44
Boletín Informativo ACHEA
Marzo-Abril 2025

Ministerio de Seguridad Pública inició su gestión

El martes 1 de abril de 2025 comenzó oficialmente la operación el Ministerio de Seguridad Pública, cuya instalación representa un cambio estructural significativo, al asumir funciones previamente a cargo del Ministerio del Interior y sumar nuevas responsabilidades y capacidades.

El Ministerio nació a partir de la ley promulgada el 27 de enero de 2025, y fue concebido como una respuesta del Estado para combatir con mayor eficacia el crimen organizado, el narcotráfico, el terrorismo y otras amenazas que afectan a la seguridad pública. Esta nueva institucionalidad se encargará del resguardo, mantención y promoción de la seguridad y el orden público, así como de la prevención del delito y la protección de las personas.

Entre sus principales atribuciones se encuentra la formulación y evaluación de políticas y estrategias de seguridad, tanto a nivel local como internacional. Para ello, se creará un Sistema de Seguridad Pública que integrará a Carabineros, Policía de Investigaciones, Gendarmería, la Agencia Nacional de Inteligencia, el Servicio de Impuestos Internos y Aduanas, entre otras instituciones.

Como el Ministro de Seguridad Pública, el Presidente Gabriel Boric designó a Luis Cordero, quien hasta entonces se desempeñaba como Subsecretario del Interior; mientras que el abogado Rafael Collado González será el Subsecretario de Seguridad Pública. Fuente: minsegpublica.cl

ACHEA Asociación Chilena de Empresas de Alarmas y Seguridad A. G.

EDITORIAL

SEGURIDAD ELECTRÓNICA: ROL COADYUVANTE COMPLEMENTARIO DE LA SEGURIDAD PÚBLICA

La ley de Seguridad Privada Nº 21.659, en su artículo 1, inciso primero, define la Seguridad Privada como el conjunto de actividades o medidas de carácter preventivas, coadyuvantes y complementarias de la seguridad pública, destinadas a la protección de personas, bienes y procesos productivos, desarrolladas en un área determinada y realizadas por personas naturales o jurídicas de derecho privado, debidamente autorizadas en la forma y condiciones que establece la ley.

Asimismo, el artículo 41 declara que las empresas de seguridad electrónica son aquellas que tienen por objeto la instalación y mantenimiento de aparatos, equipos, dispositivos, componentes tecnológicos y sistemas de seguridad con fines privados y conectados a centrales receptoras de alarmas, centros de control o de videovigilancia privados, así como la operación de dichas centrales y centros, y disponen de medios materiales, técnicos y humanos para ello.

De esta forma, y considerando algunos de los elementos del marco legal regulatorio, se deduce la importancia de las coordinaciones intersectoriales público-privadas para concretar el rol colaborativo coadyuvante complementario de la seguridad pública; no solo en el ámbito preventivo mediante diversas estrategias, sistemas de seguridad electrónica, acciones, equipos, dispositivos y componentes tecnológicos, sino también en la disuasión y persecución penal, a través del registro de hechos en imágenes que se constituyen en evidencia importante para sancionar a los responsables de los diversos ilícitos que tanto victimizan y atemorizan a la sociedad.

ACHEA AG. CREE EN ESTE ROL Y DESPLIEGA ESFUERZOS PERMANENTES PARA SU CONCRECIÓN

Presentan resultados del Informe Nacional de Homicidios Consumados en Chile 2024

El nuevo Ministerio de Seguridad Pública, encabezado por Luis Cordero, dio a conocer el Informe Nacional de Víctimas de Homicidios Consumados en Chile 2024, que arrojó un total de 1.207 víctimas de homicidios consumados durante el año. Luego de un crecimiento sostenido entre 2016 y 2022, por segundo año consecutivo se registró una disminución.

Según el estudio, en 2024 se registró una tasa de 6,0 homicidios por cada 100 mil habitantes, lo que representa una disminución de -4,8% respecto a 2023.

En términos absolutos, hubo 42 casos menos que el año anterior, cuando se registraron 1.249 víctimas fatales.

Por otra parte, diez de las 16 regiones del país registraron una disminución en la tasa de homicidios consumados por cada 100.000 habitantes en comparación con el año anterior.

El principal mecanismo de comisión de homicidios fue por armas de fuego, con el 49,5% de los casos (-3,4 puntos porcentuales menos que 2023)-, mientras que un 34,4% por objetos cortopunzantes.

Respecto a las circunstancias de la agresión, el 37,9% ocurrió en un contexto interpersonal y el 35,6% asociado a delitos y/o grupos organizados.

Por primera vez, el informe incluyó un apartado sobre víctimas de femicidio consumado, reportando 42 mujeres víctimas en 2024. De ellas, un 66,7% tenía entre 18 y 39 años, siendo el tramo de 18 a 29 años aquel que concentra la mayor cantidad de víctimas, con un 35,7%. El 83,3% de las víctimas de femicidio consumado son de nacionalidad chilena y el 16,7% son de origen extranjero.

Fuente: subprevenciondeldelito.gob.cl

Despachan a Sala del Senado proyecto sobre Seguridad Municipal

Las comisiones unidas de Gobierno y Seguridad concluyeron la votación de las indicaciones al texto, en segundo trámite constitucional, del proyecto sobre Seguridad Municipal, que fortalece la institucionalidad comunal en materia de seguridad pública y prevención del delito.

Aspectos relacionados con incompatibilidades de guardias de seguridad municipal, su rol coadyudante con Carabineros y elementos defensivos y de protección, fueron los últimos puntos abordados por las comisiones que despacharon a Sala la iniciativa que modifica la ley 18.695, orgánica constitucional de Municipalidades y otros cuerpos legales, con el objeto de fortalecer la seguridad pública y prevención del delito en los territorios locales.

Se estableció, por ejemplo, que los guardias municipales no podrán mantener negocio, empresas u otro, incompatible con la fiscalización en la comuna en que se ejerce, para evitar conflictos de intereses.

Además, cuando cursen infracciones, estarían facultados para requerir la exhibición de un documento que compruebe la identidad de las personas; y de no ser posible, deberán comunicarse con Carabineros para conducirlas a una unidad policial para identificarlas.

Fuente: Senado.cl

Se suman 1.500 cámaras para la Región Metropolitana

El gobierno se anunció que 1.500 cámaras de seguridad municipales se integrarán al programa SITIA (Sistema Integrado de Teleprotección con Inteligencia Artificial) de la Subsecretaría de Prevención del Delito y a la Central de Comunicaciones de Carabineros de Chile.

La medida forma parte del fortalecimiento de la estrategia de seguridad en la Región Metropolitana y contempla la participación de las comunas de Santiago, Lo Barnechea, Estación Central, Huechuraba, Independencia, Lo Prado, Pedro Aguirre Cerda, Peñalolén, Pudahuel, Vitacura y San Joaquín.

La Subsecretaria Carolina Leitao destacó que se ha realizado una inversión de más de 360 millones de pesos en SITIA por parte de la SPD y que la meta es ir integrando cada vez más comunas, no solo de la capital, sino también en otras regiones.

Fuente: subprevenciondeldelito.gob.cl

País Digital y Corfo apuestan por mejorar la seguridad ciudadana

Con el propósito de fortalecer la participación de pymes tecnológicas en el mercado de la teleprotección inteligente, Fundación País Digital, con apoyo de Corfo Metropolitano, presentó una iniciativa que busca consolidar el uso de tecnologías digitales, como la inteligencia artificial (IA), en la industria de la seguridad ciudadana, mediante la colaboración entre el gobierno, municipios, empresas tecnológicas y pymes del sector de seguridad.

El plan de formación busca entregar capacitación especializada y estrategias de innovación mediante la modernización y estandarización de los sistemas de teleprotección, integrando nuevos procesos que permiten mejorar hasta siete veces la capacidad de monitoreo. De este modo fortalece la prevención del delito y la seguridad ciudadana, mediante el desarrollo de competencias técnicas y la adopción tecnológica en pequeñas y medianas empresas de los sectores de telecomunicaciones, electrónica e informática, tanto para uso propio como para generar modelos de negocio. Fuente: Corfo.

Estado de la Seguridad Electrónica

Con el propósito de conocer las operaciones y entornos de seguridad electrónica en 2024, identificar las perspectivas de los proyectos del sector para este año y comprender los desafíos futuros, Genetec Inc. encuestó a profesionales de todo el mundo, para dar forma al Estado de la Seguridad Electrónica 2025, que documenta interesantes cambios en las prioridades del sector y un renovado interés por la excelencia operativa.

El 57% de los usuarios finales afirmaron que los principales desafíos eran una infraestructura de seguridad electrónica y/o de tecnología de la información (TI) obsoleta.

El 66% de los usuarios finales clasificaron el control de acceso (50%) y/o la videovigilancia (39%) como procesos clave o sistemas principales para este año.

El 49% de los usuarios finales informaron que en 2024 tenían el 100% de sus sistemas de seguridad electrónica en sitio (no en la nube). Y el 77% afirmó que los departamentos de seguridad electrónica y tecnologías de la información (TI) trabajan en estrecha colaboración.

Respecto al control de acceso, los usuarios finales quieren hacer más con su tecnología. Tradicionalmente centrados en restringir el acceso no autorizado, están buscando construir funcionalidades adicionales, eficiencia y modernidad. La gestión de visitantes (41%), la biometría (39%) y la gestión de identidades (37%) encabezan la lista de nuevas inversiones en control de acceso en 2025.

Fuente: Genetec Inc.

En cuanto a la **videovigilancia**, los integradores señalaron que los usuarios finales se centran en las cámaras y los sistemas de gestión de video (VMS) como claves entre los sistemas de seguridad electrónica antiguos a reemplazar o actualizar en 2025. También informaron que sus clientes quieren sustituir los sistemas antiguos para integrar nuevas tecnologías y acceder a nuevas funciones, como: mayor calidad de video, interfaz VMS simplificada y funcionalidades inteligentes en las analíticas de video impulsadas por Deep Learning.

Informe de ciberseguridad: Chile sufrió 27.600 millones de intentos de ataques en 2024

El último reporte de FortiGuard Labs, de Fortinet, destacó que Chile enfrentó un alza alarmante en intentos de ciberataques, pasando de 6.000 millones en 2023 a 27.600 millones en 2024. Según el informe, esta explosión responde al uso creciente de automatización e inteligencia artificial (IA) por parte de los cibercriminales.

“Nuestro último reporte de FortiGuard Labs sobre el panorama global de amenazas de 2025 deja una cosa clara: los cibercriminales están acelerando sus esfuerzos, utilizando IA y automatización para operar a niveles sin precedentes de rapidez y escala”, aseguro Derek Manky, jefe de Estrategia de Seguridad y VP global de Inteligencia de Amenazas de FortiGuard Labs.

“El manual tradicional de seguridad ya no es suficiente. Las organizaciones deben tomar una estrategia proactiva enfocada en inteligencia e impulsada por IA, confianza cero y manejo continuo de exposición a amenazas”, agregó. Fuente: El Mostrador.

Sesionó por primera vez el Consejo Nacional de Seguridad Pública

El jueves 17 de abril se desarrolló la primera sesión del Consejo Nacional de Seguridad Pública, presidida por el Ministro de la cartera, Luis Cordero, y en la que participaron las máximas autoridades de Interior, Defensa Nacional, Hacienda, Justicia y Derechos Humanos, el Ministerio Público, Carabineros de Chile, Policía de Investigaciones, Gendarmería y las subsecretarías de Seguridad Pública y Prevención del Delito.

En la instancia inaugural fueron presentados los lineamientos estratégicos y cronograma de trabajo para la presentación de la Política Nacional de Seguridad Pública, que deberá incluir una estrategia de prevención del delito, la protección y atención de víctimas, así como las medidas de combate y prevención del crimen organizado y de los actos terroristas, entre otras temáticas.. Fuente: minsegpublica.cl

¿Cuáles son los principales desafíos para el sector de la seguridad privada en Latinoamérica en 2025?

Un sondeo de Segurilatam, realizado a través de la plataforma LinkedIn, ¿preguntó por los mayores desafíos actuales para la seguridad privada en Latinoamérica. Y sus seguidores respondieron que los principales retos son: formación y profesionalización (40%), regulación y normativas (30%), tecnología y ciberseguridad (21%), reconocimiento y valoración (9%),

En efecto, la falta de capacitación adecuada puede comprometer la eficacia en la protección de bienes y personas, por lo que la profesionalización resulta esencial para garantizar servicios de calidad y mejorar la percepción pública de la industria.

Respecto a la regulación, según la Federación Panamericana de Seguridad Privada (Fepasep), se estima que por cada empresa formal de seguridad privada surgen tres clandestinas, con el riesgo de la ocurrencia de prácticas poco éticas y la consecuente afectación a la confianza en el sector.

Por otra parte, la rápida evolución tecnológica exige que las empresas de seguridad privada se adapten a las últimas soluciones aplicadas a la seguridad. Y también que presten especial atención a la seguridad cibernética tanto para proteger la información que manejan como para impedir que los ciberdelincuentes desactiven alarmas, vulneren sistemas de control de acceso o accedan a cámaras de videovigilancia.

Finalmente, en lo referente a la reputación de la industria, la percepción pública de la seguridad privada a menudo es limitada o negativa, lo que afecta la motivación de sus profesionales y la atracción de talento calificado. Mejorar la imagen del sector es vital para su desarrollo y para establecer relaciones de confianza con la sociedad. Fuente: Segurilatam.

España: Seguridad Privada 2021-2024 en cifras

La Unidad Central de Seguridad Privada (UCSP) de España ha publicado un informe sobre la evolución de los puestos de trabajo en el sector de la seguridad privada entre 2021 y 2024, con un enfoque en la incorporación de la mujer en este ámbito.

Algunos de los datos más relevantes del estudio son:

Evolución general del empleo: A 31 de diciembre de 2024, había 146.566 puestos de trabajo en el sector de la seguridad privada en el país ibérico. Esto representa un incremento del 4,30% respecto a 2023, con 5.100 profesionales más. Sin embargo, la balanza entre hombre y mujeres sigue siendo muy desigual. De los 5.100 profesionales que se incorporaron a esta actividad entre 2023 y 2024, únicamente 1.685 fueron mujeres.

Directores y directoras de seguridad: Las directoras de seguridad representan el 7,07% del total de directores, evidenciando un incremento en la presencia femenina en puestos de mando.

Jefes y jefas de seguridad: Las jefas de seguridad constituyen el 8,74% del total de jefes, mostrando una tendencia similar al punto anterior.

Detectives privados: La mayor presencia femenina se encuentra en esta profesión, con un 27,45% del total de detectives siendo mujeres.

Vigilantes de seguridad: Más del 95% de los puestos de seguridad privada corresponden a vigilantes de seguridad. De estos, el 15,98% son mujeres.

Escoltas privados: En 2024, se observó un ligero incremento en el número de mujeres ocupando estos puestos.

Vigilantes de explosivos: Se registró una tendencia similar a la de los escoltas privados, con un leve aumento en la presencia femenina. Fuente: Seguritecnia.

CAF lanzó Marco Estratégico de Seguridad y Justicia para el Desarrollo de América Latina y el Caribe

En el marco de los eventos previos a la realización de su reunión de Directorio, CAF –Banco de Desarrollo de América Latina y el Caribe– presentó su Marco Estratégico de Seguridad y Justicia para el Desarrollo (MESJD), propuesta que busca dar respuesta a los altos niveles de inseguridad, violencia y criminalidad que afectan de manera estructural al bienestar, la democracia y el desarrollo de la región.

El documento, que asume la consolidación de la seguridad como eje clave para el desarrollo sostenible e inclusivo, propone una nueva manera de pensar la seguridad ciudadana, incorporando conceptos de seguridad multidimensional y gobernanza democrática, y planteando la necesidad urgente de consolidar instituciones eficaces, legítimas y confiables, que garanticen un entorno pacífico para todos los ciudadanos.

Durante la presentación, se destacó que América Latina y el Caribe se enfrenta a una crisis de seguridad multisistémica: 9 de las 10 ciudades más violentas del mundo están en la región, y 17 de los 20 países con mayores tasas de homicidios pertenecen a ella. Esta violencia, que impacta de manera especial a jóvenes varones en situación de vulnerabilidad, coexiste con bajos niveles de confianza ciudadana en la policía, la justicia y otras instituciones fundamentales.

Asimismo, el crecimiento de la delincuencia organizada transnacional (DOT) y del cibercrimen está agravando el panorama. Se estima que el 50 % de los asesinatos en la región están vinculados a organizaciones criminales, y que cada día se registran más de 3 millones de ciberataques, lo que evidencia la urgencia de fortalecer tanto las instituciones de seguridad tradicionales como las capacidades tecnológicas y regulatorias de los Estados.

El MESJD se basa en tres principios fundamentales:

- Multidimensionalidad, la cual reconoce la complejidad y multicausalidad de la inseguridad, planteando intervenciones articuladas entre sectores como el desarrollo urbano, social, institucional y económico.
- Enfoque multinivel, que promueve la coordinación entre los niveles local, nacional y transnacional de gobierno, adaptando las respuestas a las realidades concretas de cada territorio.
- Trabajo en redes, para fomentar la articulación entre el Estado, la sociedad civil, el sector privado y la academia, con el objetivo de construir resiliencia institucional y social frente al crimen y la violencia.

Fuente: Caf.com

Boletín Informativo ACHEA

8 medidas claves para blindar su empresa contra ataques digitales

Patricio Campos, CEO de Resility y experto en esta área, comparte algunas recomendaciones para proteger los activos digitales. “La seguridad informática no es un gasto, es una inversión. Implementar estas medidas puede marcar la diferencia entre operar con confianza o enfrentar una crisis cibernética de alto impacto”, advierte.

1. **Adopción del modelo Zero Trust**
La seguridad perimetral ya no es suficiente. Implementar un enfoque de Zero Trust implica asumir que ninguna entidad, interna o externa, es confiable por defecto. Esto se traduce en aplicar la autenticación multifactor (MFA); la verificación continua de dispositivos y usuarios en la red, y la segmentación de redes, que limita el movimiento lateral de amenazas dentro de la infraestructura.

2. **Integración de IA en la ciberdefensa**
La inteligencia artificial no solo potencia los ciberataques, sino que también puede fortalecer la ciberseguridad. Herramientas basadas en IA permiten detectar patrones anómalos, prevenir fraudes y automatizar respuestas ante amenazas emergentes.

3. **Fortalecimiento de la seguridad en la nube**
Con la migración masiva a servicios en la nube, es crucial asegurar que la información esté protegida mediante cifrado de datos; la gestión de accesos, aplicando el principio de privilegios mínimos para usuarios y aplicaciones; y el monitoreo constante para identificar y mitigar vulnerabilidades.

4. **Capacitación continua del personal**
El factor humano sigue siendo una de las principales vulnerabilidades. Casi tres de cada diez empresas chilenas han enfrentado al menos un incidente de ciberseguridad en los últimos dos años, destacando la importancia de la formación en la detección de phishing; fomentar las buenas prácticas de manejo de datos; y garantizar la integridad y la confidencialidad de la información. También, impulsar el uso de credenciales robustas y únicas.

5. **Implementación de copias de seguridad**
Los ataques de ransomware han aumentado significativamente. Contar con backups actualizados y protegidos es esencial para recuperar operaciones sin ceder a extorsiones. Se recomienda la regla 3-2-1, es decir: mantener 3 copias de seguridad; contar con 2 tipos de almacenamiento diferentes; y tener 1 copia fuera de línea.

6. **Control de acceso riguroso**
Limitar el acceso a información sensible es vital. Se deben establecer políticas claras respecto a quién puede acceder a qué datos, implementando la autenticación de doble factor (2FA); la revisión periódica de permisos, para así revocar accesos innecesarios o no autorizados; y mantener un registro de actividades, con el fin de auditar acciones para detectar comportamientos sospechosos.

7. **Realización de simulaciones**
Poner a prueba la resiliencia de la organización mediante simulaciones periódicas de ataques cibernéticos permite evaluar la eficacia de las medidas de seguridad y mejorar la capacidad de respuesta ante incidentes reales.

8. **Implementación de DRP y BCP**
Tras el mega apagón sufrido por el país en febrero, se hace necesario para las empresas y la industria operar con el Disaster Recovery (DRP) o Plan de Recuperación ante Desastres, y el Business Continuity Plan (BCP) o Plan de Continuidad del Negocio. Estas medidas se ponen a prueba para verificar cómo funciona cada parte operativa de la organización, en el contexto de un determinado desastre, lo que implica, por supuesto, la seguridad informática.

Fuente: g5noticias.cl

Boletín Informativo ACHEA

Cascos que piensan y guantes que sienten: la nueva era del EPI inteligente

En el entorno laboral actual, la seguridad de los trabajadores es una prioridad. A medida que la tecnología avanza, surgen tecnologías que mejoran las condiciones laborales, como el Equipo de Protección Individual con IA o EPI Inteligente. Estos dispositivos no solo cumplen con la función tradicional de proteger físicamente al trabajador, sino que además incorporan tecnologías como sensores, conectividad inalámbrica, inteligencia artificial y análisis de datos en tiempo real.

Un EPI Inteligente puede incluir cascos con sensores de impacto, chalecos con monitorización de temperatura corporal, guantes con detección de vibraciones o gafas con realidad aumentada para recibir instrucciones. Estos dispositivos pueden detectar situaciones de riesgo de forma inmediata, alertar al trabajador o al supervisor y, en algunos casos, incluso, activar protocolos de emergencia de manera automática.

La principal ventaja de los EPI inteligentes es su capacidad de anticipación a los accidentes. Por ejemplo, un sensor de gases tóxicos integrado en una mascarilla puede alertar al usuario antes de que los niveles sean peligrosos. Del mismo modo, un arnés conectado puede enviar una señal si detecta una caída, permitiendo una respuesta rápida que puede salvar vidas.

Además de mejorar la seguridad, la reacción y la prevención, estos dispositivos permiten recopilar datos útiles sobre el entorno laboral. Esta información se puede analizar para identificar patrones de riesgo, mejorar los procesos de formación y tomar decisiones informadas sobre la prevención de accidentes. Fuente: Seguridad-laboral.es

Comienza a regir en Chile la obligación de reportar los incidentes de ciberseguridad

El 1 de marzo de 2025 comenzó a regir la obligación para todas las instituciones públicas y privadas que prestan servicios esenciales de reportar los incidentes de ciberseguridad significativos que les ocurran ante la Agencia Nacional de Ciberseguridad (ANCI).

Este deber legal recae sobre aquellas instituciones que presten servicios esenciales o importancia vital, de conformidad con la Ley Marco de Ciberseguridad N° 21.663 y su reglamento, tales como los organismos de la Administración del Estado y las empresas privadas de suministro de energía, transporte, salud, entre otros.

El reglamento establece que un incidente de seguridad tiene “efecto significativo” cuando tiene el potencial de producir efectos como la interrupción de la continuidad de un servicio esencial, la afectación de la integridad física de las personas o la vulneración de datos personales.

Los reportes de los incidentes de ciberseguridad deberán realizarse a través de la plataforma de notificación dispuesta por la ANCI, disponible en el siguiente enlace: https://portal.anci.gob.cl. Acceda aquí al texto completo del Reglamento de reporte de incidentes de ciberseguridad de la Ley N°21.663.

Fuente: allende.com / Foto: Larazon.es

Aprobado el Plan de Acción de la Política Nacional de Ciberseguridad 2023-2028 para nuestro país

El jueves 27 de marzo se llevó a cabo la primera sesión del Comité Interministerial de Ciberseguridad de Chile, creado por la Ley Marco de Ciberseguridad para asesorar al Presidente de la República en materias relevantes para el funcionamiento del país.

Durante el encuentro, se revisó y aprobó el Plan de Acción de la Política Nacional de Ciberseguridad 2023-2028 y se examinó el estado de avance del proceso de instalación de la Agencia Nacional de Ciberseguridad (ANCI) y de la implementación de la mencionada legislación. Entre sus funciones, el Comité puede proponer ajustes normativos para fortalecer el marco regulatorio en materias de seguridad digital, coordinar la implementación de la política nacional y apoyar a la ANCI en la prevención y respuesta ante incidentes.

La sesión fue encabezada por Daniel Álvarez Valenzuela, director de la ANCI, quien subrayó la importancia de la colaboración interministerial de este Comité para ejecutar un plan de acción integral que fortalezca una cultura de seguridad digital.

Definidos por la ley, también asistieron a la primera sesión el Subsecretario del Interior; el Subsecretario de Defensa, la Subsecretaria de Relaciones Exteriores, el Subsecretario General de la Presidencia, el Subsecretario de Telecomunicaciones, la Subsecretaria de Hacienda, un representante del Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación; y un representante de la Agencia Nacional de Inteligencia. Fuente: Segurilatam.com