

Chile tiene Ley de Seguridad Privada



Dotar a Chile de un sistema moderno y profesional de seguridad privada es el principal objetivo de la Ley N° 21.659, la cual entró en vigor este 28 de noviembre y en la que la Subsecretaría de Prevención del Delito (SPD) cumple un rol fundamental como ente regulador y fiscalizador.

La nueva Ley de Seguridad Privada reemplaza y actualiza una serie de normas que hasta ahora se encontraban dispersas en diferentes leyes y decretos, lo que permite generar un sistema unificado y más claro para regular a las empresas privadas, que serán clasificadas en distintos niveles de riesgo, dependiendo de los cuales deberán cumplir con exigencias más estrictas de seguridad privada; entre ellas, personal especializado y medidas adicionales de protección.

También se establecen requisitos específicos para las personas naturales que desempeñen funciones de seguridad privada, quienes deberán acreditarse ante la SPD y no ante Carabineros como sucedía hasta la fecha.

Entre las funciones que otorga la ley a la SPD está la de autorizar a las empresas de seguridad privada y las personas naturales que desarrollen labores en este ámbito; determinar las entidades a las que se exigirá contar con medidas de seguridad; aprobar estudios y planes de seguridad; sancionar infracciones; y administrar el Registro de Seguridad Privada.

Desde la entrada en vigencia de la normativa, las entidades obligadas por la ley tendrán un plazo de adecuación de seis meses para presentar su primer estudio de seguridad. Asimismo, se establece el plazo de un año para la creación del Registro de Seguridad Privada con todos sus subregistros y plataforma informática operativa, y de dos años para evaluar a las entidades obligadas actualmente, y según su riesgo, determinar las medidas de seguridad que les serán exigidas. Fuente: SPD

EDITORIAL

IMPLEMENTACIÓN DE LA LEY DE SEGURIDAD PRIVADA 21.659 OPORTUNIDADES Y DESAFÍOS

Como toda creación humana, la Ley de Seguridad Privada, sin duda, es perfectible. No obstante, cuando ya concluye el año 2025, como Asociación Chilena de Empresas de seguridad electrónica y sistemas integrales de monitoreo de alarmas, tenemos la convicción de que los procesos desarrollados, con visiones coincidentes y también diferencias propias de los distintos roles y funciones de los actores relevantes, canalizadas formalmente a través de coordinaciones público- privadas por la División de Seguridad Privada de la SPD, son la forma y estrategia adecuadas para avanzar en un cambio de paradigma de una industria tan importante que, desde su quehacer, aporta significativamente a la seguridad y bienestar de la sociedad.

Como ACHEA A.G., hemos asumido durante el diseño de la ley, su discusión e implementación, una mirada y actitud siempre positiva y propositiva; creemos que así se fortalecen las oportunidades, en los desafíos y también en las dificultades que implica este nuevo marco regulatorio, cuyo propósito -entre otros- es la modernización, profesionalización de la industria, su rol colaborativo, coadyuvante y complementario de la seguridad pública, estableciendo nuevos criterios y estándares en la institucionalidad y gobernanza del macrosistema de seguridad.

Al finalizar el 2025 y las etapas de este proceso que recién comienza, nuestro **reconocimiento y valoración a las empresas asociadas a ACHEA A.G.** que, con su motivación, esfuerzo, compromiso y permanentes iniciativas e innovación, aportan a la profesionalización de la industria, permitiendo desde su rol y funciones lo más importante: **"más y mejor seguridad para la sociedad"**.

Tal como señaló Aristóteles:

"Somos lo que hacemos día a día. La excelencia no es un acto, sino un hábito".



Empresas asociadas a ACHEA se capacitan ante entrada en vigor de la Ley de Seguridad Privada

Con el propósito de fortalecer las capacidades estratégicas y competencias técnicas de los profesionales del sector, y ante la entrada en vigor de la Ley N°21.659 de Seguridad Privada, ACHEA organizó una Jornada de Capacitación y Conversatorio para nuestras empresas asociadas, sobre los alcances de la normativa, sus implicancias disciplinarias y los desafíos y oportunidades que plantea para la industria.

En la instancia, que se desarrolló en el auditorio de Universidad Finis Terrae, se abordaron, entre otros temas: el impacto directo de la ley en la operación diaria, nuevos estándares y exigencias y el rol estratégico de la seguridad privada en la Política Nacional de Seguridad Pública.

El evento contó con un panel de expertos compuesto por autoridades de la Subsecretaría de Prevención del Delito y

Carabineros de Chile, especialistas del área del Derecho, docentes de la UFT, representantes de ASEVA (Asociación de Empresas de Seguridad Privada y Transporte de Valores) y líderes de ACHEA A.G.

“Se trata de una legislación largamente esperada, que consolida un marco regulatorio único, específico y moderno, al que contribuimos como Asociación en cada instancia y oportunidad que tuvimos durante su tramitación. Un logro del cual nos sentimos legítimamente orgullosos es la incorporación y regulación expresa de la ‘Seguridad Electrónica’, así como de la consagración de nuestro rol preventivo, coadyuvante y complementario de la seguridad pública”, señaló Víctor Herrera Pintor, expositor y Presidente de ACHEA A.G. (Fotos: Max Montecinos).

Lanzan primera experiencia municipal de SITIA Patentes

El Gobierno lanzó el piloto del Sistema Integrado de Teleprotección con Inteligencia Artificial (SITIA) - Patentes en Lo Barnechea, como parte de su agenda de innovación en seguridad. Esta herramienta permite detectar y seguir vehículos con encargo por robo mediante cámaras lectoras de patentes conectadas a la base de datos de Carabineros. Con 115 cámaras activas, Lo Barnechea es la primera comuna en usar este sistema, fortaleciendo la prevención y fiscalización. De hecho, durante su marcha blanca se incautaron cuatro vehículos robados.

SITIA promueve la interoperabilidad entre municipios, privados y Carabineros, y se complementa con la Unificación de Videos, que integra más de 2.000 cámaras en la Región Metropolitana. Además, se han firmado convenios con municipios y gobiernos regionales para consolidar una red nacional de seguridad basada en datos y tecnología.

Fuente: SPD

Experto en ciencia de datos UDD advierte sobre trabas en implementación de la Ley de Seguridad Privada

Germán Gómez, investigador del Instituto de Data Science de la Universidad del Desarrollo, asegura que Chile aún no cuenta con la infraestructura digital necesaria para gestionar el material recogido por las cámaras corporales de los guardias que se desempeñan en labores de riesgo, una de las exigencias de la nueva Ley de Seguridad Privada.

El especialista advierte que, si bien “Chile ha avanzado en digitalización, fiscalizar un sistema de esta magnitud es un desafío de otra escala. Mi lectura es que el Estado tiene la arquitectura institucional —las leyes, los reglamentos, los roles definidos—, pero la capacidad operativa tecnológica está por construirse”.

Puntualmente, identifica trabas en tres aristas: capacidad estructural para almacenar y gestionar el material en video; fiscalización y protección de datos. Sobre la primera, Gómez explica que una cámara corporal en alta definición genera entre dos y cuatro gigabytes por jornada de trabajo de 8 horas, por lo que al conservar por 120 días el material de entre 50 y 100 mil guardias privados, “lo que se almacenará equivale a la biblioteca completa de Netflix varias veces”.

Está también el costo asociado. “No todas las empresas del mercado chileno tienen capacidad de inversión en infraestructura tecnológica, y el reglamento exige cifrado de extremo a extremo, registros de auditoría completos, y que la grabación no pueda ser manipulada. Eso no se logra con un pendrive y buena voluntad; estamos hablando de inversiones significativas en hardware, software y capacitación”, puntualiza. Fuente: Portal Innova.

Gobierno presenta nueva campaña para reporte anónimo de delitos

Bajo el lema “Denuncia Seguro, tu llamado es clave”, el Ministerio de Seguridad Pública presentó la nueva campaña preventiva del Programa Denuncia Seguro, herramienta gratuita y confidencial que permite el reporte anónimo de delitos para el inicio de investigaciones policiales a través del número *4242 y el sitio www.denunciaseguro.cl

La campaña se estructura en base a cuatro ejes temáticos, que buscan abordar delitos como el tráfico de drogas próximo a establecimientos educacionales, a fin de proteger a niños, niñas y adolescentes; la tenencia ilegal de armas de fuego, las cuales generan inseguridad y amenazas al interior de los barrios; la violencia intrafamiliar, permitiendo en desarrollo de operativos policiales en flagrancia; y el maltrato animal, para visibilizar situaciones de crueldad y negligencia hacia los animales. Fuente: SPD



Boletín Informativo ACHEA

Inseguridad, las cifras del principal desafío que deberá enfrentar el Gobierno de José Antonio Kast

La inseguridad se ha consolidado como el principal desafío para el futuro gobierno de José Antonio Kast, en un contexto donde el miedo al delito en Chile figura entre los más altos del mundo.

Pese a que los índices de criminalidad son comparativamente más bajos que en otros países de la región, la ciudadanía prioriza la delincuencia como su mayor preocupación, reflejando un clima de alta tensión social.

Según datos de la Enusc 2024, se registró un incremento en diversos delitos: los robos subieron al 17,7% (frente al 16,7% en 2023), los delitos económicos alcanzaron el 11% y los hurtos en hogares llegaron al 7%. Además, los robos no violentos se situaron en un 14,3% y los intentos de robo en un 10,6%.

En contraste, las cifras de homicidios muestran una mejora relativa. La Fiscalía Nacional reportó una baja del 4% en la tasa de homicidios durante el primer semestre de 2025, alcanzando 6 víctimas por cada 100.000 habitantes. Por su parte, la Subsecretaría de Prevención del Delito registró 511 víctimas en el mismo periodo, con una tasa de 2,5 por cada 100.000 habitantes, lo que representa una disminución del 13,8% respecto al año anterior.

Sin embargo, la percepción de inseguridad sigue siendo extremadamente alta: el 87,7% de la población percibe un aumento de la delincuencia a nivel nacional. Un 63% de los chilenos considera el crimen como el principal problema del país, una cifra superior a la de México (59%) y Colombia (45%). Finalmente, el reporte de Gallup indica que solo el 39% de los consultados se siente seguro caminando solo por la noche, situando a Chile entre los seis países con mayor sensación de inseguridad en el mundo.

Esta brecha entre cifras y percepción se atribuye a la irrupción del crimen organizado y bandas como el Tren de Aragua, que han introducido delitos alarmantes como el sicariato, secuestros y trata de personas. Ante esto, expertos sugieren que el gobierno debe implementar medidas para controlar la delincuencia dura y reducir la inseguridad subjetiva mediante mayor presencia policial y el ordenamiento de la convivencia cotidiana. Fuente: Emol



Principales preocupaciones en América Latina y el Caribe



Según la Encuesta de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre confianza pública 2023-2025, la inseguridad y la violencia son las mayores preocupaciones en América Latina y el Caribe.

De acuerdo al estudio, el avance del crimen organizado y el deterioro institucional han provocado que el 60% de los ciudadanos considere la delincuencia como el principal problema de sus países.

También se destaca una crisis de credibilidad gubernamental, con solo 48% de confianza promedio. En contraste, las fuerzas armadas son la institución mejor valorada con un 55%. Además, la situación económica agrava el malestar social, pues 82% de los encuestados expresa preocupación por sus finanzas personales. Fuente: Segurilatam

Las tres zonas más inseguras de Santiago según la IA

Una inteligencia artificial analizó patrones urbanos y datos delictuales para identificar las zonas más peligrosas de Santiago. El resultado reveló tres sectores críticos:

Avenida Santa Rosa, entre La Pintana y San Ramón. Alta presencia de robos, tráfico de drogas y baja vigilancia policial.

Área norte de Renca: falta de iluminación y alta frecuencia de asaltos y portonazos.

Entorno del terminal de buses en Estación Central. Zona de alto tránsito, con hurtos frecuentes a turistas y comercio informal..

Fuente: Radio Agricultura.



Colombia: “Los drones sólo podrán emplearse para vigilancia”, nueva regla del Gobierno para seguridad privada.



El Gobierno de Colombia, a través de la Superintendencia de Vigilancia y Seguridad Privada y la Aeronáutica Civil, ha establecido un marco obligatorio para el uso de drones en la seguridad privada. Según la nueva normativa, estas aeronaves solo podrán emplearse para vigilancia y captura de imágenes o datos. Se prohíbe explícitamente el transporte de armas, materiales peligrosos o

cualquier actividad ajena al objeto de vigilancia.

Para operar, las empresas deben contar con licencia vigente y certificarse como explotadores ante la Aerocivil, cumpliendo estándares técnicos y perfiles específicos para los pilotos. Además, cada equipo debe ser registrado individualmente y reportado formalmente ante la Superintendencia. Los pilotos deben tener formación certificada y respetar estrictamente los parámetros de seguridad aérea, como límites de altura y zonas permitidas.

Para la implementación de estas medidas, se ha definido un periodo de transición con el propósito de que las compañías obtengan sus acreditaciones, manteniendo una supervisión permanente para asegurar que la tecnología se use bajo criterios de responsabilidad y legalidad.

Fuente: Infobae

México y EE. UU. refuerzan cooperación en seguridad ante ataques con drones y crimen organizado

Los gobiernos de México y Estados Unidos acordaron estrechar su colaboración en seguridad para enfrentar los ataques con drones perpetrados por cárteles en la frontera común. En la sesión del Grupo de Implementación de Seguridad (SIG) realizada en la Ciudad de México, ambas naciones pactaron conectar sus plataformas de análisis y mejorar el intercambio de inteligencia para prevenir estas amenazas aéreas de manera más eficaz.

La prioridad central del acuerdo es erradicar el tráfico de fentanilo. Mientras la administración de Donald Trump declaró recientemente esta droga como un “arma de destrucción masiva” e intensificó su campaña con bombardeos a embarcaciones en el Caribe y el Pacífico, la presidenta Claudia Sheinbaum señaló que analizará las implicaciones de dicha orden ejecutiva.



El plan también contempla agilizar las extradiciones, investigar el robo de combustible y dismantelar los flujos financieros de las organizaciones criminales. Ambas delegaciones se comprometieron a acelerar los esfuerzos contra amenazas emergentes antes de su próxima reunión programada para enero de 2026, con el fin de garantizar la seguridad ciudadana en ambos lados de la frontera. Fuente: ElExpres.com



Buenos Aires realizó 1er Encuentro Internacional de Reguladores de Seguridad Privada

El Ministerio de Seguridad de la Ciudad de Buenos Aires realizó el Primer Encuentro Internacional de Reguladores de Seguridad Privada, que contó con la participación de cerca de 300 funcionarios gubernamentales y empresarios de España y países de América del Sur, Central y el Caribe (México, Chile, Colombia, Paraguay, Brasil, Uruguay, Ecuador, Costa Rica, República Dominicana, Honduras y Panamá).

Los principales temas que se abordaron fueron el fortalecimiento del sector, la regulación y fiscalización de la seguridad privada, la innovación tecnológica, la profesionalización del servicio y la búsqueda de una convergencia normativa en los planos regional e internacional.

El ministro de Seguridad porteño, Horacio Giménez, resaltó que “la seguridad privada es un componente esencial en el Sistema Integral de Seguridad Pública, destacándose por la contribución, prevención y la protección de activos estratégicos y la promoción de empleo calificado”. Fuente: Gobierno de Buenos Aires.

España: Vigilantes no quieren trabajar en comercios por agresiones en los hurtos

El sector del retail en España atraviesa una crisis de seguridad crítica. Según el Barómetro del Hurto 2025, el 65% de las empresas de distribución no logra cubrir sus vacantes de vigilancia privada. El principal motivo de este déficit es el drástico aumento de la hostilidad: el 74% de los comercios reporta una escalada de agresiones físicas y verbales por parte de los infractores hacia el personal de las tiendas.

Alberto García, portavoz del sindicato profesional, señala que el sector padece una falta de relevo generacional preocupante, con una plantilla cuya edad media ya alcanza los 48 años y no atrae a la gente joven. Menos aún con el riesgo constante en barrios conflictivos, donde los guardias sufren insultos, escupitajos y vejaciones.

El impacto económico de esta inseguridad es significativo, con pérdidas anuales por hurtos que ascienden a 2.817 millones de euros. Las bandas organizadas son responsables del 35% de estos delitos. Además, en Barcelona el 91% de los hurtos y el 83,5% de los robos violentos son cometidos por extranjeros. Fuente: theobjective.com



Boletín Informativo ACHEA

Desafíos y limitaciones de los sistemas de detección de amenazas mediante IA

A pesar de sus beneficios y capacidades, la detección de amenazas impulsada por inteligencia artificial enfrenta varios desafíos que los líderes empresariales y tecnológicos deben considerar detenidamente antes de su implementación, especialmente en áreas críticas como la ciberseguridad.

Para fines editoriales, la siguiente infografía fue diseñada con ayuda de la Inteligencia Artificial.

Los 5 Grandes Retos de la Inteligencia Artificial

La inteligencia artificial presenta desafíos significativos que deben ser gestionados cuidadosamente. Estos abarcan desde la protección de datos y el uso ético hasta problemas inherentes al sistema como el sesgo, la falta de transparencia y el riesgo de su uso para ciberataques.

RETOS DE DATOS Y ÉTICA

PRIVACIDAD DE LOS DATOS

La IA analiza enormes cantidades de datos sensibles que requieren estrictas políticas de protección.

SESGO EN LOS ALGORITMOS

Los datos de entrenamiento sesgados pueden conducir a decisiones inexactas, injustas o discriminatorias.

USO ÉTICO

Los datos de la IA deben ser manejados únicamente por personal autorizado para fines legítimos.

RETOS DE INTEGRIDAD Y SEGURIDAD DEL SISTEMA

FALTA DE EXPLICABILIDAD

La dificultad para entender cómo un sistema de IA toma decisiones deteriora la confianza.

IA COMO HERRAMIENTA DE ATAQUE

Actores maliciosos pueden usar la IA para identificar y explotar vulnerabilidades de seguridad.





Boletín Informativo ACHEA

Expertos en ciberseguridad lograron bloquear más de 5 mil ataques bancarios en Chile y observaron aumento de amenazas a smartphones



Según un reciente informe realizado por los expertos en ciberseguridad de Kaspersky, a nivel global se han registrado 1,8 millones de ataques de troyanos bancarios (archivo, programa o fragmento de código que parece ser legítimo y seguro, pero en realidad es malicioso) que fueron bloqueados entre agosto de 2024 y junio de 2025, con un promedio de unos 5.000 por día. A pesar de la caída de casi la mitad (45,5%) respecto al año anterior (3,3 millones), advierten, el peligro no ha disminuido, sino que solo se ha transformado.

Para el caso de Chile se registraron más de 5 mil bloqueos. Y el informe señala un importante cambio en el enfoque de los ciberdelincuentes: los ataques están migrando de las computadoras a los dispositivos móviles, siguiendo el aumento del uso de los smartphones en transacciones financieras.

Hasta noviembre de este año, se identificaron tres familias activas de troyanos bancarios para Android, frente a solo una en 2024; un reflejo de la adaptación y sofisticación del cibercrimen financiero.

“Los ciberdelincuentes han desarrollado y perfeccionado técnicas avanzadas, como los ataques de Sistema de Transferencia Automatizada (ATS), que automatizan el robo de fondos directamente desde el dispositivo de la víctima, y el uso de Herramientas de Administración Remota (RAT), que garantizan acceso y control total del aparato, permitiendo manipular aplicaciones bancarias sin que el usuario lo note”, destaca Fabio Assolini, experto en ciberseguridad. Fuente: Trendic.cl

7 amenazas de ciberseguridad que enfrentarán las empresas en Latinoamérica en 2026

La firma global de ciberseguridad Kaspersky compartió recientemente su pronóstico de amenazas que enfrentarán las empresas en Chile y Latinoamérica en 2026.



1. **Troyanos bancarios “adaptados” o reescritos para su distribución a través de WhatsApp**, que permiten espiar a la víctima, enviar mensajes y finalmente, apoderarse de la cuenta.
2. **Baja de precio en los servicios de deepfake e IA** permite que los ciberdelincuentes recurran a estas tecnologías para manipular y engañar a las personas, con el objetivo de que revelen información o realicen acciones determinadas.
3. **Crecimiento de infostealers regionales**, que son programas maliciosos especializados en robar información confidencial de los usuarios para luego venderla en mercados negros, extorsionar o preparar ciberataques. La tendencia es ver los datos como “mercancía”.
4. **Más ataques a pagos NFC** (Near Field Communication o Comunicación de campo cercano), forma de comunicación inalámbrica que permite realizar transacciones sin contacto, por ejemplo, a través de celulares o relojes inteligentes, acercándolos a un terminal de pago. Para ello, ya existen billeteras y portatarjetas que bloquean la comunicación NFC.
5. **Llegada del malware de IA agéntica** (sistemas que cuentan con la capacidad para lograr objetivos específicos bajo poca supervisión de quienes los gestionan). Estos agentes de IA incorporan modelos de aprendizaje automático que imitan la toma de decisiones de los humanos, para así resolver problemas en tiempo real. Una amenaza que, por ahora, se ha dado principalmente en entornos más bien educativos, en los que se han evaluado sus capacidades.
6. **El fraude clásico adoptará nuevos métodos de distribución**. Los cibercriminales aprovecharán cualquier nuevo canal que surja para explotar sus potenciales vulnerabilidades y efectuar fraudes, engaños o robos de información. A su vez, pronostican, buscarán explotar funcionalidades nuevas en plataformas y aplicaciones ya existentes.
7. **Persistirán los dispositivos preinfectedos de fábrica**. Usualmente son realizados por grupos altamente sofisticados, que modifican códigos o piezas de hardware que se introducen en la cadena de suministro, sin que los responsables finales del ensamblado puedan detectar las manipulaciones. Fuente: La Tercera.

Informe internacional advierte expansión del crimen organizado en Chile

El índice global de crimen organizado de 2025 -publicado bianualmente por la organización con sede en Suiza Global Initiative- reveló que Chile ha empeorado progresivamente su puntuación desde 2021, debido a la consolidación en el país de bandas delictuales transnacionales como el Tren de Aragua.

El documento detalló cómo estas bandas criminales manejan el tráfico de migrantes por la frontera y su trata -que incluye su explotación. También advirtió de la expansión del narcotráfico, por la proximidad con países productores de cocaína como Bolivia.

El puntaje de criminal de Chile de este año fue de 5,48; es decir, 0,3 puntos por sobre los 5,18 obtenidos en 2023 y sobre también los 4,6 que recibió en 2021. Esto dejó al país en el octavo lugar en Sudamérica -la misma posición del reporte anterior-, con peores resultados que Argentina (5,25 puntos), Bolivia (5,12), Surinam (4,9) y Uruguay (3,57).

Chile quedó sí con mejores resultados que Colombia (que obtuvo 7,82 puntos y el segundo peor ranking a nivel internacional, después de Myanmar), además de Ecuador (7,48), Paraguay (7,48), Brasil (7,07), Venezuela (6,97), Perú (6,62) y Guyana (5,78). A nivel global, Chile quedó en la septuagésima sexta posición, entre los 193 países contabilizados.

Fuente: Ex-Ante