresas ofrecen servicios especializados en análisis de riesgos, identificación de patrones delictivos y apoyo en la implementación de tecnologías que fortalecen los sistemas de vigilancia. Esta labor conjunta con el área operativa y de prevención del *retail* permite minimizar pérdidas, proteger los activos y mejorar la eficiencia del negocio.

Además de la vigilancia física en tiendas, ¿qué otros servicios prestan las empresas de seguridad privada al sector del *retail*?

Prestan servicios complementarios de gran valor como escoltas para transporte de mercancías, monitoreo remoto y gestión de riesgos operativos y logísticos. Estos servicios permiten proteger la cadena de suministro desde el centro de distribución hasta el punto de venta.

Asimismo, se ofrece consultoría en prevención de pérdidas, control de accesos, seguridad en centros logísticos y apoyo en la implementación de protocolos ante emergencias. Esta oferta diversificada responde a las necesidades del comercio moderno, que requiere soluciones integrales y adaptadas a un entorno cada vez más exigente y competitivo.

¿Qué tipo de soluciones tecnológicas están implementando las empresas de seguridad privada en colaboración

con cadenas de *retail* para mejorar la seguridad en tiendas, almacenes, centros de distribución y transporte de mercancías?

Están implementando soluciones tecnológicas como cámaras con analítica de video, control de accesos automatizados y sistemas de monitoreo en tiempo real que permiten una gestión más precisa y eficiente de los riesgos en tiendas, almacenes y centros de distribución.

También se destacan herramientas como *software* de prevención de pérdidas, dispositivos de geolocalización para escoltas y plataformas integradas de seguridad que conectan a los diferentes actores de la operación. Estas tecnologías no sólo fortalecen la capa-

Para garantizar la seguridad en estos procesos críticos, las empresas implementan esquemas operativos especializados, con personal altamente capacitado, uso de tecnología de rastreo y monitoreo en tiempo real, y coordinación con entidades públicas y privadas. Además, se promueve el cumplimiento estricto de la normatividad vigente para asegurar un servicio legal, eficiente y confiable para el sector del *retail*.

¿Cómo se coordina la seguridad privada con las autoridades públicas en situaciones de emergencia o delitos en entornos comerciales y qué protocolos existen para asegurar una respuesta eficaz?

“En gran medida, la operación eficiente del sector del ‘retail’ depende de contar con servicios de vigilancia especializados”

cidad de reacción, sino que optimizan los recursos humanos y mejoran la trazabilidad en procesos críticos como el transporte de mercancías.

En cuanto al traslado de valores y efectivo, ¿cuáles son los principales desafíos que enfrentan las empresas de seguridad privada?

Desde Asosec identificamos que los principales desafíos en el traslado de valores y efectivo incluyen la seguridad en las rutas, la delincuencia organizada, la rotación del personal y, en algunos casos, la coordinación limitada con las autoridades. Estas condiciones exigen una planeación rigurosa y protocolos estrictos para minimizar los riesgos durante el transporte.

La coordinación entre la seguridad privada y las autoridades públicas es esencial para garantizar una respuesta rápida y eficaz ante emergencias o hechos delictivos en entornos comerciales. Esta articulación se basa, en muchos casos, en protocolos internos de las empresas que contemplan rutas de comunicación con la Policía Nacional, organismos territoriales y personal de respuesta local.

Sin embargo, aún existe una brecha significativa, ya que algunas empresas no cuentan con protocolos formalizados. Por ello, promovemos la implementación de procedimientos estandarizados y el fortalecimiento de canales de cooperación público-privada que permitan actuar de manera conjunta, reducir tiempos de respuesta y mejorar la seguridad integral. **S**



SISTEMAS DE SEGURIDAD INTEGRAL

Simplifica la gestión de la seguridad de las instalaciones con DASSnet®, la plataforma integral que permite controlar los sistemas desde un único punto.

Control de Accesos, alarmas e intrusión, incendios, CCTV, gestión de visitas...





Seguridad en el 'retail': ¿cómo prevenir hurtos físicos y fraudes en línea?

■ Por Redacción.

Según un reciente sondeo llevado a cabo por *Segurilatam* en su página de LinkedIn, los hurtos externos e internos, el fraude en el comercio electrónico y la coordinación de equipos y tecnologías, en porcentajes casi similares, son algunos de los mayores retos de seguridad en el *retail* que enfrentan las empresas de dicho sector en la actualidad.

Hurtos externos

En el caso de los hurtos externos (28%), es decir, aquellos cometidos por personas ajenas a la empresa (clientes, visitantes o delincuentes), representan el principal desafío de seguridad en el *retail* en opinión de quienes han participado en la encuesta. De cara a prevenirlos, los expertos aconsejan tener en cuenta las siguientes de medidas:

- » **Videovigilancia inteligente.** Como ha quedado de manifiesto en otro sondeo de *Segurilatam*, el CCTV con analítica de vídeo es considerada la medida más eficaz en la prevención de pérdidas en tiendas físicas. Ello es así porque permite detectar comportamientos sospechosos en tiempo real y disuadir a posibles ladrones.
- » **Vigilancia electrónica de artículos (EAS).** Asimismo, instalar etiquetas de seguridad en productos y arcos de detección en las salidas reduce significativamente los robos en tiendas físicas.
- » **Control de accesos y vigilancia presencial.** De igual manera, contar con



guardias de seguridad privada y controlar las entradas y salidas de los espacios comerciales ayuda a reducir la probabilidad de robos premeditados.

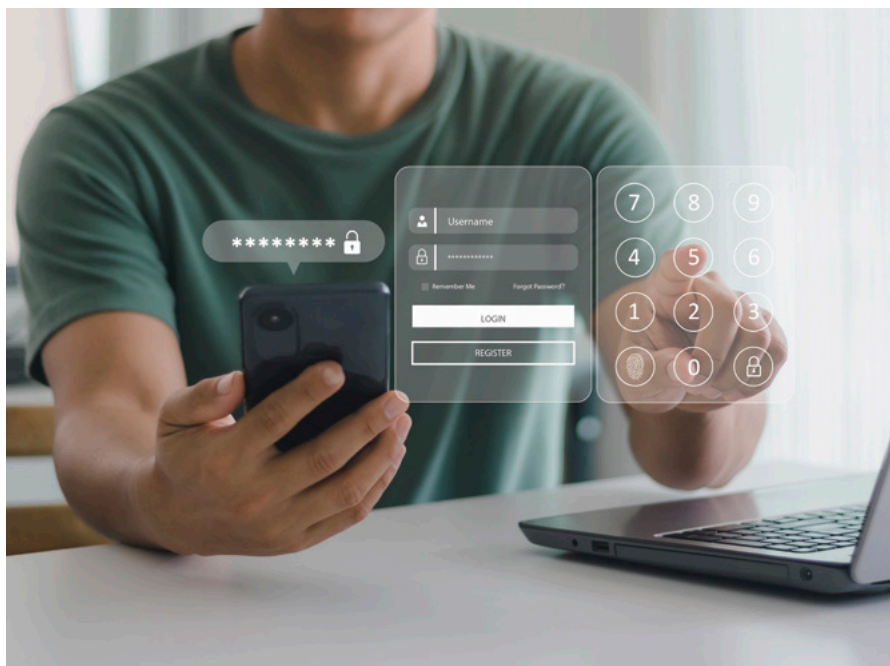
- » **Diseño estratégico del espacio.** Distribuir el mobiliario de forma que no existan zonas muertas ni puntos ciegos también mejora la supervisión visual por parte del personal de la tienda.
- » **Formación del personal de tienda.** Finalmente, es indispensable capacitar a los empleados para identificar actitudes sospechosas y actuar adecuadamente ante posibles hurtos.

Hurtos internos

En cuanto a los hurtos internos (26%) cometidos por empleados, continúan siendo, en mayor o menor medida, una preocupación para quienes velan por la seguridad en el *retail*. Suele tratarse de

robos de productos, manipulación de cajas registradoras y alteración de inventarios. Y para combatirlos se sugiere contemplar estas medidas:

- » **Auditorías e inventarios regulares.** Realizar conteos periódicos de *stock* ayuda a detectar anomalías y responsabilizar a los equipos correspondientes.
- » **Controles cruzados en la caja.** Por su parte, establecer sistemas donde más de un empleado verifica las operaciones de cobro limita la oportunidad de fraude individual.
- » **Política de cero tolerancia.** Igualmente, comunicar de forma clara que el robo interno será penalizado genera un efecto disuasorio.
- » **Supervisión tecnológica de operaciones.** Monitorizar con *software* de gestión las actividades del personal



La seguridad en el 'retail' debe combinar tecnología, procedimientos claros y una cultura organizacional basada en la ética y la prevención

en cajas y almacenes permite identificar patrones sospechosos.

- » **Clima laboral ético y saludable.** Por último, fomentar una cultura organizacional basada en la integridad reduce las motivaciones internas para delinquir.

Fraudes en línea

El crecimiento del *e-commerce* ha abierto nuevas vías de negocio, pero también ha dado lugar a un aumento de los fraudes en línea (23%) como el robo de datos, los pagos con tarjetas robadas o los pedidos falsos. Por ello, en materia de seguridad en el *retail*, las empresas del sector tienen que proteger tanto sus plataformas como a las personas que las usan de cara a mantener la confianza en el canal *online*. Para ello, deben:

- » **Implementar pasarelas de pago seguras.** Utilizar proveedores certificados que cuenten con autenticación multifactor reduce el riesgo de transacciones fraudulentas.
- » **Monitorizar el comportamiento de los compradores.** El uso de inteligencia artificial (IA) para detectar patrones anómalos facilita identificar actividades sospechosas antes de que se complete la compra.
- » **Cifrar y proteger los datos.** Asegurar que la información personal y financiera esté cifrada es una barrera para evitar que los ciberdelincuentes la intercepten.
- » **Compartir consejos de seguridad.** Del mismo modo, es importante compartir recomendaciones para los

usuarios instándoles a comprar en sitios web verificados, no compartir contraseñas ni datos sensibles y activar alertas para detectar cargos no autorizados.

Personal y tecnología

Por lo que respecta a la coordinación de equipos humanos y herramientas tecnológicas (23%), es otro de los retos de seguridad en el *retail* tanto en tiendas físicas como en plataformas digitales. En este sentido, a juicio de los expertos, una estrategia eficaz de integración requiere:

- » **Uso de tecnologías integradas.** La videovigilancia conectada a *software* de análisis, los sensores IoT y los sistemas de planificación de recursos empresariales (ERP) posibilitan un control global y centralizado.
- » **Capacitación continua.** Los equipos deben recibir formación periódica para adaptarse a nuevas amenazas y tecnologías.
- » **Protocolos claros de actuación.** Tener procedimientos definidos para actuar ante robos, fraudes o ciberataques facilita una respuesta rápida y coordinada.
- » **Colaboración con fuerzas de seguridad y asociaciones del sector.** Y compartir información sobre nuevas amenazas permite adelantarse a posibles incidentes y mejorar las prácticas del sector en su conjunto.

En definitiva, la seguridad en el *retail* exige una estrategia integral que combine tecnología avanzada, procedimientos claros y una cultura organizacional basada en la ética y la prevención. Tanto los hurtos externos e internos como los fraudes en línea y la falta de coordinación entre equipos representan amenazas reales que requieren respuestas específicas y actualizadas. **S**



Prevención de pérdidas en tiendas físicas: ¿cuál es la medida más eficaz?

■ Por Redacción.

Con el objetivo de conocer la opinión de los profesionales vinculados al sector del *retail* sobre la prevención de pérdidas en tiendas físicas, *Segurilatam* ha llevado a cabo una encuesta a través de LinkedIn en la que ha planteado la siguiente pregunta: «¿Qué medida consideras más efectiva para prevenir pérdidas en una tienda física?». Y ha obtenido los siguientes resultados:

- » CCTV con analítica de vídeo (53%).
- » Control de inventario en tiempo real (26%).
- » Etiquetas RFID (19%).
- » Vigilantes de seguridad (2%).

CCTV con analítica

Esencial en la prevención de pérdidas en tiendas físicas, dicha tecnología permite supervisar los espacios comerciales y, gracias a la inteligencia artificial (IA), también puede:

- » Detectar comportamientos sospechosos.
- » Alertar sobre posibles hurtos.
- » Generar informes automatizados.

De igual manera, la analítica de vídeo mejora la eficiencia operativa, ya que permite al personal centrarse en incidencias reales en lugar de monitorear imágenes durante horas. Esto reduce significativamente tanto el hurto externo como el interno (por parte de empleados), dos de las principales causas de pérdidas en el sector del *retail*.



Control de inventario

El control de inventario en tiempo real facilita la detección inmediata de discrepancias entre el *stock* registrado y el *stock* real, lo cual permite actuar con prontitud ante pérdidas o errores logísticos. Al disponer de una visión precisa y actualizada del inventario, los responsables de las tiendas pueden identificar patrones irregulares, evitar roturas de *stock* y reducir las oportunidades de hurto.

Etiquetas RFID

Por lo que respecta a las etiquetas RFID (identificación por radiofrecuencia), posibilitan realizar un seguimiento preciso de cada artículo desde su entrada en el almacén hasta su venta, lo que ofrece un control exhaustivo del inventario y minimiza el riesgo de pérdidas.

Asimismo, la tecnología RFID acelera los procesos de reposición y reduce los errores humanos. Aunque su coste de implantación aún representa una barrera

para algunas empresas, su eficacia en la prevención de pérdidas en tiendas físicas está ampliamente demostrada en grandes cadenas y sectores de alto valor.

Vigilantes de seguridad

Finalmente, los vigilantes de seguridad tienen un efecto disuasorio, pero su eficacia se ve limitada por varios factores. Para empezar, no pueden estar en todos los puntos de venta al mismo tiempo, lo cual reduce su capacidad de vigilancia frente a sistemas automatizados. Además, su intervención suele ser reactiva en lugar de preventiva.

Y mantener personal de seguridad, especialmente en horarios ampliados, supone un coste continuo para las empresas. Por ello, en un entorno donde se valora cada vez más la eficiencia tecnológica, es comprensible que los profesionales del sector opten por herramientas que ofrezcan una cobertura constante y análisis en tiempo real. **S**



**Del 27 al 29
de agosto**

Bogotá - Colombia

FERIA INTERNACIONAL DE SEGURIDAD

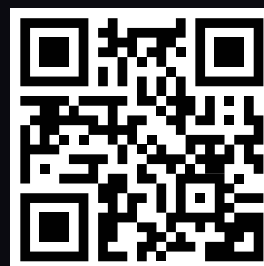
La Feria Internacional de Seguridad es el punto de encuentro donde la tecnología y el conocimiento transforman el sector, impulsando innovación, sostenibilidad y nuevas oportunidades de negocio.



BENEFICIOS DE ASISTIR A LA FERIA:

-  Acceso a Innovaciones y tendencias Globales
-  Conexión con los actores clave de la industria
-  Formación y actualización profesional
-  Pruebas en vivo
-  Actualización sobre normativas y regulaciones
-  Soluciones para Desafíos Reales
-  Acceso a conferencias y talleres de alto nivel

Regístrate en



**SEA PARTE DEL
FUTURO DE LA
SEGURIDAD GLOBAL**

ALLIED GUILDS



ORGANIZERS



MEDIA PARTNER





Tienda física y personal de seguridad, **sinónimo de confianza al comprar**

■ Por Redacción.

Con el propósito de conocer la percepción de los consumidores, en lo que a la seguridad en el sector del *retail* se refiere, *Segurilatam* ha llevado a cabo un sondeo en su página de LinkedIn planteando la siguiente pregunta: «¿Te sientes más seguro comprando en tienda física o en tienda *online*?».

Tienda física: más segura

A tenor de los datos de la encuesta, el 60% de los encuestados afirma sentirse más seguro comprando en una tienda física, frente al 4% que se inclina por la tienda *online*. Esta significativa diferencia de percepción puede deberse a varios factores que generan una mayor confianza en el entorno presencial:

- » **Presencia física del producto.** En una tienda física, los clientes pueden ver, tocar y probar los artículos antes de comprarlos, lo cual reduce el riesgo de insatisfacción.
- » **Atención personalizada.** La interacción directa con vendedores permite resolver dudas en el momento y recibir asesoramiento.
- » **Mayor sensación de control.** Al encontrarse en un establecimiento, los consumidores sienten que pueden intervenir o reclamar de forma más efectiva si surge un problema.
- » **Pagos más seguros.** Muchos compradores confían más en métodos de pago tradicionales como el efectivo o el datáfono en tienda que en las plataformas digitales.



- » **Percepción de seguridad.** La presencia de guardias de seguridad privada y medidas como las cámaras de videovigilancia del comercio incrementan la percepción de seguridad en los clientes.

Por otra parte, el 23% de quienes han participado en el sondeo considera que se siente igual de seguro tanto en una tienda física como en una tienda *online*. Una sensación equilibrada que se explica por diversos motivos:

- » **Experiencia digital previa positiva.** Usuarios que han tenido compras satisfactorias en línea tienden a confiar más en el canal *online*.
- » **Uso de plataformas reconocidas.** Comprar en tiendas *online* de marcas conocidas o *marketplaces* con políticas de protección al comprador genera confianza.

- » **Implementación de medidas de ciberseguridad.** Certificados SSL, autenticación de dos factores y pasarelas de pago seguras contribuyen a una experiencia segura.

- » **Costumbre y adaptación tecnológica.** Los consumidores más familiarizados con la tecnología están más tranquilos realizando transacciones digitales.

La reputación, esencial

Un aspecto fundamental que también se desprende de la encuesta es el valor que los consumidores otorgan a la reputación de la tienda: el 13% afirma que esta es la principal razón por la que se sienten seguros al comprar. Ya se trate de una tienda física o de una tienda *online*, la imagen de la marca influye directamente en la percepción de seguridad del cliente.

En este sentido, los directores de Seguridad Corporativa y los profesionales

de la ciberseguridad juegan un papel clave. Su labor no sólo se limita a proteger la infraestructura de su organización; además, se encargan de generar un entorno de confianza que garantice al consumidor que su compra es segura, tanto si se realiza en un local comercial como en un entorno digital.

Personal de seguridad

Otro sondeo ha puesto de manifiesto que la presencia de personal de seguridad en tiendas físicas es muy valorada por los consumidores. Así, casi la mitad de los encuestados ha afirmado sentirse más seguro en los establecimientos comerciales si los mismos cuentan con profesionales encargados de la seguridad.

Este resultado refuerza la importancia del factor humano en la seguridad comercial, demostrando que, a pesar del auge de las soluciones tecnológicas, la figura del vigilante continúa siendo un elemento esencial en la percepción de seguridad de los usuarios.

Presencia visible

Concretamente, el 49% de los encuestados otorga gran importancia a la presencia visible y activa del personal de seguridad en tiendas físicas, ya que transmite una sensación inmediata de control, prevención de riesgos y respuesta ante incidentes.

En este sentido, la figura del vigilante de seguridad, además de disuadir posibles actos delictivos, actúa como un punto de apoyo para los consumidores. Su presencia física genera confianza y en situaciones de emergencia, o ante comportamientos sospechosos, puede actuar con rapidez, lo que contribuye a mejorar la experiencia de compra.

Iluminación y entorno

En segundo lugar, con un 38% de los votos, los participantes han destacado la



iluminación y el entorno como factores que les hacen sentirse seguros en una tienda física. Este resultado pone de relieve la importancia del diseño ambiental como complemento a las medidas de seguridad convencionales.

Una tienda bien iluminada, con una distribución del espacio clara y un entorno cuidado, facilita la orientación de los clientes y reduce las zonas oscuras o rincones poco visibles que pueden generar desconfianza. Y, si bien no sustituyen al personal de seguridad, la iluminación y el entorno contribuyen a crear un ambiente en el que los compradores se sienten más tranquilos y seguros.

Señalización de las salidas

Con tan sólo el 8% de los votos, la señalización de las salidas ha sido valorada en menor medida. Esta respuesta revela una realidad interesante: aunque la señalización es un requisito obligatorio en materia de prevención de riesgos y evacuación, su presencia no genera una percepción inmediata de seguridad para el cliente medio.

Se trata de una medida de seguridad pasiva que, principalmente, es de ayu-

da en caso de emergencia. Al no estar vinculada con la vigilancia activa o la prevención directa, los consumidores no la asocian tan estrechamente con su bienestar durante una compra, a diferencia del personal de seguridad en tiendas físicas, cuya labor es percibida de forma más directa y constante.

Sistemas de cámaras

Por último, los sistemas de cámaras han obtenido el 5% de los votos, situándose como la opción menos valorada. Aunque estos sistemas tecnológicos juegan un papel crucial en el registro de incidentes y la prevención de pérdidas, los consumidores no parecen percibirlos como una herramienta inmediata de protección.

A pesar de su eficacia probada en entornos comerciales, las cámaras no ofrecen la interacción directa y la asistencia que sí proporciona el personal de seguridad en tiendas físicas. Esta diferencia explica por qué, a ojos de los compradores, la tecnología de videovigilancia no puede reemplazar, al menos por ahora, el valor añadido que aporta un vigilante en el establecimiento. **S**

El blindaje automotriz, pieza clave en la seguridad de la logística y el 'retail'

En un contexto marcado por la inseguridad en las carreteras y las calles de México, el blindaje automotriz se consolida como un elemento esencial para la protección del transporte de valores. Omar Lara, presidente de la Comisión de Blindaje Automotriz del CNB, analiza su impacto en la logística y el sector del 'retail' en el país.

■ Por Redacción.

En un país donde la seguridad en las carreteras y las calles se ha vuelto un desafío cotidiano, la industria del blindaje automotriz ha adquirido un papel protagonista en la protección de los traslados de valores y efectivo. Desde el sector logístico hasta el comercio minorista, cada vez más empresas confían en soluciones especializadas para garantizar operaciones seguras en un entorno complejo y cambiante.

Creciente inseguridad

"La importancia del blindaje automotriz en este sector crece cada día debido al incremento de inseguridad en las carreteras", afirma Omar Lara, secretario de la Mesa Directiva y presidente de la Comisión de Blindaje Automotriz del Consejo Nacional de la Industria de la Balística (CNB) de México. "Las empresas transportistas han optado por utilizar el blindaje como una opción de seguridad".

La tendencia no es nueva, pero se ha intensificado en los últimos años. El aumento de asaltos y agresiones a convoyes de transporte ha obligado al sector a buscar medidas que refuercen su seguridad más allá de los tradicionales sistemas de custodia. En ese contexto, el blindaje vehicular ha pasado de ser una medida excepcional a convertirse en una necesidad operativa.

Una industria especializada

Frente a esta demanda creciente, la industria mexicana del blindaje ha experimentado una evolución notable. "La demanda ha crecido tanto que han surgido empresas de blindaje automotriz especializadas y dedicadas exclusivamente a este segmento, es decir, al blindaje de camiones", explica Lara.

Estos vehículos cumplen funciones vitales: transportar dinero, mercancías de alto valor, equipos tecnológicos y otros activos clave para la operativa diaria de empresas comerciales y logísticas. Por ello, no sólo se trata de añadir una capa de protección física, sino de integrar un sistema de defensa completo.

"Para las empresas que prestan el servicio bajo un permiso de traslado de valores o mercancías, la Secretaría de Seguridad les exige que el nivel mínimo de blindaje sea el VPAM 6, bajo la norma europea VPAM APR (alemana), o el nivel 4 comercial, es decir, protección contra calibre 7.62x39 mm", detalla el representante del CNB.

Tecnología y estrategia

Pero el blindaje, por sí solo, no garantiza una operación segura. La eficacia del sistema depende de un conjunto de medidas complementarias que forman parte de una estrategia integral. "Por lo regular, estos vehículos incorporan sistemas

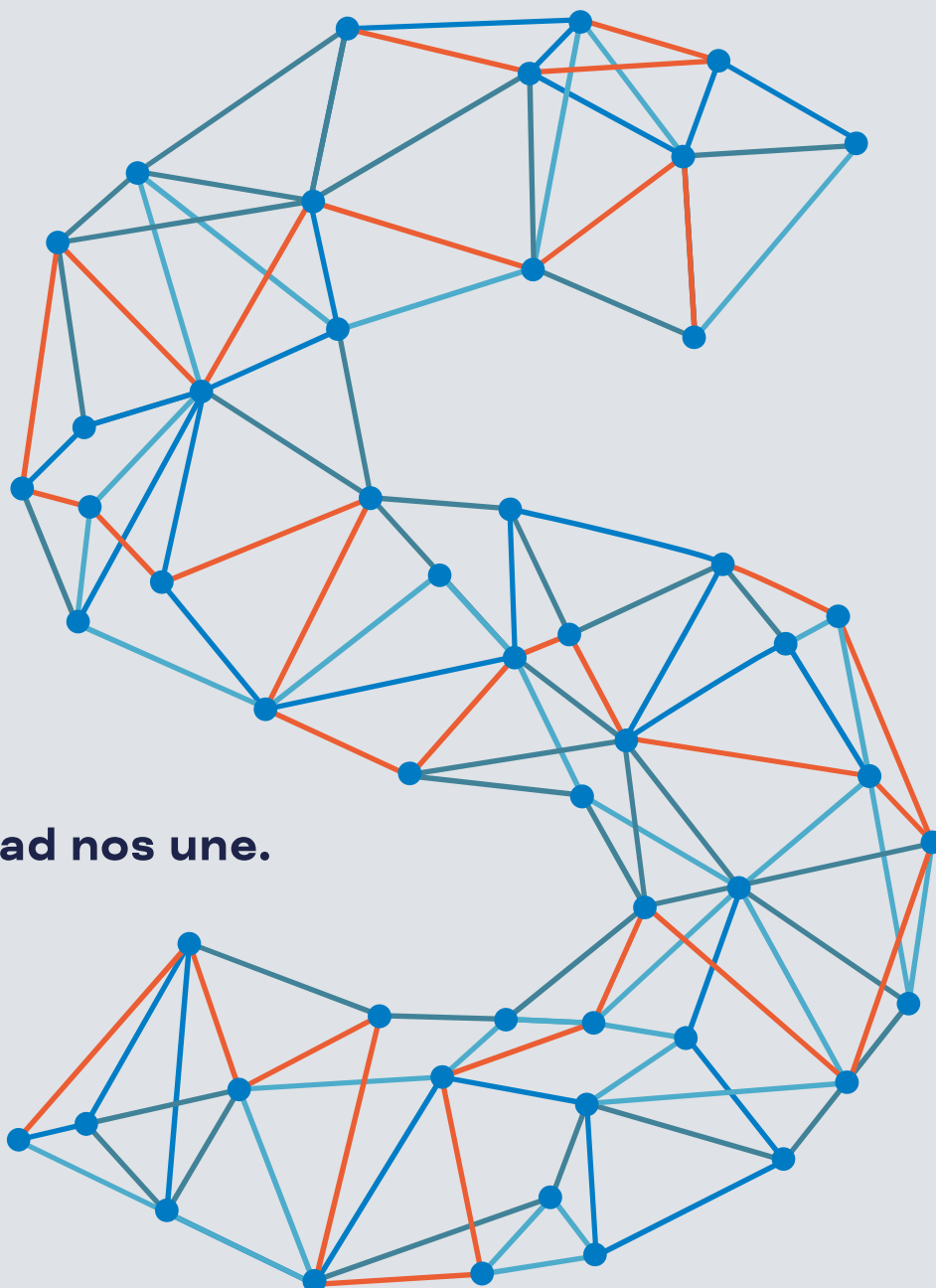


Omar Lara, presidente de la Comisión de Blindaje Automotriz del CNB.



Salón Internacional de la Seguridad

QUIERO
PARTICIPAR



La seguridad nos une.

24-27 **2026**
Feb ifema.es





“Debido al incremento de la inseguridad, las empresas transportistas han optado por utilizar el blindaje como una opción de seguridad”, explica Omar Lara

de geolocalización GPS, videocámaras en tiempo real y servicio de custodia en vehículos blindados”, precisa Lara.

La integración de estas tecnologías permite a las empresas monitorear en tiempo real el estado de cada operación y reaccionar con rapidez ante cualquier incidente. El uso de rutas inteligentes, análisis predictivo y protocolos de emergencia son ya parte del lenguaje habitual en este sector.

“Como empresas debidamente registradas ante las autoridades, ofrecemos un servicio bajo los lineamientos que permiten trasladarse por todo el territorio nacional sin contratiempos con las autoridades”, explica Lara. En ese sentido, el cumplimiento normativo es

tan importante como la tecnología implementada.

Calidad y legalidad

La labor del Consejo Nacional de la Industria de la Balística ha sido clave para establecer estándares de calidad y legalidad dentro del sector. “El CNB se encarga de aceptar y asociar empresas que reúnan los requisitos indispensables que amparan los procesos, la legalidad y la eficacia de los blindajes producidos”, señala Lara.

Estos requisitos incluyen, entre otros, certificados balísticos de los materiales utilizados, constancias emitidas por la Dirección General de Seguridad Privada (DGSP) y un cuestionario técnico

que evalúa la capacidad de la empresa. “Esto nos permite ofrecer y garantizar al usuario de blindaje automotriz la confianza en el producto adquirido”, enfatiza.

La confianza, precisamente, es uno de los activos más valiosos en este entorno. Las empresas que confían sus operaciones a vehículos blindados necesitan estar seguras no sólo de la resistencia de los materiales, sino de la trazabilidad y legalidad del proceso completo.

Menor peso, mayor eficiencia

La industria del blindaje no es ajena a la innovación. Las nuevas tecnologías están permitiendo soluciones más ligeras, resistentes y duraderas. “Las innovaciones en blindaje automotriz siguen la tendencia de reducir peso en los materiales para afectar lo menos posible los funcionamiento originales de los vehículos y, a su vez, hacer que tengan mayor vida útil”, explica Omar Lara.

Esta evolución no sólo mejora la eficiencia del vehículo blindado, sino que también reduce costes operativos y mejora la experiencia del conductor, un factor clave cuando se trata de largas rutas o condiciones de tráfico adversas.

Una industria estratégica

En el México actual, blindar un vehículo no es simplemente reforzarlo: es diseñar una herramienta logística con altos estándares de seguridad. Y, como señala Lara, “hacer sentir seguras a las personas ante un atentado es nuestra mayor responsabilidad”.

La industria del blindaje automotriz, en colaboración con autoridades, clientes y organismos reguladores, se ha consolidado como un pilar esencial en la protección del transporte de valores, en una sinergia entre innovación, estrategia y confianza que, a buen seguro, seguirá creciendo en los próximos años. **S**

LANACCESS

Discover the power of video.



vea nuestro video

Creciendo a su lado: videovigilancia con propósito



CÁMARA ESPAÑOLA
DE COMERCIO EN MÉXICO
RECONOCIMIENTO PYME 2025



www.lanaccess.com
CIUDAD DE MÉXICO | MADRID | BARCELONA | PARÍS



ONVIF® | GST

ENTREVISTA A CONCHA MARTÍNEZ CANO CON MOTIVO DEL RECONOCIMIENTO PYME 2025



Concha Martínez Cano

Directora ejecutiva de Lanaccess en Latinoamérica

“Lanaccess aporta valor con soluciones profesionales de videovigilancia ciberseguras, resilientes y de bajo consumo”

■ Por Redacción.

Para esta entrevista, Concha Martínez Cano nos recibe en las oficinas de Lanaccess en México, un espacio diáfano y luminoso situado en el corazón de Polanco, el distrito de negocios más vibrante de la CDMX. En un ambiente distendido, la directora ejecutiva de Latam nos habla de la obtención del Reconocimiento PyME 2025 por parte de la Cámara de Comercio Española y de la pasión y el compromiso que ha impulsado el crecimiento de Lanaccess en América Latina.

¿Qué ha significado para Lanaccess recibir el Reconocimiento PyME 2025 otorgado por la Cámara Española de Comercio en México?

Este premio es un honor inmenso que reconoce nuestro esfuerzo, compromiso e impacto. Nos motiva a continuar fortaleciendo los lazos económicos entre España y México y a seguir innovando para aportar aún más valor a la sociedad mexicana.

¿Qué recuerdo perdura en su memoria desde los comienzos de Lanaccess en México?

Recuerdo claramente los primeros días en México, con gran ilusión y expectativas. Comencé en el salón de mi departamento y pronto me encontré con la calidez y el entusiasmo del equipo que yo misma formé, confirmando que había tomado la decisión correcta.

¿Por qué decidieron apostar exclusivamente por talento local mexicano en sus operaciones?

Desde nuestros inicios en México, Lanaccess ha apostado por el talento local. Todo nuestro equipo es mexicano salvo yo misma. Creemos firmemente que apoyar el talento local potencia el crecimiento mutuo y fortalece nuestra presencia en el mercado.

¿Cómo describiría el ambiente laboral dentro del equipo de Lanaccess que opera en Latinoamérica?

Es inclusivo y colaborativo. Además, el equipo está compuesto de forma igualitaria por hombres y mujeres. Este equilibrio fomenta un ambiente de trabajo más enriquecedor, innovador y efectivo.

¿Qué diferencia a Lanaccess de otras empresas del sector en términos de sostenibilidad?

Nuestros dispositivos son duraderos y tienen un consumo eléctrico mínimo, lo que reduce significativamente nuestra huella de carbono. Esto refleja nuestra responsabilidad con el medioambiente y nuestro compromiso con un futuro sostenible.

bajo los estándares de calidad más altos. Esto proporciona seguridad, confianza y sostenibilidad a nuestros clientes.

Más allá de la tecnología, ¿cuál diría que es la mayor aportación de la empresa al mercado mexicano?

“Comencé en el salón de mi departamento y pronto me encontré con la calidez y entusiasmo del equipo que formamos, confirmando que había tomado la decisión correcta”

¿Cuál diría que es la esencia de la propuesta de valor de Lanaccess en el mercado mexicano?

Nuestra propuesta de valor se basa en ofrecer tecnología cibersegura, resiliente y de bajo consumo, fabricada en Europa

Nuestra aportación trasciende la venta de soluciones fabricadas en Europa. Aportamos conocimiento y expandimos el potencial de la videovigilancia en aras del progreso de la sociedad mexicana. Además, contribuimos activamen-

te a hacer del país un lugar más seguro para todos.

¿Qué aspectos de su estilo de liderazgo cree que han contribuido más a este reconocimiento?

Considero clave el desarrollo de equipos de alto desempeño a través de estrategias claras, transparencia operativa y estructuras de compensación equitativas. Mi enfoque en la resolución de conflictos mediante empatía y análisis también ha sido esencial.

Finalmente, ¿puede avanzar qué planes tiene Lanaccess para el futuro cercano en México?

Seguiremos reforzando nuestro compromiso con la innovación tecnológica y expandiendo nuestra presencia en sectores clave, manteniendo siempre altos estándares de calidad y sostenibilidad. **S**

» Lanaccess recibe el Reconocimiento PyME 2025 de la Cámara Española de Comercio en México

La Cámara Española de Comercio en México (CAMESCOM) ha otorgado a Lanaccess el Reconocimiento PyME 2025, un galardón que premia a las empresas españolas que generan un impacto económico positivo y sostenible en el país latinoamericano. La entrega de tan importante galardón tuvo lugar, el pasado 19 de junio, durante la Fiesta de Gala organizada por CAMESCOM, en la que Concha Martínez Cano, directora ejecutiva de Lanaccess en Latinoamérica, recogió el premio en nombre de la compañía.

Desde su sede en Ciudad de México, Lanaccess opera con un equipo comercial y técnico propio, formado íntegramente por profesionales mexicanos. Esta decisión estratégica ha permitido a la empresa extender su presencia en el país, adaptarse mejor al mercado local y generar oportunidades de empleo cualificado. En América Latina, Lanaccess se diferencia por ofrecer soluciones de videovigilancia inteligentes, ciberseguras y de bajo consumo desarrolladas en Europa bajo estrictos estándares de calidad. La durabilidad de sus dispositivos y su bajo consumo energético contribuyen a reducir su huella de carbono, en línea con su compromiso con la sostenibilidad.

Este reconocimiento reafirma el compromiso de Lanaccess con la innovación tecnológica orientada a la protección de personas y activos, y a la mejora de la eficiencia operativa de sus clientes. La empresa seguirá creciendo en sectores estratégicos del país con una propuesta basada en la calidad, la eficiencia y la responsabilidad social.



Seguridad y salud en el trabajo (SST) en el 'retail': desafíos, estrategia y ventaja competitiva

La SST en el *retail* enfrenta desafíos cada vez más complejos en un entorno marcado por la alta rotación de personas, la presión por reducción de costos, la transformación digital y la demanda de consumidores por prácticas empresariales sostenibles. Lejos de ser solo una exigencia normativa, la SST se está consolidando como un eje estratégico capaz de generar valor y convertirse en una ventaja competitiva.

El *retail* por su dinamismo, enfrenta riesgos diversos que exponen la salud física, mental y social de las personas, por los riesgos inherentes al "core business" del sector, destacando el riesgo psicosocial por la atención al cliente o metas comerciales exigentes. Esto afecta a trabajadores en tiendas o los que operan en centros de distribución o logística.

GIOVANNI YANCOLI

GERENTE HSEQ EN TRANSPORTES
SANTA MARÍA SPA

Además, el sector se caracteriza por una alta rotación de personas, con un gran número de trabajadores jóvenes o en su primer trabajo. Esta característica aumenta la vulnerabilidad de accidentes y enfermedades, al mismo tiempo que presenta un desafío para instalar una cultura de seguridad sólida y sostenible.

Tradicionalmente, la SST ha sido vista como un cumplimiento normativo. Sin

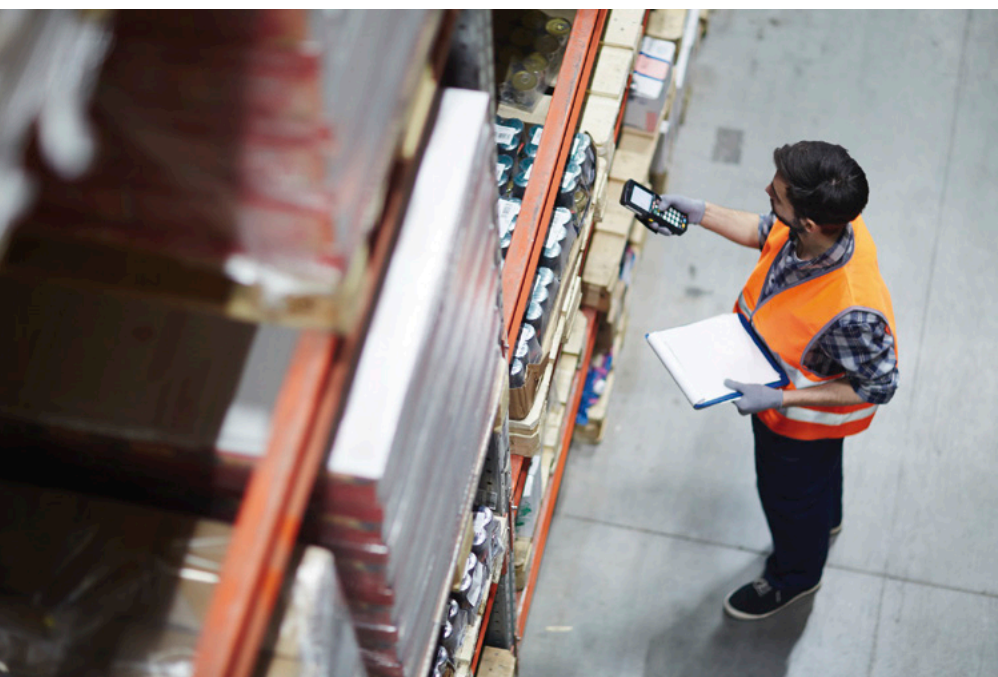


embargo, las organizaciones más avanzadas, reconocen que gestionar riesgos de forma estratégica tiene impactos positivos en la continuidad operacional, la productividad, la reputación y el compromiso de los trabajadores, en otras palabras, la sostenibilidad del negocio.

Incorporar la SST en la estrategia, permite cuidar a las personas en un entorno saludable y motivador, anticipar escenarios, optimizar procesos, reducir costos asociados a siniestros. Esto no solo contribuye a atraer y retener el talento, adicionalmente mejorará la experiencia del cliente, ya que trabajadores sanos y comprometidos entregan un mejor servicio.

SST y sostenibilidad una relación inseparable. El enfoque sostenible de los negocios exige una mirada integral del impacto económico, social y ambiental de las operaciones. En este contexto, la SST se alinea directamente con el pilar social de la sostenibilidad, al garantizar condiciones dignas y seguras para los trabajadores.

Además, consumidores, inversionistas y otros *stakeholders* evalúan cada vez más el desempeño social de las empresas. Los *retailers* que muestran compromiso con la seguridad y salud de las



personas fortalecen su reputación para operar y construyen marcas más confiables. Por tanto, invertir en SST, ya no es solo una cuestión normativa, sino un imperativo de sostenibilidad y reputación.

Prevenir como ventaja competitiva.

Gestionar estratégicamente la SST no solo evita accidentes, también genera otros beneficios. Estudios internacionales demuestran que, por cada dólar invertido en prevención, se pueden ahorrar entre 2 y 4 dólares en costos directos e indirectos de ausentismo, rotación, indemnizaciones, interrupciones operacionales y deterioro del clima laboral.

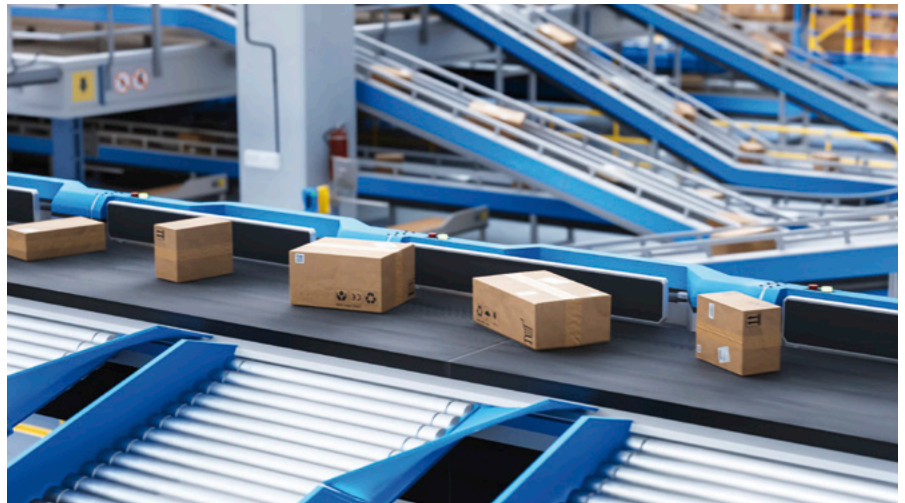
En un sector tan competitivo, donde los márgenes suelen ser estrechos y la eficiencia es clave, estos ahorros pueden marcar una diferencia significativa. Además, contar con una cultura preventiva sólida es un diferenciador para participar en nuevos mercados, negociar con proveedores responsables o atraer consumidores más conscientes.

La metodología "Balanced Scorecard" (integrando la SST a la estrategia).

Una forma efectiva de integrar la SST a la estrategia del negocio es a través del uso del "Balanced Scorecard" (BSC), una metodología desarrollada por Kaplan y Norton que permite traducir la visión y estrategia de la organización en objetivos medibles desde cuatro perspectivas: financiera, del cliente, de procesos internos y de formación y crecimiento.

Incorporar indicadores de SST en cada una de estas dimensiones fortalece la alineación entre prevención y objetivos estratégicos. Por ejemplo:

Financiera: reducción de costos por accidentes.



Cliente: mejora la satisfacción del cliente gracias a equipos más motivados y seguros.

Procesos internos: integración de controles de riesgos en operaciones críticas.

Formación y crecimiento: formación continua en seguridad y fortalecimiento de la cultura.

El BSC permite, además, realizar seguimiento, tomar decisiones basadas en datos y comunicar a todos los niveles la relevancia de la seguridad para el éxito del negocio.



Desafíos futuros. La SST en el *retail* requiere avanzar desde un enfoque reactivo a uno proactivo, esto implica:

- Fortalecer la cultura, especialmente en empresas con alta rotación, mediante liderazgo visible, formación continua e integración de la SST en todos los niveles organizacionales.
- Incorporar tecnologías como sensores, *data analytics* o herramientas móviles que permitan identificar riesgos en tiempo real y gestionar incidentes de forma más eficiente.
- Involucrar al liderazgo en la promoción activa del bienestar laboral, integrando la SST en las decisiones estratégicas y los valores corporativos.

Conclusión. La SST en el *retail* no debe entenderse como un gasto, sino como una inversión estratégica, un factor de sostenibilidad y una poderosa ventaja competitiva. Las empresas que logren integrar la prevención en su ADN estarán mejor preparadas para enfrentar los desafíos del futuro, proteger a sus equipos y destacar en un mercado cada vez más exigente y consciente. 



Control de peligros clave en supermercados de grandes y pequeñas superficies

El sector de retail en especial el dedicado a la venta de comidas y bebidas en grandes y pequeñas superficies es uno de los más importantes generadores de puestos de trabajo en Colombia y otros países. Solo en Colombia funcionan cerca de 500.000 negocios pequeños según Fenalco, y las grandes empresas, como Grupo Éxito mantienen más de 41.000 puestos directos. En Brasil se evidencia lo masivo que es este sector: 1,5 millones de personas trabajan sólo en tiendas de gran superficie y supermercados.

Sin embargo, la magnitud del sector se refleja también en su siniestralidad. La Organización Internacional del Trabajo (OIT) advierte que el comercio minorista es uno de los grupos ocupacionales expuestos a altas tasas de lesiones musculoesqueléticas, largas jornadas de trabajo y baja cobertura de protección social.

Ante este panorama, los supermercados grandes o pequeños comparten cinco peligros prioritarios que demandan una gestión preventiva robusta.

Manipulación manual de cargas

El “picking” intensivo y el reabastecimiento rápido generan movimientos repetitivos y levantamiento de bultos de 25 kg y en algunos casos pesos mayores por fuera del cumplimiento de la legislación. Resultados: lumbalgias, ausentismo y enfermedades laborales.

- Implementar ayudas mecánicas (transpaletas, mesas elevadoras) en zonas de recibo y bodega.

JAÍR O. GÓMEZ GÓMEZ
DIRECTOR HSEQ DE SINEXIA



- Rediseñar alturas de estantería para limitar la carga fuera de la zona entre hombros y rodillas.
- Pausas activas cada 90 minutos y formación continua en técnicas de levantamiento.
- Configurar recorridos y rutas de alistamiento de pedidos teniendo presente

el concepto del personal que realiza esta actividad.

Operación de equipos montacargas

Montacargas eléctricos y apiladores que conviven con clientes y “shoppers” así como equipos que son operados al



interior de centros de abastecimiento logístico.

- Separar rutas peatonales con barandas rígidas y señalización luminosa.
- Certificar operadores y recertificar con información actualizada cada dos años.
- Usar sensores de proximidad y delimitar zonas de velocidad reducida.
- Utilizar la configuración de velocidad máxima para equipos que cuentan con esta opción.
- Cierre de pasillos y retirar los clientes al momento de elevar cargas.

Almacenamiento en estanterías multinivel

El estado de las estanterías y el cuidado de estas es clave para asegurar la infraestructura, un impacto o golpe no reportado y no controlado puede ser un factor decisivo en un evento trágico.

- Implementar un programa de prevención de caída de objetos (incluir controles como stop pallets)
- Identificar visualmente la capacidad de carga máxima de la infraestructura.
- Realizar inspección diaria para la identificación de golpes y marcarlos con fecha de identificación.
- Tomar control de disminución de cargas en estanterías golpeadas.
- Realizar la investigación y trazabilidad de reparación de los golpes identificados.
- Asegurar mantenimientos anuales para ajuste de piezas de la infraestructura.

Orden y aseo

Derrames, envases sueltos y ocupación de áreas de tránsito peatonal son causas principales de resbalones: el accidente más frecuente y costoso.

- Programa 5S visible al cliente: cada turno debe entregar zona libre de obstáculos.
- Usar pisos con coeficiente de fricción $\geq 0,45$ en áreas húmedas.

- Establecer una política de identificación de superficies húmedas y tomar control inmediato tanto en zonas internas como en zonas de tránsito de clientes.
- En oficinas mantener un espacio específico dedicado para cada elemento y puertas de gabinetes cerrados.

Herramientas de corte

El uso de cortadores de seguridad o cuchillas retráctiles, tijeras y cuchillos de carnicería concentran el grupo de herramientas que más laceraciones generan.

- Garantizar los insumos de las herramientas para su reemplazo, generar entrega numerada de cuchillas con inspección diaria.
- Realizar jornadas de identificación de herramientas de corte no autorizadas o en mal estado y retirarlas de las áreas de trabajo.
- Dotar guantes con protección al corte para herramientas y protecciones anti-corte en carnicería y panadería.
- Uso de superficies fijas para realizar cortes de cajas o demás elementos.

Panorama regional de accidentalidad

Colombia. Para el primer trimestre de 2025 según el informe de siniestralidad laboral del CCS se destacan el sector de comercio al por mayor y al por menor con 11 decesos (11,2 %) ocupando el tercer lugar, entre los sectores con mayor número de fatalidades.

La OIT estima que las lesiones laborales cuestan 4 % del PIB mundial.

Los supermercados grandes o pequeños comparten una matriz de peligros ergonómicos y operativos que puede controlarse con la apropiación de una cultura de prevención, rediseño de procesos, cultura 5S, tecnología accesible y liderazgo por parte de los líderes de la operación.

Cada peso invertido en prevención evita hasta cuatro en incapacidades, reemplazos o sanciones.

La combinación de formación continua, automatización de controles, seguimiento de indicadores e identificación de líderes tanto en áreas de la dirección, administrativas y operativas es clave para consolidar una cultura preventiva sólida y sostenible. 



Trabajar seguro en el 'retail': retos y soluciones del siglo XXI

En el ámbito del *retail*, la prevención de riesgos laborales adquiere una dimensión específica que responde a las características propias de la actividad: alta rotación de personal, exposición constante al público, trabajo en turnos, manipulación de mercadería, uso de tecnologías, etc.

En línea con lo que propone la Organización Internacional del Trabajo para 2025 (donde destaca la automatización, las herramientas inteligentes, la realidad aumentada y virtual y la gestión algorítmica), se está transformando la seguridad y la salud.

Incorporar soluciones tecnológicas que puedan optimizar estrategias preventivas, a partir de la interconectividad, la automatización y el uso de datos, utilizando dispositivos de captura de imagen complementados con analítica basada en inteligencia artificial,

JUAN CARLOS CARUSO

ESPECIALISTA EN HIGIENE Y SEGURIDAD (UBA)



son herramientas que pueden permitir identificar situaciones clave en la prevención de accidentes, como el uso correcto de elementos de protección personal, delimitación de perímetros, detección de eventos específicos – como cruce de líneas o intrusiones– y el conteo automatizado de personas y vehículos, etc. El acceso simultáneo a imagen y sonido puede facilitar la

georreferenciación de eventos e intervenciones inmediatas

Riesgos laborales específicos del sector 'retail'

El sector presenta una variedad de riesgos que, aunque muchas veces subestimados por no tratarse de un ámbito considerado "de alto riesgo", pueden generar accidentes, enfermedades profesionales y un clima laboral hostil si no se abordan.

Riesgos ergonómicos y musculoesqueléticos: quizás son los más frecuentes. Las tareas de carga y descarga, reposición en estanterías, la permanencia prolongada en posición de pie, movimientos repetitivos y posturas forzadas, pueden provocar lumbalgias, tendinitis, fatiga muscular o lesiones articulares.

Riesgos psicosociales: la presión por alcanzar metas en las ventas, la atención al cliente en situaciones conflictivas, la rutina de los turnos rotativos y la precariedad laboral en algunos empleos, contribuyen al estrés laboral, ansiedad, agotamiento emocional, etc.

Riesgos eléctricos y mecánicos: en áreas como cajas, depósitos o cámaras



frigoríficas donde se utilizan equipos eléctricos (balanzas, registradoras, cintas transportadoras, montacargas) requieren mantenimiento y condiciones de uso seguras para prevenir descargas eléctricas, atrapamientos o cortocircuitos.

Riesgos de caídas y golpes: suelos o pavimentos mojados, objetos mal ubicados, estanterías inestables o zonas mal iluminadas, pueden generar caídas al mismo nivel o a distinto nivel, así como golpes contra objetos inmóviles o móviles.

Riesgos químicos y biológicos: en supermercados, tiendas de alimentación o droguerías, el personal puede estar expuesto a productos de limpieza, aerosoles, alimentos en mal estado o sistemas de refrigeración que requieren control de sustancias peligrosas.

Riesgos derivados de la seguridad física: la exposición al público conlleva un riesgo adicional relacionado con la violencia externa, como intentos de robo, agresiones verbales o físicas y situaciones de emergencia.

Estrategias de prevención y buenas prácticas

Es preciso desarrollar una cultura preventiva que involucre a todos los niveles.

1. Evaluación de riesgos y planificación preventiva.

Es esencial realizar una evaluación de riesgos inicial y periódica, adaptada a cada lugar, teniendo en cuenta su tamaño, localización, tipo de productos y trabajadores. Esta evaluación debe permitir establecer un plan de prevención específico, con medidas concretas y responsables designados.

2. Formación e información continua.

La capacitación es una de las herramientas clave. Todos los trabajadores deben conocer los riesgos de su puesto, las medidas preventivas y cómo actuar ante una emergencia.



3. Diseño ergonómico del puesto de trabajo.

La adecuación ergonómica (alturas de estanterías, sillas ajustables, organización racional del lugar) reduce los trastornos musculoesqueléticos. Asimismo, se deben fomentar técnicas de manipulación segura de cargas.

4. Protocolos ante emergencias y violencia externa.

Contar con protocolos ante robos, incendios, evacuaciones o agresiones garantiza una respuesta más rápida y eficaz, minimizando el daño tanto para las personas como para los bienes.

5. Higiene industrial y mantenimiento preventivo.

La limpieza de superficies, ventilación adecuada, revisión periódica de instalaciones eléctricas, sistemas de refrigeración y señalización de riesgos son aspectos que deben formar parte de una rutina diaria y sistemática.

6. Promoción de la salud laboral.

Más allá de evitar accidentes, la salud laboral implica fomentar hábitos saludables: alimentación equilibrada, hi-

dratación, prevención del estrés, conciliación entre vida laboral y personal, y revisiones médicas periódicas.

Responsabilidad y compromiso organizacional.

Requiere el compromiso institucional de las empresas, que deben integrar la seguridad y salud como un eje estratégico de gestión. Esto se traduce en inversión, liderazgo, participación de los trabajadores y evaluación constante de los resultados obtenidos.

Conclusión.

La seguridad y salud en el sector 'retail' es una responsabilidad de todos, porque no solo previene lesiones y enfermedades, sino que también mejora la productividad, reduce el ausentismo, y fortalece la reputación de la empresa. Invertir en prevención no es un gasto, sino una inversión en estrategia de sostenibilidad. Adaptar los espacios, capacitar al personal y promover un entorno seguro son pasos esenciales para garantizar que cada trabajador, sin importar su rol, pueda desarrollar su tarea con dignidad, salud y bienestar. 

Seguridad y salud en el trabajo: un pilar estratégico para la logística multicategoría, sustancias peligrosas y 'retail'

La implementación efectiva de la seguridad y salud en el trabajo (SST) no es solo una obligación legal o ética, sino una inversión estratégica que define la sostenibilidad y competitividad de una empresa. En sectores como la logística multicategoría, el manejo de sustancias peligrosas y el *retail*, la prevención de riesgos laborales es crítica para la continuidad operacional, la protección de los trabajadores y la reputación corporativa.

1. La cultura preventiva como eje estructural.

En toda organización moderna, la cultura preventiva debe estar integrada e impulsada desde la alta dirección. La experiencia ha demostrado que las empresas que priorizan la seguridad laboral no solo reducen accidentes, sino que también aumentan su eficiencia operativa, disminuyen los costos asociados a

KEVIN ARCE

JEFE DE PREVENCIÓN DE RIESGOS Y MEDIO AMBIENTE EN EMPRESAS DEL GRUPO TW



la rotación de personal y fortalecen su imagen pública.

La cultura preventiva se logra a través de un proceso de madurez y a través del compromiso activo de sus líderes. Esto significa incluir metas de seguridad en los indicadores clave de desempeño (KPI), asignar presupuestos específicos para la prevención de riesgos, capacitar constantemente a los equipos y pro-

mover una política de "tolerancia cero" frente a acciones o condiciones de trabajo inseguras.

2. Riesgos críticos en sectores estratégicos.

En logística, los riesgos se relacionan con el uso de maquinarias, tránsito de vehículos pesados, manipulación manual de cargas, fatiga laboral y ergonomía. La pasividad en la gestión preventiva de



estos factores puede derivar en accidentes graves y desarrollo de enfermedades profesionales a largo plazo, detenciones operativas e incluso sanciones legales.

En el manejo de sustancias peligrosas, los riesgos son aún más complejos: exposición química, incendios, explosiones, contaminación ambiental y afectaciones a la salud a corto o largo plazo. Estos escenarios exigen protocolos de seguridad y estrictos protocolos de respuesta ante emergencias y prevención de desastres, almacenamiento certificado y personal altamente capacitado.

En el *retail*, aunque muchas veces subestimado, enfrenta riesgos significativos, caídas desde altura en bodegas, riesgos eléctricos, estrés laboral y riesgos psicosociales asociados al contacto continuo con público.

3. Beneficios de una estrategia robusta en SST.

Empresas que han invertido en sistemas de gestión de seguridad y salud en el trabajo bajo estándares como ISO 45001, reportan mejoras en clima laboral, menores tiempos de inactividad, menor rotación de trabajadores y mayor atracción de talentos. Además, la SST se ha convertido en una exigencia cada vez más valorada por clientes nacionales e internacionales al momento de establecer relaciones comerciales.

Contar con una gestión proactiva permite a las empresas anticiparse a los riesgos, implementar controles efectivos y adaptarse rápidamente a las exigencias normativas vigentes como también auditorías de primera, segunda y tercera categoría.

4. Grupo de Empresas TW en Chile.

En el Grupo de Empresas TW nuestro objetivo es entregar a nuestros clientes una propuesta logística integral que aborde todos sus requerimientos siendo fundamental el cumplimiento y aplicación de las normas en materias de se-



guridad y salud en el trabajo: la seguridad no es negociable. Cada acción que realizamos, desde el despacho más pequeño hasta la maniobra más compleja, debe estar guiada por un valor que nos representa: "operamos con ética y con seguridad", constituyendo esto como uno de los pilares fundamentales de los valores de la compañía.

Conclusión: el futuro es seguro o no será.

La prevención de riesgos laborales no debe verse como costo, sino como una inversión en capital humano, continuidad operacional y sostenibilidad. Las empresas que aspiren a ser líderes en logística, Retail o manejo de sustancias peligrosas deben incorporar la SST como parte de su ADN. Los tiempos exigen no solo cumplir, sino liderar. Apostar por la SST es apostar por la excelencia. 



Prevención y protección contra incendios: **clave en la seguridad integral**

■ Por Comexa.

La prevención y protección contra incendios es uno de los pilares fundamentales para salvaguardar vidas humanas, bienes materiales y la continuidad operativa de cualquier entorno. Aunque los incendios no siempre se pueden prever, sí es posible reducir significativamente su riesgo mediante una combinación de buenas prácticas, tecnología adecuada y cumplimiento normativo.

Prevención y protección

La gestión del riesgo de incendio debe abordarse desde dos frentes: la prevención, orientada a evitar que el fuego se origine, y la protección, enfocada en mitigar sus efectos. Ambos enfoques son complementarios y esenciales para una estrategia efectiva de seguridad.

La mayoría de los incendios tiene un origen humano o técnico evitable. Por ello, la prevención parte del principio de identificar y controlar posibles fuentes de ignición.

1. Control de fuentes de calor e ignición

El fuego requiere calor, combustible y oxígeno. Reducir cualquier elemento de esta triada disminuye el riesgo. Es fundamental evitar fumar en zonas con vegetación seca o cerca de materiales inflamables, almacenar líquidos combustibles en espacios ventilados y alejados de fuentes de calor, y evitar el uso de velas en entornos no controlados.

2. Uso responsable de la electricidad

Una de las principales causas de incendio son las fallas eléctricas. Se debe



evitar sobrecargar enchufes, utilizar extensiones como solución permanente o conectar múltiples aparatos a una sola toma. La revisión periódica de instalaciones eléctricas y equipos es vital para detectar señales de sobrecalentamiento, desgaste o cortocircuitos.

3. Mantenimiento de sistemas térmicos

Calefactores, estufas y chimeneas deben mantenerse en condiciones óptimas. Cualquier acumulación de polvo, grasa o materiales combustibles en sus proximidades puede provocar una emergencia.

4. Orden y limpieza

La acumulación de desechos o materiales inflamables en espacios de trabajo, almacenes o incluso hogares aumenta la probabilidad de un incendio. Además, la falta de limpieza en filtros de aire, ventiladores y campanas extractoras puede facilitar la propagación del fuego.

5. Buenas prácticas en la cocina

La cocina es una zona crítica. No dejar ollas y sartenes sin supervisión, limpiar regularmente superficies y electrodomésticos, y contar con una tapa para sofocar un fuego por grasa puede marcar la diferencia ante una eventualidad.

Responder de forma eficaz

Incluso con las mejores prácticas preventivas, siempre existe la posibilidad de que un incendio ocurra. Por ello, es crucial estar preparados para detectarlo a tiempo y actuar con rapidez.

1. Sistemas de detección temprana

Los detectores de humo salvan vidas. Deben instalarse en todos los niveles del inmueble y cerca de las áreas de descanso. Según la norma NFPA 72, estos dispositivos deben probarse mensualmente y reemplazarse cada diez años. Complementarlos con detectores de monóxido

de carbono es altamente recomendable, especialmente en instalaciones con aparatos de combustión.

2. Extintores accesibles y funcionales

Un extintor puede detener un incendio incipiente antes de que se propague. La norma NFPA 10 establece los lineamientos para su correcta selección, ubicación, inspección y mantenimiento. Es importante que el personal sepa cómo usarlos y que se encuentren visibles, accesibles y cargados.

3. Rutas de evacuación seguras

Las vías de evacuación deben estar despejadas, bien señalizadas e iluminadas. Las puertas de emergencia deben abrirse en el sentido de la salida y nunca estar obstruidas. La norma NFPA 101 (Código de Seguridad Humana) regula las condiciones mínimas para una evacuación segura.

4. Planes de emergencia y simulacros

Un plan de evacuación bien elaborado debe incluir roles asignados, rutas alternas, puntos de reunión seguros y protocolos de comunicación. Practicarlo regularmente mediante simulacros es esencial para que todos sepan cómo actuar bajo presión.

5. Materiales resistentes al fuego

En construcciones nuevas o remodelaciones, optar por materiales con certificaciones ignífugas en muros, pisos, techos y puertas, sobre todo en zonas de riesgo como cocinas, bodegas o cuartos de maquinaria, puede evitar que el fuego se propague rápidamente.

La tecnología como aliada

Hoy en día, existen soluciones tecnológicas que refuerzan las medidas tradicionales de seguridad. Los sistemas automáticos de rociadores (regulados por la norma

NFPA 13), alarmas inteligentes, sensores conectados al Internet de las Cosas (IoT), y *software* de monitoreo en tiempo real permiten una respuesta más rápida y coordinada en caso de incendio.

En edificios de gran altura o centros con alta afluencia, contar con sistemas de notificación masiva, integración con centrales de emergencia y protocolos de defensa en el lugar puede salvar vidas.

Cultura y capacitación

Una infraestructura segura sólo es efectiva si quienes la habitan o utilizan conocen los protocolos. La capacitación continua del personal en prevención, uso de equipos contra incendios, evacuación y primeros auxilios es una in-

» **NFPA 72:** Sistemas de detección y alarma.

» **NFPA 101:** Seguridad humana y evacuación.

» **NFPA 1500:** Seguridad ocupacional para bomberos.

» **NFPA 921:** Investigación de incendios y explosiones.

Cumplir estas normas mejora la seguridad. Además, puede ser un requisito para asegurar edificios, cumplir regulaciones locales o participar en licitaciones.

Conclusión

En nuestra experiencia hemos constatado que las medidas más efectivas no sólo dependen de la tecnología, sino de

Colaborar con especialistas permite cumplir con los estándares y garantizar soluciones alineadas con las necesidades reales de cada entorno

versión que puede hacer la diferencia en una situación crítica.

Además, la cultura de seguridad debe ser promovida desde la dirección hasta el último colaborador. Identificar riesgos, reportar condiciones inseguras y participar activamente en simulacros debe ser una responsabilidad compartida.

Normativas internacionales

Las normas de la National Fire Protection Association (NFPA) ofrecen un marco de referencia técnico y actualizado para todos los aspectos relacionados con la protección contra incendios:

» **NFPA 10:** Extintores portátiles.

» **NFPA 13:** Diseño e instalación de rociadores automáticos.

su correcta planificación, instalación y mantenimiento. Desde la evaluación de riesgos hasta la integración de sistemas de detección y respuesta, la implementación adecuada marca la diferencia en momentos críticos.

Es fundamental contar con un enfoque técnico, actualizado y personalizado para cada espacio. Colaborar con especialistas permite cumplir con los estándares y garantizar soluciones alineadas con las necesidades reales de cada entorno.

La seguridad contra incendios no es sólo una tarea del departamento de protección civil o de mantenimiento, sino un compromiso colectivo. Porque cuando se trata de proteger vidas y patrimonio, cada segundo, cada decisión y cada medida preventiva cuenta. **S**



Hugo Torres Bahamón

Director ejecutivo de la Asociación Nacional de Protección Contra Incendios (ANRACI)

“Colombia necesita normas específicas que garanticen la robustez de los proyectos de protección contra incendios”

■ Por Marcela Linares Vásquez y Bernardo Valadés.

ANRACI se creó con el objetivo de “implementar y promover buenas prácticas en una industria ligada a la protección, la seguridad y la vida donde cualquier acción desarrollada de manera irresponsable va a repercutir negativamente en las personas”, comenta Hugo Torres Bahamón. El presidente de la asociación pone el foco en la normativa y señala que “necesitamos normas que guíen, regulen y controlen el desarrollo de los proyectos de protección contra incendios”.

¿Cuándo se fundó ANRACI?
¿Cuál fue la necesidad que motivó su creación?

ANRACI nació en 2015 fruto de la necesidad que tenían las empresas del sector de protección contra incendios de contar con una representación gremial que defendiera los intereses del sector. Y la motivación viene de la necesidad de implementar y promover buenas prácticas en una industria ligada a la protección, la seguridad y la vida donde cualquier acción desarrollada de manera irresponsable va a repercutir negativamente en las personas. Por eso es tan importante que la protección contra incendios se desarrolle por profesionales competentes idóneos y que conocen su labor. Y utilizando materiales, elementos, insumos y equipos apropiados debidamente certificados.

¿Podría destacar las principales acciones impulsadas desde ANRACI para erradicar malas prácticas y promover una cultura de prevención de incendios?

Un primer pilar es la capacitación. Por un lado, es importante que la sociedad sea consciente de que está expuesta al riesgo de incendio permanentemente. Por ello, uno de nuestros pilares es compartir conocimiento para que las personas puedan tomar buenas decisiones como identificar elementos de protección contra incendios apropiados, buscar ayuda de profesionales debidamente formados y capacitados, adquirir productos certificados y listados, no fijarse solamente en el precio, etc.

Por otra parte, trabajamos en la formación de las personas que laboran en nuestro sector con el fin de fortalecer sus competencias profesionales. Es primordial que las personas que trabajan en la protección contra incendios conozcan lo que hacen y tengan conocimientos sólidos, habilidades y experiencia.

Otro frente en el que trabajamos es la normativa. Necesitamos normas que nos guíen, regulen y controlen en el desarrollo de nuestros proyectos. En este sentido, hemos trabajado en normas sectoriales de competencia laboral para identificar los elementos mínimos de competencia profesional que deben tener las personas en relación a ciertas actividades críticas relacionadas con la actividad de nuestro sector. Asimismo, hemos colaborado con el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) porque necesitamos normas específicas que garanticen la robustez de los proyectos de protección contra incendios.

Y también impulsamos el *networking* mediante actividades como el evento Fire Expo Latam, que este año se celebrará del 20 de septiembre al 2 de octubre en la ciudad de Medellín.

¿Cuál es el estado actual de la normativa en protección contra incendios en Colombia? ¿Qué avances se han logrado en materia de legislación en los últimos años?

Hay una base interesante: el Reglamento Colombiano de Construcción Sismo Resistente (NSR-10), que ha tenido un importante impacto en la seguridad y el desarrollo de las edificaciones. El NSR-10 regula aspectos de edificabilidad y protección contra incendios. Pero desde 2010 no ha evolucionado y necesitamos una actualización urgente para incluir nuevas tecnologías y criterios que se correspondan a los riesgos y la realidad del mundo moderno.

Junto a ICONTEC, en ANRACI hemos venido trabajando en la formulación de códigos de incendios. Actualmente, el Comité Técnico N° T-623 Código de Protección contra el Fuego se encuentra inmerso en la elaboración de un código que, si bien inicialmente será voluntario, confiamos

en que pueda evolucionar, crecer y tener un desarrollo para que sea considerado a nivel legislativo de cara a implementarse y desarrollarse en todo el país.

¿Cómo han evolucionado las estadísticas de incendios en Colombia en los últimos años? ¿Qué datos relevantes podrían compartírnos sobre incendios estructurales y forestales?

En Colombia tenemos alrededor de 4.000 incendios estructurales registrados y declarados al año. De ellos, en torno a 1.000 incendios tienen lugar en la capital. En el caso de esta última, según un estudio del Cuerpo Oficial de Bomberos de Bogotá con estadísticas del periodo 2013-2023, los temas relacio-

ANRACI ha establecido diversas alianzas con organismos nacionales e internacionales. ¿Cómo contribuyen esas colaboraciones al fortalecimiento de la protección contra incendios en Colombia?

En ANRACI consideramos que la mejor forma de llegar a un objetivo es trabajando en equipo. Colaboramos con el International Code Council (ICC), la Red Latinoamericana de Protección Contra Incendios, asociaciones de varios países... En el ámbito nacional, destacaría el acuerdo con Acecolombia para desarrollar, entre otras iniciativas, una guía de buenas prácticas de protección contra incendios en centros comerciales, y Acoplásticos, con la que hicimos un

“Los incendios forestales son un fenómeno importante y para extinguirlos hay que mejorar en dotación, equipos y tecnología”

nados con la electricidad representan la primera causa de incendio, situándose a continuación las fuentes de calor. Por lo tanto, los riesgos más importantes son fuentes de energía y actividades que el ser humano utiliza a diario. Eso nos dice que hay un gran trabajo por hacer con la comunidad.

Asimismo, hay un gran cantidad de incendios forestales al año, pero no son tan estacionales ni agresivos como en Estados Unidos o Chile. Ahora bien, debido al cambio climático y las sequías, cuando se producen son más devastadores. En términos de volumen, más o menos, cada año se están consumiendo unas 13.000 hectáreas. Es un fenómeno importante y hay que mejorar en dotación, equipos y tecnología.

programa para las empresas de pintura, ya que tienen un riesgo importante derivado de su actividad.

Para finalizar, ¿qué innovaciones tecnológicas y tendencias emergentes en protección contra incendios consideran más relevantes?

Ya estamos viendo cómo los sistemas de protección contra incendios de las edificaciones se integran con servicios en la nube para brindar información en tiempo real y generar información que permita tomar mejores decisiones. Y en materia de sostenibilidad y respeto al medio ambiente, la espuma y los agentes limpios han ido evolucionando a nuevas tecnologías para que la extinción de incendios tenga un menor impacto en el entorno. **S**

**Sargento Carlos Ramírez**

Cuerpo Oficial de Bomberos de Bogotá

“El incendio en El Cable ha sido una de las emergencias más complejas que hemos enfrentado en Bogotá”

» Por Marcela Linares Vásquez y Bernardo Valadés.

El incendio del cerro El Cable, ocurrido en enero de 2024, fue uno de los más intensos registrados en Bogotá en los últimos años. Se extendió durante 12 días y presentó condiciones extremadamente exigentes debido a la combinación de altas temperaturas, fuertes vientos y la inclinación del terreno, lo que dificultó el control del fuego. El sargento Carlos Ramírez, del Cuerpo Oficial de Bomberos de Bogotá, nos habla de esa y otras experiencias en esta entrevista.

Como sargento y coordinador en operaciones contra incendios estructurales y forestales, ¿puede describir cómo se planifica y ejecuta una intervención compleja como la del cerro El Cable? ¿Qué desafíos técnicos y logísticos afrontan ustedes en esa clase de terreno?

En el caso de los incendios estructurales, se hace un análisis sobre la materia combustible que se está quemando, el tiempo que lleva ardiendo, el tipo de edificación, las personas que hay... En cuanto a los incendios forestales, se tiene en cuenta la altura, el camino para llegar al fuego, las posibilidades de tener fuentes de agua y los retos logísticos. Para desempeñar nuestra labor contamos con varios equipos especializados, entre ellos los dedicados a los incendios forestales y la investigación de incendios.

Usted mencionó que nunca había visto un incendio con temperaturas, vientos y extensión tan extremas como las del cerro El Cable. ¿Cómo entrenan física y emocionalmente los bomberos para enfrentarse a situaciones tan exigentes como esa?

El incendio en El Cable fue una de las emergencias más complejas que hemos enfrentado en Bogotá. Fueron 12 días continuos de operaciones en el cerro sin dejar de atender el resto de emergencias de la ciudad: incendios estructurales, escapes de gas, rescates... Todo esto gracias al liderazgo de nuestra directora, Paula Escobar, y al trabajo coordinado de nuestros equipos especializados.

Desde la formación básica, los bomberos recibimos seis meses de entrenamiento intensivo, seguido de cursos de actualización. También contamos con un plan de acondicionamiento físico diario, diseñado por entrenadores



PROTECCIÓN Y CONTINUIDAD DE OPERACIONES SENSIBLES PARA INFRAESTRUCTURAS CRÍTICAS



SCATI THERMALSCAN VISIÓN 360° DE GRANDES ÁREAS SIN PUNTOS CIEGOS



CÁMARAS THERMALSCAN

de riesgos laborales, y rutinas específicas que debemos documentar y cumplir. Además, nuestros procedimientos están estandarizados y en constante revisión.

En el uso de mangueras y equipos en cerros con gran inclinación se enfrentan a la caída de presión y el desgaste físico. ¿Cómo garantizan el rendimiento y la seguridad del personal?

Es una combinación de estrategia técnica, humana y tecnológica. Utilizamos drones para planear rutas, mapas para ubicar puntos críticos y sistemas de tendido de mangueras por tramos, con depósitos de agua intermedios y motobombas portátiles que impulsan el caudal hasta las zonas más altas. Contamos con vehículos todoterreno, cuatrimotos e incluso mulas cuando el terreno lo requiere. Nuestros equipos de protección personal son de última generación, ligeros y resistentes al calor. Un bombero forestal puede cargar entre 15 y 16 kilos, además de herramientas como motosierras o motobombas. El desgaste es alto, pero estamos preparados.

Bogotá ha fortalecido su Grupo Especializado de Búsqueda y Rescate (USAR). ¿Cómo se integra con el resto de su labor?

Todos los bomberos están entrenados en búsqueda primaria, pero cuando una emergencia escala a segundo o tercer nivel, entran los equipos especializados: técnicos en rescate, apertura de puertas, búsqueda minuciosa y rescate de compañeros atrapados. El equipo USAR está capacitado para atender estructuras colapsadas, apuntalamientos, rescates con cámaras, sonares y perros entrenados. Este trabajo conjunto y simbiótico ha permitido que el cuerpo de Bomberos de Bogotá sea reconocido por el Grupo Asesor Internacional de Operaciones de

Búsqueda y Rescate (INSARAG) como un equipo de búsqueda y rescate urbano con estándares internacionales.

Además de incendios, atienden accidentes, vertidos, inundaciones... ¿Cómo se preparan para esta diversidad de actuaciones?

La clave está en la formación continua y la especialización. Tenemos instructores para áreas como rescate vehicular, cada vez más complejo por la tecnología de los autos. Usamos análisis de riesgo con mapas de calor para identificar zonas críticas por accidentes, caídas de árboles o materiales peligrosos. Y trabajamos con el Centro de Comando, Control, Comunicaciones y Cómputo (C4) y nos

En 25 años de servicio he vivido muchos eventos significativos. Uno de los más emotivos fue un rescate vehicular en la calle 26 con carrera 30. Con el equipo técnico de rescate atendimos a una joven que, debido a sus lesiones, estuvo en coma durante un largo tiempo. Dos meses después, al recuperarse, lo único que recordaba era la voz del bombero que la acompañó durante el rescate. Me buscó y tuvimos la oportunidad de conocernos. Fue un momento muy especial, lleno de gratitud y alegría. Verla de pie, poder abrazarla, fue una experiencia realmente bonita.

También estuve en Ecuador con el equipo USAR tras el terremoto de Manabí en el año 2016. Fueron 23 días de

“¿Historias impactantes que he vivido? El terremoto de Ecuador, el atentado en el Club El Nogal o el rescate a los niños del Colegio Agustiniانو Norte son algunas de ellas”

estamos integrando cada vez más al sistema de seguridad ciudadana. Nuestra directora ha impulsado una gestión del riesgo integral que combina tecnología, conocimiento y acción social.

Además, tenemos campañas como *Comercio Seguro*, *Vivienda Segura* y *Salvando Patrias*, esta última enfocada en registrar mascotas en una base de datos para poder rescatarlas en emergencias. Y contamos con el programa *Bomberitos*, que forma a niños de 7 a 12 años de manera virtual y presencial. Así impactamos positivamente desde la prevención.

¿Podría compartir una historia que le haya impactado personalmente durante una misión de rescate o de protección contra incendios?

operación muy intensos formando parte de un equipo multidisciplinario, rescatando personas, coordinando operaciones y ayudando a una ciudad en caos. A pesar de las dificultades culturales o logísticas, fue una experiencia muy bonita, profundamente humana y enriquecedora. Definitamente, creo que Ecuador nos enseñó mucho.

Y, entre otras experiencias vividas en mi trayectoria profesional, no puedo olvidarme de la emergencia del Club El Nogal, consecuencia de un atentado con un carro bomba en el año 2003, y el rescate de los niños del Colegio Agustiniانو Norte atrapados en un bus escolar debido a un accidente de tránsito en el año 2004, una de las peores tragedias en la historia reciente de Bogotá. **S**



EXPERTOS EN SEGURIDAD FÍSICA Y ELECTRÓNICA

Made in Italy



Ofrecemos soluciones de seguridad avanzadas para sectores empresariales que exigen tecnología de vanguardia y productos que cumplen con los más altos estándares de calidad.



AUTOPISTAS



CORPORATIVO



RESIDENCIAL



CEDIS



GOBIERNO-MILITAR



BANCA



AEROPUERTOS



RETAIL

Nuestra red de expertos, partners e integradores está lista para ayudarte en cada etapa de tu proyecto de seguridad, desde la recomendación de productos hasta su implementación.

CALIDAD • SERVICIO • EFICIENCIA



/rseguridad



/RSeguridad_MX

Monte Elbruz #132 Int 301/302
Col. Polanco V Sección, Del. Miguel Hidalgo, CP. 11560, CDMX
☎ : 55 5951 9070 | www.rseguridad.com
info@rseguridad.com

Aeronaves remotamente tripuladas en la prevención y lucha contra incendios

Las aplicaciones de aeronaves remotamente tripuladas (UAV) se hacen más amplias y complejas en la medida en que muchas tecnologías convergen para hacer de los UAV una herramienta de alto valor, alto impacto y, sobre todo, de muy fácil despliegue y uso, entre otras cosas, por su relación coste-beneficio. Dos puntos del pasado Congreso Mundial de UAV en Shenzhen, celebrado del 24 al 26 de mayo, lo evidencian:

1. Durante el año pasado, China registró 26,7 millones de horas de vuelo con diferentes usos, sin incidentes, y utilizando tecnologías tanto comerciales como profesionales.
2. El impulso al concepto general de Low Altitude Economy, al que ya se adhieren varios países de la región. Este concepto contempla desde el principio un ecosistema que incluye comando y control, comunicaciones y operaciones a baja altura con trámites simplificados o incluso sin trámites aeronáuticos en algunos casos.

Incendios y regulación

A nivel mundial, la protección contra incendios es uno de los temas más regulados y supervisados del ámbito de la seguridad, sin importar el continente o el país. A continuación, se describen escenarios en los que sería ventajoso el uso de UAV en la protección contra incendios.

Uso inadecuado

Este escenario, con más de diez años de antigüedad, ha sido criticado e incluso prohibido en ciertos casos: cuando

» RAFAEL PADILLA

PRESIDENTE DEL COLOMBIA CHAPTER
WORLD UAV FEDERATION

durante un incendio aparecen personas que lanzan sus drones para captar imágenes sensacionalistas, incluso con fines comerciales. En tales casos, los operadores vuelan los UAV cerca de las llamas; el calor deforma el plástico, se pierde el dron, pero las baterías suponen un riesgo muy alto. Y cuando se vuela más alto, estos UAV representan un peligro para los helicópteros y aeronaves que forman parte de las labores de extinción. Los recientes incendios en California son un ejemplo: se llegó incluso a la persecución policial de quienes intentaban elevar un UAV en la zona.

Imágenes en tiempo real

La principal y más difundida contribución de los UAV es la posibilidad de capturar imágenes IR o termográficas del incendio y transmitir las en vivo al puesto de comando y control. Estas imágenes permiten a las cuadrillas identificar y localizar los puntos calientes desde los que se alimenta el incendio, incluso entre densas nubes de humo, optimizando la asignación de recursos.

Además, permiten valorar la altura y características del terreno afectado y



sus alrededores, ofreciendo información crítica sobre riesgos inminentes, personas o fauna en peligro, planificación de cortafuegos, ubicación de recursos (personas, vehículos, etc.). Primer aporte: información en vivo y precisa para mejorar la eficacia del combate al incendio.

Extinción directa del fuego

Los UAV están empezando a demostrar su capacidad en la lucha directa contra incendios, como se mostró en el Congreso de UAV en Shenzhen, donde se exhibieron tres categorías de soluciones:

Drones con mangueras conectadas a bombas terrestres

Estos UAV pueden levantar una manguera con una boquilla variable, sujeta bajo el tren de aterrizaje del dron. Este sistema, similar al usado en limpieza de fachadas de edificios, se conecta en tierra a una bomba que envía el líquido extintor. El operador, mediante la cámara FPV del dron, puede apuntar y hacer barridos precisos con el chorro de agua.

La presión de la bomba y el diámetro de la manguera determinan la altura de la operación. Se han reportado ca-

sos de uso desde 120 metros sobre el terreno. Este sistema resulta muy útil en puertos, refinerías u otras zonas industriales y puede adaptarse para emplear diferentes agentes según la categoría del incendio. Su principal desventaja es el alcance limitado; su ventaja, el control total del operador.

Drones con tanques de agentes retardantes

Estos UAV llevan tanques con agentes inhibidores, sujetos en placas al fuselaje. Los tanques pueden vaciar su contenido o liberarse con material fundente, permitiendo que el agente alcance la base del fuego para una mayor efectividad.

Se han desarrollado aparatos de este tipo que superan las tres toneladas, acompañados de vehículos nodriza terrestres para su transporte hasta zonas próximas al incendio. Este concepto es especialmente prometedor para bomberos urbanos en situaciones de respuesta rápida, como viviendas o edificios altos.

Drones con 'Bambi Buckets' en entornos rurales

Una variación del caso anterior es el uso de drones capaces de portar un *Bambi Bucket* suspendido de un gancho de arrastre. El caso más prometedor se ha visto en Canadá, donde grupos de UAV son desplegados anticipadamente en zonas rurales con alto riesgo de incendio (por sequía, estadísticas, etc.).

Estas operaciones se acompañan de piscinas de agua de tamaño adecuado, permitiendo una respuesta rápida que pueda contener un incendio en sus fases iniciales, especialmente en los suburbios amplios alrededor de las ciudades.

Anticipación y despliegue

Este tipo de despliegues hace posible anticiparse al riesgo de forma técnica y presupuestalmente viable en zonas con



Los UAV deben funcionar como una herramienta integrada y bajo el control confiable del equipo humano encargado de combatir el fuego

alta incidencia de incendios forestales. De esta manera se puede ofrecer una respuesta inmediata que impida su expansión.

Integración con sistemas de comando y control

En todos los casos mencionados, el uso y la efectividad de los UAV está directamente ligada al sistema de comando y control asociado. La clave es cómo el equipo que combate el incendio integra esta herramienta con los recursos tradicionales para añadir una capacidad de respuesta que hasta ahora no existía, como en el caso del despliegue anticipado en zonas de riesgo.

El ejemplo de Colombia

Queda pendiente el tema de las regulaciones del uso de UAV. En el caso de

Colombia, es posible su uso siempre que estén vinculados al PMU (Puesto de Mando Unificado), lo que tiene todo el sentido.

China, con su iniciativa Low Altitude Economy, va un paso más allá: permite el control remoto de UAV desplegados previamente, que son gestionados desde un centro remoto y no desde el sitio del suceso, en respuesta a alertas de sistemas integrados con el puesto de mando y control.

Conclusión

En resumen y para concluir, este es el punto central de la efectividad del uso de UAV en la lucha contra incendios: que funcionen como una herramienta integrada y bajo el control confiable del equipo humano encargado de combatir y aplacar el fuego. **S**



¿Cómo son valoradas las medidas contra incendios en tiendas físicas?

Por Redacción.

Las medidas contra incendios en tiendas físicas deben ser consideradas una prioridad en el sector del *retail*. Sin embargo, la percepción que suscitan entre los consumidores es diversa. Así, según un reciente sondeo de *Segurilatam* en LinkedIn, mientras el 45% las considera insuficientes o confusas, el 41% opina que son correctas pero mejorables. Y en porcentajes menores, el 9% reconoce que no se fija en ellas y el 5% cree que son adecuadas y visibles.

Insuficientes o confusas

El hecho de que las medidas contra incendios en tiendas físicas sean consideradas insuficientes o confusas puede

sugerir una brecha entre la normativa vigente y su aplicación. Y tal percepción podría deberse a que los encuestados, basándose en su experiencia, estiman que extintores, pulsadores de alarma, detectores de humo o salidas de emergencia no están debidamente señalizados o no son lo suficientemente visibles o accesibles.

A ello se suma, en ocasiones, la ausencia de una formación específica del personal para actuar en caso de emergencia y la carencia de protocolos y comunicaciones que orienten tanto a los empleados como a los clientes sobre cómo actuar en una situación de riesgo.

Correctas pero mejorables

Otra de las respuestas mayoritarias reconoce la existencia de medidas contra incendios en tiendas físicas, aunque en

ella se sugiere que podrían optimizarse. Por ejemplo, reforzando la señalización, actualizando los sistemas, asegurando su operatividad y adaptando las soluciones a la tipología del local y al flujo de personas.

De igual manera, la optimización podría apuntar a la mejora en la formación continua del personal, la integración de tecnologías de seguridad más eficientes y, como en la respuesta anterior, una comunicación clara, precisa y accesible con instrucciones para responder con prontitud a una emergencia.

Invisibles para algunos

Llama la atención que el 9% de los encuestados admita que nunca se ha fijado en las medidas contra incendios en tiendas físicas. Un dato que pone de manifiesto bien una despreocupación por parte de los consumidores, bien una escasa o nula concienciación sobre la importancia de la seguridad en esos espacios. En este sentido, cobra importancia, de nuevo, la necesidad de visibilizar la protección contra incendios en los establecimientos comerciales.

Adecuadas y visibles

Por último, una minoría señala que, a su juicio, las medidas contra incendios en tiendas físicas son adecuadas y visibles. Eso denota que se fijan en ellas y que, afortunadamente, hay espacios comerciales que cumplen la normativa y se toman muy en serio la protección de sus activos, trabajadores y clientes.

Margen de mejora

Una segunda encuesta de *Segurilatam* en LinkedIn revela que, aunque la ma-





Llama la atención que el 9% de los encuestados admita que nunca se ha fijado en las medidas contra incendios en tiendas físicas

yoría de los usuarios afirma conocer las medidas básicas de protección contra incendios en tiendas físicas, aún existe un margen de mejora en la concienciación pública. Concretamente, se ha planteado la siguiente pregunta: «¿Sabes qué medidas básicas de protección contra incendios debe tener una tienda física?». Y se han obtenido estos resultados:

- » Sí, las conozco bien (64%).
- » Más o menos (16%).
- » Muy poco o casi nada (12%).
- » No tengo ni idea (8%).

Aunque positivas en términos generales, estas respuestas ponen de relieve la necesidad de reforzar la cultura preventiva en entornos comerciales, especialmente en una región tan diversa como

América Latina, donde los marcos normativos pueden variar significativamente entre países.

Riesgo elevado

En el ámbito del *retail*, la protección contra incendios es un aspecto crítico de la seguridad. Por su naturaleza, una tienda física combina múltiples elementos de riesgo: concentración de personas, aparatos eléctricos, materiales inflamables, espacios cerrados y, en ocasiones, sistemas de climatización o almacenamiento mal ventilados.

De ahí que toda tienda física, independientemente de su tamaño, deba contar con una serie de medidas básicas de protección contra incendios alineadas con las mejores prácticas internacionales y adaptadas a las normativas locales.

Medidas básicas

En ese sentido, si bien las legislaciones pueden diferir, las siguientes son consideradas medidas básicas de protección contra incendios en tiendas físicas:

- » **Extintores portátiles.** Deben estar a la vista y bien señalizados. Y también revisarse periódicamente. Su número y tipo dependerán del tamaño del local y los materiales almacenados.
- » **Sistemas de detección de humo o calor.** Son fundamentales para alertar con prontitud y tienen que estar conectados a una central de alarmas.
- » **Iluminación y señalización de emergencia.** Es clave para una evacuación segura. Las salidas han de estar claramente identificadas y libres de obstáculos.
- » **Capacitación del personal.** Todo el equipo tiene que conocer los protocolos básicos ante un incendio: uso de extintores, rutas de evacuación y puntos de reunión o zonas de seguridad.
- » **Planes de evacuación.** Deben ser visibles y estar actualizados. En algunos países de América Latina, su elaboración y registro ante las autoridades locales es obligatorio.
- » **Revisión periódica de instalaciones eléctricas.** Una de las causas más comunes de incendios es el mal estado del cableado o la sobrecarga de enchufes.

Además de estas medidas básicas de protección contra incendios en tiendas físicas, es importante señalar que, en función del tamaño y ocupación del local, su ubicación y la normativa específica de cada país, los establecimientos comerciales han de considerar otras medidas complementarias. Entre ellas, rociadores automáticos, boquillas o hidrantes, alarmas acústicas y visuales, y puertas cortafuego. **S**

Tecnología menos letal y la reforma de 2025: **oportunidad para la defensa legítima**

Desde una perspectiva técnica y con base en la experiencia operativa, es preciso señalar que la denominación “no letal” resulta conceptualmente imprecisa. En el ámbito de la seguridad, todo instrumento de control genera un nivel de impacto fisiológico que, aunque no pone en riesgo la vida, sí busca inducir una respuesta corporal con fines de contención. En este sentido, los dispositivos BYRNA deben considerarse tecnologías “menos letales”, dado que su diseño se orienta a neutralizar amenazas mediante la aplicación de energía controlada, sin generar daño irreversible.

En un contexto de creciente inseguridad en muchas regiones de México, el debate sobre las armas de fuego y los mecanismos legales de defensa personal cobra una relevancia sin precedentes. La reforma publicada en mayo de 2025 a la Ley Federal de Armas de Fuego y Explosivos (LFAFE) ha introducido cambios clave que redefinen los límites entre lo permitido y lo restringido, aclarando un tema que por años se movió en una zona gris: el uso de dispositivos de defensa no letal como los lanzadores BYRNA.

Claridad legal

Por décadas, las leyes mexicanas dejaron lagunas respecto al uso de armas de aire, gas o pistón, lo que generó incertidumbre tanto en usuarios civiles como en profesionales del sector privado de seguridad. El principio de funcionamiento de dispositivos como los BYRNA se asemeja al de un arma de fuego (lanza proyectiles), pero sin usar pólvora ni provocar daño letal.

» **JOSÉ LUIS CALDERÓN GONZÁLEZ**
DIRECTOR DE NOLETAL

La reforma de 2025 introdujo el artículo 1º Bis, que define qué constituye un arma de fuego: «Se entiende por arma de fuego todo instrumento que cuente con cañón y que lance a través de éste un proyectil o bala por la acción de una deflagración de pólvora; por sus efectos similares a un arma de fuego, se incluyen en esta categoría las armas accionadas por algún tipo de gas inerte, aire comprimido o pistón que generen una energía cinética superior a los 140 Joules».

Esto significa que cualquier dispositivo que funcione por gas o aire comprimido pero no supere los 140 Joules de energía cinética está legalmente exento de ser clasificado como arma de fuego.

Aún más relevante resulta el artículo 13 reformado de la misma ley, que establece expresamente: «Se permiten las armas accionadas por gas, aire comprimido o pistón no superiores a los 140 Joules de energía cinética, así como los utensilios, herramientas o instrumentos similares que se utilicen para labores de campo o de cualquier oficio, arte, profesión o deporte; sin embargo, su uso debe limitarse al local o sitio en el que se



empleen. Cuando las armas a que hace referencia el párrafo anterior sean transportadas por necesidades de trabajo o para el ejercicio de un deporte, se deben demostrar esas circunstancias».

Aunque esta redacción no incorporó expresamente el término “dispositivos menos letales”, sí reconoce explícitamente el uso de herramientas impulsadas por gas o aire en labores profesionales, lo cual es una base sólida para justificar la legalidad del uso de tecnologías como BYRNA, particularmente cuando se integran en esquemas de protección, vigilancia y autoprotección.

Tecnología no letal

Los dispositivos BYRNA operan con cartuchos de CO₂ y disparan proyectiles calibre .68 y .61 pulgadas con una energía muy por debajo del umbral de 140 Joules. Por ejemplo, el modelo BYRNA LE (Law Enforcement) tiene una velocidad promedio de 100 m/s y una energía de aproximadamente 41.9 J/in². Esto coloca a toda la familia de productos BYRNA fuera del espectro regulado como armamento letal.

Esto representa un marco legal claro que permite a ciudadanos responsables y profesionales de la seguridad incorporar tecnologías como BYRNA en sus actividades. Siempre que su uso esté vinculado a fines legítimos –como protección personal, vigilancia privada o resguardo de instalaciones– y se justifique su aplicación con responsabilidad, estos dispositivos pueden ser transportados y utilizados dentro de lo permitido por la ley, sin necesidad de licencias especiales ni trámites complejos.

Fundamento adicional

La Ley Nacional sobre el Uso de la Fuerza (LNUF), en su artículo 3, define las armas menos letales como «aquellas a través de las cuales se disminuyen las funciones corporales de un individuo, reduciendo al mínimo el riesgo de causarle lesiones que pongan en peligro su vida». Esta definición refuerza la naturaleza jurídica de los dispositivos BYRNA como herramientas válidas y legales de uso proporcional de la fuerza.

Portación y uso

Un punto importante es el artículo 10 constitucional y su interpretación tradicional, donde la portación de armas se limita al domicilio. Pero al no tratarse de un arma de fuego, los dispositivos BYRNA pueden portarse y utilizarse dentro de los límites de la legalidad, siempre que se justifique su uso legítimo y proporcional en escenarios de protección personal o ejercicio profesional conforme al marco legal aplicable.

En contextos privados, como resguardar un negocio, escoltar a una persona vulnerable o proteger instalaciones, BYRNA se posiciona como una alternativa legal y eficaz para disuadir, contener o neutralizar amenazas sin incurrir en responsabilidad penal por uso de la fuerza letal.



Integrador de soluciones

En México, la marca NOLETAL es agente autorizado de BYRNA y ha desarrollado un modelo integral que va más allá de la simple venta de equipo. La propuesta incluye:

- Capacitación a usuarios operativos, requisito establecido en la Ley Nacional sobre el Uso de la Fuerza.
- Formación para mandos administrativos sobre control de inventarios, trazabilidad y resguardo.
- Entrenamiento técnico especializado para mantenimiento preventivo y correctivo de los dispositivos.

Esto convierte a NOLETAL en un aliado estratégico para particulares, empresas, dependencias de gobierno o cuerpos policiales que deseen integrar herramientas de defensa intermedia dentro del marco legal vigente.

Seguridad sin violencia

En un país donde las armas de fuego suelen generar miedo y polarización, el uso de tecnología menos letal abre una puerta responsable, progresiva y moderna

hacia la autoprotección y llena un vacío táctico en el uso progresivo de la fuerza. Dispositivos como los BYRNA permiten:

- Defenderse sin matar.
- Disuadir sin escalar.
- Responder sin poner en riesgo la vida propia ni la de terceros.

Hoy, con el respaldo legal claro, la tecnología disponible y aliados como NOLETAL, es posible consolidar un nuevo paradigma de seguridad para civiles, empresas y profesionales.

Si bien la reforma de 2025 no incluyó expresamente una categoría específica para dispositivos menos letales como los BYRNA, sí representa un paso firme hacia un marco más moderno y acorde con la realidad que enfrenta México.

BYRNA no es un equipo deportivo o recreativo. Es una plataforma integral de seguridad preventiva que combina tecnología de neutralización a distancia, una gama de accesorios como fundas, lámparas, miras, proyectiles especializados y programas de formación para su uso profesional. La decisión está en nuestras manos. **S**

América Latina y la Directiva NIS2: descarga el 'eBook' de ALCEA

Aunque la NIS2 es una directiva europea, su impacto trasciende fronteras. En América Latina, donde la digitalización avanza rápidamente, los principios de la NIS2 pueden servir como referencia para el desarrollo de marcos normativos locales. Países como México, Brasil, Colombia y Chile han comenzado a fortalecer sus estrategias de ciberseguridad y resiliencia, y la experiencia europea puede ofrecer lecciones valiosas.

Infraestructuras críticas

La cooperación internacional en ciberseguridad es esencial, especialmente en infraestructuras críticas de sectores como energía, salud y transporte, que son vulnerables a ataques transnacionales. Además, muchas empresas latinoamericanas operan en mercados europeos o colaboran con entidades sujetas a la NIS2, por lo que adoptar prácticas alineadas con esta directiva puede facilitar la integración y el cumplimiento normativo, lo que garantizará la correcta continuidad de negocio de manera global.

La ciberseguridad se ha convertido en un pilar esencial para la protección de los activos estratégicos de los Estados. La Directiva NIS2 (Network and Information Security Directive 2), adoptada por la Unión Europea (UE), representa un avance significativo en la regulación de la seguridad de las redes y sistemas de información. Esta normativa no sólo afecta a los países europeos, sino que también tiene implicaciones globales, incluyendo América Latina, donde la digitalización avanza a pasos agigantados.

» VÍCTOR HUGO MANZANILLA

RANGEL

MANAGING DIRECTOR EN ALCEA
MÉXICO



La Directiva NIS2 es una actualización de la Directiva NIS original de 2016. Su objetivo es establecer un nivel común elevado de ciberseguridad en todos los Estados miembros de la UE. A diferencia de su predecesora, la NIS2 amplía el alcance de las entidades obligadas, endurece los requisitos de seguridad y establece sanciones más severas por incumplimiento. También introduce mecanismos de cooperación entre los Estados miembros, como el Grupo de Cooperación y la Red de Equipos de Respuesta a Incidentes de Seguridad Informática CSIRT (Computer Security Incident Response Team), que permiten compartir información sobre amenazas y coordinar respuestas ante incidentes transfronterizos.

Sectores contemplados

La NIS2 clasifica los sectores en dos grandes grupos: esenciales e importantes. Los sectores esenciales incluyen energía, transporte, banca, salud, infraestructuras digitales y telecomunicaciones. Los sectores importantes abarcan servicios en la nube, plataformas digitales, redes sociales, administracio-

nes públicas, fabricación de productos claves y operadores satelitales. Esta clasificación refleja la creciente dependencia de la tecnología en todos los aspectos de la vida cotidiana y la necesidad de proteger estos sectores frente a amenazas cibernéticas.

Las infraestructuras críticas son fundamentales para el funcionamiento de la sociedad moderna. Su interrupción puede provocar consecuencias devastadoras, como apagones masivos, colapsos en el transporte, interrupciones en servicios sanitarios o fallos en sistemas financieros. La NIS2 busca proteger estos activos mediante la implementación de medidas de seguridad robustas y la mejora de la resiliencia organizacional. También promueve la colaboración entre entidades públicas y privadas, así como la cooperación internacional.

Gestión de riesgos

Cumplir con la NIS2 exige requisitos de gestión de riesgos en ciberseguridad tales como:

» **Evaluación continua de riesgos.** Las entidades deben identificar, analizar

y gestionar los riesgos que afectan a sus sistemas de información, incluyendo amenazas internas, externas y de terceros.

- » **Políticas de seguridad de la información.** Deben establecer políticas claras que cubran la protección de datos, control de accesos, seguridad física y lógica, y continuidad del negocio.
- » **Gestión de incidentes.** Se requiere la capacidad de detectar, responder y recuperarse de incidentes. Los incidentes significativos deben notificarse a la autoridad competente en un plazo máximo de 24 horas.
- » **Seguridad en la cadena de suministro.** Las organizaciones deben evaluar y mitigar los riesgos derivados de proveedores y terceros que tengan acceso a sus sistemas críticos.
- » **Criptografía y protección de datos.** Se exige el uso de tecnologías de cifrado y medidas de protección de datos personales y sensibles.
- » **Gestión de vulnerabilidades.** Las entidades deben implementar procesos para identificar, evaluar y corregir vulnerabilidades en sus sistemas.
- » **Autenticación y control de accesos.** Deben aplicar mecanismos de autenticación robusta y gestionar los privilegios de acceso de forma segura.
- » **Capacitación y concienciación.** Todo el personal debe recibir formación periódica en ciberseguridad, especialmente quienes ocupan roles técnicos o de liderazgo.
- » **Gobernanza y responsabilidad.** La alta dirección es responsable del cumplimiento de NIS2. Esto implica supervisión directa, asignación de recursos y reporte a las autoridades.
- » **Auditoría y documentación.** Las organizaciones deben mantener registros actualizados de sus medidas de seguridad, evaluaciones de riesgos y respuestas a incidentes disponibles



para inspección por las autoridades competentes.

Múltiples oportunidades

El cumplimiento de la Directiva NIS2 puede fortalecer la confianza de clientes, socios y ciudadanos, mejorar la eficiencia operativa y facilitar el acceso a financiación europea. También impulsa la innovación al fomentar la adopción de tecnologías seguras y la transformación digital en entornos críticos. Las organizaciones que implementen la NIS2 de forma efectiva estarán mejor preparadas para enfrentar los desafíos del futuro digital.

La Directiva NIS2 marca un hito en la protección de infraestructuras críticas y en la consolidación de una cultura de ciberseguridad en Europa y el mundo. Su enfoque integral combina requisitos técnicos, responsabilidad organizacional y cooperación internacional, y ofrece

un modelo robusto para enfrentar las amenazas digitales del siglo XXI. Para América Latina, la NIS2 representa una oportunidad de aprendizaje y adaptación que puede contribuir a fortalecer la seguridad digital en la región. En un entorno global interconectado, la ciberseguridad debe ser una prioridad compartida, y la NIS2 ofrece un marco sólido para avanzar en esa dirección.

Descarga el 'eBook'

Desde ALCEA comprendemos que su infraestructura crítica merece protección en todos los frentes. NIS2 no es sólo una directiva; se trata de una hoja de ruta para garantizar la resiliencia ante el aumento de las amenazas. Es por ello por lo que hemos creado un eBook que puede descargarse desde el siguiente enlace: <https://www.alceaglobal.com/es/knowledge-base>. 

La ciberseguridad, ¿el punto débil de los sistemas de seguridad?

Los sistemas de seguridad física y, en general, los dispositivos IoT conectados a Internet son susceptibles de recibir un ciberataque. Y un ciberataque podría conllevar, por ejemplo, que un ciberdelincuente desactivase un sistema de intrusión, inutilizase un sistema de videovigilancia, robase y/o eliminase imágenes, deshabilite un control de accesos o abriese una cerradura electrónica, acarreamando, a su vez, consecuencias para la seguridad de instalaciones y personas que podrían ser muy graves a nivel operativo, económico, legal y reputacional.

Vulnerabilidades

A continuación, cito algunos casos relacionados con vulnerabilidades en sistemas de seguridad que se han hecho eco en el mundo de la ciberseguridad.

AVTECH. En enero de 2025, Qualys publicó un informe técnico sobre la *botnet* Murdoc donde se recogía que dispositivos de la marca AVTECH, fabricante taiwanés de sistemas de videovigilancia, se habían visto afectados desde julio de 2024 por este *malware* que explotaba la vulnerabilidad identificada CVE-2024-7029. Este *malware* permite tomar control remoto de los dispositivos, lo que puede implicar su inutilización, el robo de imágenes y el uso de los dispositivos como vectores de ataque a otros sistemas.

Verkada. El 9 de marzo de 2021, la compañía estadounidense Verkada, fabricante de sistemas de videovigilancia y control de acceso, publicó un informe relativo a un incidente de seguridad en el que exponía que sus dispositivos habían sido ciberatacados por un grupo de hackers liderado por el suizo Tillie Kottmann.

JUAN CARLOS FÚNEZ
RESPONSABLE DE IT EN CASMAR



Se estima que pudo acceder a unas 150.000 cámaras de seguridad instaladas en hospitales, cárceles, escuelas y empresas como Tesla y Cloudflare.

Applied Risk. En 2018 y 2019, el experto en ciberseguridad industrial Gjoko Krstic, de la compañía holandesa Applied Risk, analizó vulnerabilidades en edificios inteligentes y demostró que era posible desactivar alarmas, abrir o bloquear puertas electrónicas, controlar ascensores, interceptar sistemas de videovigilancia, etc., aprovechando vulnerabilidades en redes wifi y en los dispositivos y sistemas conectados a ellas.

¿Qué podemos hacer?

En este contexto, ¿qué podemos hacer para intentar que los sistemas de seguridad sean lo más ciberseguros posible? Algunas claves para alcanzar ese objetivo son:

Mantener los dispositivos actualizados con la última versión de *firmware* y *software* disponible. La NVD (National Vulnerability Database) gestionada por el NIST (National Institute of Standards and Technology) es la base de datos oficial de vulnerabilidades del Gobierno de EEUU. Su objetivo es recopilar, analizar y

publicar información sobre vulnerabilidades de seguridad en *software*, *hardware* y sistemas conectados. Y ofrece detalles técnicos de vulnerabilidades (CVE), puntuaciones de severidad (CVSS), información de productos afectados, soluciones y enlaces a parches, etc.

Algunos ejemplos de vulnerabilidades identificadas por la NVD con afectación en sistemas de seguridad son:

- CVE-2024-7029. Afectó a dispositivos AVTECH permitiendo la infección por el *malware* Murdoc.
- CVE-2023-28808. Afectó a dispositivos Hikvision permitiendo la ejecución remota de código y el acceso no autenticado.
- CVE-2021-33044. Afectó a dispositivos Dahua permitiendo el acceso no autorizado con posibilidad de control total del dispositivo.

Gracias a esta base de datos, una vez identificada una vulnerabilidad, los fabricantes pueden publicar una nueva versión de *firmware* con el fin de eliminar la vulnerabilidad en cuestión de sus dispositivos.

Utilizar contraseñas complejas, nunca utilizar contraseñas por defecto y usar sistemas multifactor si es posible.



Innovación que transforma la seguridad en soluciones más inteligentes

Descubre
nuestras
soluciones
con IA



Se entiende por contraseña compleja la que tiene doce caracteres o más, números, letras mayúsculas, letras minúsculas y símbolos, además de no guardar ninguna relación con los datos de los usuarios que las generan ni con los sistemas en los que se emplean. Todo ello con el fin de dificultar que la contraseña pueda ser deducida o que sea fácil de hackear mediante un ataque de fuerza bruta o de diccionario. Por ejemplo, la *botnet* Mirai en 2016 afectó a cámaras IP y DVR OEM fabricados por marcas como XiongMai Technologies porque usaban credenciales por defecto como admin/admin o root/12345.

Evitar puertos predeterminados, deshabilitar los innecesarios y utilizar comunicaciones cifradas con el protocolo TLS. Volviendo al caso de la *botnet* Mirai, escaneaba Internet en busca de dispositivos IoT (como cámaras de videovigilancia) con puertos abiertos y credenciales por defecto. Si encontraba abierto el puerto 23 (telnet) que permite el acceso remoto sin cifrado, el *malware* intentaba acceder al dispositivo utilizando contraseñas por defecto como admin/admin. Por otro lado, siempre deben utilizarse interfaces web y comunicaciones seguras como HTTPS, que cifra mediante TLS la comunicación, lo que imposibilita que la información sea accesible para un atacante. En este sentido, de utilizarse un acceso web HTTP sin cifrado, los datos que viajan serán fácilmente accesibles para un atacante.

Configurar la red de forma segura:

- Segmentar la red implementando VLAN a nivel de *switch* para evitar que los sistemas de seguridad sean accesibles para cualquier dispositivo, sistema o persona que esté conectado a la red.
- Utilizar conexiones remotas VPN para acceder desde fuera de la red a los sistemas de seguridad con el fin de evitar que estos estén expuestos en Internet.



- Permitir el acceso a la red únicamente a los dispositivos autorizados, por ejemplo, mediante el control de la MAC.

Instalar dispositivos certificados como ciberseguros.

Algunos ejemplos:

- ETSI EN 303 645. Estándar europeo para la ciberseguridad de dispositivos IoT de consumo, que garantiza una serie de requisitos mínimos como no usar contraseñas por defecto, permitir actualizaciones seguras, cifrado de datos y protección contra accesos no autorizados.
- ETSI EN 18031. Estándar europeo complementario al EN 303 645, centrado en la evaluación de la seguridad de productos IoT.

Monitorear el tráfico de red en busca de comportamientos anómalos.

Aporta los siguientes beneficios:

- Detección temprana de amenazas. Permite identificar comportamientos anómalos como conexiones no autorizadas, escaneos de puertos o tráfico hacia servidores desconocidos.
- Prevención de ataques. Al detectar patrones inusuales, se pueden bloquear acciones maliciosas antes de que causen daño (por ejemplo, un intento de exfiltración de datos desde una cámara IP).

- Visibilidad completa de la red. Ayuda a entender qué dispositivos están conectados, cómo se comunican y si están actuando fuera de lo esperado.

- Respuesta rápida a incidentes. Facilita la investigación y contención de incidentes de seguridad, reduciendo el tiempo de exposición.

- Cumplimiento normativo. ISO 27001 y ENS exigen capacidades de monitoreo y registro de eventos de red. Detección de dispositivos comprometidos. Si se detecta que una cámara o cualquier otro dispositivo de un sistema de seguridad envía datos a una IP desconocida, puede ser señal de que ha sido infectado o atacado.

Formar al personal en ciberseguridad básica contribuye a:

- La configuración adecuada en cuanto a ciberseguridad de los distintos dispositivos de los que se compone un sistema de seguridad.
- La identificación de amenazas tempranas detectando, por ejemplo, comportamientos anómalos o accesos sospechosos.
- La capacidad para responder adecuadamente en caso de producirse un incidente. **S**

Su asesor
de confianza

Servicios Cloud

Fábrica de
Software

Control de Acceso

Resolvemos
Problemas de
Negocio

Control de
Asistencia

Estacionamientos

Diseño
Ingeniería
Instalación

MAGNETIC[®]
ACCESS TO PROGRES[™]

FAAC


WOLPAC

AXESS TMC
ZucchettiGroup

 **AIPHONE**[®]

 Microsoft


PERCo

 **GALLAGHER**[™]


BG
electronics
Creating big ideas

Teratronik
LATAM

INDECT

ELKA

Medios que dejan huella ■

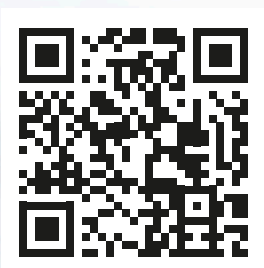
#caminandojuntos

SEGUR**LATAM**

SUSCRÍBETE
GRATIS
NEWSLETTER



ANÚNCIATE
CON
NOSOTROS



Darte a conocer exige un nuevo camino.
Caminemos juntos.

Ecosistema de **GRUPO BORRMART.**

CANAL VÍDEO Y PODCAST

AUDIENCIAS DIGITALES B2B

MARKETING AUTOMATION

CONTENT MARKETING

AGENCIA DIGITAL

EVENTOS & NETWORKING

ESTRATEGIAS DE REDES SOCIALES

SEO & EMAIL MARKETING

ESTUDIOS DE MERCADO

ECOMMERCE **K**_{PRO}

BORRMART

Medios que dejan huella

Seguridad nacional en transformación: nuevo marco legislativo en México

Por Redacción.

En el mes de julio, el Senado mexicano aprobó un paquete legislativo que transforma el modelo de seguridad pública en el país. Desde la militarización de la Guardia Nacional hasta la protección de menores en el turismo, el nuevo marco normativo busca reforzar la coordinación institucional, la inteligencia estratégica y el respeto a los derechos humanos, aunque no sin generar polémica. Estas leyes marcan un punto de inflexión en la política de seguridad del nuevo gobierno federal encabezado por **Claudia Sheinbaum**.

Guardia Nacional

Coincidiendo con el sexto aniversario de su creación, la Guardia Nacional ha sido oficialmente transferida a la estructura de la Secretaría de la Defensa Nacional (Sedena). Con la aprobación de la nueva **Ley de la Guardia Nacional**, se consuma su transformación de cuerpo civil con formación policial a fuerza operativa de mando militar, bajo el control de un general de División en activo nombrado por el presidente.

Esta legislación otorga nuevas atribuciones: la Guardia Nacional podrá realizar operaciones encubiertas, intervenir comunicaciones y geolocalizar personas, siempre con orden judicial. También se habilita el intercambio de información con el Centro Nacional de Inteligencia (CNI) y el Consejo Nacional de Seguridad, consolidando su papel en tareas de inteligencia.

Además, los elementos de este cuerpo podrán solicitar licencias para participar



en procesos electorales, ampliando su margen de actuación política. La ley introduce cambios en códigos militares, régimen de ascensos y el tratamiento de faltas internas, que pasan a depender del fuero militar, mientras el servicio civil seguirá bajo el fuero federal.

Estas modificaciones han generado un debate nacional sobre la militarización de la seguridad pública, cuestionando si este giro fortalece la seguridad o erosiona los principios democráticos de control civil.

Seguridad Pública

La **Ley General del Sistema Nacional de Seguridad Pública**, también avalada por el Senado, articula un modelo de gobernanza más integrado para la seguridad pública, con base en la Estrategia Nacional de Seguridad 2024–2030. Su

objetivo es claro: establecer reglas comunes, mejorar la colaboración entre niveles de gobierno y profesionalizar a los cuerpos de seguridad.

Entre sus ejes se encuentra la creación de una Subsecretaría de Inteligencia e Investigación Policial, adscrita a la Secretaría de Seguridad y Protección Ciudadana (SSPC), encargada de anticipar amenazas mediante análisis estratégicos. La norma establece un Sistema Nacional de Información que unifica registros sobre armamento, detenciones, mandamientos judiciales, delitos, personal operativo y vehículos robados, entre otros.

Asimismo, se potencia la certificación y formación continua mediante una Academia Nacional de Seguridad Pública, garantizando derechos laborales, pensiones y prestaciones para el personal.

También se establecen mecanismos de fiscalización con la Auditoría Superior de la Federación para vigilar el uso de recursos públicos.

La Guardia Nacional queda formalmente incorporada en esta ley como un actor clave, asegurando su participación en mesas de coordinación operativa y conferencias de seguridad a nivel federal, estatal y municipal.

Inteligencia y privacidad

En cuanto a la **Ley del Sistema Nacional de Investigación e Inteligencia en materia de Seguridad Pública**, pretende reforzar la capacidad institucional del Estado para combatir el crimen organizado mediante inteligencia criminal avanzada.

Uno de sus puntos más controvertidos es que autoriza el acceso directo, sin orden judicial previa, a registros biométricos, fiscales, bancarios, vehiculares y de telecomunicaciones tanto públicos como privados. Esta información será centralizada en una nueva Plataforma Central de Inteligencia, operada por el (CNI), lo que permitirá generar productos analíticos para el Ministerio Público.

Se contempla además la creación de un Consejo Nacional de Inteligencia en Seguridad Pública y una subsecretaría específica dentro de la SSPC, lo que refuerza la estructura operativa. Esta ley se articula con el Sistema Nacional de Seguridad Pública, favoreciendo la interoperabilidad entre distintos niveles del Estado.

Sin embargo, la oposición (PRI, PAN y Movimiento Ciudadano) ha manifestado su rechazo, alertando sobre una posible deriva hacia el "gobierno espía" y el debilitamiento de la privacidad ciudadana. Mientras el oficialismo defiende que se garantiza la legalidad, los críticos temen que esta norma sienta las bases de un modelo de vigilancia masiva sin controles democráticos suficientes.



El nuevo marco normativo busca reforzar la coordinación institucional, la inteligencia estratégica y el respeto a los derechos humanos

Turismo seguro

En un ámbito completamente distinto, pero igualmente crucial, se ha reformado la **Ley General de Turismo** con el objetivo de combatir la explotación sexual infantil en destinos turísticos. Esta reforma responde a estadísticas alarmantes: según el INEGI, más de cuatro menores son víctimas de abuso sexual cada día en México, y se calcula que 600.000 turistas sexuales visitan el país anualmente.

La ley impone nuevas obligaciones a los prestadores de servicios turísticos, como la implementación de protocolos preventivos para detectar delitos contra menores en instalaciones físicas y plataformas digitales. También se exige verificar la filiación o tutela de adultos

que viajen con menores, bajo riesgo de negar el servicio y notificar a las autoridades.

De igual manera, se fortalece el papel institucional de la Secretaría de Turismo, que deberá coordinar acciones con el Sistema Nacional de Protección de Niñas, Niños y Adolescentes (SIPINNA) y capacitar al sector turístico en la detección de situaciones de riesgo. Los prestadores de servicios turísticos estarán obligados a elaborar un informe anual de prevención de la trata y explotación de menores.

Esta reforma representa un paso firme hacia una política de turismo responsable y transparente, donde la protección de la infancia pasa a ser un eje rector del desarrollo del sector. **S**

La seguridad privada y los retos significativos ante el empleo de drones

La seguridad privada se encuentra en el trance de los albores del nuevo milenio, marcado por el avizoramiento de una serie de cambios tecnológicos, próximos a marcar la prestación de un servicio remunerado, que se tornará más tecnificado ante el advenimiento de la tecnología aeronáutica de las aeronaves pilotadas a distancia, también denominada drones.

Dentro de un fortalecido conjunto conceptual, ello implica el empleo de la inteligencia artificial y la ciberseguridad en aras de maximizar la aplicación de una nueva herramienta tecnológica destinada a reforzar los lazos entre el sector privado y cada Estado-nación. Ambos entes se consolidan a través del esfuerzo direccionado a garantizar los derechos humanos de cada persona dentro de un contexto más complejo y dinámico donde la previsión de las ame-

» **GEOG. JOSELINO DEL VALLE SERRANO MARTÍNEZ**
ESPECIALISTA EN SEGURIDAD CIUDADANA

nazas resulta vital para evitar pérdidas tanto humanas como de activos tangibles e intangibles.

Dispositivos muy útiles

En este sentido, se destacan varios referentes mundiales que confirman el empleo de los drones en el campo de la seguridad. LISA Institute señala que «los drones son y serán de gran utilidad para la policía, seguridad privada, militares



y personal de emergencias, ya que les permitirá actuar de forma más eficaz y segura».

A medida que los entes encargados de garantizar la seguridad y la defensa en cada Estado-nación adquieran drones para determinadas acciones, según su naturaleza y competencias, las empresas encargadas de la prestación del servicio de vigilancia y seguridad privada también los incorporarán.

Adaptación e innovación

Según J.C. Oviedo, «la adaptación y la innovación son principios que han regido el curso de las organizaciones en la historia humana; la supervivencia de estas depende de su capacidad para adaptarse al entorno en que operan y del grado de innovación que imprimen a sus procesos».

La fuente señala el uso de los drones en la seguridad y vigilancia privada como una valiosa herramienta de soporte tecnológico, integrada a los centros de monitoreo, desde donde pueden utilizarse para labores de detección y control, especialmente en grandes superficies o instalaciones que así lo requieran.



Protección y monitoreo

Por su parte, Juan David Tinjaca Galeano establece que el empleo de drones en la vigilancia reduce el riesgo para el personal de seguridad, salvaguardando su vida en caso de una posible intrusión de grupos armados en instalaciones protegidas e infraestructuras críticas.

Y agrega que los drones nos facilitan la visualización desde la altura, detectando personas con posible intención de perpetrar acciones en nuestro lugar vigilado. También nos permiten verificar constantemente los sitios vulnerables con su cámara de alta resolución en tiempo real, tomando decisiones rápidas con excelentes resultados. Como se trata de sitios extensos, el desgaste físico de nuestros vigilantes es menor al usarlos como grupo de reacción inmediata en caso de ser requeridos.

Eventos públicos y ámbito corporativo

Por lo que respecta a LISA Institute, indica que el personal de seguridad privada, al operar casi siempre en recintos privados, podría hacer mayor uso de esta tecnología, conforme a la normativa vigente, aunque aún no se haya incorporado completamente a sus medios habituales.

En eventos públicos como conciertos, festivales u otros eventos masivos, donde la seguridad privada también presta sus servicios, Tinjaca Galeano señala que los drones pueden proporcionar una vigilancia aérea que complementa la seguridad terrestre.

Del mismo modo, en el seguimiento de activos y personas en el ámbito corporativo, los drones pueden utilizarse para monitorear la ubicación y seguridad de activos valiosos o personal VIP. Además, pueden ser desplegados para identificar incidentes en tiempo real, proporcionando una visión aérea que ayuda



a coordinar la respuesta de los equipos de seguridad y emergencia.

Reducción de costes

Según el sitio web de IDC, los drones en la seguridad privada han transformado la forma en que se abordan los desafíos de seguridad en diversos sectores. Estas poderosas herramientas voladoras ofrecen una amplia gama de beneficios, pero también plantean desafíos y exigen el cumplimiento de regulaciones específicas.

El uso de drones puede conducir a una reducción significativa de costes y recursos. En comparación con las patrullas tradicionales, los drones son más económicos de operar y requieren menos personal. Además, la recopilación de datos y la vigilancia realizada por drones puede ser más eficiente y precisa, ahorrando tiempo y recursos valiosos.

Casos prácticos

Las empresas de seguridad privada han incorporado drones a sus plantillas para dar respuesta a la creciente demanda de una vigilancia más inteligente, eficaz y rentable. Como principales usos, se resalta su capacidad para alcanzar zonas

de difícil acceso, permitiendo un control más riguroso del material en naves de almacenaje y logística, así como el control de zonas extensas mediante planos aéreos. Esta tecnología permite supervisar escenarios amplios sin apenas desplazarse, lo que resulta útil para la vigilancia de fincas, pistas de esquí, campos de golf, puertos deportivos, etc. También permite programar rutas, así como reconocer rostros y matrículas con precisión.

Conclusión

El empleo de drones en el sector de la seguridad privada ha venido creciendo de forma paulatina y significativa. Las empresas encargadas de la prestación del servicio de vigilancia y seguridad privada son conscientes de que su capacidad para realizar tareas complejas y operar en entornos difíciles convierte a los drones en una herramienta ideal para el desempeño de actividades orientadas a brindar protección. Estas empresas están invirtiendo en esta tecnología para optimizar la eficacia y eficiencia de sus sistemas de seguridad, y así poder responder de forma rápida frente a potenciales situaciones de amenaza, vulnerabilidad o riesgo que sean detectadas. **S**

Curso Superior en Contrainteligencia y Seguridad de la Fundación Borredá

La Fundación Borredá ha abierto el periodo de inscripción para el Curso Superior en Contrainteligencia y Seguridad 2025, impartido por profesionales del ámbito civil, las Fuerzas Armadas, las Fuerzas y Cuerpos de Seguridad y expertos en inteligencia, contrainteligencia y seguridad corporativa.

El programa se puede realizar tanto en formato presencial (en Madrid, España) como *online* (síncrono o asíncrono) de septiembre a noviembre. Y el objetivo del curso es la formación de auténticos profesionales en los procedimientos de Contrainteligencia y Seguridad para que sean capaces de apoyar a la dirección de las empresas en aspectos como:

- » La planificación estratégica en apoyo a la toma de decisiones.
- » La determinación integral de los factores de una situación y su comprensión en un análisis predictivo.
- » El conocimiento y empleo de las metodologías más apropiadas para la explotación de la información disponible, formulación de posiciones y reglas de negocio.
- » La auditoría y el diagnóstico de los procesos de Contrainteligencia y Seguridad en el seno de la empresa u organización y la identificación de las fortalezas y debilidades de esta.
- » El análisis de las diferentes opciones que se ofrecen a las empresas para organizar sus propios recursos dedicados a Contrainteligencia y Seguridad.
- » La desinformación y las *fake news* (detección y tratamiento).
- » La amenaza interna.



¿A quién está dirigido?

El curso está dirigido a directivos de organizaciones de todos los tamaños con responsabilidad en la dirección estratégica de las mismas, así como a titulados superiores que busquen especializarse en inteligencia aplicada al ámbito corporativo. Y también a profesionales de áreas como diplomacia y economía, titulados superiores de departamentos de ventas, *marketing*, comunicación o recursos humanos, etc. No obstante, podrá ser realizado por cualquier persona, aunque no tenga acreditado grado universitario alguno.

Contenidos

El programa del curso aborda una amplia gama de contenidos:

- » Contrainteligencia y Seguridad Corporativa.
- » Amenazas y riesgos.
- » Diseño del modelo de amenaza.
- » Metodología para analizar riesgos.

- » Análisis en Contrainteligencia y Seguridad.
- » Document and Media Exploitation (DOMEX).
- » Contribución de contrainteligencia a OPSEC y protección de la organización.
- » Seguridad de la Información.
- » Ciberseguridad.
- » Otras facetas de la Seguridad.

¿Cuál será la metodología?

El curso se va a llevar a cabo mediante una metodología de *blended learning*, combinando la modalidad presencial con sesiones *online*. La metodología se basa en el trabajo autónomo del alumno y la realización de actividades prácticas bajo la supervisión de un profesor-tutor. Se introducirá una metodología participativa, altamente dinámica y con un enfoque práctico que permitirá entender la contrainteligencia y la seguridad y su implementación efectiva en entornos corporativos. Más información en la página web www.fundacionborreda.org. 



Curso Superior en
**Contrainteligencia
y Seguridad**



CURSO 2025

Curso Superior en “Contrainteligencia y Seguridad”
(Titulación del Instituto Superior de Investigación Empresarial)

Duración: Septiembre 2025 – Noviembre 2025

Nº de créditos ECTS : equivalente a 13 ECTS

Modalidad: presencial y/o on-line síncrono

Precio: 2.000€



Abierto período de inscripción

Plazas limitadas

Más información: eva.martin@fundacionborreda.org

Conquista Google con 'Segurilatam'

En el mercado actual, donde la competencia es feroz, la visibilidad lo es todo. *Segurilatam* es tu socio estratégico para lograr que tu marca destaque en Google. Con campañas optimizadas para SEO ayudamos a empresas a mejorar su visibilidad en buscadores. *Segurilatam* es el puente que necesitas para que tus clientes potenciales te encuentren en Google.

¿Por qué apostar por 'Segurilatam'?

» **Palabras clave estratégicas.** Nuestra revista dispone de multitud de palabras clave valiosas muy bien posicionadas relacionadas con el sector de la seguridad. Además, trabajamos nuestro posicionamiento de forma constante para conseguir

más impresiones y clics gracias al SEO.

» **Inversión eficiente.** Sin necesidad de costosas campañas, alcanzamos visibilidad orgánica gracias a nuestra autoridad en el sector de la seguridad. Cuando contratas nuestros servicios de SEO transfieres parte de dicha autoridad y notoriedad de nuestra revista *online* a tu página web. Esto puede hacer que Google y otros buscadores mejoren tu posición por palabras clave, mejorando también tu tráfico y conversiones.

» **Contenidos variados.** Desde entrevistas a presentaciones de producto, en *Segurilatam* logramos resultados efectivos en una amplia variedad de contenidos.

» **Autoridad.** Quienes buscan información en Google, además de buscar tu

empresa, contrastan información mediante medios independientes como la revista *Segurilatam*. Ello es una razón más e indispensable para desarrollar una estrategia de *marketing* de contenidos con tu revista.

» **Diferenciación.** Destaca ante la competencia. El contenido editorial en tu revista puede ser la diferenciación que marque la diferencia en el proceso de decisión de tu potencial cliente.

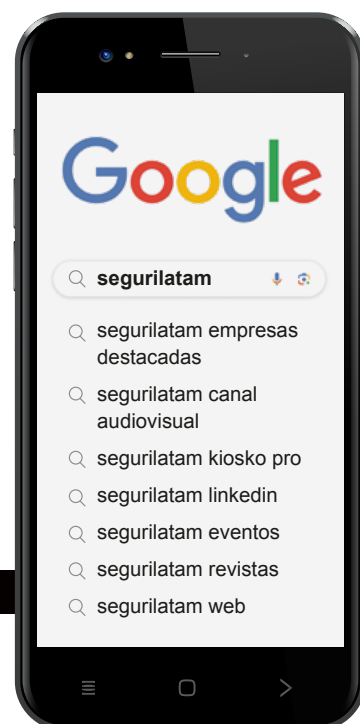
Empresas líderes en el sector de la seguridad han confiado en nosotros para impulsar su visibilidad, posicionando desde innovaciones hasta servicios.

Descubre el poder del SEO con *Segurilatam* y todas las posibilidades del *marketing* digital solicitando ya nuestro *mediakit* digital. **S**

#CaminandoJuntos

DEJANDO HUELLA EN GOOGLE ¿Y TÚ?

BORRMART
Medios que dejan huella



#CaminandoJuntos

DEJANDO HUELLA EN GOOGLE.

¿Y TÚ?

Trabajamos para lograr los posicionamientos clave en el sector de la industria de la seguridad



**ANÚNCIATE CON
NOSOTROS**

B  **RRMART**

Medios que dejan huella



II CONGRESO MEXICANO DE DIRECTORES DE SEGURIDAD

Seguridad corporativa: eje estratégico para la protección de las organizaciones

Tras el éxito cosechado en la primera edición, 'Segurilatam' organizó, el pasado 27 de mayo, el II Congreso Mexicano de Directores de Seguridad en la CDMX. Al igual que el encuentro del año pasado, este nuevo evento sectorial para un aforo exclusivo y limitado tuvo lugar en La Roma Centro de Negocios, en cuyo auditorio se dieron cita en torno a 200 profesionales del ámbito de la Seguridad Corporativa y proveedores del sector.

Por Redacción. Fotos: Gabriela Soto, Marcela Linares Vásquez y AMESP.

Acompañado de **David Romero**, presidente de la Comisión de Seguridad de la Cámara Española de Comercio en México, **Javier Borredá García**, director de *Segurilatam*, observó en su discurso inaugural que "los riesgos han cambiado: ya no sólo enfrentamos amenazas físicas, sino también digitales, sociales, reputacionales y humanas. Y es en este nuevo panorama donde los directores de Seguridad deben asumir con claridad su rol como guardianes, líderes, analistas y constructores de entornos resilientes y confiables".

Geopolítica, alta dirección y seguridad perimetral

A continuación, se llevó a cabo el panel *Geopolítica: el rol del director de Seguridad en el nuevo orden mundial*. Moderado por **Mario Arroyo Juárez**, director del Instituto Iberoamericano de



La segunda edición del Congreso Mexicano de Directores de Seguridad organizado por 'Segurilatam' puso de relieve que la seguridad corporativa se ha convertido en un eje estratégico para la protección y la resiliencia de las organizaciones.

Liderazgo en Seguridad Privada SC, contó con la participación de **Juan Ramón Cánovas**, director de Seguridad Corporativa y Resiliencia de Iberdrola México; **Dora Cortés**, directora de Seguridad en L'Oréal; y **Juan Raúl Chin**, Regional Security Manager North America and Latin America Markets en HP.

El II Congreso Mexicano de Directores de Seguridad prosiguió con el panel *Seguridad Corporativa y alta dirección*. En este caso, la moderación corrió a cargo de **David Romero**, director de Seguridad, Salud y Servicios Corporativos de Banco Sabadell México, quien abordó la relación entre los profesionales de las áreas de

Patrocina



Seguridad y los ejecutivos de las organizaciones con **Guillermo Hassey**, National Security Officer en Daimler Truck México; **Dagoberto Santiago**, Sr. Director of Global Security for PepsiCo Latam; **César Rojas**, Regional Security Director North Latam Cluster en Bayer; y **Mario Franco**, Security Director for Mexico & Central America en Schneider Electric.

Y antes del *coffee break* para intercambiar impresiones y hacer *networking*, **Enrico Iacoi**, director general en RS, impartió la ponencia *Inversión inteligente en seguridad perimetral: mitigación de riesgos y protección del activo empresarial*.

Seguridad integral y soluciones tecnológicas

Seguidamente, **Juan Ramón Cánovas** disertó sobre la seguridad integral como parte del negocio, una interesante charla seguida de la presentación de soluciones tecnológicas para departamentos de Seguridad Corporativa a cargo de:

- » **Víctor Hugo Manzanilla Rangel**, Managing Director en ALCEA Mexico, firma especializada en la protección de infraestructuras críticas de diferentes sectores (energía, agua, telecomunicaciones, transporte, minería, petróleo y gas), con soluciones integrales de seguridad.
- » **José Luis Calderón González**, socio fundador de Noletal, empresa dedicada a la comercialización de tecnologías tácticas no letales para infraestructuras y ciudades, así como a la capacitación especializada, asesoría legal y desarrollo de protocolos operativos para garantizar su uso responsable.
- » **Darwin Bejarano**, consultor técnico para Latam en ManageEngine, que, a través de *software* para la administración de redes y dispositivos, seguridad y mesas de ayuda, se dedica a alinear TI con el negocio mediante un enfoque global integral.



Dircurso inaugural: Javier Borredá García, director de 'Segurilatam', se dirige a los asistentes del II Congreso Mexicano de Directores de Seguridad.



Juan Ramón Cánovas, Dora Cortés, Juan Raúl Chin, Mario Arroyo y Javier Borredá García tras la celebración del panel dedicado a la geopolítica.



Guillermo Hassey, Dagoberto Santiago, César Rojas, Mario Franco y David Romero debatieron sobre la relación entre las áreas de Seguridad Corporativa y la alta dirección.



Enrico Iacoi, director general en RS, dedicó su presentación en el II Congreso Mexicano de Directores de Seguridad a la inversión inteligente en seguridad perimetral.



Juan Ramón Cánovas, director de Seguridad Corporativa y Resiliencia de Iberdrola México, disertó sobre la seguridad integral como parte del negocio.



Víctor Hugo Manzanilla Rangel, Managing Director en ALCEA México, firma especializada en la protección de infraestructuras críticas de diferentes sectores.

» **Jorge Uribe**, director comercial de Grupo IPS, todo un referente en el sector de la seguridad privada con 30 años de historia. Actualmente, la empresa fundada por **Armando Zúñiga Salinas** destaca por su innovación, compromiso social y excelencia laboral.

Departamentos de Seguridad

La agenda del II Congreso Mexicano de Directores de Seguridad también puso en valor el desempeño de los departamentos de Seguridad en las organizaciones. Bajo la moderación de **Ana Luisa Guzmán**, directora de Seguridad Corporativa en Grupo GICSA, dicho asunto fue tratado por **Marco Antonio Sanmiguel**, Country Security en Heineken México; **Juan Antonio Bernal**, Director Regional de Seguridad y Gestión de Crisis México, ARCAC & Chile en General Electric Vernova; y **Chesus Miguel Gay Grao**, Country Manager en SCATI.

Al respecto, los expertos analizaron cuestiones como el rol principal de las áreas de Seguridad Corporativa, el avance de la tecnología aplicada a la seguridad o las propuestas de los ejecutivos de Seguridad en su calidad de consultores y gerentes integrales de los negocios.

Y, tras ellos, **José Arellano**, Vertical Sales Manager de Genetec, compartió algunos datos del informe *Estado de la Seguridad Electrónica 2025*. Se trata de la última edición del reporte de la firma especializada en *software* de seguridad, un documento que brinda un análisis exhaustivo de las tendencias en evolución en las operaciones de seguridad electrónica.

Evolución de la dirección de Seguridad 2025-2030

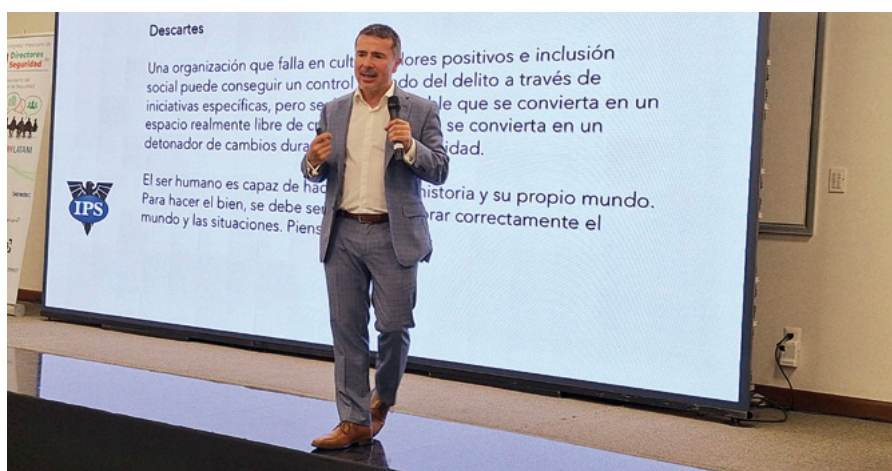
Y el II Congreso Mexicano de Directores de Seguridad concluyó con un panel moderado por **Javier Borredá García**, dedicado a la evolución de la seguridad corporativa



José Luis Calderón González, socio fundador de Noletal, empresa dedicada a la comercialización de tecnologías tácticas no letales, y Javier Borredá García.



Darwin Bejarano, consultor técnico para Latam en ManageEngine, compañía que tiene como objetivo alinear TI con el negocio mediante un enfoque global integral.



Jorge Uribe Maza, director comercial de Grupo IPS, todo un referente en el sector de la seguridad privada en el territorio mexicano con 30 años de historia.

en el periodo 2025-2030, en el que tomaron parte **Ricardo Escobedo**, Corporate Security Regional Manager en Delta Air Lines; **Martín Calvo**, Head of Corporate Security en Volkswagen de México; y **Fernando Martín Gómez Villarreal**, director de Seguridad Global en Gentera.

Expertos que compartieron su visión sobre las amenazas y tecnologías emergentes que redefinirán la gestión de seguridad en los próximos años, las habilidades que deberán atesorar los directivos de seguridad, la alineación de los programas de seguridad con las políticas ambientales, sociales y de gobierno corporativo (ESG, por sus siglas en inglés) y las normativas tanto locales como internacionales.

En definitiva, el II Congreso Mexicano de Directores de Seguridad se saldó con un gran éxito, pues sirvió "para construir, aprender juntos de los aciertos y errores, debatir los nuevos enfoques con respeto y apertura, y fortalecer las redes de confianza, porque la seguridad no se logra en soledad, sino a través de alianzas estratégicas", destacó **Javier Borredá García** ante una exclusiva y selecta audiencia.

Conclusiones

Finalizado el congreso y analizadas las ponencias de los expertos que participaron en él, el equipo de *Segurilatam* ha extraído las siguientes conclusiones:

- » **La seguridad como eje estratégico.** La seguridad se ha convertido en un componente central en la estrategia organizacional, enfrentando amenazas físicas, digitales, sociales y reputacionales.
- » **Geopolítica y el rol del director de Seguridad.** Se debatió cómo la geopolítica influye en la seguridad corporativa, destacando la necesidad de que los directores de Seguridad ac-

túen como actores geoestratégicos en un entorno global cambiante.

- » **Relación con la alta dirección.** Se abordó la importancia de una comunicación efectiva entre los departamentos de Seguridad y la alta dirección, promoviendo una cultura de prevención y responsabilidad compartida.
- » **Inversión en seguridad perimetral.** Se destacó la necesidad de inversiones inteligentes en seguridad perimetral para mitigar riesgos y proteger los activos empresariales, resaltando la importancia de soluciones tecnológicas avanzadas.
- » **Valor de los departamentos de Seguridad.** Se reconoció el papel fundamental de los departamentos de Seguridad como consultores y gerentes integrales del negocio, subrayando su contribución a la resiliencia organizacional y la gestión de crisis.
- » **Evolución hacia 2030.** El congreso concluyó con una visión prospectiva sobre la evolución de la seguridad corporativa entre 2025 y 2030, destacando la necesidad de adaptarse a amenazas emergentes y alinear los programas de seguridad con políticas ambientales, sociales y de gobernanza (ESG).
- » **Necesidad de creación de una carrera universitaria de Dirección de Seguridad.** Y en el último panel también se debatió sobre la necesidad de incorporar perfiles profesionales a los departamentos de Seguridad y lo positivo que resultaría contar con una titulación específica avalada por los reguladores para profesionalizar el gremio.

En resumen, el II Congreso Mexicano de Directores de Seguridad reafirmó la importancia de la seguridad como un componente esencial en la estrategia empresarial, promoviendo la colaboración interinstitucional y la adaptación a un entorno global dinámico. **S**



Marco Antonio Sanmiguel, Juan Antonio Bernal, Chesus Miguel Gay Grao y Ana Luisa Guzmán participaron en el panel sobre el valor del departamento de Seguridad.



José Arellano, Vertical Sales Manager de Genetec, compartió algunos datos del informe 'Estado de la Seguridad Electrónica 2025', un documento de imprescindible consulta.



Ricardo Escobedo, Martín Calvo, Fernando Martín Gómez Villarreal y Javier Borredá García pusieron el broche final al II Congreso Mexicano de Directores de Seguridad con un panel sobre la evolución de la seguridad corporativa en el periodo 2025-2030.

Galería de imágenes del II Congreso Mexicano de Directores de Seguridad



'Stand' de ALCEA / ASSA ABLOY.



Jaquelin Leon (CAME) y Gabriela Soto ('Segurilatam').



'Stand' de COMEXA.



'Stand' de DORLET.



'Stand' de Grupo IPS.



'Stand' de ManageEngine.



Representantes de Motorola Solutions y MRKTEC.



'Stand' de NOLETAL.



'Stand' de RODHE.



'Stand' de RS.



'Stand' de SCATI.



Buen ambiente y camaradería durante el evento.



Foto de familia del congreso.



El 'backstage' del 'catering' preparando tacos al pastor.

SICUR 2026 congregará al sector de la seguridad del 24 al 27 de febrero

El Salón Internacional de la Seguridad (SICUR) ha comenzado los preparativos para la celebración de su 25ª edición, que tendrá lugar del 24 al 27 de febrero de 2026. Organizada por Ifema Madrid, la feria busca consolidar su dimensión y representatividad y atraer al público joven, visibilizando oportunidades laborales y conectando talento emergente con el sector de la seguridad integral.

Tras SICUR 2024, que congregó a 46.000 profesionales de 80 países y 654 expositores, SICUR 2026 basará su oferta en las áreas de Seguridad Laboral, Seguridad Contra Incendios y Emergencias y Security, así como en una interesante agenda de jornadas que se desarrollará en los espacios Foro SICUR, SICUR Cyber y Exo Corner. Además, como ya es tradición en cada edición, se convocará SICUR Innovación con el objetivo de reconocer el esfuerzo en I+D de los expositores, visibilizando los productos y servicios más vanguardistas al servicio de la seguridad.

Presencia de Grupo Borrmart

Como es habitual, Grupo Borrmart tendrá una destacada presencia en el próximo SICUR. Así, contará con espacios expositivos en los que estarán representadas las publicaciones *Segurilatam*, *Seguritecnia*, *Red Seguridad* y *Formación de Seguridad Laboral*. Y como en ediciones anteriores, desempeñará un importante papel en SICUR Cyber, que contará con un completo programa de ponencias y mesas de debate donde voces autorizadas de empresas e instituciones abor-



Arriba: SICUR 2024 congregó a 46.000 profesionales y 654 expositores. Abajo: Uno de los 'stands' de Grupo Borrmart en el Salón Internacional de la Seguridad.

darán temas relacionados con la ciberseguridad desde la perspectiva técnica, legal y formativa.

El Comité Organizador de SICUR 2026 está conformado por representantes de la Asociación Española de Empresas de Seguridad (AES), Tecnifuego, la Asociación Profesional de Compañías Privadas

de Servicios Seguridad (APROSER) y la Asociación de Empresas de Equipos de Protección Personal (ASEPAL). Además, cuenta con la participación del resto de asociaciones representativas de la oferta y la demanda en seguridad, así como de organismos oficiales y Fuerzas y Cuerpos de Seguridad. **S**

**Patricia Acosta**

Directora de la Feria Internacional de Seguridad ESS+

“La feria ESS+ lo tiene todo: innovación, conexiones, actualización y capacitación”

■ Por Redacción

Del 27 al 29 de agosto, en el recinto ferial Corferias de Bogotá, se llevará a cabo la Feria Internacional de Seguridad ESS+ 2025, el evento de referencia en soluciones tecnológicas aplicadas a la seguridad para la región Andina, Centroamérica y el Caribe. Patricia Acosta, directora de ESS+, ha atendido a ‘Segurilatam’ para explicar qué innovaciones presentarán los expositores en la feria y qué foros académicos podrán disfrutar los visitantes.

En comparación con 2024, ¿cómo encaran esta edición? ¿Esperan registrar un número similar de expositores y visitantes en ESS+ 2025?

Esta edición la encaramos con una novedad destacada: hemos creado el Security Circle Lounge, un espacio reservado para los tomadores de decisiones que asistan a la feria con áreas destinadas a reuniones y un pequeño auditorio para tertulias. En cuanto a su segunda pregunta, esperamos un incremento en el número de visitantes, ya que hemos puesto en marcha una promoción muy dirigida a los diferentes sectores verticales del mercado usuario de tecnologías de seguridad.

¿Qué innovaciones serán protagonistas en ESS+ 2025?

ESS+ 2025 será una plataforma de lanzamiento para la innovación, el epicentro de nuevos desarrollos tecnológicos, inteligencia artificial (IA) aplicada, *edge computing* y soluciones de seguridad autónomas. Las empresas participantes presentarán sus productos más innovadores para la región en el esperado Pitch de Innovación.

Entre las novedades para sectores económicos destacamos, en primer lugar, el ámbito del transporte y la movilidad segura, donde veremos telemática avanzada para flotas, rastreo satelital y monitoreo en tiempo real, así como soluciones en videotelemática, IA, *big data* y control de combustible. Hay un interés creciente por parte de sectores como la logística, el transporte público y la seguridad vehicular.

En cuanto a los entornos educativos, se están desarrollando controles de acceso inteligentes con validación en tiempo real, videovigilancia con reconocimiento facial y análisis de comportamiento, además de plataformas de

gestión remota adaptadas a ambientes híbridos y medidas específicas de ciberseguridad educativa.

La seguridad hospitalaria es otro foco importante, con controles de acceso en zonas críticas, videovigilancia continua y protocolos de emergencia, así como un fortalecimiento de la ciberseguridad frente a amenazas digitales junto con la capacitación del personal para gestionar situaciones conflictivas.

En cuanto a la protección de infraestructuras críticas, destacan la vigilancia con drones, cámaras térmicas y sistemas biométricos, así como la ciberseguridad industrial aplicada a sistemas SCADA/OT. También se incorporan equipos diseñados para operar en entornos extremos como minas y plantas petroleras y energéticas.

Cada vez se habla más sobre la integración entre seguridad física y digital. ¿De qué manera ESS+ 2025 abordará esta convergencia? ¿Tendrán un protagonismo especial temas como la ciberseguridad o la IA?

La IA estará claramente al servicio de la seguridad, con detección en tiempo real, análisis predictivo y automatización sin intervención humana. Además, se integrará con ciudades inteligentes, hogares conectados y corporaciones. Las redes de videovigilancia inteligente interconectadas permitirán gestionar de forma eficiente infraestructuras urbanas, la movilidad y los espacios públicos.

La sostenibilidad está cada vez más presente en todos los ámbitos, incluida la seguridad y la organización de eventos.

Así es. Corferias, el recinto más importante de Colombia y sede de ESS+, fue recientemente certificado como Carbono Neutro. Lidera campañas de sostenibilidad y está comprometido con la me-

jora continua del Sistema de Gestión de Sostenibilidad, promoviendo el cuidado del medio ambiente. Las distintas ferias que se realizan allí, incluida ESS+, están alineadas con los Objetivos de Desarrollo Sostenible (ODS), destacando especialmente los ODS 9 (Industria, Innovación e Infraestructura) y 11 (Ciudades y Comunidades Sostenibles).

¿Qué actividades formativas y de divulgación tienen previstas para esta edición? ¿Hay algún contenido o ponente que le gustaría destacar?

Para esta edición contamos con varios foros gremiales. Entre ellos, ALAS TLKS X – Voces que inspiran, historias que transforman y los Premios ALAS, que recono-

¿Qué papel juega la feria ESS+ en la generación de alianzas y oportunidades de negocio a nivel regional e internacional?

Gracias a la rueda de negocios, logramos concertar alrededor de 200 reuniones, previamente acordadas, entre la oferta y la demanda tanto a nivel nacional como internacional. La feria ESS+ actúa como un verdadero punto de encuentro para la generación de alianzas estratégicas.

Desde su posición como directora de ESS+, ¿cómo ve la evolución del sector de la seguridad en América Latina? ¿Qué desafíos y oportunidades identifica a corto y medio plazo?

“El nuevo Security Circle Lounge es un espacio reservado a tomadores de decisiones que asistan a la feria con áreas destinadas a reuniones y un pequeño auditorio para tertulias”

cen los mejores proyectos de seguridad en Latinoamérica. También tendremos el foro Looking into the Future, organizado por la Asociación Latinoamericana de Seguridad (ALAS).

Además, se celebrará el Congreso de Gestión de Riesgos organizado por COLADCA bajo el lema *Una mirada crítica a los grandes desafíos del entorno*, el simposio Seguridad humana y protección de activos de ASIS y la Universidad Militar Nueva Granada y el congreso CIPROCI sobre protección contra incendios, normativas NFPA y diseño seguro. Igualmente, habrá un espacio especial para los reconocimientos de la revista *El Mundo Cambió* y el Foro de Ciudades Seguras de la Asociación de Ciudades Intermedias.

Las oportunidades están, sin duda, en el crecimiento de las *smart cities*, la modernización de los hogares, la creciente conciencia sobre la necesidad de proteger infraestructuras críticas, la mejora de las condiciones de los trabajadores y la preparación ante desastres naturales. Todos estos son campos de acción clave para el sector de la seguridad, sin dejar de lado la implementación de soluciones integrales en todos los ámbitos de los países.

¿Qué les diría a quienes aún no han decidido si acudirán a la feria como expositores o visitantes? ¿Por qué deberían estar presentes en ESS+?

ESS+ lo tiene todo: innovación, conexiones, actualización y capacitación. **S**

PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

El Mundial de Fútbol 2026, protagonista del VII Congreso Mexicano PIC

La séptima edición del Congreso Mexicano de Protección de Infraestructuras Críticas (PIC) de 'Segurilatam' se celebrará en la Ciudad de México en noviembre. En esta ocasión, el evento estará centrado en la seguridad de los servicios esenciales destinados a sustentar el normal desarrollo del Mundial de Fútbol 2026 que tendrá lugar en las sedes mexicanas.

■ Por Redacción.

En el mes de noviembre, *Segurilatam* llevará a cabo el VII Congreso Mexicano de Protección de Infraestructuras Críticas (PIC). Como en ediciones anteriores, este evento de referencia en América Latina volverá a reunir a expertos del sector público y privado en la Ciudad de México con el objetivo de debatir, compartir experiencias y proponer soluciones sobre la seguridad de los servicios esenciales que sustentan el funcionamiento de la sociedad mexicana.

Mundial de Fútbol 2026

Concretamente, el VII Congreso Mexicano PIC pondrá el foco en un acontecimiento internacional que atraerá la atención de millones de personas: el Mundial de Fútbol de 2026. Junto a Estados Unidos y Canadá, México será uno de los países anfitriones de la competición de selecciones nacionales y acogerá partidos en varias sedes. Por ello, el foro organizado por *Segurilatam* analizará cómo reforzar la seguridad de las infraestructuras críticas para garantizar el normal desarrollo de la Copa Mundial de la FIFA 2026 en suelo mexicano.

En este sentido, la celebración de un evento deportivo de esta magnitud requie-



rirá una estrategia de seguridad física y cibernética robusta. Y, además, avalar la prestación de servicios esenciales como el transporte, el suministro eléctrico, el abastecimiento de agua, las telecomunicaciones, la atención sanitaria...

Medidas y planes

Por ello, en el VII Congreso Mexicano PIC se abordará la necesidad de implementar medidas preventivas y planes de contingencia en sectores clave cuya operatividad resultará imprescindible para que el Mundial 2026 se desarrolle con normalidad y sin interrupciones:

- **Transporte y movilidad urbana.** Será crucial reforzar la seguridad en aeropuertos, estaciones de ferrocarril y metro, redes de autobuses y vías de comunicación con las sedes para asegurar la movilidad, así como la capacidad de respuesta ante posibles incidentes.
- **Suministro eléctrico y de agua potable.** La estabilidad energética y el abastecimiento hídrico serán fundamentales para el funcionamiento de los estadios, las instalaciones logísticas, los hoteles, los centros de prensa y otras infraestructuras asociadas al evento.

- » **Telecomunicaciones.** En el VII Congreso Mexicano PIC se destacará la importancia de contar con redes de comunicación seguras y resilientes para soportar la demanda de los medios de comunicación, los aficionados y los organismos oficiales durante el torneo.
- » **Distribución de alimentos y cadenas de suministro.** Asimismo, se pondrá de relieve la necesidad de proteger los centros logísticos y de distribución que garanticen el abastecimiento de productos de primera necesidad en las ciudades sede.
- » **Sistema financiero.** Ya sea a través de efectivo u otros métodos, durante el Mundial 2026 se realizarán millones de pagos y transacciones en México. De ahí que sea primordial que el sistema financiero funcione a pleno rendimiento y con seguridad.
- » **Sanidad y servicios de emergencia.** Otro eje prioritario será el fortalecimiento del sistema de salud y los ser-

vicios de emergencia para responder con eficacia y prontitud en caso necesario.

- » **Administración y seguridad pública.** Y, finalmente, los servicios esenciales vin-

que reunirá a representantes de instituciones gubernamentales, operadores de infraestructuras críticas, expertos en seguridad integral y proveedores de servicios para usuarios del ámbito PIC,

Los expertos que participarán en el VII Congreso Mexicano PIC compartirán conocimientos y buenas prácticas en la antesala del Mundial

culados a las administraciones de los tres órdenes de gobierno (federal, estatal y municipal), como los policiales, deberán estar a la altura de las circunstancias para robustecer los servicios básicos y velar por el orden público.

Foro estratégico

Sin duda, el VII Congreso Mexicano PIC será un espacio de análisis estratégico

quienes compartirán conocimientos y buenas prácticas en la antesala del Mundial de Fútbol 2026.

Próximamente, *Segurilatam* ofrecerá información relativa a la agenda del congreso y abrirá la solicitud de inscripciones para asistir presencialmente. Como en anteriores ediciones, será un evento exclusivo de aforo limitado al que se accederá por invitación personal. **S**

» Mundial de Fútbol 2026: claves del torneo en México

El próximo Mundial de Fútbol se celebrará del 11 de junio al 19 de julio de 2026 con un total de 48 selecciones nacionales. El partido inaugural se disputará el jueves 11 de junio de 2026 en el Estadio Azteca de la Ciudad de México, uno de los recintos más emblemáticos del mundo y único estadio que habrá albergado tres Copas Mundiales (1970, 1986 y 2026). Por su parte, la gran final tendrá lugar el domingo 19 de julio de 2026 en el MetLife Stadium de East Rutherford (Nueva Jersey, Estados Unidos), con capacidad para más de 80.000 espectadores.

Esta es la primera vez que una Copa Mundial de la FIFA se celebra en tres países; concretamente, en Estados Unidos, Canadá y México. En el caso de este último, contará con tres ciudades sede que albergarán partidos. Los estadios seleccionados y sus respectivas ubicaciones son: el emblemático Estadio Azteca (83.000 espectadores), en la Ciudad de México; el Estadio Akron (48.000 espectadores) en Zapopan, Jalisco; y el Estadio BBVA (53.500 espectadores), en Guadalupe, Nuevo León. El Gobierno de México espera recibir más de 5,5 millones de visitantes adicionales durante el Mundial de Fútbol 2026, lo que podría generar ingresos por más de 3.170 millones de dólares (unos 60.000 millones de pesos). Para ello, las sedes están trabajando en incrementar su oferta hotelera.



ALARMAS



Av las Condes n1 7219. Santiago de Chile
Tel.: +56 600 5000 133
Web: www.verisure.cl

ASOCIACIONES



Asociación Mexicana de Empresas de Seguridad Privada

Montecito n° 38 Piso 18 oficina 18
Colonia Nápoles. Benito Juárez 03810 (México D.F.)
Tel.: +52 55 1054 6180
Web: www.amesp.mx
E-mail: contacto@amesp.mx



COLADCA

Tel.: +57 311 5339969
Web: www.coladca.com
App: <http://wix.to/8EBEAXU>
Email: coladca@gmail.com
Redes Sociales: @COLADCA



Av. P.º de la Reforma 404, piso 1, Juárez, Cuauhtémoc, 06600 Ciudad de México.
Tel. +52 1 55 1321 1289
Web: <https://asis.org.mx/>
E-mail: socios@asis.org.mx



Consejo Nacional de la Industria de la Balística

Sófocles N°150 Int.001 Polanco III Sección,
Alcaldía Miguel Hidalgo
11540 Ciudad de México
Tel.: +525547446224
Web: www.consejonacionaldelaindustria-delabalistica.com
E-mail: gerencia@consejonacionaldelaindustriadelabalistica.com
contacto@consejonacionaldelaindustriadelabalistica.com

CCTV



Lago Zurich n° 219. Plaza carso II oficina 1502. Col. Ampliación Granada Miguel Hidalgo. 11529 Ciudad de México
Tel.: +52 55 6723 1936
Web: www.dahuasecurity.com
E-mail: sales@dahuattech.com



Avenida del Ejército Nacional 505 Chapultepec Morales, Granada Miguel Hidalgo 11520. Ciudad de México, CDMX
Tel.: +52 55 2875 1417
E-mail: mexico@lanaccess.com



Lago Zurich n° 219. Plaza carso II, Torre II. Col. Ampliación Granada. Miguel Hidalgo. 11529 Ciudad de México
Tel.: +52 55 2624 3613
Web: www.hikvision.com
E-mail: sales.mexico@hikvision.com



Paseo de los Laureles 458-203, Bosque de las Lomas
05120 Ciudad de México
Te.: +52 55 5259 9511
Web: www.marchnetworks.com

CIBERSEGURIDAD



Mercaderes 20, oficina 502 Colonia San José Insurgentes. 03900 Ciudad de México
Tel.: +52 55 6394 3390
Web: www.latam.kaspersky.com
E-mail: info@kaspersky.com



Paseo de los Tamarindos 90. Bosque de las lomas
05120 Ciudad de México
Tel.: +1 877 425 2624
Web: www.akamai.com



Calle 113 # 7-45, Oficina 1210 Teleport Business Park-Torre B Bogotá D.C., 110111
Oficina: +57 1 705 3570
Móvil: +57 300 339 6273

CONTROL DE ACCESO



Calle 86ª Bis n° 1522 piso 5, Bogotá
Tel.: +57 1 432 2970
Web: www.alceaglobal.com/es



5863 NW 159th Street
Miami Lakes, Florida 33014
Tel.: +1 305 433 3307
Web: www.came.com
E-mail: marketingamericas@came.com



Insurgentes Sur 553, Código 2, Escandon I Secc
11800 Ciudad de México
Tel.: +52 55 5292 8418
Web: www.zktecolatinoamerica.com
E-mail: gm.latam@zkteco.com

COMUNICACIONES



Cra #115-06 Edificio Tierra Firme,
of 1003. Bogotá
Web: www.hytera.la
E-mail: meradeo@hytera.la

GUARDIAS INTRAMUROS



Calzada Parque Orizaba 15. Despacho 6,
Lomas del parque Naucalpan de Juarez
55390 Ciudad de México
Tel.: +52 55 5527 2199
Web: www.almaba.com.mx
E-mail: comercializacion@almaba.com.mx



Calle Liverpool n° 96. Colonia Juárez
06600 Ciudad de México
Tel.: +52 55 5591 0409
Web: www.gcseguridadintegral.com
E-mail: ventas@seguridadgc.com



Calle Lucerna 10, Juárez
06600 Ciudad de México
Tel.: +52 55 5525 3242
Web: www.grupoipsmexico.com
E-mail: contacto@grupoipsmexico.com



Juan Del Mar y Bermedo 1040
Cercado de Lima, 15083
Tel.: +51 1 204 5200
Web: www.liderman.com.pe



Transversal 23, n° 95-53
Bogotá
Tel.: +57 1 344 4420
Web: www.prosegur.com.co



Calzada del hueso 955. Coapa,
Granjas de coapa
14330, Ciudad de México
Tel.: +5255 5483 4400
Web: www.serviseg.com.mx
E-mail: atencionacienes@serviseg.com.mx



Calle 25b #31ª-31, Bogotá
Tel.: +57 1 269 7473
Web: www.servisiondecolombia.com
E-mail: comercial@servisiondecolombia.com

INGENIERÍA DE SEGURIDAD



Avenida Ejercito Nacional 530. Polanco
11550 Ciudad de México
Tel.: +52 55 7826 8755
Web: www.desico.com
E-mail: comercial@desico.com

INTEGRADORES



Calle 65 #1350, Bogotá
Tel.: +57 1 743 1101
Web: www.abetelnet.com



Calle Zaragoza 73
Tels.: 55 1539 9215 - 55 4555 7484 WhatsApp
Web: www.comexa.com.mx
E-mail: livia.prado@comexa.com.mx

DISTRIBUIDORES



Calle 26 n° 85-55. Oficina 302. Bogotá
Tel.: +57 320 275 8076
Web: www.casmarcolombia.co
E-mail: info@casmarcolombia.co



Cra 29 #77 33, Bogotá
Tel.: +57 1 630 2958
Web: www.eleseg.com
E-mail: eleseg@eleseg.com



Iztacihuatl n° 158
Col. Florida. Del. Álvaro Obregón
C.P.: 01030 CDMX
Tel.: +52 55 6308-4067
Web: www.rodhe.com.mx
E mail: info@rodhe.com.mx

PROTECCIÓN CONTRA INCENDIOS



Via Porton n°5
37010 Verona- Italia
Tel.: +57 311 281 0400
Web: www.cristanini.com
E-mail: cristanini@cristanini.it

PROTECCIÓN INFRAESTRUCTURAS ESTRATÉGICAS



Paseo de la Reforma 115, piso 4.
Lomas de Chapultepec
11000 Ciudad de México
Tel.: +52 55 5630 0393
Web: www.eximco.cc
E-mail: contacto@eximco.cc

PROVEEDORES DE ERP PARA VIGILANCIA



PBX +(57) 1 749 56 77
Celular: +(57) 311 267 52 24
Whatsapp: +(57) 318 306 62 33
info@avancys.com.co
www.avancys.com

Datos internos
Contacto: Manuel García
Email: mgarcia@avancys.com.co
Teléfono: 318 3504491
www.avancys.com

PROTECCIÓN EJECUTIVA



Av Presidente Juárez 2016, Los reyes.
54073 Tlalnepantla de Baz,
Ciudad de México
Tel.: +52 55 5374 1665
Web: www.bromyasociados.com.mx
E-mail: contacto@bromyasociados.com.mx

SEGURIDAD DE LA INFORMACIÓN



Av Paseo de la Reforma 300, Cuauhtémoc
06600 Ciudad de México
Tel.: +52 55 4000 5607
Web: www.corpurios.com
E-mail: contacto@corpurios.com

TRANSPORTES BLINDADOS



Francisco I. Madero n° 234 pte. Fracc,
Industrial el lechugal
Santa Catarina, nuevo León.
Tel.: +52 81 8124 6666
Web: www.tps.com.mx
E-mail: ventasmt@tps.com.mx



PROTECCIÓN DE
INFRAESTRUCTURA CRÍTICA

DISEÑO - CONSULTORÍA - SUMINISTRO - INSTALACIÓN - CONSERVACIÓN



UNA NUEVA CULTURA EN PROTECCIÓN PERIMETRAL

🌐 www.eximco.cc

☎ + 52 (55) 4631 2247

✉ contacto@eximco.cc



◆ Experiencia ◆ Tecnología ◆ Seguridad



**AÑOS
DESDE 1995**



Grupo IPS, ***líderes*** en seguridad privada.

grupoipsmexico.com

