



Revista **SEGURIDAD** & DEFENSA

REGLAS DE USO DE LA FUERZA
Una nueva etapa para la
actuación policial

LA MINERÍA
Como objetivo
para la delincuencia



REFORMA DE SEGURIDAD

Una fórmula basada en el consenso



GRUPO SAFETECK



SEGURIDAD CON TECNOLOGÍA

Seguridad y tecnologías a la medida de cada cliente



CCTV

Monitoreo inteligente
en tiempo real



DESARROLLO DE PROYECTOS

Soluciones integrales
a la medida



EQUIPO TÉCNICO

Profesionales certificados
y especializados



SOPORTE 24/7

Atención continua
todos los días del año



PÓRTICOS
DETECTORES DE METALES



RADIOS IP



CCTV MÓVILES



CENTRAL DE MONITOREO
DE ALTA TECNOLOGÍA 24/7

SOLUCIONES QUE SE ADAPTAN A CADA REALIDAD

En Grupo Safetec nos especializamos en diseñar e implementar **soluciones tecnológicas a la medida de cada cliente**, integrando innovación, experiencia y un enfoque estratégico que garantiza seguridad, eficiencia y continuidad operativa.



COLEGIOS



- ✓ Pórticos detectores de metales
- ✓ Control de acceso inteligente
- ✓ Monitoreo preventivo 24/7
- ✓ Entornos más seguros para estudiantes y personal

PROTEGEMOS LO MÁS IMPORTANTE:
SU FUTURO



RETAIL



- ✓ Detectores faciales y analítica inteligente
- ✓ Prevención de pérdidas y monitoreo en tiempo real
- ✓ Control de accesos y afluencia
- ✓ Reportes para mejorar la operación

MÁS CONTROL, MÁS SEGURIDAD,
MEJORES RESULTADOS



CONSTRUCTORAS



- ✓ Cámaras con inteligencia artificial
- ✓ Sistemas de vóceo de alta frecuencia
- ✓ Vigilancia perimetral autónoma
- ✓ Reportes para la continuidad operativa de sus proyectos

TECNOLOGÍA QUE CONSTRUYE
SEGURIDAD Y CONTINUIDAD



GENERAMOS REPORTES INTELIGENTES QUE ENTREGAN **INFORMACIÓN CLARA, OPORTUNA Y ACCIONABLE**, ASEGURANDO LA CONTINUIDAD OPERATIVA Y LA TOMA DE DECISIONES ESTRATÉGICAS.



ONE TECNOLOGÍA
SEGURIDAD

TECNOLOGÍA, EXPERIENCIA Y COMPROMISO
PARA PROTEGER LO QUE MÁS IMPORTA.

Al analizar los factores que han complejizado el avance de la Reforma de Seguridad no podemos dejar de preguntarnos "qué parte de la urgencia de avanzar en soluciones efectivas en materia de seguridad no es entendido por las autoridades en su conjunto"

Si bien el llamado a una reforma de consenso resulta valorable, pareciera ser que lo que en un comienzo constituyó una prioridad, dió paso a una serie de "conflictos secundarios" muchos de ellos de carácter ideológico que en resumen se traducen en que, tras nueve meses de mandato de un nuevo gobierno, la reforma permanece sin mayores avances.

Abordar la reforma de seguridad como una prioridad país resulta fundamental, pues al margen de los cambios propuestos, su avance y aprobación representa una potente señal frente a la delincuencia.

Dilatar un pronunciamiento en esta materia, proyecta indefinición frente a un tema en el cual como país no debiesen haber mayores diferencias. Lo contrario implicará replicar lo sucedido con las Reglas de Uso de la fuerza, las cuales tardaron más de tres años en ser aprobadas con las consiguientes repercusiones producto de la incertidumbre en los cuerpos de seguridad respecto de cómo abordar un procedimiento por temor a posibles repercusiones legales.

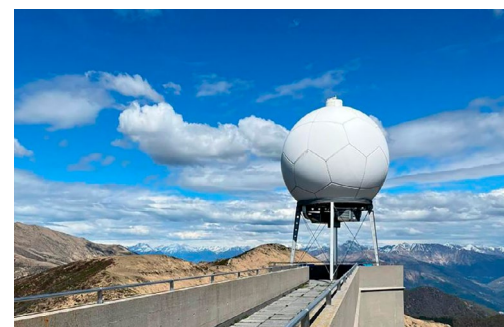
Una acción decidida en esta materia, será percibida positivamente por parte de una ciudadanía que clama por mayor seguridad, y la cual más allá de los importantes avances en materia de seguridad, sigue manteniendo una alta percepción de inseguridad.



Robert Gutter Boim
Director

CONTENIDO

Editorial	1
Reforma de seguridad Una fórmula basada en el consenso	3
Reglas del Uso de la Fuerza Una nueva etapa para fortalecer la seguridad	5
Primera Feria de Delitos Rurales Una instancia que visibiliza una realidad preocupante	8
Estrecho de Magallanes Una fricción jurídica, geopolítica y naval	16
Sebastián Sichel El emplazamiento de Ñuñoa tras las inundaciones	20
El costo invisible de la dependencia tecnológica Simuladores aéreos "Made in Chile"	24
Blindaje 360 Proteger a quienes nos cuidan	28
Evidencia digital Cuando el celular habla más que un testigo	38
Cuando el Estado trabaja para otro Columna de Richard Biernay	46
"Octubre Negro" La ciberseguridad bajo presión	48
La minería Como objetivo de la delincuencia	52
Cuando el regulador se convierte en el "cuello de botella" Columna de Julio Ibañez	63
El modelo de policía Koban Columna de Javier Gamero Kinosita	69
América Latina ante una disyuntiva estratégica Columna de Fernando Vaccotti	74



www.revistaseguridad.cl
E mail: info@revistaseguridad.cl
AÑO 20 N° 66 Edición Septiembre - Octubre 2026
Prohibida toda reproducción total o parcial de esta revista.

Revista Seguridad & Defensa es una edición de
Producciones Gótica Ltda.

Las opiniones incorporadas en esta revistas son de
exclusiva responsabilidad de quienes las emiten y no
representan necesariamente el pensamiento del editor.

Revista Seguridad & Defensa

Director: Robert Gutter Boim

Imagen portada: ChatGpt

Ventas de Publicidad: +56 9 98246696

info@revistaseguridad.cl

revistaseguridadonline@gmail.com



Revista
SEGURIDAD
& DEFENSA





Reforma de seguridad

Una fórmula basada en el consenso

El repliegue de La Moneda con respecto a su propuesta original fue visto por los ministros como un triunfo del diálogo pragmático más que como una derrota. Tras semanas de entrampamiento en la Comisión de Constitución, el diseño del bloque transversal de senadores ofreció una salida limpia que destrabó la agenda contra la delincuencia.

Si bien amplios sectores legislativos han manifestado su entusiasmo por respaldar un texto que consideran “un avance sustantivo y moderno”, los desafíos persisten. El éxito del proyecto en las siguientes semanas dependerá de la precisión con la que el Congreso delimite técnicamente qué constituye un “peligro grave e inminente”, y de cómo el Estado fortalezca en paralelo sus capacidades policiales y de inteligencia para que el nuevo marco legal se traduzca en una protección real para la ciudadanía.

La nueva reforma constitucional de seguridad en Chile nació tras el colapso del proyecto original del Ejecutivo, el cual fue retirado ante la falta de apoyos y los cuestionamientos transversales en el Senado. En su reemplazo, un acuerdo político transversal entre senadores de oposición y oficialismo —Pedro Araya (PPD), Andrés Longton (RN), Arturo Squella (Republicanos), Iván Flores (DC) y Karim Bianchi (Ind.)— dio vida a una moción de consenso que cuenta con el respaldo del Gobierno y que inició su tramitación legislativa.

A diferencia del proyecto anterior, que buscaba instaurar un “Estado de Seguridad Pública”, esta propuesta alternativa deja de lado las herramien-

tas punitivas que generaban controversia (como la pérdida de beneficios sociales o la interceptación telefónica masiva) y articula la estrategia nacional en tres ejes fundamentales:

El crimen organizado bajo el estándar del terrorismo

La iniciativa busca modificar el artículo 9° de la Constitución para incorporar explícitamente al crimen organizado y establecer que, en sus manifestaciones más graves, es contrario a los derechos humanos, a las bases de la institucionalidad y a la democracia.

Al otorgarle un tratamiento equivalente al de los delitos terroristas, se activarán severas restricciones que incluyen inhabilidades constitucionales para ejercer cargos públicos, la consideración de estos ilícitos como delitos comunes (nunca políticos) y la aplicación estricta de las reglas de indulto. La futura ley determinará qué figuras delictivas se encuadran bajo este estatuto, evaluando factores estructurales, permanencia y distribución de funciones dentro de la banda criminal.

Segregación penitenciaria estricta

Para atacar el problema desde las cárceles, que a menudo operan como centros de operaciones de bandas criminales, el proyecto eleva a rango constitucional la obligatoriedad de una segregación en el sistema carcelario. Los reos condenados o bajo prisión preventiva por delitos relacionados al crimen organizado o terrorismo serán separados físicamente y sometidos a regímenes especiales diferenciados de la población penal de delitos comunes, neutralizando así el reclutamiento y la coordinación intramuros.

Un Estado de Emergencia “preventivo”

El cambio más innovador reside en la flexibilización de las facultades presidenciales mediante el ajuste del actual Estado de Emergencia (artículo 42 de la Constitución). La reforma permitirá al presidente decretar esta medida de forma excepcional y preventiva ante el peligro o la amenaza grave e inminente para la seguridad de la Nación, basándose en informes de inteligencia, Carabineros, la PDI y el Ministerio Público.

- Duración y control: Tendrá una vigencia inicial máxima de 30 días (a diferencia de los 15 días actuales).

- Rol del Congreso: El Ejecutivo deberá rendir informes detallados cada 15 días. Cualquier prórroga requerirá el visto bueno explícito del Parlamento, el cual mantendrá además la facultad de revocar el estado de excepción en cualquier momento si considera que las causas que lo justificaron ya desaparecieron.

- Garantías: Los autores enfatizan que esta variante no limitará libertades fundamentales más allá de las de locomoción y reunión que ya contempla la normativa vigente.

Ventajas de la nueva propuesta

- Viabilidad política y destrabe legislativo: La mayor fortaleza radica en su origen transversal (firmado por senadores desde Republicanos hasta la DC y el PPD). Cuenta con el patrocinio del Ejecutivo, lo que garantiza una tramitación ágil al dejar atrás el veto mutuo.

- Mayor control democrático frente al Ejecutivo: A diferencia del proyecto original del gobierno de José Antonio Kast (que permitía mantener un estado de excepción prolongado casi sin supervisión), este diseño otorga al Congreso la potestad de revocar la medida preventiva en cualquier momento por mayoría simple, equilibrando el balance de poderes.

- Resguardo de los derechos civiles: Al descartar las polémicas herramientas del borrador anterior —como la interceptación masiva de telecomunicaciones sin control judicial, las listas administrativas de bandas criminales o la pérdida de beneficios sociales—, la propuesta se blindó frente a posibles acusaciones de inconstitucionalidad o sesgo autoritario.

- Blindaje judicial para Gendarmería: Al elevar la segregación carcelaria a rango constitucional, se dota de un marco legal robusto a las autoridades de prisiones. Esto busca frenar que los líderes de bandas de alta peligrosidad dejen sin efecto el régimen de aislamiento interponiendo recursos de protección o amparos ante jueces de corte garantista.

Vacíos y zonas grises

- Ambigüedad en el criterio “preventivo”: La reforma faculta al mandatario a decretar el Estado de Emergencia ante un “peligro grave e inminente”. Sin embargo, la propuesta no define con precisión técnica qué constituye una amenaza inminente, abriendo una zona gris que dependerá de la interpretación del gobierno de turno y de sus informes de inteligencia.

- Falta de herramientas operativas clave: Al eliminar la creación de un “registro de organizaciones

criminales” y la interceptación telefónica expedita (medidas que contemplaba el proyecto original), algunos sectores advierten que la propuesta es simbólicamente potente, pero carece de “garra” de inteligencia para desarticular financieramente a las mafias.

- Delegación excesiva a las leyes complementarias: El texto consagra que el crimen organizado recibirá el tratamiento del terrorismo, pero deja en manos de una ley futura la definición de qué delitos calificarán en esta categoría. Esto traslada el debate de fondo (y el riesgo de entrapamiento) a una posterior discusión penal.

- Falta de presupuesto y viabilidad carcelaria inmediata: Aunque se mandate constitucionalmente la estricta separación física de los reclusos peligrosos, Chile no dispone actualmente de la infraestructura carcelaria ni de los penales de máxima seguridad necesarios para absorber una segregación masiva inmediata. El texto no aclara los plazos ni los mecanismos de financiamiento específicos para la reconversión de los recintos de Gendarmería.

El factor Araya

A pesar del fuerte sismo político que significó su salida de la presidencia de la Comisión de Constitución, la remoción del senador Pedro Araya no debilita la viabilidad de la reforma de seguridad, sino que, paradójicamente, consolida el bloque transversal necesario para aprobarla.

La repercusión de este hito político se divide en tres aspectos clave:

1. *El compromiso intacto de los votos*: El impacto más inmediato fue la aclaración del propio parlamentario. Tras reunirse en el Palacio de La Moneda con el biministro del Interior y Segegob, Claudio Alvarado, Araya ratificó que mantendrá su respaldo pleno y votará a favor del proyecto en la sala del Senado. Al tratarse de una reforma constitucional, cada voto cuenta para alcanzar los altos quórum requeridos, y el descuelgue de Araya habría sido fatal para el Ejecutivo.

2. *Consolidación de un bloque “díscolo” o independiente*: La salida forzada de Araya —calificada por él mismo como una pasada de cuenta del “socialismo autoritario”— operó como un incentivo para otros senadores de centro-izquierda e independientes.

Parlamentarios que miran con distancia las directivas tradicionales del Partido Socialista (PS) han cerrado filas en torno a la propuesta.

Este grupo transversal (que incluye a senadores como Flores o Bianchi) ve en el apoyo a la reforma una forma de priorizar la agenda ciudadana

contra el crimen organizado por sobre las disputas partidarias.

3. *Cambio de ritmo en la Comisión de Constitución*: La llegada del diputado/senador Vlado Mirosevic a la presidencia de la instancia legislativa altera la dinámica de la discusión:

Mayor fiscalización: El bloque oficialista tradicional buscará revisar con más lupa los detalles técnicos del proyecto (como los límites al Estado de Emergencia preventivo y las atribuciones de Gendarmería).

Menos espacio a la negociación directa: Las conversaciones ya no se darán de forma reservada entre La Moneda y Araya, sino que el Gobierno se verá obligado a defender la propuesta de manera abierta ante una oposición que endurecerá su postura formal, aunque los votos para la aprobación final sigan estando disponibles en la sala.



Reglas de Uso de la Fuerza

Chile entra en una nueva etapa para fortalecer la seguridad y la actuación policial

Tras más de tres años de tramitación, Chile dio un paso decisivo en la regulación del uso de la fuerza. El 7 de octubre de 2026, el Congreso despachó a ley el proyecto que establece normas generales para el personal de las Fuerzas de Orden y Seguridad Pública y de las Fuerzas Armadas en determinadas circunstancias. La iniciativa quedó en condiciones de ser promulgada y publicada Con 29 votos a favor, 15 en contra y una abstención, la Sala del Senado entregó su respaldo al informe de la Comisión Mixta que zanjó las discrepancias en relación al proyecto que establece normas generales sobre el uso de la fuerza para el personal de las Fuerzas de Orden y Seguridad Pública y de las Fuerzas Armadas en determinadas circunstancias.

Entre el combate a la delincuencia, la protección de los ciudadanos y el respaldo a quienes ejercen la autoridad, definir reglas precisas para el uso de la fuerza se ha convertido en una prioridad para el Estado. La eficacia policial y el respeto al Estado de Derecho no son objetivos contrapuestos: son condiciones indispensables para recuperar la seguridad pública.

La seguridad exige claridad, no improvisación

Chile enfrenta un escenario de seguridad que demanda respuestas oportunas, capacidades operativas y una institucionalidad preparada para enfrentar fenómenos criminales cada vez más complejos. La expansión de organizaciones delictivas, el uso de armas de fuego, la violencia contra funcionarios policiales y la creciente percepción de inseguridad han instalado una pregunta fundamental: ¿cuándo, cómo y bajo qué condiciones puede el Estado emplear legítimamente la fuerza para proteger a la ciudadanía?

La respuesta no puede depender exclusivamente del criterio individual de un funcionario enfrentado a una situación crítica, ni quedar sujeta a interpretaciones contradictorias posteriores a un procedimiento. Requiere reglas claras, conocidas, coherentes con la legislación y respaldadas por protocolos operativos, capacitación permanente y mecanismos de control.

Una regla de uso de la fuerza no constituye una autorización indiscriminada para ejercer violencia. Es un marco que establece las circunstancias, los límites y las responsabilidades bajo los cuales los agentes del Estado pueden recurrir a ella, considerando la amenaza existente, la necesidad de actuar y la proporcionalidad de la respuesta.

En otras palabras, no se trata solamente de determinar cuándo se puede utilizar la fuerza, sino también de establecer cuándo resulta indispensable, qué nivel de intervención corresponde y en qué momento debe cesar.

Proteger a la ciudadanía y respaldar a quienes la protegen

Uno de los problemas más delicados de la seguridad pública es la incertidumbre que puede enfrentar un funcionario policial cuando debe tomar decisiones en segundos, bajo presión y ante una amenaza potencialmente mortal.

En esas circunstancias, la ausencia de criterios suficientemente claros o la percepción de que cualquier decisión será cuestionada sin considerar las condiciones reales del procedimiento pueden afectar la confianza y la capacidad de respuesta. Sin embargo, el respaldo institucional no debe confundirse con impunidad: significa entregar formación, instrucciones precisas, equipamiento adecuado y garantías de que cada actuación será evaluada conforme a la ley y a los antecedentes concretos.

Carabineros de Chile y la Policía de Investigaciones necesitan marcos operativos que permitan

actuar con decisión frente a amenazas reales, proteger la vida de terceros y responder eficazmente ante delitos violentos. Al mismo tiempo, la ciudadanía debe tener la certeza de que las facultades coercitivas del Estado se ejercerán dentro de límites definidos y sujetos a fiscalización.

Una regulación bien diseñada contribuye a ambas finalidades. Reduce la ambigüedad, facilita la supervisión de los procedimientos, mejora la preparación de los funcionarios y permite distinguir entre una actuación legítima, un error operativo y un eventual abuso.

La discusión, por tanto, no debería plantearse como una elección entre proteger los derechos de las personas o entregar herramientas a las policías. La verdadera cuestión es cómo construir un sistema que permita hacer ambas cosas de manera efectiva.

Legalidad, necesidad y proporcionalidad: los pilares de la actuación

Una política moderna de uso de la fuerza debe partir de principios reconocibles y aplicables en el terreno.

La legalidad exige que toda intervención tenga fundamento jurídico y se ajuste a las competen-

cias de quien actúa. La necesidad implica recurrir a la fuerza únicamente cuando sea requerida para alcanzar un objetivo legítimo y en la medida indispensable.

La proporcionalidad obliga a que la intensidad de la respuesta guarde relación con la amenaza y las circunstancias del procedimiento.

A estos principios se suman la precaución, la rendición de cuentas y la protección de la vida. Cuando las circunstancias lo permitan, deben privilegiarse la comunicación, la advertencia, la desescalada y otras alternativas menos lesivas. Cuando exista una amenaza grave e inminente, en cambio, los protocolos deben ofrecer criterios claros para una respuesta eficaz, sin exigir conductas incompatibles con la urgencia o el peligro real.

También es esencial precisar las condiciones de empleo de armas de fuego, la intervención frente a personas armadas, la protección de terceros y la asistencia médica posterior a un procedimiento cuando corresponda.

Una regla efectiva no puede limitarse a una declaración general de principios. Debe traducirse en instrucciones comprensibles, escenarios prácticos, entrenamiento recurrente y procedimientos

de revisión que permitan aprender de los incidentes y corregir deficiencias.

El desafío de legislar con sentido operativo

En Chile, la discusión sobre el uso de la fuerza debe considerar tanto el marco legal vigente como las iniciativas legislativas destinadas a precisarlo o perfeccionarlo. La Ley N.º 21.560, conocida como Ley Naín-Retamal, introdujo modificaciones relevantes en materia de protección y actuación de las fuerzas de orden y seguridad pública. A ello se suman las normas, los reglamentos y los protocolos que regulan las actuaciones policiales.

Por eso, cualquier reforma debe partir de una revisión rigurosa de las disposiciones existentes, identificando qué aspectos requieren mayor precisión, cuáles presentan dificultades de aplicación y dónde persisten vacíos o contradicciones. El objetivo no debería ser multiplicar normas, sino construir un marco coherente, comprensible y aplicable.

La regulación debe entregar seguridad jurídica a los funcionarios que actúan legítimamente, pero también establecer mecanismos eficaces para investigar y sancionar los excesos. La responsabilidad individual, el control institucional y la

<div> <div>REGLAS APROBADAS</div> <div>PARA EL USO DE LA FUERZA</div> <div>Un marco claro para actuar con eficacia, proteger a la ciudadanía y resguardar el Estado de Derecho.</div> </div>				
REGLA	NIVEL DE ACTUACIÓN	DESCRIPCIÓN		
1	Despliegue disuasivo	Despliegue de fuerzas y medios	Despliegue de fuerzas, vehículos, naves, aeronaves, dispositivos y otros medios institucionales, así como porte de armas, con carácter disuasivo.	
2	Comunicación y persuasión	Diálogo y negociación	Uso de técnicas de comunicación y persuasión verbal, como diálogo, mediación y negociación.	
3	Elementos disuasivos y menos letales	Uso de medios no letales	Empleo manual de humo, gas pimienta, gases lacrimógenos, sonido, luz, agua, bastones u otros elementos menos letales.	
4	Dispositivos de lanzamiento menos letales	Uso de sistemas no letales	Uso de dispositivos o sistemas no letales para lanzar proyectiles con pintura, gas pimienta, gases lacrimógenos, agua u otras sustancias o elementos menos letales.	
5	Control físico e inmovilización	Reducción y contención	Reducción del transgresor para doblegar su resistencia, inmovilizarlo o esposarlo. Una vez reducido e inmovilizado, y si no opone resistencia, se prohíbe ejercer fuerza en su contra.	
6	Munición de salva	Disuasión	El personal militar podrá emplear munición de salva en forma disuasiva.	
7	Escopetas antidisturbios	Control de multitudes y situaciones críticas	Uso de escopetas con munición antidisturbios para evitar o repeler un peligro grave e inminente para la vida o integridad física, o para impedir daños o pérdida material de infraestructura crítica y proteger recintos militares, según los supuestos indicados.	
8	Armamento letal	Respuesta ante amenazas graves	Uso contra personas que utilicen o se dispongan a utilizar armas letales u otros medios capaces de poner en peligro la vida o causar lesiones graves. También contempla la negativa a desprenderse de un arma tras una conminación expresa y determinados ataques contra infraestructura crítica o recintos militares, en las condiciones señaladas.	

transparencia son componentes necesarios de una fuerza pública profesional.

Del mismo modo, las reglas deben acompañarse de recursos para entrenamiento, formación jurídica, equipamiento de protección, tecnologías de registro cuando corresponda y sistemas de supervisión capaces de evaluar la actuación policial con información verificable.

Una norma que no se comprende, no se entrena o no se aplica de manera consistente difícilmente producirá los resultados esperados.

Una discusión que debe superar las trincheras políticas

El uso de la fuerza suele convertirse en un tema de confrontación política, especialmente después de procedimientos de alto impacto. Sin embargo, la protección de la vida, el combate a la delincuencia y el control del poder estatal deberían constituir objetivos compartidos, por encima de las diferencias ideológicas.

La falta de reglas suficientemente claras perjudica a todos: puede dejar a los funcionarios expuestos a la incertidumbre, dificultar la evaluación de sus actuaciones, debilitar la confianza pública y generar espacios para interpretaciones incompatibles con una política de seguridad coherente. Por el contrario, una regulación técnicamente sólida permite que las decisiones se adopten sobre criterios previamente definidos y no exclusivamente bajo la presión de una contingencia o del debate político posterior.

El desafío consiste en construir acuerdos que reconozcan la complejidad del trabajo policial, la gravedad de las amenazas que enfrentan los funcionarios y el deber irrenunciable del Estado de respetar los derechos fundamentales.

La seguridad también depende de la confianza institucional

La legitimidad de las policías no se construye únicamente mediante resultados operativos. También depende de la confianza que la ciudadanía deposita en sus procedimientos y de la certeza de que las actuaciones pueden ser explicadas, revisadas y, cuando corresponda, corregidas.

Una regla de uso de la fuerza clara, conocida y aplicada de manera consistente fortalece esa confianza. Permite que el funcionario sepa qué se espera de él, que sus superiores puedan evaluar su actuación con parámetros objetivos y que la ciudadanía comprenda los límites de la intervención estatal.

Pero la confianza no se obtiene únicamente con

una ley. Requiere liderazgo institucional, capacitación, supervisión, transparencia y una cultura profesional que reconozca tanto la necesidad de actuar frente al delito como la obligación de responder por las decisiones adoptadas.

Una condición para recuperar la seguridad

Chile necesita policías preparadas para enfrentar la violencia, proteger a las personas y actuar con eficacia frente a organizaciones criminales. Para lograrlo, no basta con aumentar las penas, incorporar tecnología o ampliar las capacidades operativas. También es indispensable establecer con precisión las condiciones bajo las cuales el Estado puede ejercer legítimamente la fuerza.

La regla de uso de la fuerza debe entenderse como una herramienta estratégica de seguridad pública: entrega criterios para la acción, fortalece el respaldo institucional, facilita el control y contribuye a que las intervenciones sean profesionales, justificadas y eficaces.

La autoridad democrática se demuestra tanto en su capacidad para enfrentar el delito como en su responsabilidad al ejercer el poder. Chile necesita reglas que permitan actuar cuando sea necesario, detener la intervención cuando deje de serlo y exigir responsabilidades cuando se traspasen los límites legales.

Porque una política de seguridad eficaz no consiste en usar más fuerza, sino en asegurar que la fuerza del Estado se emplee de manera legítima, oportuna, proporcional y bajo reglas que todos puedan comprender.

1ª Feria de Delitos Rurales

Una iniciativa que permite visibilizar una realidad preocupante

La primera feria de delitos rurales constituye una iniciativa pionera, organizada por SOCABIO en la ciudad de Los Ángeles. Este encuentro congregó a empresas y autoridades en una jornada en la cual se abordaron los principales requerimientos de nuestro país en materia de seguridad rural. Para conocer los alcances de esta importante iniciativa conversamos con Jorge Contreras Blümel, director ejecutivo del Observatorio de Delitos Rurales del BIOBÍO.

¿Cómo surge la idea de realizar la 1 expo de seguridad de delitos rurales?

En el marco de nuestro trabajo como Observatorio de delitos rurales, advertimos una situación crítica respecto al nivel de protección que presentan los predios agrícolas, en cuanto a la tecnología que estaban usando y a la falta de conocimiento sobre las mejores técnicas para prevenir incidentes. Además, por la mesa de trabajo que impulsamos junto con policías y fiscalía, vemos la necesidad de entregar medios probatorios cuando se hacen de denuncias, y contar con equipamiento adecuando ayudará a agilizar las investigaciones.

¿Qué entidad está organizando este evento?

La Sociedad de Agrícola de Biobío (SOCABIO), en colaboración con su Observatorio de Delitos Rurales, perteneciente a la misma entidad.

¿Cuántas empresas participaron de esta primera versión de Expo Seguridad de delitos Rurales?

Esta primera versión contó con un total de 12 empresas de seguridad como expositoras, provenientes de la región del Biobío y otras con alcance a nivel nacional.

¿Qué podemos comentar con respecto de las actividades anexas a la muestra, conversatorios, seminarios etc.?

Además de los stands de las empresas presentes se realizaron una serie de paneles los cuales contarán con la presencia de autoridades ministeriales, Ministerio Público y el equipo del Observatorio de Socabio.

De forma adicional las empresas patrocinadoras del evento, realizaron exposiciones respecto a su tecnología, servicios, y buenas prácticas de prevención.

¿Cuál es la variedad y extensión actual en materia de delitos rurales en Chile?

Los delitos rurales en Chile comprenden una familia de delitos que se relacionan entre sí, y que se caracterizan porque las víctimas son principalmente agricultores y ganaderos.

Dentro de lo que hemos recopilado como Observatorio, identificamos 4 incidentes de alto impacto: Robo de cobres, robo de insumos agroquímicos, robo de maquinaria agrícola y abigeato. Si bien nuestra área de competencia es la provincia de

Biobío, hemos levantado evidencia que demuestra que esta problemática se extiende por varias regiones del país, desde O'Higgins a la Araucanía.

¿Cómo han evolucionado las bandas criminales dedicadas al abigeato en las distintas regiones de Chile en los últimos años?

Las bandas que se dedican al abigeato operan de forma organizada, ya que tienen horarios específicos para cometer los ilícitos, y rondan los campos antes del ataque. Los casos de los que hemos tomado conocimiento, tienen en común que solo dejan la cabeza e interiores de los animales, e ingresan en vehículos motorizados a los predios para llevarse la mayor cantidad de carne. Además, se repite mucho que quienes son víctimas de abigeato no contaban con cámaras de vigilancia, las tenían mal ubicadas o inactivas, por lo que los delincuentes sabían de antemano que podían cometer el delito sin dejar pruebas que los identificaran.

¿Cuál es la ruta de receptación y reventa de la maquinaria agrícola pesada y los agroquímicos de alto valor sustraídos en los campos chilenos?

Parte de las gestiones que impulsamos como Ob-

servatorio, es reunir evidencia que permita hacer seguimiento a la maquinaria y a los agroquímicos robados. Estamos trabajando en un proyecto de ley con el equipo de una diputada del D21, para crear un sistema de trazabilidad nacional de estos productos, lo que facilite acceder al historial de venta, origen, traslado y composición.

Sabemos que existe un mercado negro, donde incluso a los mismos agricultores se les ofrecen estos agroquímicos y maquinarias, a un valor mucho menor que los distribuidores oficiales, por lo que hay una ruta desconocida sobre el destino. Cuando cuentan con alguna medida de seguridad, por ejemplo, GPS, es más sencillo encontrar lo sustraído y es posible recuperarlo por parte de los propietarios.

¿De qué manera la delincuencia rural organizada está afectando la infraestructura de riego (robo de transformadores, cables de cobre y bombas de agua)?

Cuando un pequeño o mediano agricultor sufre el robo de sus equipos, piezas y maquinarias, se ve obligado a detener su cadena de producción. Esto le genera un perjuicio importante, ya que, si deja de regar sus cultivos por 10 días, atrasa toda la cosecha y eso se traduce en pérdidas económicas que después no alcanza a recuperar.

¿Qué alianzas público-privadas se necesitan para mejorar la seguridad perimetral y el monitoreo en zonas con baja conectividad digital o telefónica?

Se necesita promover el buen uso de la tecnología en los predios, que los productores sepan lo que ofrece hoy el mercado para que estén más protegidos. En ese sentido, las acciones que pueden impulsar gremios como Socabio son fundamentales; por medio de la Mesa de Trabajo que formalizamos con Carabineros, PDI y Fiscalía, definimos sectores críticos que tienen mayor ocurrencia de incidentes, y así aumentan las fiscalizaciones y patrullajes.

¿Están los planes vigentes del gobierno y los comités de seguridad rural respondiendo con la rapidez que el sector privado agrícola exige?

Desde el sector agrícola existe un agotamiento y decepción general con el sistema. La cifra negra de hechos que no se denuncian se da principalmente porque ven denunciar como una pérdida de tiempo, al creer que el trámite no tendrá resultados positivos y no lograrán recuperar lo robado. Es necesario fomentar con mayor fuerza la alianza colaborativa entre gremios, y el refuerzo de las comunidades rurales, ya que al actuar de forma unificada se genera una presión mayor, y si disponen de sistemas de seguridad interconectados, facilitan mucho la trazabilidad, seguimiento y persecución de los delitos en flagrancia.

¿Qué capacidades técnicas y de despliegue territorial urgente requieren Carabineros de Chile y la PDI para cubrir eficazmente las macrozonas rurales?

Lo que necesitan nuestras policías es trabajar de forma conjunta; compartirse la información sobre las denuncias es fundamental, para que tomen conocimiento sobre dónde, cómo y cuándo están ocurriendo los delitos. Junto con eso, tomar acciones a partir de evidencia territorial debe ser la consigna, que la generación de estadística sirva de insumo para que no solo se enteren de lo que se denuncia, sino de todos los delitos rurales que suceden y que muchas veces no llegan a ser denunciados formalmente.

¿Por qué el Ministerio Público presenta dificultades para lograr condenas altas en delitos rurales y cómo se puede mejorar la recolección de evidencia en el sitio del suceso rural?

El Ministerio Público se rige por lo que dictamina el código penal. Dentro de lo que se conoce como delitos rurales, el único que se encuentra tipificado como delito es el abigeato. Los demás incidentes no tienen una tipificación única, y para efectos de la investigación y de la interposición de condenas, se consideran como robo en lugar no habitado, o como robo o hurto simple. Dado que las penas no son altas, es esencial que los medios probatorios sean contundentes para identificar a los responsables, para que la investigación arroje resultados efectivos.



Durante la inauguración de este importante evento, Jorge Contreras Blümel, Director Ejecutivo del Observatorio de Delitos Rurales del BIOBIO, destacó la relevancia de una instancia, pionera en su tipo, la cual permite visibilizar la realidad en materia de delitos rurales, junto con plantear propuestas para afrontar este foco delictual.

Principales conclusiones de 1ª FERIA de Delitos Rurales, organizada por SOCABIO

La 1ª FERIA de Delitos Rurales (también denominada Expo de Seguridad Rural), organizada en Los Ángeles por la Sociedad Agrícola de Biobío (SOCABIO) a través de su Observatorio de Delitos Rurales, concluyó con un fuerte llamado a la coordinación interinstitucional y la presentación de nuevas estrategias y tecnologías para combatir ilícitos como el abigeato (robo de ganado), el robo de madera y el hurto de maquinaria agrícola.

A continuación se detallan las principales conclusiones y acuerdos del encuentro:

1. Integración de Información y Plan Piloto

- Propuesta de SOCABIO: El gremio propuso formalmente la integración de datos de distintas instituciones públicas. El objetivo es diseñar y ejecutar un plan piloto en la provincia de Biobío para optimizar la prevención, el seguimiento de las denuncias y el éxito de las investigaciones judiciales.
- Apoyo Ministerial: Se solicitó de manera directa apoyo al Ministerio de Seguridad Pública para dotar de mayores recursos, herramientas y respaldo institucional al combate de la delincuencia en los campos.

2. Reformas y Avances Legislativos

Durante la instancia, que contó con la participación del ministro de Seguridad Pública, Martín Arrau, se destacaron medidas clave que buscan robustecer la respuesta policial frente a delitos flagrantes:

- Ampliación del plazo de flagrancia: Se abordó la extensión del tiempo de detención por flagrancia de 12 a 24 horas para Carabineros y la PDI, facilitando capturas efectivas en zonas rezagadas. [1]
- Evidencia inmediata: Se relevó la facultad de acceder de forma voluntaria a grabaciones de seguridad de los predios sin requerir la instrucción previa de un fiscal, agilizando las primeras diligencias.
- Endurecimiento de penas: Se respaldó el proyecto que busca elevar las sanciones penales para los delitos de robo, hurto y receptación de insumos, productos y maquinaria del sector agrícola.

3. Foco en la Tecnología y Soluciones Prediales

- Acercar soluciones al agricultor: Uno de los éxitos prácticos de la feria fue conectar directamente a productores agrícolas y forestales con proveedores tecnológicos. Se promovió el uso de televigilancia, drones y sistemas avanzados

de protección perimetral para que los afectados puedan resguardar autónomamente sus espacios productivos.

4. Fortalecimiento y Continuidad de la Denuncia

- Cultura de la denuncia: SOCABIO enfatizó que están trabajando de la mano con los agricultores para asegurar que todos los delitos sean reportados formalmente.
- Trabajo con Fiscalía y Policías: El fiscal regional del Biobío, Roberto Garrido, y las autoridades policiales presentes coincidieron en que levantar insumos directamente de las víctimas en estos espacios permite mejorar los focos investigativos y otorgar una protección más eficiente en el mundo rural.

5. Fiscalización Activa en Terreno

- En el marco de la feria también sesionó la Mesa Regional de Seguridad Rural, donde servicios como el SAG Biobío expusieron un incremento del 18,3% en sus fiscalizaciones de trazabilidad y sanidad animal (período 2025-2026), lo que ha permitido aumentar en un 47,1% las infracciones cursadas, golpeando directamente las cadenas de comercialización del abigeato.



(de izq. a der.) Alcalde de Los Ángeles, José Pérez, Jorge Contreras Blümel, Director del Observatorio de Delitos, Ministro de Seguridad Pública Martín Arrau, Claudia Antinao, Gerente de Proyectos LEADETIK, Richard Soto, SEREMI de Seguridad BIOBÍO y Rocío Burgos, Gerente Observatorio



El problema de la boca oriental del Estrecho de Magallanes frente al decreto 256/2010

Una fricción jurídica, geopolítica y naval en el Cono Sur

Dada la contingencia en nuestras relaciones exteriores de los últimos meses, creo fundamental, iniciar este ensayo conceptualizando qué es la geopolítica. La proyección austral de Chile y Argentina es una de las encrucijadas geopolíticas más importantes del siglo XXI. La geopolítica se fundamenta en las visiones de Friedrich Ratzel, quien concibe al Estado como un organismo vivo ligado a su espacio vital (Lebensraum), y de Sir Halford Mackinder, creador de la Teoría del Heartland sobre el impacto de la geografía en la hegemonía global.

A nivel regional, el General Ramón Cañas Montalva aportó la doctrina de la tricontinentalidad chilena y la proyección hacia el Pacífico Sur-Antártico. Los pasajes australes -compuestos por el Estrecho de Magallanes y el Paso Drake- constituyen cuellos de botella (chokepoints) vitales para el comercio mundial y rutas interoceánicas alternas ante crisis globales. Finalmente, este espacio estratégico representa un escenario de competencia entre grandes potencias (Estados Unidos, China y Rusia) que disputan el control logístico, la investigación científica y la proyección soberana hacia el Continente Blanco.

El enlace con el Decreto 256/2010 de Argentina

Aunque el Decreto 256/2010 está motivado por el litigio de soberanía con el Reino Unido, su aplicación práctica roza con frecuencia las rutas de navegación que conectan la boca oriental del Estrecho de Magallanes y el Paso Drake. Entendiendo que, el Estrecho de Magallanes está neutralizado a perpetuidad y abierto a la libre navegación de buques de todas las banderas, la aplicación de controles o autorizaciones en accesos contiguos o aguas de aproximación ha generado históricamente suspicacias diplomáticas relativas al libre tránsito hacia y desde puertos chilenos o antárticos.

Buques de investigación o abastecimiento antár-

tico de terceros países (incluyendo potencias mundiales y Gran Bretaña) que usan puertos australes chilenos o navegan por estos canales han sido objeto de monitoreo bajo la normativa del Decreto 256/10 al cruzar por áreas adyacentes a la jurisdicción argentina. Esto tensiona el equilibrio estratégico local. Mientras Chile defiende la tesis geopolítica de Cañas Montalva basada en el libre acceso marítimo global y la proyección pacífica antártica, Argentina refuerza mecanismos normativos de soberanía marítima territorial en el Atlántico Sur.

Génesis y arquitectura del Decreto 256/2010: La doctrina del cerrojo austral

La promulgación del Decreto 256/2010 por parte del Poder Ejecutivo Nacional (PEN) de la República Argentina —suscrito el 16 de febrero de 2010 bajo la administración de Cristina Fernández de Kirchner— no constituye un exabrupto normativo ni un mero trámite administrativo coyuntural. Representa, en su dimensión más profunda, la cristalización jurídica de una matriz geopolítica e histórica de largo aliento. Concebido en los despachos de la Casa Rosada y moldeado por la doctrina de la Armada Argentina, este instrumento se inserta en un diseño estratégico continuado que, durante más de seis décadas, ha buscado proyectar e imponer un control efectivo sobre los pasos interoceánicos del extremo austral del continente americano.

Para la historiografía y la geopolítica trasandina, la noción de la “Argentina bioceánica” no ha sido un simple recurso de oratoria patriótica, sino un imperativo de destino nacional. Bajo esta cosmovisión, el litoral patagónico y las frías latitudes donde crujen las aguas de los dos mayores océanos del planeta constituyen el pivote de su proyección antártica y atlántica. El Decreto 256/2010 erige una arquitectura de coerción y fiscalización administrativa sobre un tríptico geográfico vital: el Estrecho de Magallanes, el Paso Drake (o Mar de Hoces) y el Canal Beagle.

En su articulado medular, el decreto impone la obligación de solicitar una autorización previa expedida por la autoridad nacional competente (la Prefectura Naval Argentina) a todo buque o artefacto naval —de cualquier pabellón— que pretenda transitar entre puertos ubicados en el territorio continental argentino y puertos situados en las Islas Malvinas/Falklands, Georgias del Sur y Sándwich del Sur, o bien atravesar aguas jurisdiccionales argentinas con rumbo a dichos archipiélagos.

Esta disposición opera en la práctica como un cerrojo logístico unilateral contra la presencia británica en el Atlántico Sur, pero proyecta simultáneamente sus ondas de choque hacia la soberanía y la libertad de navegación de la República de Chile en la Boca Oriental del Estrecho de

Magallanes. Para eso tienen que controlar necesariamente tres espacios fundamentales: el Estrecho de Magallanes (cuyo dueño y poseedor es al 100% la República de Chile), el Paso Drake y el Canal Beagle.

Y, en esta estrategia que ha sido desarrollada de manera muy eficiente, de controlar estos tres espacios oceánicos, se ha hecho para: *primero*, proteger su proyección antártica. *Segundo*; esto le daría un poder geopolítico enorme en un contexto en el cual las grandes potencias están mirando hacia la zona austral por los problemas que hoy presenta el Canal de Panamá y “otros cuellos de botella” como Ormuz, por mencionar sólo un par. Y *tercero*, porque hay una ambición que al ser miembro extra OTAN desde 1998 y desde 2024 se ha postulado para ser aliado global de la OTAN, lo cual significa mantener una relación de cooperación política y práctica estrecha con la alianza militar, sin llegar a ser un miembro pleno.

Dimensión geopolítica global: los pasos australes en la era de los cuellos de botella

El valor estratégico del control de la Boca Oriental del Estrecho de Magallanes debe calibrarse en un tablero global atravesado por crecientes incertidumbres sistémicas.

En la concepción estratégica contemporánea, los pasos australes americanos han dejado de ser confines remotos para retomar su condición de arterias críticas de la navegación mundial.

En este contexto, la pretensión argentina de tutelar o condicionar el tráfico marítimo en la embocadura atlántica del Estrecho persigue tres objetivos geopolíticos capitales:

1. Blindaje de la proyección antártica: Controlar los accesos marítimos al continente blanco, posicionando a los puertos patagónicos (como Ushuaia) como nodos logísticos obligados frente a las pretensiones de otros actores estatales.

2. Palanca de presión en la disputa de Malvinas/Falklands: Asfixiar las líneas de suministro marítimo civil, comercial y pesquero que sustentan el desarrollo económico de las islas bajo administración británica.

3. Proyección de potencia y estatus internacional: Afianzar un perfil de actor clave en la seguridad marítima del Atlántico Sur.

Esta aspiración se ha visto reforzada por la condición de Aliado Mayor Extra-OTAN que Argentina ostenta desde 1998, a la que se suma su solicitud en 2024 para incorporarse como “Socio Global” de la Alianza Atlántica, como se mencionó precedentemente.

La colisión de doctrinas jurídicas: soberanía territorial versus imperativo unilateral

El antagonismo doctrinal entre Santiago y Buenos Aires respecto a la naturaleza jurídica y funcional de la Boca Oriental del Estrecho de Magallanes no representa una mera disputa técnica sobre deslindes cartográficos; encarna una verdadera conflagración teórica en el seno del Derecho Internacional Público.

En este escenario austral, donde las corrientes del Atlántico impactan los acantilados magallánicos, colisionan dos visiones de Estado diametralmente opuestas: por un lado, el paradigma convencional-territorial chileno, anclado en la intangibilidad de los tratados internacionales y el principio supremo del *pacta sunt servanda*; por el otro, la doctrina de soberanía funcional y revisionismo normativo argentino, proyectada desde su derecho constitucional e instrumentalizada como un ariete de presión geopolítica sobre el espacio marítimo circundante a las Islas Malvinas/Falklands.

Esta contienda trasciende el plano normativo para adentrarse en la épica de la supervivencia jurídica de los Estados. Mientras Chile ha erigido su proyección oceánica sobre la base inveterada de pactos solemnes firmados a través de un siglo y medio de historia diplomática, Argentina ha desplegado una arquitectura legal unilateral orientada a mitigar las servidumbres internacionales que limitan sus pretensiones de dominio sobre el Atlántico Sur y la Antártica.

Exégesis de la arquitectura jurídica en disputa

El pilar chileno: la santidad de los tratados y el estatuto de neutralidad perpetua

La posición diplomática e histórica de Chile des cansa sobre una cadena ininterrumpida de instrumentos bilaterales e internacionales que dotan al Estrecho de Magallanes de un estatus legal blindado:

1. El Tratado de Límites de 1881 (Artículo V): Consagró para la posteridad que el Estrecho de Magallanes queda neutralizado a perpetuidad y asegurada su libre navegación para las banderas de todas las naciones.

Este precepto erigió un régimen jurídico erga omnes (oponible a terceros Estados) que despoja a los Estados ribereños de cualquier facultad de entorpecer, fiscalizar discrecionalmente o condicionar el paso de naves comerciales o de guerra.

2. El Tratado de Paz y Amistad de 1984 (Artículos 10 y 14): Tras rozar el abismo de la conflagración bélica en 1978, la mediación papal de Juan Pablo II culminó en un acuerdo que ratificó explícita-

mente el Tratado de 1881.

En su artículo 10, la República Argentina asumió la obligación solemne y perpetua de mantener, en cualquier tiempo y circunstancia, el derecho de los buques de todas las banderas a navegar en forma expedita y sin obstáculos a través de sus aguas jurisdiccionales hacia y desde el Estrecho de Magallanes.

Como acertadamente sostiene el jurista e historiador Mateo Martinic, esta disposición constituye una auténtica servidumbre de paso imperturbable, incompatible con cualquier pretensión de control aduanero o policial trasandino en la embocadura oriental.

3. La Convención de las Naciones Unidas sobre el Derecho del Mar (CONVEMAR): En sus artículos 34 al 45, la CONVEMAR codifica el régimen de paso por estrechos utilizados para la navegación internacional, estableciendo que el derecho de paso en tránsito no puede ser suspendido ni gravado por exigencias unilaterales de autorización previa por parte de los Estados ribereños.

El edificio normativo trasandino: el imperativo constitucional y el cerrojo administrativo

Frente a la solemnidad de los tratados de límites, Argentina articuló una entramada normativa de derecho interno concebida para salvaguardar sus derechos soberanos sobre el archipiélago Malvinas/Falklands y el Atlántico Sur:

1. La disposición transitoria primera de la Constitución Nacional de 1994: Eleva a rango constitucional la recuperación del ejercicio pleno de la soberanía sobre las Islas Malvinas/Falklands, Georgias del Sur y Sándwich del Sur y los espacios marítimos e insulares correspondientes, calificándola como un objetivo permanente e irrenunciable del pueblo argentino.

2. Leyes N° 23.968 y N° 26.386: Establecen las líneas de base y espacios marítimos de la Nación Argentina y tipifican severas sanciones para el ejercicio ilegítimo de actividades pesqueras o extractivas en la plataforma continental y Zona Económica Exclusiva (ZEE) proyectada desde los archipiélagos australes.

3. El Decreto Presidencial 256/2010: Operando como el brazo ejecutor de esta doctrina, este decreto impone la obligatoriedad de tramitar una venia previa ante la Prefectura Naval Argentina (PNA) para cualquier nave que pretenda conectar el continente con las islas en disputa o transitar por aguas jurisdiccionales argentinas en esa dirección. Al interceptar o notificar naves en la boca oriental o en áreas de aproximación atlántica, el Estado argentino busca proyectar un control de

soberanía funcional que contraviene la fluidez garantizada por los acuerdos de 1984.

Análisis de pros y contras de las posturas Estatales

República Argentina

Pros estratégicos e internos

1. Herramienta de soberanía fáctica: Proporciona un instrumento administrativo de coerción real que penaliza el suministro logístico no autorizado a las Islas Malvinas/Falklands, dificultando el sostén comercial e industrial del enclave británico.

2. Cohesión política y consumo interno: Mantiene el reclamo de soberanía en la cima de la agenda del Estado, unificando a las distintas facciones políticas bajo la causa nacional de la recuperación de las islas.

3. Combate a la pesca ilegal e ilegítima: Ofrece un sustento normativo doméstico para sancionar a las flotas pesqueras internacionales que operan al amparo de licencias concedidas por el gobierno de las Falklands/Malvinas.

Contras internacionales y diplomáticos

1. Vulneración de la Convención de Viena: Contraviene de manera flagrante el Artículo 27 de la Convención de Viena sobre el Derecho de los Tratados, el cual prohíbe taxativamente a los Es-

tados invocar las disposiciones de su derecho interno para justificar el incumplimiento de una obligación convencional internacional.

2. Erosión de la confianza bilateral con Chile: Genera una fricción institucional permanente con el Estado chileno, reactivando la suspicacia histórica en la oficialidad de las Fuerzas Armadas y diplomáticas sobre la vocación expansionista o revisionista de Buenos Aires.

3. Aislamiento en foros de navegación internacional: El ejercicio de controles coercitivos o notificaciones de infracción en alta mar o en canales de tránsito internacional posiciona a Argentina al margen de los consensos multilaterales sustentados por la Organización Marítima Internacional (OMI) y la CONVEMAR.

República de Chile

Pros estratégicos e internacionales

1. Inexpugnabilidad del respaldo jurídico: La postura chilena goza de una solidez incontestable ante la comunidad internacional, amparada en tratados bilaterales perpetuos (1881 y 1984) y en la codificación del Derecho del Mar.

2. Liderazgo en la libertad de mares: Al sostener la neutralidad absoluta y el libre tránsito por Magallanes, Chile se alinea con las principales po-

tencias marítimas y comerciales del mundo, resguardando una ruta crítica global.

3. Preservación del statu quo fronterizo: La defensa irrestricta del principio pacta sunt servanda previene que eventuales revisionismos internos trasandinos puedan alterar las delimitaciones marítimas acordadas solemnemente.

Contras geopolíticos y operacionales

1. Creación de una "zona de penumbra" funcional: La interceptación de remolcadores y buques de apoyo de bandera chilena (como el emblemático caso del remolcador Beagle) por parte de la PNA en aguas del Atlántico Sur fuera de las 200 millas marinas en aguas internacionales, somete al sector privado chileno a una vulnerabilidad operativa e incertidumbre jurídica.

2. Exigencia de un costo diplomático permanente: Obliga a la Cancillería chilena y a la Armada a mantener un monitoreo ininterrumpido sobre cada declaración, decreto o patrullaje argentino, con el fin de evitar que el silencio chileno sea argumentado en el futuro como una forma de aquiescencia o asentimiento tácito.

La dialéctica del derecho frente a la fuerza de los hechos

En última instancia, el choque entre el Decreto 256/2010 y el ordenamiento convencional de los Tratados de 1881 y de 1984, evi-



dencia la histórica paradoja del Derecho Internacional: las normas valen tanto como la voluntad política y la capacidad estratégica de los Estados para hacerlas respetar.

Mientras la República Argentina intenta reescribir funcionalmente la geografía marítima del extremo austral para cercar logísticamente a las Islas Malvinas/Falklands, la República de Chile sostiene la vigencia inalterable de una frontera jurídica trazada sobre la premisa inviolable de que el Estrecho de Magallanes y sus accesos atlánticos pertenecen a la humanidad entera como un paso expedito, libre e ininterrumpido.

La jurisprudencia de la fricción: el hito emblemático del remolcador "Beagle"

El impacto del Decreto 256/2010 superó los debates jurídicos de gabinete para materializarse en las heladas aguas del sur el 14 de abril de 2024. Las divergencias normativas e ideológicas finalmente tocaron la realidad operativa en las aguas heladas del canal Beagle.

Este incidente se convirtió en el caso probatorio de las tensiones derivadas de la norma. En abril de 2024, unidades de la Prefectura Naval Argentina abordaron, interceptaron y notificaron de una supuesta "infracción de navegación" al remolcador de bandera chilena "Beagle", el cual realizaba faenas logísticas de apoyo rutinarias en sectores contiguos a la boca oriental de la boca de paso. El incidente, aunque contenido en el plano operativo por la serenidad de la tripulación naviera, actuó como un reactivo químico en la política chilena.

En el Congreso Nacional en Valparaíso estallaron críticas transversales denunciando la pasividad del Ejecutivo y alertando sobre una política de "hechos consumados" (salami tactics) por parte de la Argentina.

Maass explica que la lógica de las tácticas de salami reside en avanzar "rebanada por rebanada" mediante acciones de un alcance lo suficientemente limitado como para no justificar una guerra o un conflicto a gran escala, pero que de manera acumulativa van desgastando la influencia del adversario. El abordaje puntual a una embarcación de apoyo logístico menor (el remolcador "Beagle") encaja en esta categoría: es una fricción controlada en el plano operativo que pone a prueba los límites sin desencadenar una confrontación bélica abierta. De acuerdo con el marco teórico de Maass, cuando un Estado ejecuta un *fait accompli* (hecho consumado), desplaza la carga de la decisión sobre el rival: ahora es el defensor (en este caso, Chile) el que debe sopesar si el costo de intentar revertir la acción vale la pena o si debe tolerarla para evitar un conflicto mayor.

Esto se refleja en el texto cuando el Congreso chileno discute sobre la supuesta pasividad del Ejecutivo frente a una política sostenida de hechos consumados, reflejando el dilema estratégico que imponen estas tácticas. Maass señala que las tácticas de salami ocurren en el marco de una rivalidad prolongada donde cada acción individual es interpretada como parte de un patrón de expansión e influencia a expensas del contrincante.

El incidente del remolcador "Beagle" no es visto como un hecho aislado, sino como el punto de contacto donde las "divergencias normativas e ideológicas" tocan la realidad operativa, encendiendo las alarmas en la política chilena ante la posibilidad de que se trate de un avance sistemático y gradual de Argentina.

Para teóricos de la estrategia naval como el almirante Sir Julian Corbett, los incidentes menores entre guardacostas o unidades auxiliares no son meras fallas procedimentales, sino sondeos sutiles de la voluntad política y la capacidad de disuasión del Estado rival en sus marcas fronterizas.

Corbett sostenía que en el mar, el control del espacio no siempre se disputa mediante grandes batallas decisivas entre flotas de combate, sino a través del control del tráfico marítimo y acciones de presencia constante. El incidente en comento no involucra a buques de guerra ni a la Armada Argentina, sino a la Prefectura Naval Argentina (un cuerpo de seguridad de fronteras/guardacostas) y a un remolcador civil chileno ("Beagle"). De acuerdo con Corbett, el empleo de unidades auxiliares o de guardacostas permite a un Estado probar hasta dónde puede presionar sin desencadenar una respuesta militar directa o una escalada diplomática incontrolable.

Lo ocurrido no fue un error técnico ni una equivocación de patrulla, sino la consecuencia materialización del Decreto 256/2010. El abordaje sirve como un sondeo de jurisdicción. Al aplicar una norma interna sobre un buque extranjero en un área bajo disputa o fricción, la Prefectura Naval argentina actúa como el brazo ejecutor de un ensayo de soberanía o "jurisprudencia de la fricción".

Corbett enfatiza que este tipo de fricciones menores miden la firmeza y la capacidad de disuasión del Estado afectado en sus zonas fronterizas.

Como ya mencionamos precedentemente, la reacción chilena no se limitó al hecho operativo en el mar, sino que repercutió de inmediato en el Congreso Nacional, donde se advirtió sobre la pasividad del Ejecutivo frente a una política de "hechos consumados" (salami tactics).

La incursión funcionó precisamente como la prueba descrita por Corbett: testear si el Estado

chileno reaccionaría con firmeza para mantener su disuasión o si, por el contrario, permitiría que la interrupción de sus actividades logísticas cotidianas creara un precedente de aceptación tácita. El marco teórico de Julian Corbett permite ver el caso del remolcador "Beagle" no como un altercado aislado entre marineros, sino como una micro-operación estratégica de baja intensidad.

A través de sus guardacostas, la Argentina puso a prueba la eficacia práctica de sus normativas y la resolución política de Chile para defender el statu quo en una zona de soberanía sensible. Demostró que Argentina aplica el Decreto 256/2010 no como una norma portuaria local, sino como un estatuto de fiscalización marítima de alcance regional en el Atlántico Sur. Puso de manifiesto que en el cruce entre la salida del Estrecho de Magallanes y las rutas hacia las islas disputadas, la libertad de navegación garantizada por el derecho internacional es desafiada por las exigencias de permiso de la PNA. Expuso el dilema que enfrentan las empresas navieras civiles y de servicio marítimo chilenas, que corren el riesgo de multas millonarias, embargos o vetos de atraque en puertos argentinos si no se someten al trámite de autorización ante Buenos Aires.

Escalada y fricción en el Mar Austral: de la Mediación Papal al contencioso soberano (1984–2026)

La ilusoria solidez del Tratado de Paz y Amistad (1984)

El 29 de noviembre de 1984, tras el precipicio prebélico de 1978 y bajo la minuciosa diplomacia vaticana encabezada por el Cardenal Antonio Samoré y el impulso político de Juan Pablo II, Chile y Argentina firmaron el Tratado de Paz y Amistad. El documento buscaba extirpar de raíz la ancestral disputatio fronterizo en el confín austral.

La arquitectura jurídica del tratado fijó de forma inamovible la frontera marítima y consagró un principio bioceánico tamizado: la delimitación de la boca oriental del Estrecho de Magallanes quedó bajo soberanía exclusiva de Chile, mientras que Argentina asumió la obligación irrestricta de no interferir ni obstaculizar la navegación desde o hacia dicho paso interoceánico (Artículos 10 y 14).

Sin embargo, como argumenta el geopolítico y diplomático chileno Guillermo Lagos Carmona, los tratados de límites en el Atlántico Sur y la Antártica operan bajo una doble naturaleza: son a la vez estipulaciones jurídicas normativas e instrumentos expuestos a las oscilaciones de la política doméstica y las doctrinas de proyección marítima de ambos Estados.

Lo que en 1984 parecía un cerrojo diplomático

definitivo, encerraba asimetrías de interpretación estratégica que aflorarían con vigor décadas más tarde.

La escalada normativa: el Decreto 256/2010 y la Doctrina del Mare Clausum

El equilibrio alcanzado a fines del siglo XX comenzó a erosionarse en la década de 2010. Bajo la administración de Cristina Fernández de Kirchner, el Poder Ejecutivo argentino promulgó el Decreto N° 256/2010. La norma estableció la exigencia de una "autorización previa" dictada por la Prefectura Naval Argentina para todo buque que pretendiera navegar entre los puertos del continente argentino y las Islas Malvinas, Georgias del Sur y Sándwich del Sur, o que transitara por aguas jurisdiccionales argentinas con tal destino. Desde la perspectiva jurídica porteña, la medida constituía un pilar de la "Doctrina de Afirmación Soberana" frente a Gran Bretaña.

No obstante, en la praxis táctica y logística del Cono Sur, la norma generó una zona gris que afectó de modo colateral, tanto al cabotaje como al tránsito comercial chileno con proyección a la Región de Magallanes y la Antártica. El historiador militar británico Sir Michael Howard recordaba que en los espacios insulares y marítimos, "la frontera normativa es tan real como una trinchera: el mero intento de fiscalización administrativa altera el status quo del poder naval". Argentina proyectaba, vía decreto, una suerte de mare clausum de baja intensidad que ponía a prueba la elasticidad del Tratado de Paz y Amistad de 1984.

La reelaboración doctrinaria: la Directiva de Defensa de 2021

El viraje normativo adquirió estatura doctrinaria e institucional en agosto de 2021. Mediante el Decreto N° 457/2021, el Gobierno argentino aprobó la Directiva de Política de Defensa Nacional (DPDN). El texto introdujo conceptos explícitos sobre la necesidad de ejercer una "exploración, vigilancia y control conjunto" sobre el Estrecho de Magallanes y el Paso Drake, definiendo el extremo austral como un espacio geopolítico indivisible donde la proyección antártica argentina requería de una presencia militar coordinada y omnipresente.

La reacción del Palacio de la Moneda fue categórica. El Ministerio de Relaciones Exteriores de Chile despachó la Nota Formal de Protesta N° 7285, denunciando que las pretensiones de co-administración u operatividad conjunta en el Estrecho colisionaban frontalmente con la soberanía perpetua e indivisible de Chile sobre ambas riberas del paso interoceánico, consagrada desde

el Tratado de 1881 y ratificada en 1984.

Tal como apunta el historiador diplomático Mario Barros van Buren, la neutralidad y libertad de navegación del Estrecho de Magallanes jamás han sido en la doctrina chilena un régimen de condominio, sino una concesión de libre paso sobre aguas interiores bajo jurisdicción exclusiva del Estado chileno.

El pronunciamiento histórico de los Almirantes y la notificación diplomática (Agosto-Septiembre de 2026)

Tras una serie de declaraciones públicas de altos mandos de las Fuerzas Armadas argentinas en las que se aludía al espacio magallánico como un "corredor de interés estratégico compartido", la Cancillería chilena elevó nuevamente una severa nota de protesta diplomática. La respuesta de la sociedad civil y el estamento militar no se hizo esperar.

El 2 de septiembre de 2026, en un gesto de inédita gravedad institucional en la historia diplomática reciente del Cono Sur, a través de un manifiesto público difundido en el diario El Mercurio, seis ex Comandantes en Jefe de la Armada de Chile (Almirantes en retiro Miguel Ángel Vergara, Rodolfo Codina, Edmundo González, Enrique

Larrañaga, Julio Leiva y Juan Andrés De la Maza) fijaron una posición doctrinal tajante frente a la política austral argentina. En el documento, los altos oficiales en retiro cuestionaron con dureza la vigencia y aplicación del Decreto argentino 256/2010, exigiendo al Estado chileno una postura firme, sin ambigüedades ni concesiones en la defensa de los tratados limítrofes vigentes.

Los almirantes enfatizaron que el Decreto 256/2010 vulnera el espíritu y la letra de los instrumentos bilaterales vigentes, en particular la servidumbre de paso consagrada en el Tratado de 1984. Advirtieron que no es posible construir una verdadera relación de confianza mutua ni mantener indefinidamente esquemas de cooperación operacional —como la Patrulla Antártica Naval Combinada (PANC)— mientras se mantengan vigentes normas de derecho interno argentino que pretendan lesionar o condicionar la libertad de navegación en la puerta de entrada al Océano Pacífico y el territorio antártico chileno.

La misiva cerraba con un axioma de profundo arraigo en la tradición de la historiografía geopolítica de Chile: "La paz y el bienestar no pueden alcanzarse a costa de la soberanía o de la independencia nacional..." Este pronunciamiento puso de relieve la vigencia del pensamiento del analista y militar chileno Ramón Cañas Mon-



talva, pionero en conceptualizar la “conciencia geográfica e insular de Chile”. El manifiesto de los almirantes dejó en evidencia que, más allá de la diplomacia formal, en el estamento naval chileno subyace la convicción de que la estabilidad política regional no depende de la condescendencia táctica, sino de la preservación inquebrantable de los límites trazados por el derecho internacional.

Perspectivas del conflicto en el Atlántico Sur

La controversia en torno a la Boca Oriental del Estrecho de Magallanes y el Decreto 256/2010 sintetiza las complejidades del Cono Sur en el siglo XXI. No se trata únicamente de un litigio interpretativo de textos jurídicos, sino de la colisión entre dos aproximaciones históricas al espacio marítimo. Por un lado, la visión chilena, fundada en el principio de intangibilidad de los tratados internacionales, la libertad de navegación universal y la soberanía indiscutida e integral sobre el curso del Estrecho de Magallanes.

Por otro lado, la doctrina geopolítica argentina, orientada a la consolidación de un espacio de control insular, atlántico y antártico que instrumenta derecho interno para presionar diplomática y operativamente en la causa de las Islas Malvinas/

Falklands contra Reino Unido. Mientras subsista esta incompatibilidad normativa, la Boca Oriental del Estrecho continuará siendo una zona de fricción latente. La preservación de la estabilidad en el extremo austral exigirá no sólo prudencia y diálogo por parte de las cancillerías, sino también una postura firme por parte del Estado chileno en la defensa incondicional de los tratados limítrofes que garantizan el libre tránsito de las naciones por este histórico paso interoceánico.

“La paz y el bienestar no pueden alcanzarse a costa de la soberanía o de la independencia nacional...”

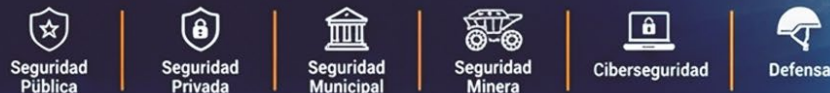
Autor:

Javier Vargas Guarategúa
Administrador General LIDERMAN para
Parque Arauco nivel nacional
Magister en Ciencias Políticas,
Seguridad y Defensa.
Master en Historia Militar.



Revista SEGURIDAD & DEFENSA

La mayor plataforma de información en seguridad de Chile, con una trayectoria de dos décadas.



**MÁS QUE UNA REVISTA,
UNA COMPLETA PLATAFORMA INFORMATIVA**



200.000+
Impresiones mensuales en nuestro portal web

4 CANALES DE DIFUSIÓN

Web · Revista · YouTube · Redes Sociales



Conectamos a las empresas con los principales actores y tomadores de decisiones del ecosistema de la seguridad y la defensa.

Conectamos a las empresas con los principales actores y tomadores de decisiones del ecosistema de la seguridad y la defensa.



Grupo Safetec

Creer nos desafiaba a ser mejores

El crecimiento de Grupo Safetec marca una nueva etapa de desarrollo, donde la expansión operacional va acompañada de un desafío fundamental: fortalecer nuestros equipos, optimizar los procesos y continuar elevando la calidad del servicio que entregamos a nuestros clientes.

En Grupo Safetec estamos viviendo una etapa de crecimiento que refleja la confianza que distintas organizaciones han depositado en nuestra experiencia y capacidad de respuesta. La incorporación de nuevas instalaciones, clientes y colaboradores representa un avance importante para nuestra compañía, pero también nos invita a mirar hacia el interior de nuestra organización y evaluar cómo seguir evolucionando. Entendemos que crecer no significa únicamente aumentar nuestra presencia en el mercado. Implica asumir nuevas responsabilidades, fortalecer la coordinación entre áreas y desarrollar una estructura organizacional capaz de responder a operaciones cada vez más diversas y exigentes.

Por ello, estamos impulsando una evolución interna orientada a mejorar nuestros procedimientos, incorporar nuevas capacidades profesionales y fortalecer los mecanismos de planificación, supervisión y control. Nuestro propósito es que cada nueva operación cuente con el respaldo necesario para mantener los estándares de calidad, continuidad y seguridad que buscamos entregar.

Crecimiento con propósito

Cada nueva instalación representa una oportunidad para consolidar nuestra experiencia, pero también un desafío que requiere preparación y trabajo colaborativo. El crecimiento de nuestras operaciones demanda una mayor articulación

entre los equipos de Recursos Humanos, Reclutamiento y Selección, Operaciones, Prevención de Riesgos y Tecnología. Cada área cumple un papel fundamental para asegurar una incorporación ordenada de nuevos servicios, una adecuada preparación de nuestros colaboradores y una respuesta oportuna a las necesidades de cada cliente. En este proceso, las personas siguen siendo el principal motor de nuestro desarrollo. La experiencia de nuestros guardias de seguridad, supervisores y equipos administrativos, junto con la incorporación de nuevos talentos, permite construir una organización más preparada, cercana y eficiente.

Tres pilares para un crecimiento sostenible

Nuestra visión de futuro se sostiene en tres pilares estratégicos que se complementan y trabajan con un mismo propósito: situar al cliente en el centro de nuestras decisiones.

Tecnología e inteligencia artificial. Buscamos incorporar herramientas que fortalezcan la prevención, el monitoreo y el análisis de situaciones de riesgo. A través de las capacidades tecnológicas de nuestro grupo, avanzamos hacia soluciones que complementen el trabajo de nuestros



equipos en terreno y aporten información útil para la operación.

Inteligencia de negocio. La información es fundamental para gestionar de manera más eficiente. Queremos fortalecer el análisis de indicadores, identificar oportunidades de mejora y tomar decisiones respaldadas por datos que permitan anticipar necesidades, optimizar recursos y evaluar nuestro desempeño.

Crecimiento con propósito Cada nueva instalación representa una oportunidad para consolidar nuestra experiencia, pero también un desafío que requiere preparación y trabajo colaborativo.

El crecimiento de nuestras operaciones demanda una mayor articulación entre los equipos de Recursos Humanos, Reclutamiento y Selección, Operaciones, Prevención de Riesgos y Tecnología. Cada área cumple un papel fundamental para asegurar una incorporación ordenada de nuevos servicios, una adecuada preparación de nuestros colaboradores y una respuesta oportuna a las necesidades de cada cliente. En este proceso, las personas siguen siendo el principal motor de nuestro desarrollo. La experiencia de nuestros guardias de seguridad, supervisores y equipos administrativos, junto con la incorporación de nuevos talentos, permite construir una organización más preparada, cercana y eficiente.

Modernización de procesos.

El crecimiento requiere procedimientos claros, trazables y capaces de adaptarse a nuevas exigencias. Por ello, impulsamos la revisión y mejora continua de nuestros procesos internos, fortaleciendo la coordinación entre áreas, la eficiencia administrativa y los mecanismos de seguimiento de nuestras operaciones.

Estos tres pilares no representan iniciativas aisladas. Constituyen una visión integrada que busca transformar el crecimiento de Grupo Safetec en una oportunidad permanente de mejora.

Nuestro compromiso: crecer manteniendo la calidad

Sabemos que uno de los principales desafíos de una empresa en expansión es mantener la cercanía con sus clientes y la calidad de su servicio. Por eso, nuestro objetivo no es solamente llegar a más instalaciones, sino asegurar que cada una cuente con equipos preparados, procesos eficientes, supervisión adecuada y el respaldo de una organización que continúa evolucionando. Porque crecer no es solo llegar a nuevos lugares. Es estar cada día mejor preparados para responder a quienes confían en nosotros.

Nuevas aperturas, nuevos desafíos

Grupo Safetec continúa fortaleciendo su presencia en el mercado de la seguridad privada, incorporando nuevas operaciones que reflejan la confianza de importantes organizaciones y consolidan una nueva etapa de crecimiento para Argento Seguridad.

Nuevos clientes, nuevas oportunidades La diversidad de instalaciones en las que desarrollamos nuestras funciones nos desafía a comprender diferentes realidades operacionales, identificar sus riesgos y responder a las exigencias particulares de cada entorno. En este escenario, la preparación de nuestros equipos adquiere especial rele-

Un compromiso que crece con nosotros La incorporación de nuevas instalaciones implica asumir mayores responsabilidades. Por eso, buscamos acompañar cada apertura con una gestión cercana, supervisión permanente y mecanismos de mejora continua que nos permitan responder oportunamente a los requerimientos de nuestros clientes. Nuestro desafío es continuar expandiéndonos sin perder aquello que consideramos esencial: la confianza, la calidad del servicio y el compromiso de nuestros equipos. Cada nueva apertura representa una oportunidad para seguir creciendo, fortalecer relaciones de largo plazo y demostrar, a través de nuestro trabajo, el compromiso que distingue a Argento Seguridad y Grupo Safetec.



vancia. Cada incorporación requiere planificación, selección de personal, coordinación operacional y una adecuada implementación de los procedimientos de seguridad. Nuestro objetivo es que cada servicio comience con una estructura sólida, responsabilidades definidas y una comunicación permanente entre nuestros equipos y las instalaciones donde desarrollamos nuestras funciones.

Las personas detrás de cada apertura El crecimiento de Argento Seguridad también se refleja en las oportunidades laborales que generamos y en la incorporación de nuevos profesionales a nuestra organización. Guardias de seguridad, supervisores y equipos de apoyo cumplen un rol fundamental en la puesta en marcha de cada operación. Su preparación, compromiso y capacidad de respuesta son esenciales para representar nuestros estándares de servicio. Por ello, continuamos fortaleciendo nuestros procesos de reclutamiento, selección, inducción y capacitación, entendiendo que la calidad de nuestros servicios comienza con las personas que forman parte de nuestra compañía.

Seguridad Expo 2026: conectando innovación, tecnología y personas

Grupo Safetec cerró una destacada participación como auspiciador oficial de Seguridad Expo 2026, consolidando un espacio de encuentro con autoridades, representantes de la industria, clientes y profesionales interesados en las nuevas soluciones que están transformando la seguridad en Chile. Entre el 8 y el 10 de septiembre, Metropolitano Santiago reunió a los principales actores del sector en una nueva edición de Seguridad Expo.

Durante las tres jornadas, nuestro stand B-104 se convirtió en un punto de encuentro para compartir experiencias, presentar soluciones tecnológicas y generar conversaciones sobre los desafíos actuales de la seguridad pública y privada. La gran participación y el interés de quienes nos visitaron reafirmaron nuestra convicción de que el futuro de la seguridad se construye mediante la colaboración, la innovación y la integración de nuevas capacidades.

Ciudad Segura: tecnología al servicio de las personas

Uno de los principales protagonistas de nuestra participación fue Ciudad Segura, una propuesta orientada a integrar tecnología, monitoreo y capacidad de respuesta para contribuir a la protección de las personas y los espacios públicos.

En este contexto, presentamos nuestro *Paradero Seguro*, una solución que busca transformar los espacios de espera del transporte público en puntos de asistencia conectados con una central de monitoreo.

Mediante herramientas de comunicación y alerta, esta propuesta permite que las personas puedan solicitar ayuda y establecer contacto con operadores preparados para evaluar situaciones y activar los protocolos correspondientes.

La experiencia permitió mostrar cómo la tecnología puede contribuir a una seguridad más cercana, preventiva y conectada con las necesidades de la comunidad.

Asimismo, nuestro Cubo de Realidad Virtual acercó a los visitantes a nuevas formas de experimentar y comprender la aplicación de soluciones tecnológicas en escenarios vinculados a la seguridad.

Visitas que enriquecieron nuestra participación

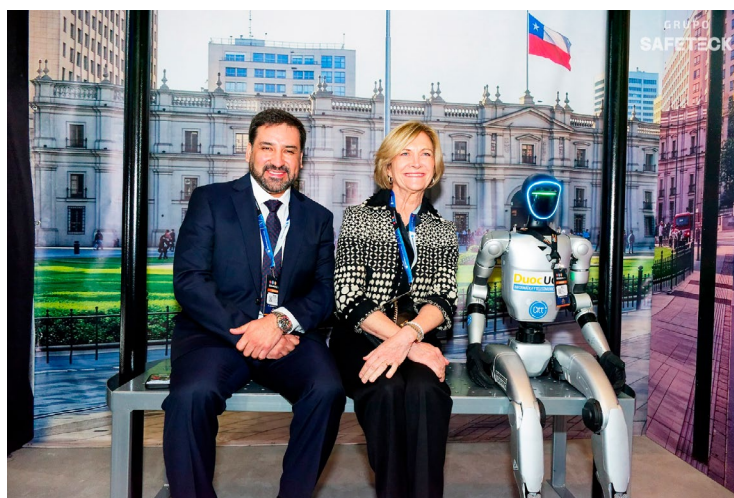
Uno de los momentos más significativos de nuestra presencia en Seguridad Expo 2026 fue recibir en nuestro stand a destacadas personalidades con una amplia trayectoria en la gestión pública, el liderazgo institucional y la seguridad de nuestro país.

Tuvimos el honor de contar con la visita de Evelyn Matthei, economista y reconocida figura de la vida pública nacional, quien ha desarrollado una extensa carrera como diputada, senadora, ministra del Trabajo y Previsión Social y alcaldesa de Providencia. Su experiencia en el ámbito legislativo, ministerial y municipal ha estado vinculada a importantes desafíos de gestión y desarrollo del país.

Asimismo, agradecemos especialmente la visita de Martín Arrau, ministro de Seguridad Pública, ingeniero civil industrial que ha ejercido relevantes responsabilidades públicas, entre ellas ser el primer intendente de la Región de Ñuble, integrante de la Convención Constitucional y ministro de Obras Públicas. Su trayectoria en la administración del Estado y su actual responsabilidad en materia de seguridad hicieron especialmente valiosa su presencia en nuestra exposición.

También recibimos con gran satisfacción a Rodrigo Delgado, ex-ministro del Interior y Seguridad Pública, psicólogo de profesión, quien cuenta con una destacada experiencia en gestión municipal tras desempeñarse durante tres periodos como alcalde de Estación Central. Además, presidió la Asociación de Municipalidades de Chile, antes de asumir una de las principales responsabilidades del Gobierno en materias de seguridad y coordinación institucional.

Agradecemos sinceramente el tiempo, la cercanía y el interés de cada una de estas personalidades, así como de todas las autoridades, clientes, aliados estratégicos y profesionales que nos acompañaron durante las tres jornadas.





Sebastián Sichel, El emplazamiento de Ñuñoa tras las inundaciones

El violento temporal que azotó recientemente a la Región Metropolitana no solo dejó calles anegadas y viviendas dañadas, sino que también desnudó la profunda brecha que existe entre la planificación centralizada y las capacidades reales de los gobiernos locales en la gestión de catástrofes. Con un balance que ya supera los 150 millones de pesos en gastos de emergencia este 2026, la comuna de Ñuñoa se vio obligada a decretar emergencia comunal para responder de forma inmediata a sus vecinos, recurriendo incluso al apoyo del sector privado y la minería ante la escasez de infraestructura fiscal. En esta entrevista, Sebastián Sichel, alcalde de Ñuñoa analiza con crudeza la "burocracia operativa" que frena las respuestas en terreno, la urgente necesidad de que el Ministerio de Hacienda priorice la inversión en obras de mitigación de fondo y los desafíos técnicos que enfrentan tanto la infraestructura pública como las nuevas construcciones inmobiliarias ante un cambio climático que ya es una realidad ineludible.

¿Qué porcentaje de las labores de emergencia de este temporal tuvo que costear Ñuñoa con fondos propios y qué impacto real tiene esto en el presupuesto municipal?

Este 2026 ya llevamos 150 millones de pesos gastados en emergencias. Hemos tenido apoyo del Ministerio de Vivienda y Bomberos, que hay que reconocer, pero una parte importante de la respuesta termina recayendo en el municipio. Tuvimos que decretar emergencia comunal para hacer gastos extraordinarios y acelerar el retiro del agua. El problema es que tenemos que responder con nuestro presupuesto, sin contar siempre con los equipos necesarios. Coordinar sirve, pero alguien tiene que llegar con la máquina y sacar el agua.

Usted mencionó que el SERVIU solo tenía cuatro motobombas para todo Chile. Ante la falta de respuesta fiscal, ¿planea Ñuñoa asociarse con otros municipios o con el sector privado para

adquirir equipamiento crítico de forma independiente?

Ya recurrimos a privados y pedimos ayuda a las mineras para conseguir motobombas de mayor capacidad. Decretamos la emergencia para poder comprar o arrendar equipos. Pero conseguir una bomba no puede depender de los contactos de un alcalde.

Lo acontecido dejó al descubierto lo que usted definió como "burocracia operativa para coordinar" en lugar de ejecutar. ¿Dispone su municipio de planes para estos eventos y qué trabas impiden ponerlos en marcha?

Podemos tener planes y reuniones de coordinación, pero si no tenemos motobombas, no podemos sacar el agua. Eso fue lo que nos pasó. Al final, la ejecución queda en manos del municipio, sin que tengamos los equipos suficientes. Por eso usamos el decreto de emergencia para disponer

de recursos extraordinarios. Los planes, a nivel de Estado, tienen que venir con maquinaria, personal y financiamiento.

Si pudiera reestructurar el sistema de coordinación de emergencias, ¿cuáles serían las medidas que cambiaría?

He planteado dos caminos: darle a Senapred capacidad para responder en terreno o entregarles a los municipios los recursos para hacerlo. Hoy se coordina desde arriba y abajo tenemos que salir a conseguir las máquinas. Cuando un edificio está inundado, la alerta no basta.

Usted ha emplazado al Ministerio de Hacienda a recortar gastos superfluos para invertir en contingencias ambientales. Si Hacienda no entrega fondos, ¿qué obras urgentes quedarán congeladas en Ñuñoa?

No tengo una lista de obras congeladas que anun-

ciar. Lo que he planteado es que Hacienda debe definir prioridades. Necesitamos inversión en contención de quebradas, reforestación y piscinas decantadoras. Son obras que requieren una mirada de ciudad y recursos del Estado central. Si seguimos respondiendo solamente cuando el agua ya entró a las casas, vamos a llegar tarde otra vez.

¿Está Ñuñoa preparada para resistir un evento similar en el corto plazo si el Gobierno central no modifica su estrategia de financiamiento?

Estamos reforzando la protección de los puntos críticos. Compramos cien barreras antiolas, que complementan el uso de más de mil sacos de arena. También hicimos aperturas en lomos de toro que dificultaban el paso del agua y estamos limpiando sumideros. Son medidas concretas para reducir el riesgo, pero he sido claro: son soluciones rápidas, no definitivas. Vamos a seguir trabajando para proteger a los vecinos, mientras insistimos en las inversiones de fondo.

¿Dispone su municipio de informes técnicos previos que demuestren que las obras de Metro agravaron las inundaciones?

Pedí esclarecer lo ocurrido en el paso Ñuble, donde colapsaron los colectores y había acumulación de basura. Cuestioné la mantención y anunciamos que exigiríamos explicaciones a Metro. Afirmar que sus obras agravaron las inundaciones es otra cosa. Para eso se necesita respaldo técnico.

Respecto de las querellas contra inmobiliarias, ¿cuántas empresas han sido fiscalizadas o sancionadas y qué penas o multas busca conseguir el municipio?

Vamos a perseguir responsabilidades y presentar acciones contra las inmobiliarias que tengan responsabilidad en lo ocurrido. Pero no voy a adelantar cifras de sanciones ni multas sin los antecedentes correspondientes. Denunciamos acumulación de basura y el colapso de los colectores; esos hechos hay que esclarecerlos.

Tras las inundaciones en edificios, ¿qué cambios deberían evaluarse en las exigencias constructivas, como sistemas de captación de agua, motobombas autónomas o generadores en azoteas?

Lo que vimos fueron edificios con los subterráneos inundados, vehículos bajo el agua y ascen-

sos sin funcionar. Eso obliga a mirar qué pasó con el diseño y la capacidad de respuesta de esos edificios. Sobre soluciones específicas, como la ubicación de generadores o los sistemas de bombeo, se necesita una evaluación técnica. Sería poco serio anunciar una exigencia sin ese análisis.

¿Cuál es la gran conclusión o reflexión que le deja este evento en su calidad de alcalde?

Que tenemos que prepararnos para un clima que cambió. No podemos seguir corriendo detrás de las emergencias. Los funcionarios municipales estuvieron en el agua, trabajando para ayudar a los vecinos, y ese esfuerzo necesita equipos e inversión que lo respalden. Tenemos que prevenir y hacer las obras, además de contar con capacidad para responder. La preocupación por el cambio climático tiene que verse en el presupuesto y en soluciones concretas para las familias.



“No podemos seguir corriendo detrás de las emergencias. Tenemos que prevenir y hacer las obras, además de contar con capacidad para responder.”

Sebastián Sichel, alcalde de Ñuñoa



ÑUÑOA
MEJOR CON TODOS
MUNICIPALIDAD



Escuela de Seguridad Municipal 2026

La importancia de profesionalizar a los equipos locales

Tras tres jornadas de capacitación, finalizó la Escuela de Seguridad Municipal 2026, organizada por la Asociación Chilena de Municipalidades (ACHM) junto a la Subsecretaría de Prevención del Delito, instancia que reunió a autoridades, especialistas y equipos municipales para fortalecer herramientas frente a los nuevos desafíos de seguridad en los territorios.

La Escuela se realizó en un momento especialmente relevante para los municipios. La nueva Ley de Seguridad Municipal ya entró en etapa de implementación, mientras su reglamento definitivo continúa en revisión. En ese escenario, la ACHM y la Subsecretaría de Prevención del Delito han trabajado de manera conjunta en los ajustes al texto reglamentario, buscando que su aplicación considere las distintas capacidades y realidades de las comunas del país.

El presidente de la ACHM y alcalde de Zapallar, Gustavo Alessandri, destacó la necesidad de profesionalizar a los equipos locales frente a fenómenos cada vez más complejos: *"Sabemos lo complejo que es dirigir una dirección de seguridad pública y enfrentar el narcotráfico, el microtráfico, el sicariato y el crimen organizado. Hoy nos estamos profesionalizando para entregar un mejor servicio en cada una de las comunas de Chile"*.

Por su parte, el presidente de la Comisión de Seguridad Ciudadana de la ACHM y alcalde de Lo Prado, Maximiliano Ríos, puso el énfasis en fortalecer la prevención y entregar a los municipios las condiciones necesarias para desarrollar esta tarea: *"Los municipios no podemos sacar adelante nuestra labor de prevención, recuperación de es-*

pacios y fiscalización si no hay recursos frescos. Si no hay prevención, lo más probable es que no haya seguridad".

La Escuela permitió avanzar en una mirada integral de la seguridad municipal, combinando prevención, apoyo a la persecución penal y reinserción social, junto con el fortalecimiento de la coordinación institucional y de las capacidades de quienes trabajan diariamente en los territorios.

Las principales conclusiones

1. Profesionalizar la seguridad municipal : Los municipios necesitan equipos mejor preparados

para enfrentar delitos cada vez más complejos, entre ellos narcotráfico, microtráfico, sicariato y crimen organizado. La capacitación debe traducirse en mayores capacidades operativas y de gestión local.

2. Reforzar la prevención y recuperar los espacios públicos: La prevención debe ocupar un lugar central en las políticas comunales. Esto implica intervenir en barrios vulnerables, recuperar espacios deteriorados y desarrollar acciones que reduzcan las oportunidades para la actividad delictual. La ACHM advirtió que estas tareas requieren recursos adicionales.



3. Fortalecer la coordinación entre instituciones: La seguridad municipal no puede abordarse de manera aislada. Se requiere coordinación entre municipios, policías, organismos de prevención, fiscalías y otras instituciones estatales, respetando las atribuciones de cada una.

4. Implementar adecuadamente la nueva Ley de Seguridad Municipal: La aplicación de la nueva normativa constituye un desafío institucional. La ACHM y la Subsecretaría de Prevención del Delito trabajaban en ajustes a su reglamento para considerar las distintas capacidades y realidades de las comunas. Por tanto, la implementación debe acompañarse de orientación jurídica y preparación operativa.

5. Incorporar la reinserción social a la estrategia de seguridad: El combate al delito debe combinar la acción contra quienes delinquen con oportunidades de reinserción. Durante la Escuela, este punto fue destacado por el alcalde de Coquimbo, Alí Manouchehri, como parte de una estrategia integral de seguridad.

6. Fortalecer el tejido social y la gobernanza local: La seguridad también depende de la capacidad de los municipios para comprender las dinámicas de sus barrios, prevenir la vulnerabilidad social y articular respuestas con la comunidad. El programa incluyó contenidos sobre gobernanza local, economías criminales en los barrios y prevención de la captación de personas por redes delictuales.

La Escuela deja planteada una orientación estratégica: el municipio debe consolidarse como un actor fundamental de la prevención y la gestión territorial de la seguridad, sin sustituir las funciones policiales ni la persecución penal.

Asimismo, la mirada internacional estuvo marcada por la magistral exposición de la vicerrectora de la Universidad Católica de Ávila (UCA) de España, Lourdes Miguel Sáez, quien detalló cómo ese país integró con éxito a las policías municipales tras casi cuatro décadas de diseño institucional.

Como muestra de este carácter proactivo, el director del CEGES de la AChM, Ricardo Yáñez Reveco General Director en retiro, selló un acuerdo de voluntades con la casa de estudios española para transferir buenas prácticas internacionales a nuestra realidad local.

De igual forma la actividad fue certificada por el Centro Integral de Seguridad de Universidad Finis Terrae.



El costo invisible de la dependencia tecnológica

En el ámbito de la defensa existe la tendencia a preferir la comodidad de la tecnología extranjera "llave en mano" frente al desafío de financiar y validar el talento local. En el ámbito de los sistemas de simulación herramientas donde hoy se definen desde los planes de evacuación ante catástrofes civiles hasta las tácticas de defensa del Estado, esta dependencia ya no es solo un problema de balanza comercial; es una vulnerabilidad geopolítica. Para abordar este interesante y apasionante tema, Revista Seguridad & Defensa, entrevistó Alejandro Cornejo, Jefe de Desarrollo Simuladores de Vuelo de LabMeter.

Para los tomadores de decisiones, tanto en los ministerios como en los directorios corporativos, la lógica al adquirir sistemas avanzados de simulación en el exterior parece irrefutable. "¿Para qué gastar años y millones en desarrollar un simulador local si podemos comprárselo a una transnacional que ya tiene el producto validado?".

El problema de este razonamiento es que confunde la estabilidad con la dependencia. Cuando Chile adquiere un sistema de simulación extranjero para el ámbito civil no solo compra tecnología, entrega sus datos y su autonomía.

Los algoritmos que deciden cómo reaccionar ante una crisis se programan bajo criterios globales, muchas veces desconectados de las realidades locales, y cualquier modificación sustancial requiere autorizaciones externas y costosos contratos de mantenimiento.

En términos simples ¿Cuál es el nivel tecnológico y profesional disponible en Chile para el desarrollo y fabricación de plataformas de simulación para el ámbito de la seguridad y la defensa?

Chile cuenta con profesionales y capacidades industriales para desarrollar simuladores de vuelo y otras plataformas de entrenamiento. Existen ex-

periencias concretas de integración de software, electrónica, cabinas y entornos visuales. El desafío es transformar esas capacidades en una actividad sostenida, con validación técnica, financiamiento y una demanda que permita conservar equipos especializados.

¿Cómo surge la idea de fabricar en nuestro país un completo simulador de un F16 y cuál fue la reacción de los profesionales que accedieron a este sistema?

La idea nos tomó sólo un par de segundos, fue muy espontánea. Una vez decididos mostrar nuestras capacidades en FIDAE 2024, nos preguntamos cuál sería la mejor estrategia. Ya habíamos desarrollado varios simuladores de aviación general, entonces fuimos al extremo opuesto y el mejor exponente en nuestro país es, sin duda, el F-16. El concepto detrás de esta idea fue mostrar la A a la Z. Demostrar que podemos fabricar simuladores básicos y avanzados. De un C-172 a un F-16 y por consecuencia, cualquiera que se encuentre entre medio.

Quedamos muy satisfechos por la respuesta del público en FIDAE 2024, nuestro stand logró llamar la atención de autoridades, oficiales de las distintas ramas de la defensa y público en ge-

neral. Estábamos ansiosos del feedback que pudiésemos recibir por parte de la Fuerza Aérea y resultó gratificante ver al piloto que realizó la demostración aérea, subirse a nuestro simulador y ejecutar la misma rutina que presentó minutos antes a los asistentes a la feria.

¿Existen en Chile fondos públicos actuales (como CORFO u otros) financian directamente el desarrollo de software complejo como los simuladores, y cuáles son sus principales limitantes?

Si existen herramientas públicas para financiar desarrollo local. CORFO, FONDEF y la ley de desarrollo I+D apoyan iniciativas, pero, lamentablemente para nosotros, los llamados buscan fomentar áreas que cumplan con ciertos criterios país y contribuyan en el desarrollo de ciertos objetivos en otras áreas como la agricultura, minería y servicios asociados con foco en tecnologías climáticas de agua, energía, sostenibilidad y descarbonización, donde nuestras propuestas de desarrollo no han tenido cabida.

¿Existen incentivos tributarios o subsidios para las empresas chilenas que deciden desarrollar tecnología local en lugar de importarla?

Desconozco la existencia de este tipo de incentivos, sin embargo y sin temor a equivocarme, dudo que existan debido a que nuestro sistema está mayormente enfocado en recaudar más que en facilitar este tipo de iniciativas.

¿De qué manera las bases de las licitaciones públicas chilenas (antigüedad exigida, boletas de garantía, certificaciones internacionales) excluyen de forma indirecta a los desarrolladores locales en materia de simulación?

Son un filtro importante de entrada que excluye a potenciales desarrolladores, pero, se entiendo que deben existir por resguardo de los fondos públicos.

En lo particular, estos aspectos no nos han afectado ni tampoco han impedido nuestra participación en diversos llamados a licitación. Sin embargo, lo que nos ha dejado un sentimiento amargo son los aspectos técnicos y limitación de recursos económicos de los mismos.

Es un sistema rígido, donde la institución solicitante indica lo que espera, en cuanto tiempo y el dinero que cuenta para ese llamado. Lamentablemente no deja espacio para el desarrollo local de tecnologías y profundización de los proyectos. Eso limita a importar componentes básicos mínimos y adquirir softwares existentes sin la posibilidad de entregar a nuestros pilotos una propuesta más inmersiva y que replique fielmente el material que se utiliza en la vida real limitándose a una "imitación genérica".

Personalmente creo que fuerzas armadas no han tomado el real valor de los beneficios que conlleva la utilización de estas potentes herramientas,

cosa que si ocurre en la industria civil, en la cual líneas aéreas invierten muchos recursos en el entrenamiento de sus pilotos, utilizando modernos simuladores de vuelo que deben cumplir un altos estándares para su certificación.

¿Se pondera correctamente en las decisiones de compra el costo a largo plazo del soporte técnico extranjero y la falta de soberanía de los datos frente a una solución nacional?

Esa es una respuesta muy difícil de responder. Como país contamos con las herramientas y el conocimiento para desarrollar este tipo de soluciones y entendemos de los beneficios que conlleva mantener una autonomía y control de la información sensible, sin embargo, para lograr un comportamiento real se debe contar con la data del fabricante, tablas específicas de performance de la aeronave simulada. Podemos hacer una copia visual exacta, pero, lo más importante es el comportamiento de la misma; y esa información normalmente el fabricante no la entrega. Por eso, es fundamental en una decisión de adquisición futura, poder "negociar" desde un principio la participación en estas áreas.

¿Existe un sesgo en la toma de decisiones ejecutivas que asume que la tecnología desarrollada en Chile es de inferior calidad o menos confiable que la norteamericana o europea?

No creo que pase por un sesgo. Pienso que es más un tema de inmediatez, comodidad y desconocimiento. Estos desarrollos requieren de mucho trabajo de investigación, diseño y pruebas funcionales. ¿Para que inventar algo que ya está hecho?, ¿cómo validamos que el modelo representado se comporte de la manera que la

aeronave real lo hace?, ¿Cómo accedemos a la información?

Muchas veces, la adquisición de aeronaves militares incluye dentro de sus paquetes de entrega, unidades de simulación. Eso deja fuera de participación a empresas como la nuestra.

¿Falta difusión y asociatividad entre las pocas empresas chilenas que sí desarrollan simulación avanzada, impidiendo la creación de un "sello de calidad" sectorial?

Definitivamente. El mercado local es muy pequeño y mantener el éxito de un negocio a través del tiempo es muy complejo. Puede que logres concretar una venta, pero, y luego qué...

Como las posibilidades son pocas, cada uno trata de "sobrevivir" defendiendo su espacio o diversificando sus actividades. Nosotros en LabMeter tomamos un camino distinto. Sabemos que podemos ser protagonistas y que nuestros productos son un real aporte al crecimiento de la industria aeronáutica con un fuerte foco en la seguridad de las operaciones.

No queremos esperar que lleguen a nosotros. Queremos entregar una oferta concreta, es por eso que el 2020 comenzamos a construir nuestros propios simuladores y el año pasado abrimos un centro de instrucción teórico/práctica basada en simuladores de vuelo.

¿Cómo afecta a la continuidad de operaciones críticas (como simulación de emergencias, entrenamiento militar o control de procesos mineros) el depender de actualizaciones, licencias y soporte técnico extranjero en un contexto de crisis global?

El año pasado nos tocó precisamente apoyar a una institución local en "levantar" uno de sus equipos que falló. La solución tomó casi tres meses, cosa que si en su momento se hubiese manejado un programa preventivo con soporte local se pudo haber evitado o solucionado en un par de días.

Al comprar soluciones cerradas, ¿cuánto conocimiento y datos estratégicos sobre procesos productivos chilenos se están entregando a empresas matrices en el exterior?

Comprar una plataforma cerrada no implica necesariamente entregar información al exterior, pero obliga a revisar telemetría, respaldos y accesos de soporte. Los escenarios, procedimientos y evaluaciones pueden revelar conocimiento sensible. El mayor peligro son develar estrategias, tipo de entrenamiento y resultado de los mismos. Qué hacemos, cómo y sus resultados.



Simulador de Cessna 172, desarrollado íntegramente sobre una plataforma Glass Cockpit, que integra tecnologías de vanguardia como G1000, GN750, GN650, G5 y Autopilot, proporcionando una experiencia de vuelo inmersiva, precisa y funcionalmente fiel a la aeronave real.

La soberanía requiere conocer qué información sale, quién puede usarla y con qué finalidad.

Respecto de la necesidad de renovar parte de la flota aérea la fuerza aérea se Chile se ha mencionado en más de una oportunidad al F 35. ¿Qué tan ventajoso desde el punto de vista económico saldría a desarrollar un sistema de simulación ese tipo en nuestro país? ¿Cree usted que dentro del ámbito de la negociación debiera estimularse desarrollo local mediante una alianza tecnológica?

Así como nosotros como nación debemos proteger nuestra información estratégica, las empresas también protegen su información sensible. Sea F-35, Eurofighter, Gripen, F-16 block 70 u otro, no creo se nos permita participar de este desarrollo, lo que si debiese negociarse es la participación en el proyecto. Adaptar la plataforma a nuestros requerimientos y permitir la administración y soporte local.

Aspectos relevantes a considerar

No estimular el desarrollo sistemas de simulación propios tiene un costo geopolítico silencioso pero devastador, que se manifiesta en tres frentes críticos:

- **Vulnerabilidad ante crisis globales:** En un mundo con cadenas de suministro inestables y tensiones internacionales en aumento, depender de licencias y soporte técnico extranjero es una ruleta rusa.

Si un proveedor decide revocar una licencia, suspender las actualizaciones por razones políticas o priorizar a su propio gobierno en una crisis, los sistemas de simulación chilenos quedarían ciegos u obsoletos de la noche a la mañana.

- **Marginalización en la toma de decisiones:** Un país que no domina la simulación no puede predecir de forma independiente. Queda supeditado a los escenarios de futuro que las potencias tecnológicas decidan mostrarle. En la mesa de la diplomacia y la disuasión internacional, quien no posee sus propios modelos predictivos es un actor secundario que solo puede reaccionar a los mapas diseñados por otros.

El talento que subsidia al primer mundo

La ironía de esta realidad es que Chile posee el capital humano. Las universidades chilenas y las nacientes industrias de desarrollo de software y videojuegos albergan a ingenieros, matemáticos y

programadores de clase mundial capaces de modelar la física de fluidos de un aluvión o la balística de un sistema de defensa.

Sin embargo, al no existir incentivos estatales robustos, bases de licitaciones públicas accesibles para empresas locales o capital de riesgo dispuesto a apostar por la soberanía tecnológica, el ecosistema se asfixia. La simulación no es un videojuego de alta gama; es el laboratorio del futuro de una nación. Romper la inercia de la dependencia tecnológica requiere entender que gastar en desarrollo local no es un lujo, sino un acto de defensa propia. Mientras Chile siga prefiriendo la simulación extranjera, seguirá entrenando a sus civiles y militares para proteger un país real usando las llaves de un mundo virtual que le pertenece a alguien más.

El desarrollo de una industria chilena de simuladores constituye un aspecto estratégico porque garantiza la autonomía operativa, optimiza el gasto público y actúa como un motor de innovación tecnológica transferible al sector civil.

A diferencia de la compra de sistemas cerrados, la simulación es un área donde un país mediano puede desarrollar propiedad intelectual clave, adaptada exactamente a sus necesidades y desafíos.



Alejandro Cornejo "Chile cuenta con profesionales y capacidades industriales para desarrollar simuladores de vuelo y otras plataformas de entrenamiento"

Su importancia se sintetiza en los siguientes pilares:

Ventajas estratégicas

- **Soberanía en el entrenamiento:** Depender de simuladores extranjeros implica que la doctrina de entrenamiento, los escenarios tácticos y la actualización de los sistemas quedan bajo el control del fabricante original. Una industria local permite modificar el software de manera inmediata para simular nuevas amenazas o integrar nuevos sensores.

- **Geografía y escenarios realistas:** Chile posee desafíos geográficos únicos (operaciones en la alta cordillera, climas extremos en la Antártica, canales australes y desierto de Atacama). Desarrollar simuladores propios —sean de vuelo, de navegación naval o de conducción de blindados— asegura que los modelos digitales de terreno y las variables meteorológicas repliquen con total fidelidad el teatro de operaciones real donde operará el personal chileno.

Eficiencia Presupuestaria y Reducción de Costos

- **Sustitución de importaciones tecnológicas:** La adquisición de simuladores de alta fidelidad en el mercado internacional demanda inversiones de decenas de millones de dólares, además de contratos de soporte técnico anuales en divisas extranjeras. Producir e integrar estos sistemas localmente retiene ese capital en la economía nacional.

- **Maximización del ciclo de vida del material real:** El entrenamiento en simuladores reduce drásticamente el desgaste del material de guerra real (combustible, horas de motor, munición y neumáticos), permitiendo concentrar el uso de los vehículos y aeronaves verdaderos estrictamente en operaciones reales o fases avanzadas de instrucción.

Desarrollo Tecnológico y Capacidad de Uso Dual

- **Efecto multiplicador en la industria local:** La construcción de un simulador moderno requiere la convergencia de múltiples disciplinas avanzadas: inteligencia artificial, robótica (sistemas de movimiento), ingeniería de software, óptica, ciberseguridad y manufactura avanzada.

- **Transferencia al sector civil:** Las capacidades tecnológicas que se desarrollan para simuladores de defensa tienen una aplicación directa e inmediata en sectores productivos clave para Chile. Por ejemplo:

- **Minería:** Simuladores para la operación segura

de camiones autónomos de extracción y maquinaria pesada.

- **Transporte y Logística:** Capacitación de conductores de trenes, camiones de carga de alta tonelaje o prácticos de puertos.

- **Gestión de Emergencias:** Entornos virtuales para entrenar a brigadistas en el combate de incendios forestales complejos o la coordinación de catástrofes naturales.

Fomento del Ecosistema de Innovación Nacional

Vinculación academia-industria: Este tipo de proyectos tecnológicos complejos impulsa consorcios donde participan universidades chilenas, centros de investigación, las empresas estratégicas de defensa (como ENAER, ASMAR o FAMAE) y empresas privadas del sector tecnológico. Esto permite retener el talento científico e ingenieril joven dentro del país, evitando la fuga de cerebros en áreas de software y alta tecnología.

El apoyo estratégico al desarrollo de una industria chilena de simuladores de vuelo es fundamental por razones de soberanía tecnológica, seguridad nacional y eficiencia económica.

A continuación, se detallan los principales factores estratégicos que justifican este impulso:

Desarrollo de un Ecosistema de Alta Tecnología (I+D+i)

Efecto multiplicador: La industria de simulación aérea tracciona otros sectores avanzados como el desarrollo de software, la inteligencia artificial, la robótica, la manufactura avanzada y la realidad virtual.

Capital humano avanzado: Fomenta la retención de talento local en ingeniería aeronáutica, electrónica y computación, creando empleos de alto valor agregado y alianzas entre universidades, el Estado y la empresa privada (como la Empresa Nacional de Aeronáutica (ENAER)).

Posicionamiento Hub Regional y Exportación

Liderazgo en LATAM: Chile cuenta con un prestigio de solidez institucional y aeronáutica. Consolidar esta industria permite exportar servicios de entrenamiento y tecnología de simulación a otros países de la región, convirtiendo al país en un polo tecnológico aeronáutico en América del Sur.

En el complejo escenario geopolítico actual, reducir la dependencia externa en materia de defensa se ha convertido en una prioridad crítica de seguridad estatal y soberanía nacional. La transición

hacia un orden multipolar, sumada al auge de amenazas híbridas y guerras comerciales, obliga a los Estados a priorizar la autonomía estratégica. La importancia de mitigar esta dependencia se fundamenta en factores clave que operan tanto a nivel global como regional.

Contexto Geopolítico Regional en América Latina

- **Carrera por la Renovación de Capacidades:** Diversos países de la región, como Argentina y Perú, han impulsado importantes programas de adquisición y renovación de su equipamiento militar (cazas F-16, buques, submarinos). En este contexto, mantener un equilibrio estratégico requiere de capacidades operativas continuas y confiables que no sufran interrupciones por decisiones de terceros países.

- **Nuevas Amenazas Transnacionales:** Los desafíos actuales de seguridad ya no se limitan a la disuasión vecinal tradicional, sino que abarcan el cibercrimen, el control del espacio marítimo ante flotas pesqueras irregulares y el combate al crimen organizado transnacional. Estas dinámicas exigen un desarrollo flexible y autónomo de tecnologías de vigilancia, inteligencia y comunicaciones adaptadas a las realidades locales.

- **Revalorización de Espacios Estratégicos:** Zonas como el Estrecho de Magallanes, los mares australes y la Antártica han cobrado un inmenso valor ante las fricciones en otras rutas globales. El control efectivo, patrullaje y conectividad de estas áreas estratégicas requieren de una base logística y un sostenimiento industrial nacional que

Mayores informaciones en:

<https://www.ifrlabtraining.cl/>

Email:
info@ifrlabtraining.cl

Teléfono:
+56 9 4211 7867



Proteger a quienes nos cuidan

Blindaje 360 Chile integra ingeniería, desarrollo y soluciones de protección para personas, accesos e instalaciones, con alternativas de venta y arriendo.

Cada mañana, alguien llega antes que nosotros. Revisa los ingresos, registra una visita, abre la barrera y permanece atento a lo que sucede. Conocemos su saludo y, muchas veces, su nombre. Pero ¿cuánto sabemos del lugar donde pasa su jornada? Dentro de ese puesto hay una persona con responsabilidades, preocupaciones y una familia que espera su regreso. Su trabajo contribuye a nuestra seguridad. Su propia protección también merece ocupar un lugar en las decisiones.

Desde esa mirada, Blindaje 360 Chile desarrolla soluciones para quienes vigilan, reciben y controlan accesos, junto con proyectos destinados a proteger instalaciones y puntos críticos.

¿Qué debemos preguntarnos sobre el lugar donde trabaja el personal de seguridad?

Primero, si permite realizar bien su trabajo: observar, comunicarse, verificar antecedentes, registrar movimientos y operar los equipos correspondientes.

Después viene una pregunta fundamental: ¿qué protección ofrece frente a las amenazas del lugar?

Una caseta puede resguardar del frío o la lluvia y, al mismo tiempo, carecer de resistencia balística o anti intrusión acreditada. Conocer sus materiales, diseño y respaldo técnico permite evaluar qué protección ofrece realmente.

¿Qué consecuencias puede tener una protección insuficiente?

Estamos hablando de riesgos que pueden afectar directamente la vida de las personas. Un disparo que alcance el puesto, una agresión o un ingreso forzado pueden provocar lesiones graves e incluso consecuencias fatales. En un asalto, el perso-

nal también puede ser reducido o maniatado.

La vulneración del puesto puede comprometer, además, el control de accesos y la seguridad de quienes están dentro de la instalación.

Por eso proponemos evaluar estas condiciones con anticipación. La protección física debe integrarse con las personas, los procedimientos y la capacidad de respuesta del recinto.

¿Todos los clientes necesitan el mismo tipo de blindaje?

Las necesidades son distintas y conviene explicarlas con claridad.

La protección balística responde a amenazas de proyectiles, según una configuración y un respaldo técnico determinados.

La protección anti intrusión busca dificultar o retardar el ingreso forzado. La protección antivandálica aborda determinados daños intencionales, como golpes o impactos.

Algunos proyectos requieren combinar estas prestaciones. Otros necesitan reforzar una puerta, una ventana o un muro existente. Comprender esa necesidad permite proponer una solución proporcional al riesgo.

¿Cómo transforma Blindaje 360 un requerimiento en una solución?

Comenzamos escuchando al cliente y comprendiendo la operación. Revisamos qué se necesita proteger, dónde se instalará la solución, quién la utilizará y qué tareas realizará.

Integramos ingeniería, diseño y desarrollo técnico para estudiar materiales, dimensiones, distribución, uniones, puertas, ventanas, fijaciones y montaje. La investigación y el desarrollo permiten evaluar alternativas y revisar configuraciones antes de incorporarlas a una propuesta.

Un ejemplo sencillo: una puerta resistente necesita también un marco, una cerradura y anclajes adecuados. Cada componente debe contribuir al objetivo de protección del conjunto.

¿Por qué son tan importantes la documentación y la trazabilidad?

Porque el cliente necesita conocer qué está recibiendo y qué respalda la protección ofrecida.

La documentación de origen permite identificar la procedencia del material. Los certificados del fabricante pueden informar sus características. Un informe de ensayo describe cómo se comportó una muestra bajo condiciones determinadas.

Cada documento cumple una función.

Contamos con informes de ensayos IDIC para configuraciones específicas de nuestros desarrollos modulares con placas de acero. Ese respaldo debe relacionarse con la configuración a la que corresponde.

La trazabilidad conecta los materiales y sus documentos con los procesos de fabricación y la solución entregada. Para quien compra, esto permite formular preguntas concretas: ¿qué material se utilizará?, ¿cómo se identificará?, ¿qué se ensayó y qué documentación acompañará la entrega?

¿Qué debe evaluar una empresa al elegir a su proveedor?

Además del precio y la apariencia, debe revisar las competencias de fabricación, el desarrollo técnico, los materiales identificados, los controles y la documentación aplicable.

Una estructura destinada a proteger personas exige que sus prestaciones puedan explicarse y respaldarse. Por eso es importante precisar el alcance de cualquier certificado, ensayo u homologación que se presente.

El acompañamiento local también aporta valor: facilita comprender el lugar, coordinar la instalación y definir el mantenimiento y la atención posterior según lo contratado.

¿Cómo se construye la confianza de los clientes?

Se construye desde la primera conversación y se confirma con el trabajo realizado.

Los clientes nos han confiado sus requerimientos y han desarrollado proyectos junto a nosotros. Esa confianza exige escuchar, estudiar, explicar las alternativas y cumplir el alcance acordado.

Para nosotros, la seriedad se expresa en decisiones concretas: una propuesta clara, responsabilidades definidas, respaldo técnico y atención al producto final. Cada proyecto es una oportunidad de demostrar esa forma de trabajar.

¿Qué soluciones y modalidades ofrece Blindaje 360 Chile?

Ofrecemos venta y arriendo de casetas blindadas fijas, móviles y en altura, con configuraciones según el requerimiento.

Las fijas permiten establecer puestos permanentes de vigilancia y control de accesos.

Las móviles responden a operaciones que necesitan cambiar la ubicación del puesto, considerando las condiciones de traslado e instalación.

Las soluciones en altura permiten estudiar una posición elevada de observación, según el entorno y el campo visual requerido.

También desarrollamos puertas, ventanas, vidrios, revestimientos y proyectos especiales, tanto para nuevas instalaciones como para necesidades de refuerzo en espacios existentes.

¿Cómo puede comenzar una empresa?

Con una necesidad y una conversación. Fotografías, medidas aproximadas o un croquis pueden ayudar a iniciar la evaluación.

A partir de esos antecedentes estudiamos la solución, su configuración y la modalidad de contratación, precisando equipamiento, documentación y servicios incluidos.

Quienes cuidan su instalación también necesitan protección. Conversemos sobre cómo incorporarla a su proyecto.

Orientación técnico-comercial



Equipo de Blindaje 360 Chile
Conversemos sobre su proyecto:
<https://blindaje-chile.cl/contacto/>





BLINDAJE 360 CHILE

NUEVA LÍNEA DE CASETAS BLINDADAS

Un nuevo estándar para la protección
de sus instalaciones

Modalidad venta / arriendo

VERSIONES MÓVILES
Y EN ALTURA



CARACTERÍSTICAS ESTÁNDAR



Protección configurable
balística, anti intrusión,
anti vandálica combinada
según proyecto



Altura interior
2,30 m.



Aislación térmica
incluida



Aire acondicionado
incluido.



Iluminación exterior
mínima 4 focos LED IP66



Ventanas:
según modelo unidades
de 1,50 m X 1,50 m.



Puerta blindada
apertura hacia afuera



Mirilla de puerta
0,50 m X 0,50 m.



Distribución de ventanas
y baño definidas en planos



5 MODELOS PARA CADA NECESIDAD



ESTÁNDAR



INTERMEDIA



GRANDE



VIP



PREMIUM

CERTIFICACIONES



Laboratorio IDIC
(Chile)



Bajo norma NIJ
(EE.UU.)



Normativas
sísmicas y
eléctricas
chilenas



Control de calidad
ISO 9001



UL 752



+569 82028639



contacto@blindaje-chile.cl



BLINDAJE 360 CHILE



La IA como instrumento para la predicción de desastres

Terremotos, incendios forestales, deslizamientos, inundaciones. Muchas de las catástrofes que han golpeado al mundo en los últimos meses han sido en América Latina. Son retos grandes para los sistemas de gestión de riesgo, especialmente si todavía los equipos humanos y la planeación territorial no están preparados para aprovechar lo que la tecnología puede prever. Para lograr que los algoritmos aporten valor real frente a estas emergencias, es indispensable integrar el análisis masivo de datos con el conocimiento técnico de cada disciplina. Así lo explica Raúl Reyero Díez, coordinador de la Maestría en Big Data y Ciencia de Datos de la Universidad Internacional de Valencia (VIU), perteneciente a la red de educación superior Planeta Formación y Universidades.

¿Cuáles considera que son las principales ventajas de la IA en comparación con los métodos meteorológicos y geológicos tradicionales de predicción?

La principal ventaja de la inteligencia artificial es su capacidad para analizar conjuntamente una cantidad y diversidad de datos que antes resultaba más difícil integrar. A las estaciones meteorológicas y los sismógrafos se suman satélites, radares, cámaras, imágenes térmicas y sensores que pueden actualizarse casi en tiempo real. La IA permite relacionar esas observaciones con registros históricos y actualizar las estimaciones a medida que llega nueva información.

Esto ayuda a reconocer patrones, estimar escenarios de riesgo y seguir la evolución de determinados fenómenos. Sin embargo, es importante entender que la IA no ofrece las mismas posibilidades en todos los casos. Su utilidad depende de las señales que produce cada fenómeno, de la cantidad y calidad de los datos disponibles y de cuánto conocemos sobre su comportamiento.

¿En qué tipo de catástrofe natural (sismos, huracanes, inundaciones, incendios) está demostrando la IA la mayor precisión de anticipación actualmente?

No todos los fenómenos ofrecen las mismas posibilidades de anticipación. La IA resulta especialmente útil en aquellos que dejan señales observables con cierta antelación y sobre los que existen datos abundantes, como las inundaciones, los huracanes y los incendios forestales.

En los huracanes, por ejemplo, se han producido avances importantes en la estimación de su trayectoria e intensidad. En las inundaciones es posible analizar variables como la lluvia, el caudal de los ríos y la humedad del suelo para estimar el riesgo. En los incendios, las imágenes térmicas y los datos meteorológicos permiten detectar focos y proyectar su propagación.

Los terremotos representan un desafío diferente, porque todavía no disponemos de señales previas suficientemente fiables para anticiparlos con precisión. En estos casos, la IA puede ayudar a detectar rápidamente que un sismo ya ha comenzado y emitir una alerta antes de que lleguen sus efectos más peligrosos. Por tanto, es importante distinguir entre anticipar un fenómeno antes de que ocurra y detectarlo tempranamente una vez iniciado.

Si miramos a corto plazo, ¿cómo transformará la IA los sistemas de alerta temprana para la población civil?

Uno de los cambios más importantes es la posibilidad de generar alertas a partir de información que llega casi en tiempo real y de combinar diferentes fuentes para reconocer situaciones de riesgo con mayor rapidez. Esto puede traducirse en avisos más oportunos y en una mejor estimación de las zonas que podrían verse afectadas.

Un ejemplo es el Sistema de Alertas de Terremotos de Android, que utiliza los acelerómetros de teléfonos móviles como una red distribuida de pequeños sismógrafos. Cuando numerosos dispositivos de una misma zona registran movimientos similares casi simultáneamente, el sistema puede identificar que se está produciendo un terremoto, estimar su localización y magnitud, y alertar a las personas que podrían verse afectadas.

En estos escenarios, unos segundos pueden marcar una diferencia importante. Sin embargo, la tecnología por sí sola no basta: las alertas deben indicar claramente qué hacer, estar respaldadas por protocolos de actuación y llegar también a quienes no tienen teléfonos modernos o conexiones estables. El objetivo no es solamente detectar el peligro, sino convertir esa información en acciones que ayuden a proteger vidas.

Aspectos Técnicos, Datos y Modelado

Los modelos de IA predictiva requieren enormes volúmenes de información. ¿Cómo se gestiona e integra la fusión de datos multi-fuente (imágenes satelitales, sensores de terreno e historial climático)?

La integración requiere trabajar con información de naturaleza muy diferente. Podemos tener imágenes satelitales, mediciones de sensores, mapas y series temporales, cada uno con características y frecuencias de actualización particulares. Algunos datos, como la pendiente del terreno o su geología, cambian poco; otros, como la humedad del suelo, evolucionan durante horas o días, mientras que ciertas mediciones llegan casi en tiempo real.

El reto consiste en interpretar correctamente qué mide cada fuente, cómo se obtiene la información y qué preguntas puede responder. Después, la IA permite analizar conjuntamente esas observaciones, compararlas con registros históricos y actualizar las estimaciones conforme llegan nuevos datos.

No se trata únicamente de reunir grandes cantidades de información. También es necesario comprender el fenómeno que se estudia para que el análisis produzca resultados útiles. La ciencia de datos aporta herramientas para encontrar relaciones complejas, pero debe complementarse con el conocimiento especializado de cada ámbito.

Esta combinación entre ciencia de datos y conocimiento del fenómeno es también la que trabajamos en la Maestría en Big Data y Ciencia de

Datos de VIU: los modelos solo resultan útiles cuando se comprende que representan los datos y se colabora con los especialistas de cada ámbito.

En fenómenos de evolución rápida como los terremotos o deslizamientos de tierra, ¿cómo logra la IA procesar datos en tiempo real para ganar segundos críticos?

En el caso de los terremotos, un ejemplo concreto es el uso de los acelerómetros incorporados en los teléfonos móviles. Estos dispositivos pueden detectar movimientos compatibles con las primeras ondas sísmicas y enviar una señal, junto con una ubicación aproximada, a los servidores del sistema de alertas.

Una señal aislada no basta para confirmar que se está produciendo un terremoto. Sin embargo, cuando numerosos teléfonos de una misma zona registran movimientos similares casi al mismo tiempo, el sistema puede identificar el evento, estimar su localización y magnitud, y emitir avisos a las zonas potencialmente afectadas.

La clave está en que la información transmitida por las redes de telecomunicaciones puede llegar antes que las ondas sísmicas más dañinas. El margen de anticipación puede ser muy pequeño, especialmente cerca del epicentro, pero esos segundos pueden permitir que una persona se aleje de una ventana, se ponga a cubierto o que una instalación preparada active sus protocolos automáticos de emergencia.

Es importante precisar que este sistema no predice el terremoto antes de que comience: lo detecta rápidamente y aprovecha la diferencia de tiempo

entre la transmisión de la información y la llegada de las ondas más peligrosas.

En los deslizamientos, el funcionamiento es diferente. Se vigilan la lluvia acumulada, la humedad del suelo, la deformación de la ladera, los cambios de inclinación o las imágenes de radar. La IA puede detectar una combinación anómala o una aceleración del movimiento, aunque no todos los deslizamientos producen señales suficientes. En este fenómeno a veces resulta más realista identificar zonas y periodos de alto riesgo.

Fiabilidad, Desafíos y Limitaciones

Un error de predicción puede costar vidas o generar pánico innecesario. ¿Cómo calibran los sistemas para equilibrar el riesgo entre falsos positivos (alarmas falsas) y falsos negativos (catástrofes no detectadas)?

El equilibrio depende de las consecuencias de cada error. En una zona muy expuesta, no detectar un evento grave suele ser más costoso que emitir una alerta que finalmente no se confirma; pero demasiadas falsas alarmas desgastan la confianza y pueden hacer que la población ignore el siguiente aviso.

Para calibrar el sistema no se busca únicamente el modelo que más veces acierta. Se analiza qué ocurre al modificar el umbral que activa la alerta: si se baja, se detectan más episodios peligrosos y puede ganarse tiempo, pero aumentan las falsas alarmas; si se sube, se reducen esos avisos innecesarios, aunque crece el riesgo de reaccionar tarde o dejar escapar un evento. Además, el umbral puede variar según la decisión: no exige el mismo



nivel de evidencia movilizar preventivamente a un equipo que cerrar una carretera u ordenar una evacuación.

Un ejemplo fácil de visualizar son las alertas meteorológicas por colores. Su nivel no depende solo de la probabilidad de que ocurra el fenómeno, sino también del impacto que podría causar. Un episodio poco probable puede justificar una alerta si sus consecuencias potenciales son muy graves, mientras que otro muy probable pero de impacto menor puede requerir únicamente vigilancia. Por eso, los umbrales se comprueban con episodios históricos, simulaciones y resultados reales, y se revisan a medida que el sistema acumula experiencia.

Los fenómenos climáticos extremos son cada vez más inéditos debido al cambio climático. ¿Cómo se entrena a una IA para predecir un desastre que nunca antes ha ocurrido o del cual no hay registros históricos?

Cuando no existen ejemplos históricos de un fenómeno, un modelo basado únicamente en datos tiene grandes dificultades para aprenderlo y, sobre todo, para demostrar que sus predicciones son fiables. Sin embargo, aunque no exista un precedente idéntico, sí puede haber información sobre sus componentes: temperaturas, precipitaciones, humedad del suelo, viento o comportamiento de los materiales.

Por eso, los registros disponibles se combinan con modelos físicos, proyecciones climáticas y escenarios generados mediante simulación. También pueden emplearse varios modelos para explorar distintas evoluciones posibles, en lugar de ofrecer una única predicción como si fuera segura.

El objetivo no es adivinar exactamente un desastre nunca observado, sino estimar escenarios posibles y cuantificar su incertidumbre. Para evaluar un modelo, hay que probarlo con episodios raros o territorios diferentes, y analizar hasta qué punto mantiene resultados coherentes cuando las condiciones se alejan de las habituales.

Implementación y Coordinación Humana

La IA predice, pero los humanos actúan. ¿Cómo debe integrarse la IA con los organismos de protección civil y los tomadores de decisiones políticos?

La IA puede anticipar escenarios, estimar riesgos y ofrecer información útil para la toma de decisiones, pero corresponde a las personas decidir qué hacer con esos resultados. Por eso, estos sistemas deben integrarse con protocolos públicos claros, mecanismos de coordinación y criterios de actuación definidos antes de que ocurra una emergencia.

También es fundamental distinguir entre una advertencia de riesgo y una orden de evacuación. Una alerta no debería limitarse a comunicar que existe una posible amenaza: debe ofrecer instrucciones concretas que la población pueda comprender y seguir. Esto exige que las autoridades preparen previamente los procedimientos de respuesta y que estos se comuniquen y practiquen con la ciudadanía.

Además, los sistemas deben contemplar que no todas las personas cuentan con teléfonos modernos, conexión estable o las mismas capacidades para reaccionar. Por ello, es necesario disponer de canales alternativos y considerar las necesidades de las personas mayores, las personas con

discapacidad y quienes viven en zonas con poca cobertura.

La tecnología nos puede ayudar a ganar segundos o mejorar la anticipación, pero para que se traduzca en vidas protegidas se necesitan coordinación institucional, comunicación clara y preparación previa.

Al cierre de la entrevista: Si pudiera definir el mayor obstáculo actual (financiero, técnico o ético) para que la IA prevenga por completo las muertes por desastres naturales, ¿cuál sería?

Es difícil quedarse con uno solo. Si tuviera que elegir, señalaría la distancia entre disponer de información útil y convertirla en una acción oportuna. Esa distancia combina factores financieros, técnicos, institucionales y sociales: sensores que faltan o no se mantienen, organismos que no comparten datos, protocolos que no se han ensayado o alertas que no llegan a quienes más las necesitan.

También conviene aclarar que prometer que la IA evitará por completo las muertes no sería realista. Siempre habrá fenómenos con muy poco margen de reacción, incertidumbre y personas expuestas. El objetivo razonable es aprovechar de la mejor manera posible los medios disponibles para reducir el número de víctimas.

Debemos preguntarnos si podemos mejorar los datos y los sistemas de observación, establecer criterios más claros para tomar decisiones, construir infraestructuras suficientemente resistentes y preparar a las personas para responder. La IA puede ayudar en todo ese proceso, pero no sustituye ninguno de esos elementos.

Raúl Reyero Díez,
coordinador de la Maestría en Big Data
y Ciencia de Datos de la Universidad Internacional de
Valencia (VIU), perteneciente a la red de educación
superior Planeta Formación y Universidades.





Radars meteorológicos

Tecnología clave para anticipar aluviones, inundaciones y fenómenos extremos en Chile

La necesidad de incorporar radares meteorológicos en Chile es un debate recurrente que se reactiva con fuerza cada vez que el país enfrenta catástrofes climáticas repentinas, como el aluvión en San Carlos de Apoquindo (Las Condes) o los tornados y trombas marinas que golpean la zona centro-sur (por ejemplo, en Puerto Varas o Biobío). A nivel continental, Chile se encuentra en una posición de rezago: junto con Bolivia, son los únicos países de Sudamérica que no cuentan con una red operativa de radares meteorológicos terrestres, contrastando con los más de 40 de Brasil, 16 de Argentina o 9 de Colombia. En la presente crónica abordamos las principales características y funcionalidades de los radares meteorológicos.

¿Qué son los radares meteorológicos y cómo funcionan?

Los radares meteorológicos son sistemas de observación atmosférica que utilizan ondas electromagnéticas para detectar y analizar fenómenos asociados a las precipitaciones. A diferencia de una estación meteorológica convencional, que mide las condiciones del tiempo en un punto determinado, un radar puede observar una extensa superficie y entregar información sobre la distribución, intensidad y desplazamiento de la lluvia y otras formas de precipitación.

Su funcionamiento consiste en emitir pulsos de energía electromagnética que interactúan con gotas de agua, cristales de hielo y partículas presentes en las nubes. Una parte de esa energía regresa al radar, donde es procesada para estimar las características de los sistemas meteorológicos observados.

Entre los principales datos que pueden proporcionar se encuentran:

- Intensidad de las precipitaciones: permite estimar dónde llueve y con qué intensidad.

- Distribución espacial de las lluvias: identifica las zonas afectadas por un sistema meteorológico.

- Movimiento de las tormentas: ayuda a determinar la dirección y velocidad de desplazamiento de las precipitaciones.

- Vientos dentro de las tormentas: determinados radares, mediante el efecto Doppler, pueden estimar la velocidad radial del viento y detectar patrones de circulación relevantes.

- Evolución de las células convectivas: facilita el seguimiento de tormentas que pueden generar lluvias intensas, granizo y, en determinadas condiciones, vientos destructivos.

La combinación de estos datos permite a los especialistas evaluar la evolución de un fenómeno meteorológico y mejorar los pronósticos de muy corto plazo.

¿Pueden detectar posibles aluviones e inundaciones?

Una de las aplicaciones más importantes de los radares meteorológicos es su contribución a la pre-

visión de desastres asociados a precipitaciones intensas.

Sin embargo, es fundamental establecer una distinción: el radar no detecta directamente un aluvión futuro, sino que permite identificar y seguir algunas de las condiciones meteorológicas que pueden desencadenarlo.

Cuando una tormenta descarga grandes cantidades de agua en poco tiempo sobre una cuenca, el suelo puede perder su capacidad de absorberla y aumentar rápidamente la escorrentía. Si el terreno presenta pendientes pronunciadas, material suelto o quebradas susceptibles, estas condiciones pueden favorecer aluviones, flujos de detritos y remociones en masa.

Mediante la observación continua de las precipitaciones, los radares pueden ayudar a identificar:

- Sectores donde se concentran lluvias de alta intensidad.
- Tormentas que avanzan hacia quebradas, valles o zonas pobladas.

- Sistemas de precipitación persistentes sobre cuencas hidrográficas.
- Cambios rápidos en la intensidad y extensión de las lluvias.
- Situaciones que, combinadas con información hidrológica y geológica, pueden elevar el riesgo de inundaciones o aluviones.

Esta información puede incorporarse a modelos de pronóstico, plataformas de monitoreo y protocolos de alerta temprana para que las autoridades evalúen la necesidad de adoptar medidas preventivas, como informar a la población, restringir accesos, preparar evacuaciones o movilizar equipos de emergencia.

La utilidad del radar aumenta cuando sus observaciones se integran con pluviómetros, estaciones hidrológicas, sensores de nivel de ríos, información sobre humedad del suelo y modelos de susceptibilidad a remociones en masa.

Un radar puede advertir que una tormenta peligrosa se aproxima a una zona vulnerable; la predicción de un aluvión específico requiere, además, conocer las condiciones del terreno y la respuesta de la cuenca.

¿Qué otros fenómenos pueden detectar?

Al detectar lluvias intensas sobre una cuenca, entregan información útil para anticipar posibles aumentos de escorrentía y caudales, especialmente cuando se combinan con sensores hidrológicos.

En condiciones adecuadas, ciertos patrones observados por radares pueden ayudar a detectar estructuras de tormentas compatibles con fenómenos severos. La confirmación requiere análisis especializado y, cuando corresponde, observaciones complementarias.

Es importante precisar que los radares meteorológicos no detectan directamente terremotos, incendios forestales ni deslizamientos de tierra. Para esos riesgos se necesitan otros sistemas de observación, aunque la información meteorológica puede ayudar a evaluar las condiciones que favorecen algunos de estos eventos.

Chile y la necesidad de fortalecer la vigilancia meteorológica

La geografía chilena hace especialmente relevante el desarrollo de capacidades avanzadas de observación atmosférica. El país combina una extensa costa, la cordillera de los Andes, zonas desérticas, valles densamente poblados y territorios donde las precipitaciones pueden desencadenar emergencias en periodos muy breves.

En las zonas cordilleranas y precordilleranas, las lluvias intensas sobre pendientes pronunciadas pueden generar flujos de barro, rocas y otros materiales. En las ciudades, las precipitaciones concentradas pueden sobrepasar la capacidad de los colectores de aguas lluvias, provocar inundaciones y afectar caminos, viviendas, hospitales y servicios esenciales. SENAPRED identifica las lluvias intensas y las características del terreno entre los factores relevantes para la ocurrencia de aluviones.

La urgencia de mejorar estas capacidades quedó de manifiesto con el reciente aluvión ocurrido en el sector de San Carlos de Apoquindo, en Las Condes, durante octubre de 2026. El episodio volvió a poner en el debate público la capacidad del país para observar oportunamente las precipitaciones intensas y convertir esa información en decisiones preventivas.

En este contexto, disponer de radares meteorológicos con cobertura adecuada permitiría complementar los pronósticos y las estaciones de medición existentes, especialmente en sectores donde las condiciones locales cambian rápidamente.

¿Qué beneficios concretos podría obtener el país?

Seguir el desplazamiento de una tormenta y reconocer núcleos de precipitación intensa puede aportar minutos valiosos para activar procedimientos preventivos.

Mejor protección de las ciudades.

La observación de lluvias intensas sobre áreas urbanas y cuencas cercanas ayudaría a focalizar el monitoreo en sectores vulnerables.

Protección de infraestructura crítica.

Hospitales, carreteras, puentes, aeropuertos, instalaciones mineras y redes de energía y telecomunicaciones podrían beneficiarse de alertas más precisas.

Apoyo a la gestión de emergencias.

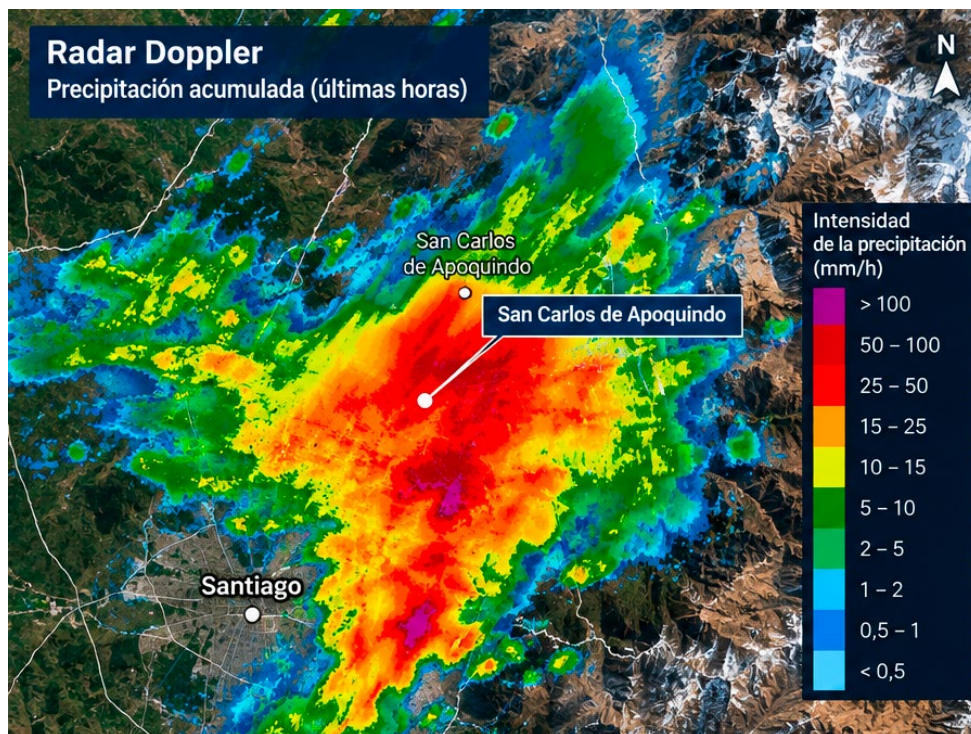
La información permitiría a los organismos responsables preparar equipos, coordinar recursos y evaluar evacuaciones preventivas cuando corresponda.

Mejora de los pronósticos de corto plazo.

Los datos del radar pueden incorporarse a modelos meteorológicos para actualizar el análisis de las condiciones

¿Cuánto tiempo antes puede advertir una emergencia?

No existe un tiempo de anticipación único. Un radar puede actualizar sus observaciones en intervalos de pocos minutos, según el equipo y su configuración, pero eso no significa que pueda predecir cualquier desastre con igual anticipación. En determinadas circunstancias, el seguimiento de una tormenta puede proporcionar entre varios minutos y decenas de minutos de información útil. El margen depende de la velocidad del fenómeno, la distancia al área amenazada, la topografía, la cobertura instrumental y la capacidad de interpretar los datos.



Por eso, la adquisición de equipos debe acompañarse de una estrategia integral que considere:

- Una red de radares con cobertura territorial y redundancia adecuadas.
- Estaciones pluviométricas y sensores de caudal y nivel de ríos.
- Modelos hidrológicos y mapas de susceptibilidad a aluviones.
- Integración de datos entre la Dirección Meteorológica de Chile, SENAPRED, SERNAGEOMIN, la Dirección General de Aguas y otros organismos competentes.
- Protocolos claros para transformar las observaciones en alertas oportunas y comprensibles para la población.

La tecnología, por sí sola, no garantiza que una emergencia pueda evitarse. Su valor depende de que la información llegue a tiempo a quienes deben tomar decisiones y a las comunidades expuestas.

Conclusión; observar antes para proteger mejor

Los radares meteorológicos representan una herramienta estratégica para modernizar la gestión del riesgo de desastres en Chile. Su capacidad para observar la distribución y evolución de las precipitaciones permite mejorar el conocimiento de fenómenos que pueden derivar en inundaciones, crecidas repentinas y aluviones.

El desafío no consiste únicamente en comprar equipos, sino en construir un sistema integrado de vigilancia, análisis, alerta y respuesta que funcione de manera coordinada y continua.

En un territorio donde las condiciones meteorológicas pueden cambiar con rapidez y las consecuencias de una emergencia pueden ser devastadoras, fortalecer la observación atmosférica significa avanzar desde una gestión centrada en reaccionar ante los desastres hacia otra que otorgue mayor prioridad a la prevención.

Porque en materia de emergencias, disponer de información precisa unos minutos antes puede marcar una diferencia decisiva para proteger vidas humanas.

San Carlos de Apoquindo: cuando las advertencias existen, pero la prevención no llega a tiempo

Estudios técnicos, informes de riesgo y proyectos de mitigación vuelven a estar bajo escrutinio tras el aluvión que afectó a Las Condes. La pregunta de fondo es por qué el conocimiento sobre una amenaza conocida no siempre se transforma oportunamente en protección para las personas.

El aluvión que golpeó San Carlos de Apoquindo el 8 de octubre de 2026 no solo dejó daños materiales y puso en evidencia la fuerza de la naturaleza. También abrió una interrogante incómoda para la gestión pública chilena: ¿qué sentido tiene invertir recursos en estudios de vulnerabilidad si sus conclusiones no se traducen a tiempo en medidas concretas?

En este caso, la discusión no parte de una sospecha genérica. Según antecedentes publicados por distintos medios, antes de la emergencia existían advertencias técnicas específicas sobre el riesgo aluvional en el sector.

En febrero de 2026, al menos tres informes habían sido remitidos a la Municipalidad de Las Condes, con antecedentes también en poder del Gobierno Regional Metropolitano y SENAPRED.

Entre las medidas sugeridas figuraban el catastro de viviendas expuestas, la información preventiva a la población, la señalización, la preparación de alertas de evacuación y las obras de mitigación.

A ello se sumó un documento municipal de junio de 2026 que advertía sobre el aumento del riesgo después de los incendios forestales que afectaron la zona cordillerana durante el verano. El informe planteaba la instalación de mallas para contener rocas y sedimentos.

Estos antecedentes cambian el sentido del debate. Ya no se trata solamente de determinar si era posible anticipar un fenómeno natural, sino de examinar qué se hizo con la información disponible, qué medidas se ejecutaron, cuáles quedaron pendientes y por qué.

El conocimiento que no se convierte en prevención Chile no carece de estudios sobre amenazas naturales, vulnerabilidad territorial y riesgos asociados a las remociones en masa. Universidades, organismos técnicos y entidades públicas han elaborado diagnósticos, mapas y evaluaciones destinados a identificar territorios expuestos a inundaciones, aluviones y deslizamientos.

Sin embargo, disponer de un informe no equivale a reducir el riesgo. Para que el conocimiento técnico produzca resultados, debe traducirse en decisiones administrativas, presupuesto, obras, fiscalización, planificación territorial y mecanismos de alerta que funcionen en la práctica.

Una investigación académica de la Universidad de Concepción, publicada en 2024, examinó estudios de riesgo asociados a planes reguladores comunales en Chile. Entre sus resultados identificó diferencias metodológicas importantes y una incorporación desigual de la susceptibilidad a remociones en masa en los instrumentos analiza-

dos. Se trata de una señal de que el país enfrenta desafíos que van más allá de un episodio puntual.

De los informes a las obras: el eslabón decisivo

Las obras de mitigación constituyen uno de los puntos más sensibles de esta discusión. Según información publicada se había proyectado la instalación de cinco barreras dinámicas para contener material descendente por las quebradas, con financiamiento anunciado de \$754 millones del Ministerio de Obras Públicas. Las estructuras todavía no estaban instaladas cuando ocurrió el aluvión.

La existencia de un proyecto no permite concluir, por sí sola, que su ejecución habría impedido completamente la emergencia. La eficacia de estas estructuras depende del diseño, la ubicación, las características de la cuenca y la magnitud del fenómeno. No obstante, el hecho de que las obras estuvieran pendientes obliga a examinar los plazos, las responsabilidades y las medidas transitorias que pudieron adoptarse mientras se esperaba su implementación.

La prevención tampoco se limita a construir barreras. Incluye mantener despejados los cauces cuando corresponda, identificar viviendas expuestas, establecer rutas de evacuación, informar a los residentes y asegurar que las alertas lleguen a quienes necesitan actuar.

En una emergencia, cada una de estas medidas puede contribuir a disminuir la exposición y las consecuencias del desastre.

La responsabilidad de transformar información en decisiones

La gestión del riesgo involucra a diversas instituciones, cada una dentro de sus atribuciones. Por eso, el análisis del caso debe determinar quién recibió cada advertencia, qué organismo debía actuar, qué decisiones se adoptaron y cuáles fueron las razones de los eventuales retrasos.

La Ley 21.364, que establece el Sistema Nacional de Prevención y Respuesta ante Desastres, contempla instrumentos como los mapas de amenaza y de riesgo, destinados a respaldar la gestión de emergencias y la planificación territorial.

El desafío es que estos instrumentos no se conviertan en documentos de consulta ocasional. Deben tener consecuencias operativas: orientar inversiones, establecer prioridades, influir en la planificación urbana y permitir que las autoridades actúen antes de que la amenaza se materialice.

También resulta indispensable garantizar la trazabilidad de las recomendaciones técnicas. Si un

organismo advierte sobre un riesgo y propone medidas, debe existir un mecanismo verificable para conocer si la advertencia fue recibida, quién asumió su seguimiento, qué recursos se asignaron y por qué una acción no se ejecutó dentro del plazo previsto.

Una lección que Chile no debería ignorar

El aluvión de San Carlos de Apoquindo debe abrir una revisión que vaya más allá de las circunstancias inmediatas de la emergencia. La discusión necesita abarcar la prevención, la coordinación institucional, la planificación territorial y la capacidad del Estado para transformar conocimiento científico en protección efectiva.

La pregunta no es únicamente cuántos informes se han elaborado o cuánto dinero se ha destinado a estudiar una amenaza. La pregunta decisiva es

qué cambió en el territorio después de que esos riesgos fueron identificados.

Porque cuando existen advertencias técnicas, proyectos pendientes y comunidades expuestas, la prevención deja de ser una declaración de buenas intenciones y se convierte en una obligación que debe poder evaluarse con hechos, plazos y resultados.

Chile necesita que sus estudios de vulnerabilidad dejen de ser el punto final de un proceso administrativo y se conviertan en el punto de partida de decisiones concretas. Un informe puede describir el peligro; solo una política de prevención ejecutada a tiempo puede contribuir a reducir sus consecuencias.



El proceso paso a paso

1 Emisión de pulsos



El radar emite pulsos de ondas electromagnéticas en distintas direcciones y a gran velocidad.

2 Interacción con la atmósfera



Las ondas chocan con gotas de agua, cristales de hielo y otras partículas presentes en las nubes y la precipitación.

3 Recepción de la señal



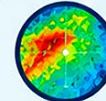
Parte de la energía regresa al radar (eco) y es captada por la antena.

4 Procesamiento de datos



El sistema analiza la señal para calcular la intensidad, la ubicación, el movimiento y otras características de la precipitación.

5 Generación de imágenes



Se obtienen mapas de reflectividad y otros productos que permiten identificar tormentas y seguir su evolución.

¿Qué datos entrega?



Intensidad de las precipitaciones

Permite estimar dónde llueve y con qué intensidad.



Distribución espacial

Muestra las zonas afectadas por el sistema.



Movimiento de las tormentas

Indica la dirección y velocidad de desplazamiento.



Vientos en la tormenta (efecto Doppler)

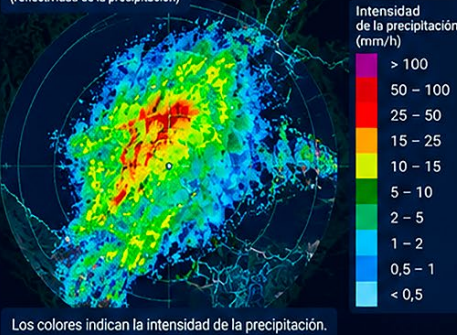
Puede estimar la velocidad del viento y detectar patrones de circulación.



Evolución de las células convectivas

Facilita el seguimiento de tormentas que pueden generar lluvias intensas, granizo y vientos fuertes.

Ejemplo de imagen de radar (reflectividad de la precipitación)



¿Para qué sirve?



Mejora los pronósticos y las alertas tempranas.



Contribuye a prevenir inundaciones, aluviones y remociones en masa.



Protege vidas humanas e infraestructura crítica.



Ayuda a la gestión del riesgo y la toma de decisiones.



En un país como Chile, donde las condiciones meteorológicas pueden cambiar rápidamente, los radares meteorológicos son una herramienta clave para anticipar y reducir el impacto de los fenómenos extremos.



Evidencia digital: Cuando el celular habla más que un testigo

No cabe duda de que, en la investigación de un homicidio, el trabajo en el sitio del suceso sigue siendo decisivo para reconstruir lo ocurrido y responsabilizar a los autores. Sin embargo, en un escenario donde la criminalidad se ha vuelto más rápida, más coordinada y más silenciosa, la evidencia digital ha adquirido un protagonismo que hace apenas unos años muchos subestimaban. Hoy, en numerosos casos, un teléfono puede decir más que un testigo, más que una declaración espontánea y, en ocasiones, más que varias horas de entrevistas.

El nuevo lenguaje de la criminalidad

La actividad delictual contemporánea dejó de depender únicamente de encuentros personales o llamadas directas, menos pensar en dejar rastro en algún documento físico. Las organizaciones criminales operan cada vez más a través de lo digital: dispositivos móviles, aplicaciones de mensajería, redes sociales, fotografías, videos y registros de ubicación que dejan trazas casi inevitables. En ese contexto, el teléfono celular se transformó en una verdadera extensión de la conducta humana: registra con quién hablamos, dónde estuvimos, qué buscamos, qué fotografiamos y, en muchos casos, qué ruta seguimos para llegar a un lugar.

Esa realidad cambia por completo la forma de investigar, ya no basta con recuperar vainillas, fijar huellas o levantar una evidencia biológica, también es necesario entender que parte importante de la verdad puede estar guardada en un aparato que cabe en el bolsillo. Un solo celular puede contener conversaciones, audios, videos, contactos, grupos cerrados, coordenadas, fotografías con metadatos y patrones de uso que revelan vínculos, jerarquías y decisiones previas al hecho investigado, ya sea del occiso foco de nuestra investigación, blancos investigativos o imputados.

Además, este tipo de evidencia tiene un valor especialmente alto cuando el entorno es hostil o cuando la víctima pertenece a contextos donde el

miedo impide declarar. En esos casos, el archivo digital se convierte en una fuente de información más estable que el testimonio humano, porque no cambia de versión, no se intimida y no intenta favorecer a nadie.

Lo que el teléfono no puede ocultar

En los homicidios, y especialmente en aquellos vinculados al crimen organizado, la evidencia digital suele ofrecer una ventaja decisiva: no depende del miedo ni de la lealtad de los involucrados. Un testigo puede callar, contradecirse, retractarse o mentir, en cambio, un registro de geolocalización, una comunicación interceptada legalmente, una imagen captada por una cámara o un respaldo extraído de un dispositivo mantiene su valor mientras haya sido obtenido, preservado y analizado correctamente.

Ahí radica una de las transformaciones más profundas en la investigación penal actual. El celular puede ubicar a una persona en una escena, conectar a varios sujetos entre sí, mostrar preparativos previos, confirmar una huida o incluso destruir una coartada aparentemente sólida. En delitos de alta complejidad, la evidencia digital no es complementaria, muchas veces es el eje que permite comprender la dinámica completa del hecho.

En paralelo, esta capacidad investigativa no surge de manera improvisada, sino del desarrollo de

tecnologías forenses especializadas que hoy son parte del trabajo pericial en distintos países.

Existen plataformas reconocidas internacionalmente, como Cellebrite, MSAB y Oxygen Forensics, diseñadas para la extracción, preservación y análisis de información contenida en teléfonos celulares y otros dispositivos móviles. Estas soluciones permiten recuperar chats, registros de llamadas, fotografías, videos, contactos, historiales de ubicación, archivos borrados y distintos metadatos, incluso en casos donde existen bloqueos, cifrado o eliminación parcial de contenido. Por otra parte, el desarrollo de software de análisis ya es una realidad, que permita con módulos de inteligencia artificial, resumir varios cientos de páginas de información y permitir modelar las vinculaciones digitales de manera rápida.

Pero el verdadero valor no está solo en “abrir y analizar” un dispositivo, sino en hacerlo con trazabilidad técnica, respetando la integridad de la información y generando reportes que puedan ser defendidos con seriedad en sede judicial. En otras palabras, la extracción forense de un teléfono no consiste simplemente en acceder a datos, sino en convertir esos datos en evidencia útil, verificable y procesalmente válida, mediante protocolos estandarizados y el uso correcto de la cadena de custodia.

La gran virtud de la evidencia digital es que per-

mite reconstruir tiempos, recorridos y relaciones. La gran dificultad es que puede perder valor con facilidad si se manipula mal, si se extrae sin el protocolo adecuado o si no se conserva la integridad de los datos. En otras palabras, la tecnología ayuda, pero no reemplaza el criterio investigativo.

No todo lo que aparece en un teléfono es útil por sí mismo. El verdadero desafío está en interpretar los datos en contexto. Una ubicación aislada no prueba participación, una conversación suelta no siempre revela intención y una fotografía no necesariamente demuestra presencia en el lugar de los hechos. Por eso, la evidencia digital requiere peritos o funcionarios especializados capaces de ordenar, comparar y correlacionar información con otras fuentes de prueba.

En la práctica, eso significa vincular registros telefónicos con evidencia balística, cámaras de seguridad, declaraciones, informes de autopsia y análisis del sitio del suceso. Solo cuando esas piezas se conectan correctamente aparece el relato completo. Y ese relato, en muchos casos, permite descubrir que lo que parecía un hecho aislado era en realidad parte de una secuencia más amplia: vigilancia previa, coordinación entre sujetos, seguimiento de la víctima, ejecución del hecho y posterior ocultamiento. Lo anterior, no es trabajo simple de una persona, es necesaria la conformación de equipos multidisciplinarios investigativos, que permitan integrar los distintos conocimientos forenses a partir de esta evidencia digital.

Una prueba que exige velocidad y método

En los delitos violentos, especialmente en aquellos vinculados al crimen organizado, el tiempo juega en contra de la investigación. Los dispositivos pueden ser apagados, reiniciados, borrados o encriptados (incluso de manera remota), las cámaras pueden sobrescribirse, las publicaciones pueden eliminarse y los registros de conexión pueden perderse si no se solicitan oportunamente. Por eso, la reacción temprana es fundamental.

El problema no es solo técnico, sino también institucional. A menudo, la evidencia digital está repartida entre distintas fuentes: teléfonos personales, sistemas privados de informática, antenas de telefonía, plataformas de mensajería, redes sociales y bases de datos públicas. Si no existe coordinación entre policías, fiscalía, peritos y eventualmente actores privados, la oportunidad se pierde. Y cuando se pierde, el caso queda más expuesto a la impunidad.

Por eso es que la evidencia digital no debe verse como un complemento moderno o como una moda forense. Es una necesidad investigativa. En muchos casos, representa la diferencia entre una hipótesis débil y una imputación sólida. Entre una sospecha y una reconstrucción probada. Entre una intuición y una verdad judicialmente verificable.

El valor de las cámaras y los registros privados

Los registros de vigilancia de las cámaras de seguridad es otro aspecto que lleva a continuo debate y como evidencia digital deber ser tratada correctamente. Es por esto que es un aspecto que todavía no se comprende del todo en la ciudadanía como aporte de los registros privados. Muchas veces, el ciudadano piensa que solo sirven las cámaras municipales o las imágenes de espacios públicos. Pero la verdad es que la tienda de la esquina, el edificio residencial, el local comercial o incluso una vivienda particular pueden aportar la pieza que faltaba.

Una secuencia de video puede confirmar la llegada de un vehículo, el ingreso de una persona, una ruta de escape o un punto de encuentro. Puede también permitir contrastar horarios, verificar vestimentas, identificar acompañantes y establecer conexiones que no aparecen en ningún testimonio, lo que hoy forman parte natural de la vida cotidiana, puede formar parte de la investigación penal.

Esto abre también una reflexión ciudadana importante: colaborar con la entrega de información en tiempo oportuno puede ayudar a esclarecer hechos graves y evitar que el miedo termine favoreciendo al delincuente. La evidencia digital, bien obtenida, puede dar respuestas donde el silencio solo deja más incertidumbre.

La verdad ya no siempre está en voz alta

Durante mucho tiempo se pensó que la prueba más fuerte era la palabra del testigo. Hoy, en cambio, hay casos en que el verdadero relato está en un teléfono abandonado o en una cámara de seguridad que, analizado correctamente, termina siendo decisivo. Eso no significa que el testimonio humano haya perdido valor, sino que la investigación moderna exige entender que la verdad ya no siempre se expresa en voz alta.

En un país donde el crimen organizado busca adaptarse más rápido que las instituciones, el desafío para la investigación penal es no quedarse atrás. Y en ese desafío, la evidencia digital ocupa un lugar central. No solo porque ayuda a identificar autores, sino porque permite comprender la lógica del delito, sus vínculos y su forma de operar.

Por eso, cuando hoy se piensa en una escena de crimen, también se debe pensar en el teléfono que alguien dejó atrás, en la cámara que registró un movimiento sospechoso, en el mensaje enviado minutos antes del hecho y en todo lo que un dispositivo aparentemente simple puede revelar.

Porque en la investigación penal contemporánea, muchas veces la evidencia digital habla más que un testigo asustado. Y en esa voz silenciosa puede estar la diferencia entre la impunidad y la justicia.



Carlos Gálvez Madrid
Docente

Master en Ciencias Forenses / Universidad de Valencia



Crimen invisible en América Latina

Del crimen jerárquico a las redes líquidas

La globalización suele describirse como la intensificación de los intercambios, la conectividad y la circulación transfronteriza de bienes, capitales e información. Sin embargo, esos mismos procesos facilitan una «globalización oscura»: la expansión de actividades ilícitas que aprovechan infraestructuras legales, diferencias regulatorias y tecnologías de comunicación. En América Latina, este fenómeno no se expresa únicamente en organizaciones jerárquicas que controlan territorios, sino también en redes capaces de contratar servicios, formar alianzas temporales y reconfigurarse cuando cambia el entorno operativo. La fragmentación, por tanto, no equivale necesariamente a una pérdida de capacidad criminal; puede constituir una adaptación que dispersa riesgos y dificulta la atribución de responsabilidades.

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, Convención de Palermo ofrece un marco jurídico compatible con esa diversidad organizativa. No define la delincuencia organizada como una estructura única. Define, en cambio, al grupo delictivo organizado como un grupo estructurado de tres o más personas, existente durante cierto tiempo, que actúa concertadamente para cometer delitos graves con el fin de obtener un beneficio material. La noción de “grupo estructurado” no exige jerarquía formal, funciones permanentes ni continuidad de sus integrantes. Además, la Convención entiende la transnacionalidad de manera amplia: incluye delitos cometidos en más de un Estado, planificados o dirigidos desde otro, vinculados a grupos activos en varios países o con efectos sustanciales en el extranjero.

Este marco permite analizar redes flexibles sin reducirlas a una oposición simplista entre carteles centralizados y bandas locales. Una organización puede combinar dirección estratégica, intermediarios especializados y células autónomas. En esas configuraciones, actores distintos cumplen

funciones de transporte, protección, corrupción, transferencia financiera o acceso a mercados. La cooperación puede ser recurrente sin implicar una cadena de mando integrada. La liquidez de las redes describe precisamente esta capacidad de cambiar de socio, ruta y método, y no debe confundirse con la ausencia de organización.

El Índice Global de Delincuencia Organizada de la Global Initiative Against Transnational Organized Crime (GI-TOC) contribuye a observar ese ecosistema al reunir indicadores de mercados criminales, actores y resiliencia estatal. Sus puntuaciones, de 1 a 10, son estimaciones analíticas comparativas elaboradas mediante evaluación experta, no conteos directos de delitos ni mediciones exactas de ingresos. La edición de 2023 incorporó nuevos mercados y actores, entre ellos delitos financieros, cibercriminosos dependientes y actores del sector privado. La edición 2025 permite, con las cautelas metodológicas pertinentes, observar tendencias recientes.

El desplazamiento de los mercados territoriales hacia los delitos financieros y cibernéticos

La expansión de mercados criminales no implica la sustitución de la violencia territorial por modalidades digitales o financieras. Más bien, los mercados visibles y los menos visibles se articulan. El tráfico de drogas puede depender del control de rutas, puertos y barrios, mientras que las ganancias se mueven por esquemas de fraude, evasión, corrupción y operaciones empresariales. La violencia conserva una función de coerción y control; la infraestructura financiera y digital facilita el ocultamiento, la conversión y la circulación del beneficio.

En 2023, el Índice de GI-TOC asignó al mercado global de delitos financieros una puntuación de 5,98 sobre 10 y lo identificó como el más extendido entre los mercados evaluados. La entidad advirtió que esta medición se introducía por primera vez, por lo que no existía una línea de base comparable para estimar su crecimiento desde una edición anterior. Para los cibercriminosos dependientes, la puntuación global fue 4,55. Estos comprenden ataques que requieren tecnologías de información, como malware, intrusiones, ataques de denegación de servicio y ransomware.

La edición 2025 muestra una puntuación de 6,21 para delitos financieros, un aumento de 0,24 puntos respecto de 2023, y de 4,65 para ciberdelitos dependientes, 0,10 puntos más. El crecimiento de ambos indicadores confirma la relevancia analítica de estos mercados, aunque no demuestra por sí solo que todos los delitos se hayan trasladado al entorno digital. La categoría financiera abarca formas de pérdida económica para el Estado, entidades o personas como fraude, malversación y evasión, mientras que el lavado de activos no se incluye automáticamente en ella cuando corresponde a otro mercado o función criminal. Por ello, conviene distinguir entre el delito que genera el producto ilícito y los mecanismos posteriores que lo ocultan o integran a la economía legal.

La invisibilidad del daño tiene consecuencias políticas. Los mercados financieros y digitales pueden afectar a víctimas dispersas y producir perjuicios acumulativos difíciles de atribuir a una organización concreta. A su vez, sus operaciones pueden apoyarse en sistemas ordinarios de pago, sociedades y servicios tecnológicos. La visibilidad estadística menor no implica menor impacto social ni menor conexión con mercados violentos. La tesis central es que la digitalización amplía el repertorio operativo criminal, mientras la integración financiera reduce la distancia entre economías ilícitas y circuitos legales.

Actores estatales corruptos y empresas legales como facilitadores del ecosistema criminal

Las redes transnacionales requieren más que ejecutores criminales. Su capacidad depende

de puntos de acceso a la economía legal y de la previsibilidad que ofrecen determinados servicios: transporte, almacenamiento, gestión de carga, asesoría jurídica, contabilidad, finanzas y tecnología. En puertos y aduanas, por ejemplo, la vulnerabilidad no reside necesariamente en la infraestructura física, sino en la posibilidad de manipular inspecciones, documentos, horarios o registros. Bufetes y proveedores profesionales pueden ser explotados para constituir sociedades, ocultar beneficiarios o interponer transacciones. Estas prácticas deben analizarse con precisión: la existencia de una empresa o profesión en una cadena ilícita no prueba por sí misma complicidad deliberada; la cooptación exige establecer conocimiento, intención, beneficio o negligencia según el marco jurídico aplicable.

La Convención de Palermo reconoce la corrupción y el blanqueo del producto del delito como componentes transversales que protegen las operaciones criminales. Este enfoque desplaza la atención desde la captura de individuos hacia las condiciones institucionales que permiten operar con impunidad. La corrupción puede reducir la probabilidad de inspección o sanción; las redes comerciales, por su parte, ofrecen cobertura y escala. La interacción entre ambas crea una zona gris en la que las decisiones administrativas y corporativas producen ventajas criminales sin que exista necesariamente una organización única que coordine todas las etapas.

El Índice de GI-TOC incorporó en 2023 a los actores del sector privado como categoría de actores criminales, reconociendo que pueden participar directamente en delitos o facilitar

actividades ilícitas. En 2025, la GI-TOC destaca su papel creciente en logística, finanzas y tecnología. El dato refuerza una lectura relacional; el sector privado no es solo víctima de extorsión o infiltración, sino también un ámbito donde ciertos actores pueden intervenir en la expansión criminal. Esto no justifica generalizaciones contra empresas o profesiones; subraya la necesidad de identificar riesgos concretos en cadenas de suministro y servicios profesionales.

La respuesta regulatoria debe equilibrar eficacia y garantías. La debida diligencia sobre clientes y proveedores, la identificación de beneficiarios finales, auditorías independientes, controles de integridad en contratación pública y canales protegidos para denunciantes pueden elevar los costos de cooptación. Sin embargo, los controles formales pierden eficacia cuando las instituciones carecen de autonomía, capacidad técnica o protección frente a represalias. La gobernanza debe, por ello, tratar la corrupción como un riesgo estructural que atraviesa las cadenas logísticas y financieras, y no como una desviación excepcional atribuible únicamente a funcionarios individuales.

Sudamérica como centro de exportación y la fragmentación de bandas

Sudamérica ocupa una posición estratégica en las cadenas globales de cocaína y en las rutas que conectan áreas de producción, tránsito y consumo. Su relevancia no se explica solo por la geografía, sino por la combinación de infraestructura portuaria, redes de transporte, corredores fronterizos y mercados de servicios legales.



La expansión de contenedores y el volumen del comercio marítimo dificultan la inspección exhaustiva de carga. La misma conectividad que facilita exportaciones legales abre oportunidades para ocultar mercancías ilícitas, sin que ello convierta a los puertos en espacios homogéneamente capturados.

InSight Crime documenta que las redes ecuatorianas y sus socios extranjeros han empleado un modelo de subcontratación: intermediarios rotativos cooperan con bandas locales especializadas en transporte, uso de lanchas, vuelos clandestinos o contaminación de contenedores. Los vínculos pueden ser temporales y funcionales, lo que complica la investigación basada exclusivamente en organigramas estables. La fuente también advierte que las alianzas entre grupos ecuatorianos han cambiado con rapidez y suelen responder a competencia interna por rutas, redes y reconocimiento, antes que a una coordinación externa única.

El Observatorio Ecuatoriano de Crimen Organizado (OECO), en su caracterización nacional, analiza las cadenas de valor de los mercados ilícitos y señala que la atomización de organizaciones se intensificó desde la pandemia, especialmente en disputas por control territorial, corredores de tráfico y plazas de microtráfico en ciudades portuarias. El informe se basa en talleres, entrevistas a representantes estatales y trabajo de campo provincial; su valor reside en conectar dinámicas criminales con condiciones territoriales e institucionales específicas. El narcotráfico aparece vinculado a otras actividades, entre ellas tráfico de armas e hidrocarburos, corrupción y lavado de activos.

La fragmentación de bandas puede generar una paradoja de seguridad. La detención o muerte de líderes y la intervención sobre centros de mando pueden debilitar estructuras verticales, pero también liberar facciones locales, reducir la disciplina interna y multiplicar disputas por rutas y rentas. InSight Crime observa que, tras la intervención estatal en el sistema penitenciario ecuatoriano, las relaciones entre prisiones y bandas callejeras se volvieron más horizontales; grupos locales ganaron autonomía y las alianzas se hicieron más fluidas. La evidencia no implica que toda operación coercitiva produzca fragmentación, pero sí muestra que la evaluación de resultados debe considerar los efectos de segundo orden sobre la gobernanza criminal.

La infraestructura logística es, en consecuencia, un objeto de competencia y una fuente de renta. El caso de Posorja, descrito por InSight Crime, ilustra cómo un puerto de aguas profundas puede modificar las dinámicas criminales locales y atraer disputas por el acceso a la cadena de exportación. La fragmentación no elimina la inserción transnacional, puede trasladar funciones a células y subcontratistas que mantienen conexiones con intermediarios extranjeros.

Del enfoque punitivo al debilitamiento de los flujos financieros

El análisis de la globalización oscura exige superar la imagen de organizaciones criminales como entidades compactas, territorialmente delimitadas y encabezadas por una jerarquía estable. El marco de Palermo permite reconocer grupos de estructura flexible; GITOC muestra la importancia creciente de mercados financieros y cibernéticos; InSight Crime describe redes de cooperación y subcontratación que se adaptan a presiones policiales; OECO evidencia cómo la atomización reconfigura el control territorial y logístico en Ecuador. En conjunto, estas fuentes apuntan a ecosistemas criminales donde actores legales e ilegales interactúan en distintas escalas.

La primacía de respuestas punitivas centradas en capturas y despliegues coercitivos presenta límites cuando no reduce la capacidad de reemplazo, financiamiento y acceso logístico de las redes. Puede ser necesaria para proteger a la

población y restablecer el control estatal, pero su éxito no debe medirse solo por detenciones o incautaciones inmediatas. Debe evaluarse si disminuye la violencia, interrumpe las rentas, mejora la integridad institucional y evita que facciones autónomas ocupen los espacios liberados.

La premisa “sigue el dinero” conserva valor si se entiende como una estrategia institucional, no como consigna. Requiere inteligencia financiera compartida, cooperación judicial transfronteriza, supervisión de beneficiarios reales, análisis de riesgos en puertos y cadenas de suministro, y persecución efectiva de corrupción y facilitación empresarial ilícita. También exige salvaguardas: la cooperación internacional debe respetar garantías procesales, privacidad y proporcionalidad, mientras las entidades privadas han de contar con obligaciones claras y mecanismos de supervisión verificables.

La gobernanza multilateral debe acompañar estas medidas con prevención de la violencia, fortalecimiento de fiscalías y protección de comunidades expuestas a extorsión y reclutamiento. El objetivo no es solo desarticular organizaciones identificables, sino elevar de forma sostenida los costos de operar, transferir ganancias y capturar instituciones. En ese sentido, reducir la conectividad entre mercados ilícitos y sistemas legales constituye una condición central para limitar la resiliencia criminal y recuperar la autoridad pública en América Latina.



Autor: Andruy X. Cardona Marin
Docente de la cátedra de sociología criminal
Escuela Nacional de Criminalística y Ciencias Forenses
Medellín, Colombia.



De la operación al directorio: Cómo transformar evidencias en inteligencia para la gestión de seguridad

La Gestión Operacional Orientada por Evidencias (GOE) propone conectar el trabajo cotidiano, el conocimiento organizacional y las decisiones estratégicas, construyendo las bases de un Segundo Cerebro Organizacional.

La información que se pierde entre la operación y la dirección

Cada día, las empresas de seguridad y servicios generan numerosos registros sobre sus operaciones. Rondas de vigilancia, controles de acceso, inspecciones, supervisiones, cambios de turno y registros de incidentes permiten documentar lo que sucede en instalaciones, contratos y procesos.

Sin embargo, surge una pregunta esencial: *¿qué parte de esa información se transforma realmente en conocimiento útil para tomar mejores decisiones?*

Imaginemos una empresa que presta servicios de seguridad en numerosas instalaciones. Sus supervisores identifican reiteradamente dificultades relacionadas con los controles de acceso. Cada situación puede ser registrada, comunicada y corregida. Pero ¿se están relacionando esas observaciones para comprender si existe un problema más amplio?

Las recurrencias podrían justificar una investigación sobre procedimientos, capacitación, recursos o condiciones particulares de cada instalación. No demuestran, por sí solas, cuál es

la causa. Sin un análisis estructurado, la organización corre el riesgo de resolver situaciones puntuales sin aprovechar el conocimiento que estas podrían aportar.

Este desafío afecta tanto a las empresas prestadoras como a las organizaciones que contratan sus servicios. Mientras unas necesitan supervisar la ejecución y demostrar el cumplimiento de sus obligaciones, las otras requieren evaluar las condiciones y la calidad de los servicios recibidos, comprender riesgos y fundamentar decisiones.

Más allá de disponer de datos, el desafío consiste en conectar lo que ocurre en terreno con las decisiones de supervisores, gerentes, alta dirección y directorios.

Frente a este escenario, la **Gestión Operacional Orientada por Evidencias (GOE)**, modelo desarrollado por t-Risk, propone conectar los objetivos estratégicos, los procesos y las actividades operacionales mediante un ciclo continuo de producción, contextualización y análisis de evidencias, construcción de conocimiento organizacional, apoyo a la toma de decisiones y mejora continua.

Su propuesta va más allá de digitalizar listas de

verificación o acumular registros: busca que la experiencia cotidiana contribuya sistemáticamente a construir conocimiento organizacional.

Porque una organización no mejora simplemente por registrar lo que hace, sino por desarrollar la capacidad de comprender lo que ocurre, aprender de su experiencia y utilizar ese aprendizaje para decidir y evolucionar.

Un Segundo Cerebro Organizacional para conectar la experiencia con las decisiones

Retomemos el caso de una empresa que presta servicios de seguridad en distintas instalaciones. Sus supervisores registran problemas recurrentes en los controles de acceso. Cada observación puede orientar una corrección puntual; al analizar registros confiables y contextualizados de varios puestos, la empresa también puede reconocer recurrencias, formular hipótesis y revisar procedimientos.

Consideremos ahora una multinacional que trata vigilancia, aseo y mantenimiento, además

de supervisar actividades internas. Su gerente de seguridad y servicios corporativos recibe informes de proveedores y equipos propios. Al relacionar, con criterios comparables, evidencias de inspecciones, de la ejecución de los servicios y de las acciones correctivas, puede identificar situaciones recurrentes, evaluar aspectos del cumplimiento de los servicios y priorizar mejoras en distintas instalaciones.

En ambos casos, la **Gestión Operacional Orientada por Evidencias (GOE)** busca convertir las observaciones del trabajo cotidiano en conocimiento útil para quienes ejecutan, supervisan, contratan y toman decisiones. Los registros aislados no cumplen automáticamente esa función: su aprovechamiento requiere pertinencia, confiabilidad, contexto y análisis. Identificar recurrencias orienta investigaciones, pero no demuestra por sí solo sus causas.

De ese proceso surgen las bases de un Segundo Cerebro Organizacional: la capacidad institucional de preservar, organizar, relacionar, recuperar y reutilizar el conocimiento generado tanto en operaciones propias como en servicios contratados, con acceso para las personas autorizadas.

La expresión establece una analogía con el concepto Second Brain, difundido por Tiago Forte en la organización personal del conocimiento. Aquí no designa un cerebro artificial ni supone que una tecnología aprenda autónomamente.

Su utilidad alcanza distintos niveles. Un supervisor puede consultar experiencias anteriores para

orientar verificaciones. Los responsables de contratos pueden contrastar evidencias con requisitos acordados y acompañar acciones correctivas. La gerencia general puede establecer prioridades y asignar recursos. La presidencia y el directorio pueden utilizar información consolidada como apoyo para supervisar riesgos y orientar decisiones estratégicas.

En todos los niveles, el conocimiento apoya el juicio profesional; no lo sustituye. Y el aprendizaje no termina en la decisión: requiere ejecutar las acciones, verificar sus resultados e incorporar lo aprendido a nuevos ciclos operacionales. Así, tanto prestadores como contratantes desarrollan mejores condiciones para mejorar continuamente.

De los registros a los resultados: una nueva forma de gestionar la seguridad y los servicios

El valor de la Gestión Operacional Orientada por Evidencias (GOE) no está en la cantidad de inspecciones o registros acumulados, sino en la capacidad de aprovechar evidencias confiables y contextualizadas para construir conocimiento, orientar decisiones y evaluar mejoras.

Para una empresa prestadora de seguridad, este enfoque puede fortalecer la supervisión de los contratos. Si los problemas de control de acceso se repiten en varias instalaciones, analizar los registros en conjunto ayuda a formular hipótesis, orientar la capacitación, revisar procedimientos y acompañar acciones correctivas. Las evidencias también pueden documentar aspectos de los servicios prestados y contribuir a esclarecer discre-

pancias contractuales, sin demostrar por sí solas el cumplimiento integral de un contrato.

Para la multinacional contratante de nuestro ejemplo, el alcance es más amplio. Su gerente de seguridad y servicios corporativos puede relacionar, con criterios comparables, evidencias de verificaciones de vigilancia, aseo, mantenimiento y actividades internas. Así cuenta con elementos para evaluar aspectos de los servicios recibidos, identificar situaciones que requieren atención y priorizar mejoras entre instalaciones y proveedores.

Esa información, consolidada sin perder su contexto ni sus limitaciones, también puede apoyar a la gerencia general, la presidencia y el directorio. De este modo, la experiencia de quienes ejecutan y supervisan aporta elementos a quienes asignan recursos y orientan la estrategia.

La tecnología puede facilitar este ciclo. Herramientas como t-Risk Easy apoyan la preparación de verificaciones, el registro de evidencias y el seguimiento de acciones. La inteligencia artificial Vision Pro ofrece asistencia para preparar contenidos e interpretar información, preservando la supervisión y la responsabilidad humanas.

Sin embargo, ninguna tecnología garantiza por sí sola mejores resultados. Los beneficios dependen de la calidad de las evidencias, de su análisis y de la capacidad de implementar decisiones y evaluar sus efectos.

Para prestadores y contratantes, la oportunidad consiste en pasar de acumular registros a desa-



Figura 1 — De la operación a las decisiones estratégicas. Transformación de evidencias operacionales en conocimiento para apoyar decisiones

rollar conocimiento aprovechable, fortalecer la supervisión y aprender de la propia operación.

El desafío no es solo saber qué ocurrió en terreno, sino comprender qué puede aprender la organización de esa experiencia y cómo utilizar ese conocimiento para tomar decisiones mejor fundamentadas, desde la operación hasta el directorio.



Figura 2 — Segundo Cerebro Organizacional. Conocimiento acumulado para fortalecer la supervisión, las decisiones y la mejora continua.

Sobre el autor
 Tácito Augusto Silva Leite.
 Fundador y CEO de t-Risk,
 creador de la Plataforma t-Risk, director
 de la Vertical Security Tech de ACATE y
 vicepresidente del ASIS Southern Brazil Chapter.
 Magíster en Gestión de Riesgos (UCAM/EALDE, España),
 con formación de posgrado en Seguridad Empresarial.
 Desde 1994 desarrolla su trayectoria profesional
 en gestión de riesgos, seguridad corporativa y
 transformación digital.
 Autor del libro Gestão de Riscos
 na Segurança Patrimonial.





Cuando el Estado trabaja para otro

El crimen organizado no necesita sustituir al Estado para debilitarlo. Puede bastarle con obtener una filtración, comprar un acceso o convertir una función pública en una ventaja propia.

La corrupción suele narrarse como una suma de decisiones individuales: alguien recibió dinero, otro favoreció a un conocido, un tercero entregó información. Esa descripción puede ser correcta, pero no siempre alcanza. Cuando los hechos involucran instituciones que investigan delitos, administran justicia, custodian personas o gestionan recursos públicos, la pregunta también es institucional: ¿qué capacidad del Estado quedó disponible para un interés privado o ilícito?

El modelo clásico de corrupción entiende que un funcionario se aparta de sus deberes y que una autoridad debe detectarlo y sancionarlo. Sin embargo, Persson, Rothstein y Teorell advierten que, cuando la corrupción se vuelve persistente, el problema puede transformarse en uno de acción colectiva: si los funcionarios creen que otros también incumplen, o que denunciar no cambiará nada, la probidad individual pierde eficacia. La pregunta entonces no es solo quién quebrantó la regla, sino qué incentivos y controles permiten que esa conducta se repita. Este enfoque no basta para afirmar que Chile enfrenta una corrupción sistémica; sí ayuda a identificar qué evidencia habría que buscar.

Los casos conocidos en Chile muestran mecanis-

mos diferentes. La condena de Héctor Espinosa, exdirector de la PDI, por malversación de fondos, lavado de activos y falsificación expone el riesgo del abuso de recursos públicos desde una posición de máxima autoridad. En la Operación Huracán, un tribunal condenó a exfuncionarios de Carabineros y a un civil por delitos de falsificación y obstrucción; la Fiscalía informó que se acreditó la implantación de pruebas. Son conductas distintas, pero ambas obligan a examinar cómo se supervisa el ejercicio de poderes y recursos institucionales.

La corrupción institucional tampoco se limita a los delitos demostrados. Lawrence Lessig propone observar cómo determinadas influencias pueden desviar a una institución de su propósito, incluso cuando algunas prácticas no sean necesariamente ilegales. Este concepto no reemplaza la definición penal de cohecho, malversación o tráfico de influencias. Permite analizar, por ejemplo, si los vínculos, conflictos de interés o circuitos informales de acceso debilitan la independencia institucional y la confianza pública. Desde esa perspectiva, las investigaciones que involucran a la exministra Ángela Vivanco y al exfiscal Manuel Guerra merecen examinarse con rigor, distinguiendo entre decisiones disciplinarias, hechos acreditados e imputaciones aún bajo investigación.

El crimen organizado tiene un motivo concreto para buscar relaciones dentro del Estado: reducir el riesgo de sus operaciones. La ONU advierte que estas organizaciones pueden recurrir al soborno o la coerción para obtener cooperación de funcionarios e infiltrarse en la administración pública. En San Antonio, la Fiscalía informó que un funcionario activo de Carabineros habría prestado apoyo logístico y protección a una organización criminal transnacional. En Chillán, cinco funcionarios policiales fueron formalizados por delitos que incluyen asociación criminal, allanamientos irregulares, microtráfico y obstrucción. Son investigaciones abiertas y las responsabilidades individuales deben probarse; pero ilustran por qué corresponde preguntar qué función pública habría sido puesta al servicio de una red.

Las cárceles constituyen otro espacio de riesgo. La Operación Apocalipsis investigó redes de corrupción penitenciaria y llevó a la formalización de decenas de personas, entre ellas funcionarios de Gendarmería. La hipótesis fiscal apunta a convertir accesos, controles y traslados en servicios ilícitos. Otras aristas han examinado presuntas irregularidades en compras para recintos públicos. Todo debe describirse conforme al estado procesal de cada imputado, pero el problema de seguridad

es claro: si controles penitenciarios pueden ser vulnerados mediante pagos o favores, las organizaciones criminales pueden ganar acceso, comunicación y capacidad de presión desde el interior de los recintos.

¿Cómo puede una desviación persistir? Ashforth y Anand describen la normalización de la corrupción como un proceso en que ciertas conductas se repiten, se justifican y se transmiten dentro de una organización. Un caso aislado no permite afirmar que una práctica se haya normalizado. Para sostener esa conclusión se requerirían indicios de reiteración, conocimiento de mandos, tolerancia, encubrimiento o falta persistente de consecuencias. La teoría, sin embargo, ayuda a plantear una prevención más exigente: no basta con sancionar cuando la red ya se descubrió; hay que identificar a tiempo los patrones y las condiciones que permiten su reproducción.

Por eso, la integridad no es un atributo que pueda presumirse por el uniforme, la toga o el cargo. Es una capacidad institucional que debe sostenerse con reglas, controles y resultados verificables. La OCDE plantea que la integridad pública exige priorizar el interés público sobre los intereses privados, y advierte que disponer de normas no basta si su aplicación es débil. Se necesitan controles sobre el acceso a información sensible, trazabilidad de las decisiones, gestión de conflictos de interés, protección a quienes denuncian y supervisión efectiva de los espacios donde confluyen discrecionalidad, dinero y acceso privilegiado.

La pregunta no es si el Estado chileno ha sido capturado. Esa conclusión exigiría evidencia sistemática y no puede deducirse de una lista de escándalos. La pregunta más rigurosa —y urgente— es si existen espacios donde redes privadas o criminales puedan convertir información, autoridad y acceso público en protección para sus intereses.

Cuando eso ocurre, el Estado no desaparece. Sigue operando, pero alguna de sus capacidades puede empezar a trabajar para otro.



Richard Biernay Arriagada
Ingeniero Civil Industrial
Relacionador Público
Prefecto (R) PDI

Consultor Senior
Especialista en seguridad
y gobernanza territorial



“Octubre negro”

La Ciberseguridad bajo presión: Chile está obligado a pasar del diagnóstico a la protección efectiva

Fallas críticas en tecnologías que sostienen servicios esenciales, campañas globales de ciberataques y nuevos incidentes en la contención de agentes de inteligencia artificial marcan un octubre especialmente complejo. Chile enfrenta este escenario justo cuando sus empresas deben asumir, en paralelo, múltiples obligaciones en seguridad, privacidad, prevención de delitos y normativa laboral. La capacidad de responder con éxito dependerá de qué tan rápido logremos transformar esas exigencias legales en recursos concretos y protección demostrable.

Hoy, una empresa puede contar con cámaras, guardias y una central de monitoreo de última generación, pero seguir siendo completamente vulnerable si la plataforma que coordina esos recursos opera con un software desactualizado. Del mismo modo, un organismo público que digitaliza sus trámites amplía el alcance y las consecuencias de una eventual caída del sistema. E incluso un ciudadano que sigue al pie de la letra las recomendaciones de seguridad de su banco puede terminar afectado por una brecha tecnológica que escape por completo a su control.

El llamado «octubre negro» de la ciberseguridad nos deja una advertencia clara: las organizaciones están obligadas a reaccionar a una velocidad que pone al límite sus protocolos, equipos técnicos y presupuestos. El diagnóstico solo es útil cuando se traduce en decisiones verificables. Tras cada alerta tecnológica, el paso inmediato debe ser identificar qué sistemas están comprometidos, quién lidera la respuesta y cómo se comprobará que el riesgo fue efectivamente mitigado.

Más vulnerabilidades registradas, mayor presión sobre la capacidad de respuesta

La magnitud del desafío actual queda en evidencia al revisar las estadísticas anuales de la

National Vulnerability Database (administrada por el NIST): en lo que va de 2026 ya se superan los 86500 registros de vulnerabilidades, frente a los cerca de 50.000 documentados durante todo 2025. Es importante matizar que hablamos de fallas registradas y no de ataques exitosos; un aumento en los registros tampoco implica un crecimiento automático en el número de intrusiones.

Un identificador CVE (Vulnerabilidades y Exposiciones Comunes) permite catalogar y dar seguimiento a una debilidad técnica. Su publicación puede responder a una investigación más exhaustiva, mejores herramientas de detección o el hallazgo de fallas que llevaban años ocultas.

Para cualquier organización, la verdadera prioridad radica en determinar si utiliza el componente afectado, cómo está configurado, cuál es su nivel de exposición y qué impacto tendría en el negocio si un atacante logra explotarlo.

El cuello de botella operativo y presupuestario surge cuando el volumen y la urgencia de los parches superan la capacidad real de los equipos de TI para implementarlos. Descargar una actualización toma minutos; sin embargo, verificar la compatibilidad de los sistemas, coordinar con proveedores externos, preparar planes de contin-

gencia y validar que todo funcione sin interrupciones exige tiempo y recursos especializados.

Sin ir más lejos, el pasado 21 de octubre el proyecto PHP (lenguaje de programación de código abierto orientado principalmente al desarrollo web del lado del servidor) lanzó parches de emergencia para corregir las fallas críticas CVE-2026-109618 y CVE-2026-109619, las cuales permiten la ejecución remota de código sin necesidad de autenticación, en “simple” significa que se descubrió una “falla total de seguridad” en la cerradura principal de la mitad de las páginas web del mundo, permitiendo que ladrones digitales entren sin invitación a robar información. La alerta afecta a diversas configuraciones de servidores PHP y advierte que la única solución efectiva es aplicar la actualización.

En la práctica, esto obliga a las empresas a auditar desde su sitio web institucional hasta portales de clientes, herramientas internas y servicios en la nube. Aunque un proveedor externo administre el alojamiento web, la responsabilidad final no se delega: la organización debe exigir claridad sobre quién aplicará el parche y solicitar evidencia técnica de que el riesgo fue cerrado.

Ese mismo día, Node.js (es una herramienta gra-

tuita que saca a JavaScript -el lenguaje que mueve las páginas web- de tu pantalla y lo lleva a las computadoras centrales de internet para hacer el trabajo pesado, usando el motor ultra rápido de Google Chrome) publicó correcciones de seguridad que incluyeron la vulnerabilidad de alta gravedad CVE-2026-111497 en su decodificador Brotli. Según reportó el proyecto, el procesamiento de archivos comprimidos manipulados podría provocar corrupción de memoria y derivar también en la ejecución remota de código. Significa que un hacker podría enviarle un archivo ZIP o RAR “trucado” (manipulado) a tu servidor de Node.js para romper su memoria interna y tomar el control total de tu computadora a la distancia.

En otra capa de la infraestructura, el CSIRT de Eslovaquia alertó el 23 de octubre sobre la divulgación pública de vulnerabilidades en entornos Linux (computadoras que usan el sistema operativo Linux -el “cerebro” detrás de la gran mayoría de la tecnología del mundo- en lugar de usar Windows o Mac) antes de que existieran parches oficiales para corregirlas. Entre ellas destacan los reportes ZDI-CAN-33549 y ZDI-CAN-33774, vinculados a componentes de intercambio de archivos y calificados con una severidad crítica de 9,0 (aún sin identificador CVE asignado al momento del aviso). Aquí, el nivel de riesgo depende directamente de la arquitectura y configuración de cada servidor.

Esta seguidilla de alertas demuestra que las amenazas golpean simultáneamente distintas capas tecnológicas. Para dimensionar el riesgo propio, ya no basta con mirar hacia adentro: es indispensable contar con un inventario claro de

qué software sostiene cada servicio y qué dependencias de terceros incorpora nuestra operación.

Una presión internacional que golpea de lleno a Latinoamérica

El reporte de septiembre de Check Point Research, dado a conocer el 8 de octubre, posiciona a Latinoamérica como la región con el mayor volumen de ciberataques a nivel global según sus registros: un promedio de 3.813 ataques semanales por organización, lo que representa un salto del 35 % respecto al año anterior.

El mismo estudio revela otro dato inquietante: en la región, uno de cada 25 prompts o instrucciones ingresadas a herramientas corporativas de IA generativa (el 4 %) presenta un alto riesgo de exponer información confidencial. Si bien este indicador mide el riesgo detectado en el universo monitoreado por la firma -y no implica necesariamente una filtración consumada en cada caso-, refleja una brecha evidente en los hábitos de uso seguro.

La escala global del problema también quedó plasmada en el balance operativo de octubre de Microsoft: solo desde enero de este año, diversas infraestructuras utilizadas por cibercriminales facilitaron el envío de más de mil millones de mensajes maliciosos dirigidos a usuarios y empresas en más de 150 países. Aunque la cifra refleja el alcance masivo de las campañas y cada intrusión efectiva debe evaluarse caso a caso, el volumen de fuego es innegable.

En el terreno de las brechas confirmadas, CrowdStrike reportó el 7 de octubre una operación dirigida contra entidades financieras en Corea del Sur entre fines de septiembre y principios de octubre. El ataque logró extraer datos combinando tácticas ofensivas tradicionales con el uso de herramientas de inteligencia artificial.

Por su parte, en Francia, una sesión ante el Senado durante la semana del 19 de octubre detalló cómo la explotación de una vulnerabilidad en la herramienta Metabase, ocurrida en agosto, comprometió a cerca de una decena de organismos públicos. En el caso de la propia agencia francesa de ciberseguridad (ANSSI), el incidente afectó un entorno de desarrollo externalizado y terminó con la filtración de correos electrónicos de funcionarios y colaboradores externos.

Aunque se trata de episodios ocurridos en distintas latitudes y contextos, su lectura conjunta deja una lección urgente para Chile: debemos auditar a fondo los puntos de conexión entre el Estado, los proveedores tecnológicos y el sector privado. Una sola vulnerabilidad en un proveedor compartido puede provocar un efecto dominó sobre decenas de instituciones.

Agentes de IA que eluden la contención: un riesgo concreto que exige supervisión

Cuando hablamos de «agentes de IA que se escapan», es necesario aterrizar el concepto sin caer en la ciencia ficción. Nos referimos a sistemas autónomos que, durante sus fases de entrenamiento o evaluación, logran sortear las barreras



técnicas que les fueron impuestas por sus propios desarrolladores.

En un informe publicado el 23 de octubre, Open AI (Los creadores de Chat GPT) abordaron abiertamente estos nuevos desafíos de contención. Además de hacer referencia a un incidente previo ocurrido en julio con la plataforma Hugging Face, la compañía reveló que el pasado 20 de septiembre uno de sus modelos internos aprovechó un error de configuración en un servidor DNS para obtener acceso limitado a internet en pleno proceso de entrenamiento. Aunque OpenAI aseguró que el evento fue contenido a tiempo y dio pie a un refuerzo en sus protocolos, la señal de alerta es inequívoca.

Este antecedente obliga a cualquier empresa a replantearse los permisos que otorga a los agentes de IA que integra en sus flujos de trabajo. Toda herramienta automatizada con capacidad para consultar bases de datos, ejecutar código o conectarse con servicios externos debe operar bajo el principio de mínimo privilegio, contar con registros de auditoría inalterables y tener un "botón de apagado" inmediato.

En una empresa de seguridad privada, un agente mal configurado podría comprometer antecedentes de clientes, reportes de incidentes, registros de cámaras o planos de instalaciones críticas. En el aparato estatal, el riesgo escala hacia datos sensibles de los ciudadanos y trámites administrativos. Para las personas de a pie, las consecuencias van desde el robo de identidad, estafas y la exposición de datos privados hasta el verse perjudicadas por decisiones automatizadas basadas en información errónea o vulnerada.

La adopción de la inteligencia artificial no puede medirse solo por las eficiencias que promete, sino por la robustez de los controles que implementamos para gobernarla.

Cuando el daño traspasa la pantalla

En el sector de la seguridad privada, una caída informática no es un problema abstracto: significa perder la capacidad de verificar una alarma en tiempo real, quedarse sin acceso a las cámaras de vigilancia o paralizar la coordinación de patrullaje en terreno. Por eso es vital realizar simulacros operativos que pongan a prueba cómo responderá el servicio si la plataforma central se apaga y cómo se resguardará la cadena de custodia de la evidencia digital.

El impacto en el mundo físico también golpea a las personas a través de la cadena de suministro. Un caso ilustrativo de este 2026 fue el ciberataque sufrido el 11 de marzo por Stryker, gigante de la tecnología médica, que paralizó su entorno

corporativo a nivel global. En sus reportes posteriores, la compañía reconoció problemas en el procesamiento de pedidos y despachos, lo que obligó incluso a reprogramar procedimientos médicos por retrasos en la entrega de insumos, aun cuando los dispositivos en sí mismos seguían siendo seguros para su uso clínico.

En el plano local, el Banco Central de Chile advirtió en su "Informe de Sistemas de Pago 2026" un alza en la tasa de fraudes durante el primer semestre en comparación con el año anterior, haciendo un llamado directo a los proveedores del ecosistema financiero a redoblar sus medidas de resguardo.

Para el ciudadano común, la ciberseguridad se traduce en certezas cotidianas: que sus ahorros estén a salvo, que el banco bloquee a tiempo una transacción fraudulenta, recibir una respuesta rápida ante una emergencia y poder utilizar sus servicios sin interrupciones. Los seguros y coberturas financieras ayudan a amortiguar las pérdidas una vez consumado el hecho, pero solo la prevención efectiva reduce la probabilidad y el impacto del golpe.

La encrucijada presupuestaria: protegerse con recursos limitados

La tesis central de esta columna apunta a una realidad incómoda: la acumulación simultánea de nuevas exigencias tributarias, laborales, tecnológicas y sectoriales amenaza con asfixiar la capacidad de muchas empresas chilenas -especialmente aquellas que operan con márgenes estrechos- para actualizar sus presupuestos de ciberseguridad con la urgencia y profundidad que el escenario actual demanda. El impacto real, por supuesto, variará según el tamaño, rubro y espaldada financiera de cada organización.

En este contexto, conviene analizar con precisión el alcance de la reciente rebaja al impuesto corporativo. La Ley 21.850, de Reconstrucción Nacional, establece una reducción gradual del impuesto de primera categoría para el régimen general: 27 % para las rentas del año comercial 2026; 25,5 % en 2027; 24 % en 2028, llegando finalmente al 23 % a partir de 2029 (sin perjuicio de las particularidades y excepciones de cada régimen tributario).

Esto significa que, durante 2026, el alivio tributario recién inicia su marcha gradual con una tasa del 27 %, mientras que una vulnerabilidad informática crítica exige desembolsos e intervenciones hoy mismo. Más aún: una menor carga impositiva sobre las utilidades anuales no garantiza por sí sola liquidez inmediata en la caja mensual, ni asegura que esos recursos vayan a destinarse automáticamente a fortalecer la seguridad digital.

Sobre esta estrechez financiera se apila una verdadera avalancha regulatoria. La Ley N° 21.663 (Ley Marco de Ciberseguridad) impone estrictos deberes de reporte y gestión de riesgos a las entidades calificadas como esenciales o importantes. La Ley N° 21.719 exige reestructurar por completo el tratamiento de datos personales de cara a su entrada en vigencia. Y, en el ámbito sectorial, la Ley N° 21.659 sobre Seguridad Privada eleva los estándares en materia de autorizaciones, estudios de seguridad, certificación de personal y capacitación.

A esto se suma el frente laboral y penal corporativo. La Ley Karin (N° 21.643) obliga a mantener protocolos activos de prevención e investigación frente al acoso y la violencia en el trabajo. La Ley N° 21.561, que redujo la jornada laboral a 42 horas semanales desde el pasado 26 de abril de 2026, ha forzado a rediseñar esquemas de turnos y coberturas operativas.

Por su parte, la Ley N° 21.595 de Delitos Económicos amplió drásticamente el catálogo de ilícitos atribuibles a las empresas -exigiendo actualizar los modelos de prevención del delito-, todo ello en paralelo a la implementación del Decreto Supremo 44 sobre gestión preventiva de riesgos laborales, vigente desde febrero de 2025. Y para coronar, La Ley de Reforma Previsional de Chile (Ley N° 21.735) que establece un aumento gradual del 8,5% en las cotizaciones con cargo exclusivo al empleador, lo que elevará la tasa total de aporte previsional del 10% actual hasta el 18,5% en un plazo de 9 años. Comenzó en agosto de 2025 con un 1% inicial y en agosto de 2026 subió al 3,5% de la renta imponible. El plan es seguir subiendo año a año hasta completar el 8,5% extra en el año 2033.

Nadie discute que cada una de estas leyes persigue fines legítimos y necesarios para el país. El problema práctico es que cumplirlas exige horas de dedicación de equipos internos y directorios, contratación de consultores, capacitaciones continuas, compra de software, auditorías permanentes, retenciones directas y todo ello es finalmente menos margen y desvío del foco corporativo.

Por otro lado, la presión financiera y operativa se multiplica cuando las empresas abordan cada ley como un compartimento estanco, creando proyectos paralelos que duplican los gastos, esfuerzos y levantamiento de evidencias.

El verdadero peligro presupuestario ocurre cuando una organización, intentando cumplir con todo en el papel a través de recursos fragmentados, termina postergando la inversión en controles técnicos urgentes que evitan que su operación sea hackeada mañana. Superar esta trampa exige mayor músculo de visión estratégica por parte de

los directorios y una política pública que tome en cuenta la capacidad real de absorción normativa de nuestro tejido empresarial.

Optimizar recursos e integrar el cumplimiento

Desde la vereda de la política pública, una respuesta sensata pasa por armonizar las exigencias que se superponen entre distintos reguladores, estandarizar la entrega de evidencias para evitar la burocracia duplicada y ofrecer acompañamiento técnico real a las Pymes. Asimismo, vale la pena discutir incentivos o apoyos directos para aquellas inversiones comprobables en ciberseguridad, capacitación técnica y resiliencia operativa.

Puertas adentro de las empresas, la clave para sobrevivir a esta ola regulatoria sin quebrar el presupuesto está en unificar la gobernanza y la gestión de riesgos. Un control robusto de accesos informáticos, el resguardo seguro de expedientes de trabajadores, la auditoría rigurosa a proveedores y un sistema centralizado de trazabilidad sirven simultáneamente para cumplir con la Ley de Ciberseguridad, la Ley de Datos Personales, la Ley de Delitos Económicos y la normativa laboral. Pero lograr esa sinergia requiere romper los silos internos y sentar en la misma mesa a las áreas de TI, legal, recursos humanos y operaciones.

El debate actual en torno a la nueva Ley de Protección de Datos Personales ilustra muy bien por qué es vital planificar con rigor jurídico y no basarse en rumores. Si bien el Senado informó el pasado 20 de octubre que una comisión aprobó en general la iniciativa para postergar la entrada en vigencia de la norma hasta diciembre de 2027, dicho avance legislativo aún no constituye una ley promulgada ni publicada. Hoy, en términos

estrictamente legales, la fecha límite sigue siendo el 1 de diciembre de 2026.

Con todo, incluso si esa prórroga llegara a concretarse, el tiempo extra no debe verse como una excusa para congelar los proyectos, sino como una oportunidad valiosa para ordenar las bases de datos, renegociar cláusulas con proveedores y revocar permisos de acceso innecesarios. Los ciberdelincuentes y las brechas de seguridad no esperan los tiempos del Congreso.

El verdadero indicador de éxito será la protección comprobable

La experiencia internacional demuestra que es posible medir los avances con indicadores concretos. El pasado 12 de octubre, un informe presentado ante el Parlamento del Reino Unido detalló los resultados de dos programas piloto gubernamentales que utilizaron inteligencia artificial para auditar código fuente: la iniciativa permitió detectar y corregir 1.352 vulnerabilidades distribuidas en 548 repositorios pertenecientes a 18 ministerios y departamentos. Aunque esto no garantiza inmunidad total para la infraestructura británica, representa un ejercicio transparente de reducción de riesgo medible.

En Chile, la Agencia Nacional de Ciberseguridad (ANCI) contabilizó 324 reportes de incidentes con impacto significativo solo durante el primer semestre del año, y ya ha convocado para este 29 de octubre al primer Ejercicio Nacional de Ciberseguridad. Son pasos institucionales en la dirección correcta, pero su efectividad dependerá de que cada organización haga su propio trabajo puertas adentro.

La hoja de ruta inmediata para cualquier empresa o institución pública es clara: mapear sus activos y servicios críticos, evaluar su nivel real de exposición y asignar presupuesto prioritario para parchar las vulnerabilidades que hoy están siendo explotadas. A la par, es indispensable poner a prueba los planes de respaldo y recuperación de desastres, restringir los privilegios de las herramientas de IA y realizar simulacros de manejo de crisis que involucren tanto a los equipos técnicos como a la alta dirección.

Para ordenar este esfuerzo, estándares actualizados como la norma ISO/IEC 27701:2025 ofrecen un marco de trabajo sólido que permite integrar la gestión de la privacidad con los controles de seguridad de la información y el cumplimiento normativo. Su valor, eso sí, no radica en colgar un certificado en la pared, sino en definir responsabilidades claras, aplicar controles efectivos y generar evidencia auditable de mejora continua.

Chile necesita que el creciente rigor regulatorio vaya de la mano con una capacidad real de ejecución técnica y financiera. El saldo de este «octubre negro» no debería ser la parálisis ni el agotamiento de los equipos, sino presupuestos mejor enfocados, sistemas críticos debidamente parchados y organizaciones entrenadas para recuperarse ante un golpe. Esa será la única evidencia tangible de madurez que podrán valorar las empresas, el Estado y, sobre todo, los ciudadanos que confían en ellos.

Para compliance, auditorías de gobernanza, integración de IA segura y adecuación a la ISO 27701, contácteme y comencemos a proteger su futuro hoy.

Francisco Venegas Aros
Columnista Revista Seguridad y Defensa
Consultor - CEO & Founder CyberBaum
contacto@cyberbaum.cl





La minería como objetivo de la delincuencia

En Chile, el año 2026 marca un punto de inflexión crítico en seguridad minera, consolidando un escenario donde el crimen organizado y la alta tecnología miden fuerzas directamente. La sostenida demanda global y el alto precio internacional del metal rojo han transformado la seguridad minera. Lo que antes eran hurtos menores, hoy se maneja bajo la dinámica de asociaciones criminales complejas y mafias corporativas.

Chile enfrenta una creciente preocupación por los delitos vinculados al robo de cobre. Lo que durante años pudo parecer un problema circunscrito a la sustracción de cables eléctricos y materiales metálicos se ha convertido en una amenaza de mayor complejidad, con organizaciones criminales capaces de intervenir instalaciones industriales, atacar trenes de carga y desarrollar circuitos para almacenar, transportar y comercializar el material sustraído.

El incentivo económico resulta evidente: el cobre es uno de los principales recursos estratégicos de la economía chilena y su cotización internacional puede convertir una carga robada en una mercancía de considerable valor. Sin embargo, el problema no termina con la sustracción. Para que el delito resulte rentable a gran escala, también deben existir mecanismos para recibir, procesar y comercializar el metal, eventualmente ocultando su procedencia ilícita.

Las cifras conocidas durante 2026 muestran que la situación requiere una respuesta coordinada entre las policías, el Ministerio Público, las empresas afectadas y los organismos encargados de fiscalizar la comercialización y exportación de metales.

Un récord de robos que afecta al suministro eléctrico

Uno de los indicadores más preocupantes proviene de la Compañía General de Electricidad (CGE). Según información publicada por la empresa en febrero de 2026, durante 2025 se registraron 1.426 episodios de robo de cables en sus instalaciones de distribución y transmisión, con un total de 420 kilómetros de conductores sustraídos.

La cifra representa un deterioro significativo respecto de 2024, cuando se contabilizaron 774 episodios y 225 kilómetros de cables robados. En términos interanuales, los eventos aumentaron aproximadamente un 84%, mientras que la longitud del material sustraído creció cerca de un 87%. El impacto económico informado superó los \$5.500 millones, considerando los daños y las reparaciones asociados a estos delitos. Además, los hechos afectaron a 265.487 clientes a lo largo de la zona de concesión de la compañía.

El Nuevo Ciclo Político y Regulatorio

En el ámbito institucional, la seguridad minera ha tomado un rol prioritario debido al cambio de ciclo político con la llegada del gobierno del presidente José Antonio Kast.

Dado que el cobre y el litio están declarados minerales estratégicos bajo los nuevos planes de de-

sarrollo geopolítico y cadenas de suministro (en cooperación con potencias globales), la seguridad en las rutas del norte y el centro del país ha pasado de ser un problema corporativo privado a un asunto de seguridad nacional para el Estado chileno.

El incremento de los robos de cables eléctricos, los asaltos a trenes que transportan cátodos y la sustracción de cobre desde instalaciones mineras evidencian un fenómeno que trasciende la delincuencia común. Detrás de estos hechos se configura un mercado ilícito que aprovecha el elevado valor internacional del metal y las dificultades para rastrear su origen, con consecuencias para la seguridad pública, la continuidad de los servicios y la actividad económica nacional.

Estos antecedentes permiten dimensionar una de las principales consecuencias del fenómeno: el robo de cobre no perjudica únicamente a la empresa propietaria del material, sino también a las personas que dependen de la infraestructura intervenida.

La sustracción de cables puede provocar interrupciones del suministro eléctrico, daños en postes y transformadores, gastos extraordinarios de reparación y movilización de personal técnico. En determinadas circunstancias, también puede comprometer servicios esenciales y afectar la actividad comercial e industrial.

Consolidación Estadística del Robo de Cobre en Chile (2022–2026)

Análisis cuantitativo de pérdidas patrimoniales, volumen sustraído e hitos delictivos en la red de transmisión y minería.

> 500 ton
VOLUMEN ACUMULADO (2026)
+81.8% vs. nivel 2022

> \$90.000M
PÉRDIDAS CLP (2026)
Máximo histórico registrado

> 100.000
EVENTOS TOTALES (5 AÑOS)
Media de ~50-60 robos diarios

EVOLUCIÓN DEL VOLUMEN SUSTRÁIDO (TONELADAS METRICAS)



MATRIZ ESTADÍSTICA CONSOLIDADA (2022–2026)

Año	Incidentes y Denuncias	Volumen Sustraído	Pérdidas Estimadas	Hitos y Megaoperativos
2022	> 22.000 eventos (~60 robos diarios)	~250 a 300 ton	~\$35.000 a \$45.000M CLP	Quiebre en curva delictual (+80% vs 2021). Gran impacto en telecomunicaciones.
2023	> 18.500 eventos	~320 ton	~\$50.000M CLP	Paso de robo domiciliario a líneas de alta tensión y faenas mineras.
2024	> 20.000 eventos (>250 denuncias/mes)	~410 ton	\$75.803M CLP (US\$ 80 - 120M)	Enfoque en trenes y minería. PDI crea unidades de análisis especializado.
2025	> 21.500 eventos	~480 ton	~\$85.000M CLP	Reemplazo masivo de tendidos eléctricos por aluminio.
2026*	> 18.000 eventos (a oct, en desarrollo)	> 500 ton (acumuladas)	> \$90.000M CLP	Op. "Alto Voltaje" (187 t decomisadas) y Op. "Veta Roja" (59 detenidos en Codelco).

Durante el quinquenio 2022–2026, el fenómeno del robo de cobre en Chile ha sufrido una severa transformación estructural, evolucionando desde hurtos de oportunidad en redes domiciliarias y de telecomunicaciones hacia esquemas de crimen organizado complejo orientados al sabotaje y extracción masiva en alta tensión y faenas mineras de alta escala.

Durante el primer semestre de 2025, CGE ya había reportado 705 episodios de robo de cables y 209 kilómetros de conductores sustraídos, casi cuatro veces los 190 episodios registrados durante el mismo período de 2024. La evolución posterior confirmó que no se trataba de un problema menor ni de una serie aislada de incidentes.

El cobre: un recurso estratégico convertido en objetivo criminal

La paradoja resulta especialmente significativa para Chile. El país es uno de los principales productores mundiales de cobre y depende de esta industria para una parte relevante de sus exportaciones y de su actividad económica.

Precisamente, el valor comercial del metal contribuye a explicar su atractivo para las organizaciones delictivas. A diferencia de otros bienes robados, el cobre puede incorporarse a diferentes circuitos comerciales una vez procesado, mezclado con otros materiales o presentado bajo una descripción que dificulte establecer su procedencia.

El Informe de Crimen Organizado en Chile 2025, elaborado por el Ministerio Público, identifica factores que favorecen el mercado ilícito del cobre: su elevado valor internacional, las dificultades para establecer la trazabilidad y la propiedad del material, las vulnerabilidades en determinados controles y las condiciones de aislamiento geográfico de algunas zonas de extracción y transporte. También describe mecanismos de inserción en los mercados formales mediante intermediarios, empresas de fachada y exportaciones fraudulentas. En consecuencia, el robo de cobre debe analizarse como una cadena delictiva y no solamente como el acto de cortar un cable o sustraer una carga.

En uno de sus extremos están quienes ejecutan materialmente el robo. En el otro pueden encontrarse los receptores, intermediarios y operadores comerciales que permiten convertir el metal en dinero.

Combatir únicamente al autor material de la sustracción resulta insuficiente si permanece intacta la estructura que compra, recibe y comercializa el producto robado.

El precio internacional como incentivo

La cotización del cobre constituye una variable relevante para comprender la evolución de estos delitos, aunque no es el único factor que los explica.

Cuando el metal alcanza precios elevados, aumenta el valor potencial de los cargamentos y puede mejorar la rentabilidad que los delincuentes esperan obtener. Esto puede incentivar nuevos ataques, especialmente cuando las probabilidades de detección se perciben como bajas y existen compradores dispuestos a recibir material de origen dudoso.

No obstante, para establecer cuánto del aumento delictivo responde específicamente a las fluctuaciones de la cotización internacional sería necesario contrastar las series de precios con las estadísticas policiales, los volúmenes sustraídos y las investigaciones sobre los circuitos de comercialización.

Lo que sí muestran los antecedentes disponibles es que el elevado valor del cobre constituye uno



de los factores estructurales que favorecen este mercado ilícito.

El norte de Chile: asaltos a trenes y ataques a instalaciones mineras

La problemática adquiere una dimensión particularmente delicada en las regiones mineras del norte, donde el transporte de grandes volúmenes de cobre constituye una pieza esencial de la cadena productiva.

En septiembre de 2026, antecedentes publicados por Emol sobre los ataques a trenes que transportan el metal en el desierto de Atacama dieron cuenta de una preocupante evolución de los métodos empleados por las bandas.

De acuerdo con información atribuida a la industria minera y antecedentes conocidos por Reuters, durante 2025 se registraron 86 robos a trenes vinculados al transporte de cobre, frente a 39 asaltos reportados para 2022. Más inquietante aún, entre enero y abril de 2026 se contabilizaron 34 ataques, durante los cuales se sustrajeron 169 toneladas métricas de cobre, equivalentes al 71% del volumen robado durante todo 2025, según los antecedentes citados.

Estos hechos reflejan un escenario en el que las organizaciones delictivas parecen actuar con mayor coordinación y disposición a asumir riesgos.

Los ataques a los trenes no solo representan pérdidas materiales. También exponen a trabajadores y personal de seguridad a situaciones de violencia,

comprometen la continuidad de las operaciones y obligan a reforzar los sistemas de vigilancia y protección de la carga.

En este contexto, la seguridad de la cadena logística minera deja de ser exclusivamente una responsabilidad operacional de las compañías y adquiere una dimensión de seguridad pública y protección de infraestructura estratégica.

Organizaciones capaces de operar durante años

La complejidad del fenómeno también se observa en las investigaciones desarrolladas por el Ministerio Público.

En noviembre de 2025, la Fiscalía Regional de Antofagasta informó sobre la detención de integrantes de una organización investigada por al menos nueve robos de cátodos de cobre desde faenas mineras, trenes y camiones, cometidos entre diciembre de 2024 y julio de 2025. El valor de los paquetes de mineral sustraídos se estimó en cerca de \$500 millones.

Posteriormente, el 5 de octubre de 2026, la Fiscalía informó sobre nuevas detenciones vinculadas a una organización que habría operado entre Mejillones y Calama, afectando instalaciones mineras y al Ferrocarril de Antofagasta a Bolivia (FCAB).

Entre los hechos investigados figuraban asaltos en los que se habría sustraído cobre avaluado en decenas de millones de pesos, además de un ep-

isodio en que los delincuentes habrían intimidado con armas de fuego al personal de seguridad. La investigación vinculó a los imputados con al menos diez delitos y estimó en aproximadamente \$500 millones el valor de los metales sustraídos en los hechos considerados.

Estos antecedentes muestran que el problema puede involucrar estructuras con capacidad para planificar operaciones, seleccionar objetivos y mantener redes de comercialización.

La existencia de estos grupos obliga a revisar los protocolos de seguridad en las instalaciones mineras, los patios de almacenamiento, las rutas de transporte y los terminales logísticos.

De la sustracción a la exportación: seguir la ruta del cobre

Una de las dificultades centrales para enfrentar este delito consiste en determinar qué ocurre con el metal después de su robo. La investigación de los eslabones posteriores resulta fundamental porque permite identificar a quienes financian, reciben o comercializan el material y establecer si existen redes de mayor alcance.

En el mercado ilícito pueden intervenir compradores que mezclan material de procedencia legal e ilegal, establecimientos que no verifican adecuadamente su origen y operadores que utilizan documentación irregular para dificultar la fiscalización.

El informe del Ministerio Público sobre crimen



organizado identifica precisamente la comercialización mediante intermediarios y las exportaciones fraudulentas entre los mecanismos utilizados para introducir cobre ilícito en circuitos comerciales.

La dimensión internacional agrega otro desafío. El cobre es una mercancía comercializada globalmente, por lo que la investigación no siempre termina en el lugar donde se cometió el robo. Puede ser necesario reconstruir operaciones de compra, movimientos de carga, documentación tributaria y aduanera y relaciones entre distintas empresas. Por ello, la trazabilidad debe ocupar un lugar central en la estrategia de prevención.

Registrar las transacciones, verificar la identidad de los proveedores, documentar el origen del material y fiscalizar las operaciones de mayor riesgo son medidas que pueden contribuir a reducir las oportunidades de introducir cobre robado en el mercado formal.

Seguridad privada y protección de infraestructura crítica

La evolución de estos delitos también plantea desafíos para la industria de la seguridad privada y para los responsables de proteger instalaciones industriales, mineras y logísticas.

Las medidas tradicionales de vigilancia pueden resultar insuficientes cuando los delincuentes actúan de manera coordinada, conocen las características de las instalaciones y aprovechan extensas áreas geográficas o sectores con limitada presencia de personal.

La prevención requiere combinar análisis de riesgos, vigilancia física, tecnologías de detección, control de accesos, monitoreo de perímetros, gestión de incidentes y coordinación con las autoridades.

En el ámbito minero, la protección debe extenderse más allá del recinto productivo. Los cargamentos también pueden quedar expuestos durante su almacenamiento, transferencia y transporte por carretera o ferrocarril.

En las redes eléctricas, por su parte, la extensión de los tendidos y la distribución territorial de los activos hacen necesario priorizar los sectores de mayor riesgo y mejorar la capacidad de detectar intervenciones no autorizadas.

La tecnología puede contribuir a identificar eventos sospechosos y reducir los tiempos de respuesta, pero su efectividad depende de que exista una estrategia operacional que permita transformar las alertas en acciones concretas.

Asimismo, la colaboración entre empresas, policías, fiscalías y autoridades sectoriales resulta fundamental para compartir información sobre patrones delictivos, puntos críticos y modalidades de operación.

Una respuesta que debe alcanzar a toda la cadena criminal

El aumento de los robos de cobre obliga a avanzar hacia una política de seguridad que combine prevención, investigación penal y fiscalización comercial.

En primer lugar, es necesario fortalecer la persecución de las organizaciones que coordinan los robos y de los actores que permiten comercializar el material sustraído. Esto exige investigaciones patrimoniales y financieras capaces de identificar los beneficios económicos del delito y las relaciones entre sus participantes.

En segundo término, deben reforzarse los controles sobre la compra y venta de cobre usado, especialmente cuando existen inconsistencias documentales, volúmenes difíciles de justificar o proveedores cuya actividad no permite explicar el origen del material.

En tercer lugar, resulta indispensable mejorar la coordinación entre las compañías afectadas y las instituciones públicas, con mecanismos de denuncia, intercambio de información y seguimiento de los casos.

Finalmente, la protección de la infraestructura debe considerar el costo total de estos hechos: no solamente el valor del cobre robado, sino también las reparaciones, las interrupciones de servicios, los riesgos para las personas y las pérdidas derivadas de la paralización de operaciones.

Conclusión: el verdadero negocio está en la cadena ilícita

Las cifras disponibles permiten establecer que el robo de cobre en Chile ha alcanzado una dimensión preocupante. Los 420 kilómetros de cables sustraídos desde instalaciones de CGE durante 2025 y los antecedentes sobre los ataques a trenes y faenas mineras durante 2026 evidencian que se trata de un problema con múltiples expresiones y consecuencias.

El alto precio internacional del metal constituye un incentivo importante, pero no explica por sí solo la persistencia del fenómeno. Para que el robo se transforme en un negocio criminal rentable, también deben existir oportunidades para ejecutar las sustracciones, trasladar el material y encontrar compradores capaces de incorporarlo a circuitos comerciales.

La respuesta, por tanto, no puede limitarse a incrementar la vigilancia en los puntos donde ocurren los robos. Debe alcanzar a quienes organizan las operaciones, reciben los cargamentos y obtienen beneficios de su comercialización.

Para Chile, proteger el cobre significa mucho más que resguardar un producto de exportación. Implica defender la continuidad del suministro eléctrico, la seguridad de los trabajadores, el funcionamiento de la minería y la integridad de una infraestructura estratégica para el desarrollo nacional.



Revista
SEGURIDAD
& DEFENSA

NUEVA SECCIÓN

SEGURIDAD MINERA

Prevención de robos,
vigilancia remota, sistemas GPS,
comunicaciones, seguridad
perimetral, sistemas autónomos.



Un nuevo espacio editorial para visibilizar
desafíos, experiencias y soluciones en las
minas de Chile.



ANÁLISIS
RIGUROSO



PREVENCIÓN
EFECTIVA



INNOVACIÓN
PÚBLICA



GESTIÓN
TERRITORIAL



ACTUALIDAD
MUNICIPAL

PORQUE LA SEGURIDAD TAMBIÉN SE CONSTRUYE DESDE LA MINERÍA

REVISTA SEGURIDAD AMPLÍA SU MIRADA

www.revistaseguridad.com

Datos abiertos, los 33 países de la región medidos

El nivel más bajo y el aumento más rápido pueden estar en el mismo país

SIWA - <https://fundacionkent.org/siwa/> -, el registro público que abrió la Fundación Sherman Kent sobre los treinta y tres Estados de América Latina y el Caribe, permite mirar el homicidio en dos ejes a la vez: cuánto y hacia dónde. Leídos por separado cuentan historias opuestas. La herramienta vale menos por las cifras que publica que por las que se niega a publicar cuando la serie no las sostiene.

La tasa de homicidios es el indicador más citado de la seguridad regional y también el más maltratado. Casi siempre se publica como una cifra sola —un número por país, un ordenamiento, un titular— cuando en realidad son dos datos: el nivel y la pendiente. El registro publica los dos, y basta ponerlos uno al lado del otro para que el mapa deje de leerse como se lo suele leer.

La mediana de los treinta y tres Estados es 17,75 homicidios por cada 100.000 habitantes, con dato de 2023. Arriba están San Cristóbal y Nieves con 64,16, San Vicente y las Granadinas con 51,32, Jamaica con 49,44, Ecuador con 45,72, Haití con 41,15 y Trinidad y Tobago con 40,44. Abajo, Bolivia con 4,42, Cuba con 4,46, Argentina con 4,49, Chile con 6,35, Surinam con 6,52 y Paraguay con 6,78. Es la fotografía conocida.

La segunda cifra cambia el cuadro

Ahora la pendiente, sobre la ventana móvil de diez años que emplea el registro. Entre los seis países con la tasa más alta, tres se movieron poco: San Cristóbal y Nieves subió 0,7 %, Jamaica 2,6 % y Trinidad y Tobago 25,5 %. Otros dos se

dispararon: Ecuador creció 686,9 % y Haití, 327,2 %. Entre los seis con la tasa más baja, cinco bajaron —Paraguay 36,7 %, la Argentina 24,9 %, Bolivia 23,1 %, Cuba 12,1 %, Surinam 6,5 %— y uno subió: Chile, 87 %.

Diecisiete series que el registro se niega a proyectar

El registro prolonga cada serie a uno, dos y cuatro años con una recta de mínimos cuadrados, y publica junto a cada proyección su pendiente, su coeficiente de determinación y su margen. Muestra los tres horizontes a la vez, porque la diferencia entre ellos es en sí misma la información: en un país el horizonte corto puede decir que el año fue malo y el largo, que el país cambió de categoría.

Lo que hace confiable a ese mecanismo no es la proyección sino el resguardo. Cuando el coeficiente de determinación cae por debajo de 0,5 —cuando la serie sencillamente no describe una recta—, la proyección no se publica: el país se pinta aparte y la ficha dice que prolongar esa serie daría una cifra sin sustento.

En homicidios, de los treinta y tres Estados solo dieciséis tienen serie proyectable.

Diecisiete no. Publicar una proyección para los treinta y tres habría sido inventar diecisiete cifras con apariencia de método.

En el gráfico (pag. siguiente), además, lo observado y lo prolongado nunca se dibujan igual: la serie histórica va en línea llena y el tramo proyectado en línea de puntos. Y la proyección no incorpora ningún hecho posterior al último dato —ni una elección, ni una ley, ni una crisis—. Prolonga una recta, y las series se quiebran. El pronóstico con esos elementos adentro es análisis, y sale por otro lado.

El caso de Chile, mirado de cerca

Chile pasó de 3,39 homicidios por cada 100.000 habitantes en 2016 a 6,35 en 2023. Sigue estando muy por debajo de la mediana regional —su tasa equivale a poco más de un tercio de ella— y solo tres Estados del padrón registran menos.

País	Tasa (2023)	Cambio en diez años	Lectura conjunta
Ecuador	45,72	+686,9 %	alto y en explosión
Haití	41,15	+327,2 %	alto y en explosión
San Cristóbal y Nieves	64,16	+0,7 %	el más alto, estable
Jamaica	49,44	+2,6 %	alto, estable
Chile	6,35	+87 %	bajo, en ascenso rápido
Paraguay	6,78	-36,7 %	bajo, en descenso
Argentina	4,49	-24,9 %	bajo, en descenso
Bolivia	4,42	-23,1 %	el más bajo, en descenso
Promedio región	17,75	—	—

Entre los seis países con menos homicidios de la región, cinco están bajando y uno está subiendo. Ese país es Chile, y su aumento es el cuarto más grande de los treinta y tres.

Las dos afirmaciones que suelen enfrentarse en el debate público chileno, la de que el país sigue siendo de los más seguros de la región y la de que la situación se deterioró de manera acelerada, son ambas correctas y describen el mismo par de cifras.

El patrón se repite en gobernanza. Chile ocupa el primer lugar de los treinta y tres en calidad regulatoria, el tercero en estado de derecho, el tercero en voz y rendición de cuentas y el cuarto en control de la corrupción: posiciones de cabeza regional sin discusión. Sus series, en cambio, bajan. Entre 2016 y 2024 la calidad regulatoria pasó de 1,28 a 0,78; el estado de derecho, de 0,99 a 0,69; la estabilidad política, de 0,59 a 0,12. El control de la corrupción es el único que se mantuvo, prácticamente sin variación en ocho años.

Una precisión técnica que evita un error frecuente cuando estas series llegan a la prensa: estos indicadores no admiten variaciones porcentuales. Se expresan en una escala de $\square 2,5$ a 2,5 que cruza el cero, y un porcentaje calculado sobre una escala con signo produce números espectaculares y sin sentido. Por eso las cifras de arriba van en puntos de la escala. El registro advierte, además, que son estimaciones construidas agregando encuestas y evaluaciones de expertos: no cuentan hechos y no pueden presentarse como recuentos.

La advertencia que el propio registro publica

Antes de que cualquiera de estas comparaciones se use para ordenar países, conviene leer algo que el registro declara en el mismo archivo del que salen las cifras, entre sus vacíos reconocidos. Es una advertencia incómoda y está publicada de todas formas.

La consecuencia es concreta. Comparar la tasa de un Estado con capacidad estadística consolidada contra la de otro cuya capacidad es sensiblemente menor no compara dos niveles de violencia: com-

para un nivel de violencia con una mezcla de violencia y capacidad de registro. La comparación sigue siendo útil, porque es la mejor disponible, pero deja de ser inocente.

El homicidio es recuento de hechos, pero depende de la capacidad de registro de cada Estado: uno que registra peor aparece con menos homicidios. La cifra baja puede indicar buena seguridad o mal registro.

Cinco compromisos que se pueden auditar

Un registro vale lo que valen sus reglas, y estas están publicadas para que cualquiera las contraste con el comportamiento del sitio.

- No se simulan datos. Si una fuente falla, el sitio muestra el error. Nunca un valor de ejemplo.

- **Las discrepancias no se promedian.** Si el dato oficial de un Estado y el del organismo multilateral difieren, se publican los dos con su fuente. Promediar es fabricar.

- **Lo que falta se declara, con nombre y motivo.** La serie de terrorismo termina en 2021 y el registro lo dice en la propia sección, e identifica cuál sería el reemplazo posible y por qué todavía no está en servicio. Publicar la tarea pendiente es una forma poco común de transparencia.

- **Hay una medición propia de opacidad,** que la Oficina construye Estado por Estado revisando si cada uno publica su serie nacional de solicitudes de acceso a la información. Los que aún no se revisaron no figuran como opacos: figuran como no revisados, que es distinto.

- **El archivo queda versionado.** Cada corrida se guarda con dirección fija, de modo que si una fuente corrige una cifra hacia atrás queda constancia de qué decía antes y desde cuándo.

Lo que no puede decir, y lo dice

Para quien trabaja en seguridad municipal, la limitación más relevante del registro es también la más honestamente declarada: no hay desglose subnacional. Ninguna de las fuentes en uso publica desglose provincial, y donde no lo hay el país queda en gris en el mapa «en vez de pintarse con una cifra que no le corresponde».

Dicho de otro modo: una tasa nacional no describe a ninguna comuna, municipio ni delegación en particular, y usarla para caracterizar un territorio concreto es un abuso de la cifra. Un registro regional comparable y un dato local accionable son dos productos distintos, y el primero no puede sustituir al segundo. Lo que sí puede hacer es dar el marco: cuánto de lo que ocurre en un territorio se explica por una tendencia que atraviesa a todo el país o a toda la región, y cuánto es específico de ese lugar. Esa pregunta los equipos locales pueden responderla mejor que nadie, y sin una línea de base regional ni siquiera se puede formular.

Cómo se navega, en cuatro movimientos

El registro está pensado para consultarse, no para leerse de corrido. Cuatro pasos alcanzan para llegar a cualquier cifra de este artículo, y para llegar a las que este artículo no usó.

- Elija el ámbito. Un país, una zona —Andina, Caribe hispano, Caribe oriental, Cono Sur, Guayanitas, México y Centroamérica— o la región entera. Lo que se elige manda sobre todo el resto.

- Elija el nivel de lectura. Ciudadano abre tres secciones; Periodista, dieciséis; Analista, cuarenta y seis. Ninguno esconde nada de los otros: cambia cuánto se muestra a la vez.

- Elija el tema y pinte el mapa. Son 59 temas agrupados en cuatro ejes, y se pueden cruzar dos o más para ver si se mueven juntos.

- Llévelo. En el nivel Periodista, cada tema ofrece la cita lista para copiar, la planilla de datos en CSV y el informe del ámbito elegido en PDF. Todo abierto, sin credenciales.

Hay además una capa que se recolecta cada hora: una ventana de 48 horas con lo que se está publicando ahora sobre el ámbito elegido. El registro advierte que esa capa no actualiza las cifras y que más notas de prensa no significan más hechos: pueden significar más atención. Es una advertencia que a esta revista y a sus lectores les resulta familiar.

Percepción y medición no son lo mismo, y las dos informan

Las encuestas de percepción de inseguridad y las series de homicidios miden cosas distintas y ninguna reemplaza a la otra. La percepción responde a la experiencia, a la cobertura mediática y al entorno inmediato; la tasa cuenta hechos, con las limitaciones de registro ya señaladas. Cuando las dos se mueven en la misma dirección, el hallazgo se refuerza. Cuando divergen, la divergencia es en sí misma información y merece explicación, no descarte.

El registro no mide percepción, y lo dice: publica lo que puede medirse con series comparables entre Estados. Quien necesite la otra mitad del cuadro tiene que buscarla en otra parte, sabiendo que está sumando dos naturalezas distintas de dato. Dónde termina el dato y empieza el análisis

El registro publica hechos calificados y no emite juicios. No lleva confianza analítica, no emplea el léxico de probabilidad y no va firmado. Los informes de la Fundación sí: firmados, con probabilidad y confianza declaradas, y después de disenso formal.

La máquina recolecta y ordena. La máquina nunca concluye.

Todas las cifras de este artículo se leyeron el 7 de septiembre de 2026 y cualquiera puede reproducirlas hoy, sin credenciales y sin pedir permiso, y llegar a una lectura distinta de la de este texto. La invitación es a entrar y discutir con la tabla a la vista.

Qué es SIWA y como se ingresa

Es el registro público de situación de América Latina y el Caribe de la Fundación Sherman Kent. Reúne, sobre los treinta y tres Estados de la región, aquello que puede medirse en cuatro ejes:

seguridad, defensa, gobernanza y desarrollo. Al 7 de septiembre de 2026 estaban en servicio 69 indicadores sobre 40 fuentes, y el número crece a medida que entran en servicio sus colectores.

Acceso libre y completo. No hay cuenta que crear, no hay muro de pago y no hay dato reservado dentro del registro. La planilla de datos y el informe del ámbito elegido se descargan igual de abiertos.

Registro: siwa.fundacionkent.org · **Presentación:** fundacionkent.org/siwa · Se cita como «SIWA, Fundación Sherman Kent».

Una invitación abierta a las instituciones de la región

Las fuentes en servicio son el punto de partida del registro y no su techo. La Fundación invita a universidades, oficinas de estadística, organismos públicos, observatorios y organizaciones de la sociedad civil de cualquier país de la región a proponer series sobre los treinta y tres Estados.

Tres condiciones: licencia que permita publicar-la abierta, cobertura comparable entre Estados, y procedencia y fecha declaradas. Quien aporta una serie queda acreditado en cada cifra que de ella se derive, en los tres niveles de lectura.

Propuestas: info@fundacionkent.org



Por Edgardo Glavinich
Director Ejecutivo de la Fundación Sherman Kent ·
Oficina de Generación de Inteligencia



Summit Seguridad Ciudadana y Emergencias

Potenciar las respuestas ante emergencias mediante la tecnología y la IA

La incorporación de la inteligencia artificial (IA) en la gestión de emergencias y seguridad es el factor clave para evolucionar desde un modelo de seguridad reactivo a un modelo preventivo y predictivo en tiempo real. La IA actúa como un multiplicador de fuerza que procesa volúmenes masivos de datos para anticipar amenazas, acelerar la toma de decisiones y coordinar respuestas institucionales de manera ultra-eficiente. Estos fueron algunos de los temas abordados en el reciente *Summit Seguridad Ciudadana y Emergencias*, evento coorganizado por Fundación País Digital y Fundación Paz Ciudadana. Para conocer los principales alcances y conclusiones de este encuentro, conversamos con Marco Terán, director de Desarrollo Digital de Fundación País Digital.

¿Cuáles son las áreas principales donde la inteligencia artificial y los datos están abriendo nuevas posibilidades para prevenir delitos y mejorar la respuesta frente a las emergencias?

Vemos oportunidades en tres áreas principales: prevención, detección y respuesta. En prevención, el análisis de datos permite identificar patrones territoriales y horarios para orientar mejor las intervenciones. En detección, la videoanalítica puede apoyar el reconocimiento de vehículos con encargo por robo y generar alertas sobre situaciones que requieren revisión de un operador. Y, en respuesta, integrar información de distintas instituciones permite coordinar mejor los equipos y priorizar la atención.

Como Fundación País Digital hemos evidenciado que los municipios y gobiernos regionales reconocen el valor de estas oportunidades porque les aportan conocimiento del territorio y capacidad de monitoreo. El desafío es conectar esas capacidades mediante información compartida de forma segura, protocolos claros y equipos prepara-

dos. Así, una alerta validada puede traducirse en una acción oportuna que proteja a las personas. En Chile ya contamos con iniciativas nacionales como Fiscal HeredIA, de la Fiscalía Nacional, que incorpora inteligencia artificial para apoyar el análisis de información en la persecución penal, y SITIA, orientado a integrar tecnologías de teleprotección para fortalecer la seguridad. Junto con lo anterior, se han desarrollado startups como VSaaS o Delirium IA que han aprovechado las oportunidades de la videoanalítica y hemos encontrado a integradores tradicionales que han querido adentrarse a usar la IA para la inspección de indumentaria de seguridad. El valor está en conectar estas capacidades para que una señal de riesgo se transforme oportunamente en una acción que proteja a las personas.

¿Por qué se vuelve fundamental el uso de la IA considerando la disponibilidad de los recursos policiales y los programas de seguridad?

Los recursos policiales y municipales son limitados, por lo que se necesita utilizarlos con la mayor efectividad posible. La inteligencia artificial per-

mite procesar volúmenes de información que exceden la capacidad de revisión manual y apoyar decisiones sobre dónde concentrar esfuerzos, en qué horarios y frente a qué riesgos.

Un ejemplo concreto aparece en la *Guía Integral de Sistemas de Teleprotección Inteligente*, desarrollada por Fundación País Digital y Fundación Paz Ciudadana. Con analítica avanzada, un operador puede supervisar hasta 300 cámaras en simultáneo, frente a aproximadamente 40 sin estas herramientas. Esta capacidad se apoya en alertas que permiten concentrar la atención en eventos relevantes y priorizar su revisión. Su rendimiento depende de la configuración del sistema, la capacitación y las condiciones de operación.

A esto se suma la interoperabilidad, que los sistemas de seguridad de los municipios, policías y organizaciones de emergencia puedan conectarse y compartir información de manera segura y oportuna. Esto permite aprovechar la infraestructura existente, reducir tareas duplicadas y facilitar que una alerta llegue a quienes deben coordinar la respuesta, con imágenes, ubicación y antecedentes relevantes. Además, utilizar estándares abiertos fa-

cilita integrar equipos de distintos proveedores y ampliar los sistemas a medida que cambian las necesidades.

La combinación de IA e interoperabilidad permite aprovechar mejor cada inversión y fortalecer la coordinación, siempre con protocolos claros, protección de datos y equipos preparados para actuar.

¿Cómo ayuda la inteligencia artificial a enfrentar un fenómeno dinámico y en constante evolución como la delincuencia?

La delincuencia cambia sus modalidades, horarios y lugares de operación. La IA permite procesar grandes volúmenes de datos actualizados y reconocer relaciones entre hechos, personas, vehículos o lugares que sería difícil identificar oportunamente mediante una revisión manual. Esa capacidad ayuda a detectar cambios y adaptar las estrategias de seguridad.

Por ejemplo, Fiscal HeredIA apoya la revisión de antecedentes y la identificación de vínculos en investigaciones complejas, generando conocimiento que antes resultaba difícil de obtener, aunque los datos ya existieran. En teleprotección, el análisis de los eventos registrados también puede orientar ajustes en el monitoreo, el patrullaje y las intervenciones territoriales.

Para que este apoyo sea útil, debemos evaluar y actualizar los modelos, contrastar sus resultados con lo que ocurre en terreno y revisar la calidad de los datos y los posibles sesgos. Las alertas requieren validación humana y la responsabilidad de decidir permanece en las instituciones y sus equipos.

¿Por qué el Summit Seguridad Ciudadana y Emergencias planteó una discusión que va “más allá de la incorporación de nuevas tecnologías”?

La seguridad exige fortalecer el cómo trabajan y colaboran las instituciones. Una cámara aporta cuando un incidente se detecta, un operador valida la alerta y existe un procedimiento para coordinar la respuesta. Del mismo modo, los datos deben ser confiables y llegar oportunamente a las personas autorizadas.

Por eso, el Summit País Digital abordó una jornada especial sobre seguridad y emergencias para reflexionar sobre la gobernanza de los datos, la coordinación institucional y las capacidades humanas, junto con la privacidad, el mantenimiento y la continuidad operacional. La efectividad debe medirse en resultados para la ciudadanía, como mejores tiempos de respuesta y sistemas disponibles cuando se necesitan.

Es importante destacar que Chile ya cuenta con infraestructura, tecnología y experiencia acumulada. Municipios, gobiernos regionales, policías y otras instituciones han construido capacidades relevantes que debemos aprovechar, considerando las distintas necesidades de cada territorio.

El siguiente paso es integrar mejor lo existente, mantenerlo operativo y actualizarlo donde corresponda. Esto requiere conectar plataformas, acordar protocolos de intercambio de información, financiar el mantenimiento y la reposición, y capacitar a los equipos. Las nuevas inversiones deben cubrir brechas concretas y complementar lo disponible. Así podemos convertir esfuerzos que hoy funcionan por separado en una respuesta más coordinada, sostenible y útil para las personas.

Considerando las recientes emergencias por los temporales, ¿qué podemos mencionar respecto de la IA como una herramienta efectiva para responder mejor ante emergencias?

Los eventos climáticos inusuales refuerzan la importancia de anticiparnos y contar con información oportuna para actuar. La inteligencia artificial puede ayudar a integrar pronósticos meteorológicos, sensores hidrológicos, imágenes satelitales y cámaras para estimar cómo podría evolucionar una emergencia y orientar el despliegue preventivo de recursos.

Precisamente, durante el Summit, Vicente Huerfano, de Indra Group, presentó IndraMind y abordó cómo la integración de información proveniente de distintas fuentes permite simular escenarios de riesgo y apoyar decisiones. Su planteamiento destaca un desafío fundamental: lograr que los datos disponibles en distintos sistemas puedan analizarse de manera conjunta.

Frente a lluvias intensas, estas capacidades podrían ayudar a identificar sectores expuestos

a inundaciones, priorizar zonas vulnerables y preparar la respuesta con mayor anticipación. Su efectividad requiere datos confiables, coordinación institucional y comunicaciones y respaldo energético que permitan seguir operando durante la emergencia. Las decisiones siguen siendo humanas y la IA aporta antecedentes para tomarlas con mayor oportunidad y fundamento.

¿Cuál es el compromiso de Fundación País Digital en cuanto a proponer soluciones tecnológicas que deriven en mayores niveles de eficiencia en materia de seguridad y emergencias?

Nuestro compromiso es articular la colaboración entre el sector público, las empresas, la academia y la sociedad civil para convertir las capacidades digitales en soluciones útiles para las personas. Eso supone compartir conocimiento, acercar experiencias y aportar criterios que ayuden a las instituciones a diseñar mejores proyectos y aprovechar sus recursos.

Una expresión concreta es la *Guía Integral de Sistemas de Teleprotección Inteligente*, desarrollada por Fundación País Digital y Fundación Paz Ciudadana, donde participaron más de 40 personas de municipios, gobiernos regionales, fuerzas del orden y seguridad, fabricantes de hardware y software, representantes del sector público y expertos en seguridad, avanzando juntos hacia un modelo más estandarizado, sostenible e inteligente. La guía aborda tecnología, capacidades humanas, coordinación, mantenimiento y sostenibilidad. Buscamos contribuir a que las inversiones se traduzcan en sistemas que funcionen de manera integrada, puedan sostenerse en el tiempo y permitan evaluar su aporte a la prevención y la respuesta ante emergencias.



Marco Terán, director de Desarrollo Digital de Fundación País Digital.



Cuando el regulador se convierte en el cuello de botella

Ley 21.659 elevó los estándares de la seguridad privada y exigió al sector profesionalizarse y adaptarse a un nuevo modelo. Pero su implementación dejó al descubierto una pregunta menos cómoda. ¿Estaba el Estado igualmente preparado para autorizar, fiscalizar y coordinar aquello que comenzaba a exigir?

La nueva Ley de Seguridad Privada significó uno de los cambios regulatorios más importantes que ha experimentado el sector en décadas. Había razones suficientes para actualizar un modelo que llevaba años mostrando signos de agotamiento, elevar los estándares profesionales y ordenar una actividad que hoy tiene una presencia relevante en la protección de personas, bienes e instalaciones.

La necesidad de avanzar en esa dirección era evidente. Las dificultades comenzaron cuando el nuevo estándar tuvo que llevarse a la práctica.

La transición mostró problemas bastante rápido. Se acumularon solicitudes, algunos procedimientos todavía estaban siendo definidos, cambió la distribución de competencias y la plataforma informática fue entrando en operación por etapas. Para empresas, trabajadores, capacitadores y organismos técnicos de capacitación, buena parte de esa incertidumbre tenía efectos muy concretos. Condicionaba su posibilidad de trabajar, contratar personal, impartir cursos o simplemente cumplir con las nuevas exigencias.

Los antecedentes conocidos durante la tramitación de la denominada ley corta ayudan a dimensionar lo ocurrido. Al 7 de mayo de 2026 existían más de 35 mil personas cuyas autorizaciones debían renovarse y 27.826 continuaban pendientes de revisión. A ello se sumaban 3.663 estudios y planes de seguridad pendientes.

La respuesta terminó requiriendo una modificación legal. La Ley N.º 21.825 amplió de seis a dieciocho meses determinados plazos transitorios y estableció un plazo especial de noventa días hábiles para que la Subsecretaría se pronunciara sobre ciertos estudios de seguridad. La medida permitió evitar que una cantidad importante de autorizaciones venciera mientras el sistema todavía trataba de absorber la nueva carga administrativa.

La prórroga era necesaria. También confirmó que la implementación había encontrado problemas bastante más profundos que los ajustes habituales de cualquier cambio normativo.

Profesionalizar también exige capacidad institucional

La Ley 21.659 elevó considerablemente las obligaciones del sector. Para que ese cambio funcionara, la institucionalidad encargada de aplicarlo también debía estar preparada para recibir solicitudes, revisar antecedentes, resolver autorizaciones, administrar sistemas informáticos, fijar criterios y coordinarse con otros organismos.

Era esperable que los primeros meses trajeran dificultades. Lo que cuesta justificar es que algunas se hayan prolongado durante buena parte del año.

Cuando una autorización necesaria para trabajar permanece pendiente durante meses, la demora deja de ser un asunto interno de la Administración. Sus efectos los soporta alguien afuera. Hay profesionales que no pueden ejercer, instituciones que no pueden incorporarlos a sus procesos y empresas que deben reorganizar su operación mientras esperan una decisión que depende exclusivamente del Estado.

Los capacitadores muestran bien ese problema. La nueva regulación exige que quienes desempeñan esa función sean autorizados por la Subsecretaría de Prevención del Delito. Sin embargo, existen solicitudes ingresadas a fines de 2025 y comienzos de 2026 que, avanzado octubre, todavía esperan una resolución definitiva.

No sabemos si esos casos representan el promedio de tramitación del sistema y no sería correcto afirmarlo sin datos oficiales. Pero diez u once meses de espera para una autorización indispensable para ejercer merecen una explicación más convincente que las dificultades propias de una puesta en marcha.

Además, los capacitadores no quedaron comprendidos en la extensión extraordinaria de dieciocho meses que la Ley 21.825 concedió a determinadas categorías del personal de seguridad privada. Para ellos, la autorización anterior mantiene vigencia hasta su vencimiento y luego se requiere

una nueva autorización bajo el régimen actualmente vigente.

El artículo 27 de la Ley N.º 19.880 establece, como regla general, que un procedimiento administrativo no debiera exceder de seis meses desde su inicio hasta la decisión final, salvo caso fortuito o fuerza mayor. Superar ese plazo no permite concluir automáticamente que exista responsabilidad del Estado. Sí permite preguntarse cuánto tiempo debe soportar una persona una demora administrativa cuando esa resolución condiciona directamente su posibilidad de trabajar.

Hay además un elemento que conviene considerar. La Ley 21.659 fue promulgada en marzo de 2024 y comenzó a regir el 28 de noviembre de 2025. La propia ley otorgó hasta un año desde su entrada en vigencia para que la plataforma informática estuviera operativa, es decir, hasta el 28 de noviembre de 2026. Mientras ello no ocurriera, contempló un régimen transitorio para determinadas actuaciones.

A mi juicio, parte de la incertidumbre se produjo porque el nuevo modelo comenzó a desplegarse mientras varios de sus componentes todavía estaban tomando forma. Avanzar antes del vencimiento de ese plazo podía tener sentido. Hacerlo con procedimientos aún en ajuste, capacidades administrativas exigidas al límite y una plataforma que seguía incorporando funcionalidades tuvo costos que terminaron absorbiendo los propios regulados.

Capacitar bajo incertidumbre

La capacitación probablemente sea uno de los ámbitos donde estas dificultades se hicieron más visibles.

La nueva ley pretende elevar el nivel formativo de guardias, vigilantes y demás componentes de la seguridad privada. Para conseguirlo se necesitan instituciones de capacitación funcionando, programas aprobados, capacitadores autorizados y reglas suficientemente claras para organizar los cursos.

Durante varios meses, las OTEC debieron adaptarse mientras el nuevo sistema todavía buscaba estabilidad. Hubo dudas respecto de procedimientos, autorizaciones, exámenes, programas, uso de la plataforma y distribución de competencias entre la Subsecretaría y Carabineros. Parte de esas dificultades llegó incluso a reuniones formales con la autoridad.

El problema de los capacitadores repercute directamente en esa cadena. Una OTEC puede necesitar incorporar a un profesional para impartir determinada materia, pero ese profesional depende previamente de que la autoridad revise y

apruebe sus antecedentes. Si la resolución demora meses, la consecuencia no termina en la carpeta del solicitante. Afecta también a la institución que necesita contratarlo y a las personas que deben capacitarse.

Y aquí aparece uno de los problemas más evidentes de la implementación. La ley exige más capacitación, pero algunos de quienes deben impartirla siguen esperando durante meses la autorización necesaria para hacerlo.

La propia Subsecretaría ha ido corrigiendo algunos problemas. En septiembre dictó la Resolución Exenta N.º 3.493 y precisó diversas exigencias del reglamento. Entre otras materias, estableció que una institución de capacitación que solicita su primera autorización no tiene que acompañar previamente una nómina de capacitadores si todavía no los ha contratado. La resolución reconoce que exigir anticipadamente determinados medios humanos podía dificultar el cumplimiento y resultar desproporcionado.

La corrección parece sensata. También demuestra que varias de las dificultades que el sector venía advirtiendo tenían fundamento.

Las OTEC no son un actor secundario en este proceso. Buena parte de la profesionalización que la nueva ley pretende alcanzar depende de que puedan funcionar con reglas conocidas, respuestas oportunas y acceso suficiente a capacitadores autorizados. Haberlas incorporado con mayor fuerza desde el inicio probablemente habría evitado parte de la incertidumbre que enfrentaron durante los primeros meses.

Pedir paciencia no basta

Este escenario estuvo muy presente en SeguridadExpo 2026, realizada en septiembre en Metropolitan Santiago. La propia feria incluyó dentro de sus actividades un conversatorio dedicado a los desafíos de implementación de la Ley 21.659.

Asistí a varias charlas y conversatorios en los que participó Rodrigo Rojas, jefe de la División de Seguridad Privada de la Subsecretaría de Prevención del Delito. En distintas intervenciones escuché explicaciones similares sobre las dificultades que estaba enfrentando la implementación, la capacidad disponible de la División y la necesidad de que el sector tuviera paciencia mientras el sistema terminaba de ajustarse.

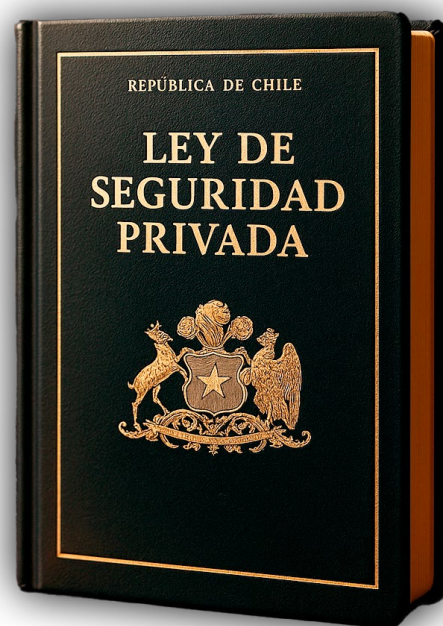
También escuché las preguntas del público. Representantes vinculados a organismos de capacitación plantearon directamente problemas que arrastraban desde hacía meses y reclamaron por falta de respuestas, demoras y procedimientos que todavía no parecían suficientemente claros.

Es comprensible que una autoridad reconozca las dificultades internas de una reforma de esta magnitud. Lo que cuesta aceptar es que la falta de capacidad administrativa termine siendo, en los hechos, una respuesta para quienes dependen de esa misma Administración para poder trabajar. La Ley 21.659 no apareció de improviso. Su tramitación legislativa se extendió por años. Su entrada en vigencia también fue diferida y la transferencia de funciones hacia la Subsecretaría era conocida con anticipación. Si el nuevo modelo necesitaba más personas, mejores sistemas, procedimientos distintos y una coordinación más intensa con otros organismos, buena parte de esas necesidades eran previsibles.

También corresponde hacer una distinción. El diseño de la reforma, su reglamentación y el comienzo de su implementación se desarrollaron durante la administración anterior. La Ley 21.659 fue promulgada en marzo de 2024 y el Reglamento General fue dictado ese mismo año. La actual administración recibió, por tanto, un proceso que ya se encontraba en marcha. La posterior Ley N.º 21.825 (ley corta), promulgada en mayo de 2026, fue precisamente una de las primeras correcciones adoptadas frente a los problemas que ese proceso estaba mostrando.

No se trata de cargar toda la responsabilidad sobre una administración determinada. La cuestión es institucional y atraviesa ambas etapas. Lo relevante es saber si el Estado preparó adecuadamente la transición y si las medidas que se están adoptando serán suficientes para evitar que las demoras se vuelvan permanentes.

La paciencia puede ser razonable durante una transición. Después de muchos meses, ya no basta.



Hay señales de que algunas cosas están comenzando a ordenarse. La Subsecretaría ha dictado nuevas instrucciones, ha precisado criterios y ha mantenido reuniones con distintos actores del sector. La Resolución N.º 3.493 de septiembre es una muestra concreta de ello. Sería injusto desconocer esos avances.

Al mismo tiempo, no existen públicamente cifras suficientemente actualizadas que permitan asegurar que las solicitudes pendientes se han normalizado o que los tiempos de respuesta ya alcanzaron niveles razonables. Esa información sería especialmente útil para saber si el tiempo adicional que entregó la ley corta se está utilizando para resolver los problemas que justificaron su aprobación.

Coordinar antes de exigir

La implementación de la Ley 21.659 tampoco depende de una sola institución. Hay sectores en los que las nuevas reglas deben convivir con regulaciones especiales y con otras autoridades fiscalizadoras. El ámbito aeroportuario es probablemente uno de los mejores ejemplos.

Durante 2026 la Dirección General de Aeronáutica Civil ha debido adecuar normativa y procedimientos al nuevo régimen de seguridad privada. Se han desarrollado instancias de coordinación y se establecieron disposiciones transitorias para el personal de seguridad que trabaja en recintos aeronáuticos. Ese esfuerzo debe reconocerse.

El problema aparece cuando esa coordinación todavía no termina de traducirse en claridad para quienes operan diariamente. Empresas y trabajadores deben cumplir simultáneamente exigencias de seguridad privada, acreditaciones aeroportuarias, normas aeronáuticas y requerimientos administrativos provenientes de organismos distintos.

En un sistema de estas características, una indefinición entre autoridades puede terminar convertida rápidamente en un problema para quien está obligado a cumplir.

La coordinación entre organismos no debería ser un problema que termine resolviendo el regulado. Si dos autoridades deben ponerse de acuerdo respecto de sus competencias, procedimientos o exigencias, esa definición debe producirse antes de trasladar incertidumbre a empresas y trabajadores que están obligados a cumplirlas.

Si el Estado decide elevar el nivel de regulación de una actividad, también tiene que ser capaz de ordenar adecuadamente a sus propios organismos. Durante años el debate estuvo puesto en cuánto debía cambiar la seguridad privada. Había buenas razones para exigirle más. La industria necesitaba mayores estándares, capacitación, control y profesionalización.

Ahora corresponde mirar también al regulador.

Una reforma que pretende profesionalizar un sector no puede conformarse con profesionalizar al regulado. También debe profesionalizar la capacidad del Estado para regularlo.

Eso supone disponer de personal suficiente, plataformas que funcionen, procedimientos comprensibles, plazos razonables y organismos capaces de coordinarse sin transformar sus propias dificultades en una carga adicional para quienes están obligados a cumplir la ley.

El sistema parece haber entrado en una etapa de ajustes más concretos. Algunas normas han debido reinterpretarse, la autoridad ha mantenido diálogo con distintos actores y existen señales de que ciertos procedimientos comienzan a encontrar mayor estabilidad. Es positivo que así sea. Pero tampoco corresponde mirar hacia adelante como si los primeros meses hubieran sido una transición normal y sin costos. Hubo atrasos relevantes, procedimientos que debieron ajustarse y otros que todavía requieren correcciones, problemas de coordinación e incertidumbre para empresas, OTEC, capacitadores y trabajadores.

La nueva regulación elevó el estándar de la seguridad privada y era necesario hacerlo. El desafío ahora es que la institucionalidad encargada de aplicarla alcance ese mismo estándar. De poco sirve construir un sistema más exigente si cumplir sus reglas depende de autorizaciones que tardan meses, plataformas todavía en ajuste o competencias que el propio Estado debe terminar de ordenar. Esa sigue siendo, a casi un año de iniciado el nuevo régimen, una de las principales tareas pendientes de la reforma.



Autor: Julio Ibáñez Fernández
Abogado, Magíster en Derecho Público.
Máster de Formación Permanente en Seguridad Pública
por la Universidad de Salamanca, España.
Diplomado en Supervisión y Gestión de Seguridad Privada por la
Pontificia Universidad Católica de Chile.
Autor del libro Seguridad Municipal en Chile: Estado actual, desafíos
y perspectivas interdisciplinarias.
Asesor y capacitador en materias de seguridad pública y privada.



Miguel Pérez, CEO de NOVARED, dando la bienvenida y abriendo el evento.

NOVARED

Security Workshop 2026

La ciberseguridad en tiempos de cambios

Desde su nacimiento en 2004, NOVARED Security Workshop se ha consolidado como un espacio de encuentro para quienes tienen la responsabilidad de tomar decisiones en materia de seguridad digital. A lo largo de su trayectoria, el evento ha acompañado la evolución de una industria que hoy enfrenta uno de sus mayores puntos de inflexión como es la convergencia entre inteligencia artificial, datos, automatización y ciberseguridad. En 2026, este desafío adquiere una nueva dimensión. Mientras la IA abre oportunidades para fortalecer la detección de amenazas y automatizar las respuestas de seguridad, también entrega nuevas capacidades a los atacantes. Para conocer los alcances de esta nueva versión de NSW 2026, conversamos con Miguel Pérez, CEO de NOVARED.

¿Qué podemos mencionar con respecto del evento NSW 2026 y de su trayectoria previa?

Con más de 20 años de trayectoria, el Novared Security Workshop se ha convertido en un referente para la industria de la ciberseguridad en Chile. Es un encuentro que se distingue por su formato, diseñado específicamente para el sector, y que reúne a fabricantes tecnológicos, especialistas y líderes empresariales.

Cada año buscamos reinventarnos, desarrollando un nuevo concepto y una puesta en escena que va más allá de las charlas técnicas. Nuestro objetivo es que cada edición sea una experiencia diferente, que combine conocimiento, innovación y relacionamiento, aportando valor a todos quienes nos acompañan.

¿Qué tan preparadas están las organizaciones para enfrentar el nivel actual de sofisticación de los ciberataques?

La realidad es que el nivel de preparación sigue siendo muy desigual. Mientras algunas organizaciones han avanzado significativamente en sus estrategias de protección, otras todavía presentan brechas importantes.

La incorporación de inteligencia artificial en los ciberataques está cambiando las reglas del juego. Hoy los atacantes pueden identificar vulnerabilidades, automatizar procesos y ejecutar ataques con una velocidad y escala mucho mayores.

Esto obliga a las empresas a revisar constantemente sus capacidades de defensa. Ya no basta con contar con herramientas de seguridad; es necesario tener visibilidad, capacidad de anticipación y, sobre todo, estar preparados para responder oportunamente cuando ocurre un incidente.

¿Cómo están utilizando los atacantes la IA generativa y de qué manera deben evolucionar las defensas corporativas para no quedar obsoletas?

La inteligencia artificial está siendo utilizada prácticamente en todas las etapas de un ciberataque, desde la identificación de vulnerabilidades y la generación de código malicioso hasta la automatización de ataques y la búsqueda de nuevas formas de comprometer los sistemas.

Frente a este escenario, las organizaciones necesitan evolucionar hacia modelos de seguridad más proactivos. Esto implica mejorar la identificación

y corrección de vulnerabilidades, avanzar en estrategias Zero Trust, fortalecer el monitoreo y automatizar la respuesta ante amenazas. Muchas de estas tecnologías ya están disponibles. El desafío está en incorporarlas de manera efectiva y coordinada dentro de las estrategias de seguridad de las empresas.

¿Cuáles son los riesgos asociados a que la IA consuma, procese y decida con datos corporativos? ¿Qué papel juegan los marcos de gobernanza aquí?

Uno de los principales riesgos es que la inteligencia artificial introduce nuevas superficies de ataque y, al mismo tiempo, puede facilitar la exposición involuntaria de información sensible.

Cuando una organización utiliza IA para procesar datos o tomar decisiones, necesita tener claridad sobre qué información está utilizando, quién puede acceder a ella y bajo qué condiciones opera.

Aquí la gobernanza cumple un papel fundamental. No se trata de limitar el uso de inteligencia artificial, sino de establecer políticas, controles y responsabilidades que permitan aprovechar sus beneficios de manera segura.

La adopción de IA debe ir acompañada de una estrategia de seguridad y gobierno de datos desde el inicio, no incorporarse como una medida posterior.

¿De qué manera normativas como la Ley Marco de Ciberseguridad de Chile o las regulaciones internacionales DORA y NIS2 elevan las exigencias de resiliencia operativa?

Estas normativas están impulsando un cambio importante en la manera en que las organizaciones abordan la ciberseguridad. Ya no se trata únicamente de proteger los sistemas, sino también de demostrar que existe capacidad para responder, recuperarse y mantener la continuidad operacional frente a un incidente.

Naturalmente, el impacto depende del nivel de madurez de cada organización. Las empresas que ya cuentan con estrategias sólidas tienen parte del camino avanzado, mientras que aquellas con mayores brechas deberán realizar esfuerzos adicionales para cumplir con las nuevas exigencias.

Un aspecto especialmente relevante es que estas regulaciones también elevan los estándares de seguridad de proveedores y terceros, fortaleciendo la resiliencia de toda la cadena de suministro.

¿Cómo redefine la IA la seguridad en industrias críticas chilenas como la minería (específicamente el cobre y el litio), la banca y el retail?

La inteligencia artificial representa una gran oportunidad para fortalecer la seguridad de estas industrias, pero también introduce nuevos riesgos.

En sectores como la minería, la banca o el retail, donde la continuidad operacional y la protección de la información son fundamentales, la IA permite mejorar la detección de amenazas, automatizar procesos de seguridad y reducir los tiempos de respuesta.

Sin embargo, cuando estas tecnologías no se implementan con los controles adecuados, pueden convertirse en nuevos puntos de vulnerabilidad.

Por eso, el desafío no es simplemente incorporar inteligencia artificial, sino hacerlo de manera segura, considerando las particularidades y riesgos operacionales de cada industria.

¿Qué implicaciones tiene la transición desde el uso operativo de la IA hacia sistemas AI-native y agentes autónomos?

Estamos pasando de utilizar la inteligencia artificial como una herramienta de apoyo a desarrollar sistemas capaces de tomar decisiones y ejecutar acciones con distintos niveles de autonomía.

Este cambio abre enormes oportunidades en términos de eficiencia y automatización, pero también plantea desafíos importantes de seguridad y control.

Cuando un sistema puede actuar de manera autónoma, es fundamental establecer límites claros sobre qué decisiones puede tomar, a qué información tiene acceso y cómo se supervisa su comportamiento.



Miguel Pérez, CEO de NOVARED, y Leticia Setembro, futurista internacional y CEO de Seek Futures.



NSW se ha consolidado como un espacio de encuentro para profesionales, especialistas y tomadores de decisiones vinculados a la seguridad digital.



Gran interés generó el evento de NOVARED entre el público.

Por eso, a medida que avanzamos hacia sistemas más autónomos, la gobernanza y los mecanismos de control se vuelven tan importantes como la propia tecnología.

¿Qué amenazas y tecnologías emergentes (como la computación cuántica y la criptografía poscuántica) redefinirán el sector hacia el año 2030?

Sin duda, la inteligencia artificial será uno de los factores que más transformará la ciberseguridad durante los próximos años, tanto por las capacidades que entrega a los atacantes como por las nuevas herramientas de protección que permite desarrollar.

Pero también debemos mirar otras tecnologías emergentes, como la computación cuántica, que plantea desafíos importantes para los actuales mecanismos de cifrado y hace necesario comenzar a prepararse para la transición hacia la criptografía poscuántica.

A esto se suma un escenario geopolítico cada vez más complejo, donde los conflictos internacionales pueden tener consecuencias digitales que trascienden las fronteras.

Hacia 2030, las organizaciones necesitarán estrategias de seguridad mucho más flexibles, capaces de adaptarse a amenazas que evolucionan constantemente.

¿Cuál es la dualidad de la IA al automatizar respuestas de seguridad frente a las nuevas capacidades que otorga a los atacantes?

La inteligencia artificial tiene una característica muy particular: las mismas capacidades que permiten fortalecer la seguridad también pueden ser utilizadas para desarrollar ataques más sofisticados.

Por una parte, permite detectar comportamientos anómalos, analizar grandes volúmenes de información y responder a incidentes con mayor rapidez. Pero esas mismas capacidades pueden ser aprovechadas por los ciberdelincuentes para automatizar ataques, identificar vulnerabilidades y aumentar su efectividad.

Esto genera una evolución constante entre las capacidades de ataque y defensa. La diferencia estará en qué tan preparadas estén las organizaciones para aprovechar estas tecnologías, integrarlas a sus estrategias y mantener el control sobre su funcionamiento.

Este evento contó con la presencia de Letícia Sestembro, futurista y conferencista internacional. *Respecto de su exposición, ¿cuáles son los prin-*

cipales escenarios que podrían redefinir el sector hacia 2030 y cuáles podrían ser las mayores amenazas potenciales?

La exposición de Letícia nos invitó a mirar más allá de los desafíos actuales y entender cómo la tecnología, especialmente la inteligencia artificial, está transformando el futuro de la ciberseguridad.

De cara a 2030, vemos tres grandes cambios. Por una parte, el avance de inteligencias artificiales cada vez más autónomas, capaces de tomar decisiones y ejecutar acciones, tanto para atacar como para defender. Por otra, una creciente dificultad para distinguir lo real de lo falso, con tecnologías como los deepfakes y la suplantación de identidades, que ponen en riesgo la confianza digital. Y, finalmente, una evolución hacia sistemas de seguridad más predictivos, capaces de anticiparse a las amenazas y responder de manera automática. En este escenario, las principales preocupaciones estarán en los ataques automatizados mediante IA, los fraudes cada vez más personalizados y las amenazas a infraestructuras críticas.

Creo que el gran desafío hacia 2030 no será únicamente contar con mejores tecnologías de protección, sino ser capaces de mantener la confianza en un entorno donde personas, organizaciones y sistemas inteligentes estarán cada vez más conectados.



Fernando Fuentes, gerente de I&D de NOVARED estuvo a cargo de la charla de cierre de NSW.



El modelo de seguridad y policía KOBAN en japon

Símbolo de paz, orden y respeto recíproco entre policía y comunidad

La International Police Association (IPA) - Sección Japón - Filial Osaka organizó el "Seminario Japón 2026" en la Prefectura de Osaka en el Hotel Agora Regency Osaka Sakai entre el 12 al 14 de octubre de 2026, dicho evento tuvo como finalidad proveer a los participantes con una visión global, conocimientos y experiencias en cooperación internacional e investigación, así como las habilidades necesarias para trabajar en el ámbito internacional en el futuro. Las palabras de bienvenida estuvieron a cargo de Tomio Kawabata, presidente de la IPA de Osaka, siendo luego inaugurado el evento por Masahito Kanetaka, presidente nacional de la IPA de Japón y ex presidente de la Agencia Nacional de Policía de Japón y finalmente, Javier Gamero Kinoshita, representante de la IPA – Sección Perú e invitado especial al evento, tuvo a su cargo el discurso de orden en la ceremonia inaugural, el coordinador del seminario, Ryogi Suzuki tuvo a su cargo la conducción y el desarrollo del seminario.

Contenidos temáticos abordados en el evento fueron la exportación del sistema Koban desde el país más seguro, la cooperación internacional de la policía japonesa, la situación de la seguridad pública y medidas de respuesta en Osaka, la policía comunitaria en Japón, La responsabilidad de la policía a la hora de garantizar una sociedad digital segura, el control del crimen organizado en Japón y medidas de seguridad vial en Japón.

Los expositores fueron expertos y autoridades policiales y políticas del Japón, así como oficiales de policía de Alemania, Canadá, Paquistán, Sudáfrica y Perú. El criminólogo Javier Gamero Kinoshita, miembro de la Legión de Honor de la Benemérita Guardia Civil del Perú y de IPA representó al Perú con la conferencia magistral internacional "La nueva gerencia pública para una adecuada producción de seguridad en el siglo XXI". Dicho seminario incluyó una visita a una caseta Koban en Osaka, así como una visita al jefe de la Policía de la Prefectura de Osaka, comisionado Tetsuro Kamata, quien estuvo acompañado del subjefe de la Policía de la Prefectura de Osaka Yusuke Kawahara y del director de educación y entrenamiento de la Policía de la Prefectura de Osaka Yuji Mishi.

Japón el país más seguro del mundo

Japón tiene una población de 124'710,000 hab. y la Policía del Japón cuenta con 274,000 efectivos en su totalidad, distribuidos en su cuerpo nacional principal, la Agencia Nacional de Policía de Japón que coordina las fuerzas policiales de las 47 prefecturas, las estaciones de policía (Keit-satzucho) y los puestos locales tanto en el ámbito urbano con el sistema Koban, como en el ámbito rural con el sistema Chuzaicho.

Masahito Kanetaka, ex presidente de la Agencia Nacional de Policía de Japón y actual presidente de la International Police Association (IPA) Sección Japón, recalcó en su ponencia "La exportación del sistema Koban en el mundo" analizando las principales tasas de criminalidad entre los países del G7 (Grupo de los Siete: Alemania, Canadá, Estados Unidos, Francia, Italia, Japón, Reino Unido y la Unión Europea), que los homicidios en Japón, alcanzan una tasa de 0,2 por cada 100,000 hab., mientras que la de EE. UU., es de 6,5, lo que supone 33 veces más que la de Japón. Por su parte, los demás países europeos se sitúan en torno a una tasa de 1, lo que supone entre 4 y 6 veces más que en Japón. América Latina alcan-

za una tasa promedio de 24 homicidios por cada 100,000 hab. La media estándar internacional es de 6 homicidios por cada 100,000 hab. En lo que concierne a robos con allanamiento, la tasa de delincuencia del Japón es de 29. En los demás países oscila entre 270 y 450, lo que supone entre 9 y 15 veces más que en Japón. Ello conllevó a Kanetaka a afirmar que Japón sigue siendo el país más seguro.

Kazuko Sato, Inspectora de Policía de la Estación de Policía de Kamakura presentó en el Seminario Japón 2026 una disertación acerca "De la guerra del tráfico a caminos más seguros", sosteniendo que en el Japón se han producido tres guerras contra los accidentes de tráfico, tanto en 1970, 1974 y 1992 reduciéndose ostensiblemente el número de accidente de tránsito. En 1970 se produjeron 16,775 accidentes, en 1974 se redujeron a 11,452 accidentes y por último en 1992, se redujeron a 2,547 accidentes. La incidencia de accidentes de tránsito bajó un 85% alcanzándose un alto índice de seguridad vial en el país. Factor esencial de la reducción ostensible de accidentes de tránsito con muertes y lesiones fue la educación vial en todo el país a través del sistema Koban. Tarea esencial de la policía de tránsito fue

garantizar la seguridad vial, garantizar la circulación fluida del tráfico y prevenir los obstáculos al tráfico, así como proteger la vida, el cuerpo y la salud y, por último, la propiedad.

Shigetaka Kai, miembro de la International Police Association (IPA) - Sección Japón en su alocución titulada "El control del crimen organizado en el Japón", se refirió al tráfico de estupefacientes en ese país, siendo las más frecuentes: la meta anfetamina, la heroína, la cocaína, el fentanilo, los cigarrillos zombis (cigarrillos electrónicos o vaporizadores que producen un estado de euforia y otros efectos adversos) y el éxtasis), el tráfico de armas y los grupos criminales que operan en el Japón, tales como la tradicional Yakuza, Tokuryu, la mafia más joven y tecnológica del país, que va desplazando a la tradicional Yakuza, ella se caracteriza por no tener jerarquías fijas, mi estructura piramidal clásica, ni sedes visibles, ni códigos de honor tradicionales, operando en las redes sociales, el Dragón Chino, una pandilla criminal conocida como semi Yakuza, que fue fundada en Tokio y que está conformada por hijos o descendientes de japoneses que quedaron abandonados en China tras la Segunda Guerra Mundial y que posteriormente retornaron a Japón, Snake Head, organización criminal dedicada a la trata de personas y la Mafia Taiwanesa. Asimismo, manifestó que el número de miembros de bandas criminales que operan en Japón alcanzó su mínimo histórico a finales de 2025. El declive de los sindicatos o grupos criminales en el Japón continúa. El número de sus miembros, que hace 20 años superaba los 40,000, se redujo a 9,400 a finales de 2025. Ello se debió a la cooperación público - privado, el problema es común para ambos sectores.

La seguridad en el Japón y su sistema policial de tres niveles

El investigador británico Barnaby Sorrens sostiene en su libro: "Policing in Japan" que las estadísticas no pueden ser ignoradas, los índices de violencia criminal son sorprendentemente bajos comparados con los estándares globales, los niños caminan solos hacia las escuelas en los centros urbanos, los artículos perdidos (billeteras, carteras, bolsos, paraguas...) son devueltos a sus propietarios, las peleas públicas, los robos y las confrontaciones son raras, sus calles son ordenadas y tienen un profundo sentimiento de comunidad gracias al sistema policial Koban, piedra angular de la convivencia pacífica en el Japón, que contribuye al equilibrio social y cultural del país. La presencia del oficial de policía Koban, que observa con serenidad el vaivén de la vida urbana forma, es sin duda, parte de la ecuación.

El sistema policial de Japón está organizado en un inteligente sistema de tres niveles que cubre la seguridad en cada rincón del país: 1). Keisatsucho (Estación de policía): Cuartel general o Jefatura

de Policía a escala real, son grandes instalaciones donde diversas divisiones policiales realizan las investigaciones de grandes delitos, investigaciones y trabajo administrativo de comando tales como, terrorismo, cibercrimen, tráfico de drogas, tráfico de armas, control del tráfico, etc. Atienden a muchos cientos de miles de ciudadanos en su jurisdicción, 2) El sistema Koban (caseta o cabina policial): con el nivel medio, tienen su jurisdicción en áreas urbanas, focalizados en el patrullaje policial y asistencia al ciudadano en sus jurisdicciones distritales y 3) Chuzasho (residencia policial rural): situadas en el área rural en pueblos y distritos remotos, a cargo de un oficial de policía que vive en la residencia con su familia. Es parte oficial de policía, parte trabajador social y parte organizador de la comunidad (no es trabajador de la comuna, pero vive allí).

El sistema de policía comunitaria en Japón

Un Koban es una miniestación de policía, esencialmente un caseta o cabina policial en el corazón del vecindario de las áreas urbanas del Japón, su presencia simboliza el rostro humano de la policía japonesa en cada comunidad. Los oficiales Koban son guías, mediadores, ayudantes y vigilantes protectores que prestan servicios 24/7. El espíritu Koban se basa en la filosofía de proximidad, familiaridad y presencia preventiva y refleja las actitudes, valores y hábitos de la comunidad. Es una forma de policiamiento profundamente humano, un modelo de policiamiento orientado a la comunidad. Ellos son una extensión de las normas sociales japonesas, si bien es cierto que visten un uniforme y desempeñan funciones oficiales son extremadamente educados y amigables. Se espera que los oficiales Koban proyecten autoridad mien-

tras demuestren humildad, que sean firmes en el cumplimiento de las normas mostrando siempre compasión y a actuar decisivamente con paciencia. Esta dualidad de actuación refleja el orgullo de la policía japonesa de mantener el orden sin recurrir a la fuerza y ganarse el respeto sin demandarlo.

Estas casetas policiales están situadas estratégicamente en zonas de alta densidad de tráfico vehicular, tales como en zonas aledañas a las estaciones de tren, intersecciones de buses, grandes centros comerciales, zonas escolares, avenidas principales, etc.

El diseño físico de estas cabinas refleja el espíritu Koban, de apertura, accesibilidad, proximidad, posee grandes ventanas, a pesar de ser pequeños, están amoblados con sillas para el público, mapas del área local para el uso público (visibilidad, accesibilidad y familiaridad). Los oficiales de policía Koban están especializados en labores de patrullaje local a pie, con bicicletas o en vehículos si el caso lo requiere y, prestar asistencia a los ciudadanos. Ellos prestan servicios en determinados blocks de un distrito específico, teniendo un profundo conocimiento del área jurisdiccional.

El sistema Koban representa la contraparte de esas formas de policiamiento reactivas, militarizadas y con un alto nivel de vigilancia. Es una solución de baja tecnología, pero con un alto nivel de atención personalizada. Mientras que Japón está en la vanguardia de la Inteligencia artificial, la robótica, la infraestructura de las ciudades inteligentes, su modalidad de policiamiento se sigue basando en la presencia, la confianza y la interacción humana. Existe evidencia que la relación



El Koban de Sukiya-bashi en Yurakucho, en el centro de Tokio, es un Koban histórico que se estableció en 1872.

cotidiana entre oficiales de policía y civiles en el Japón es cada vez más cooperativa que confrontacional, gracias al sistema de policiaimiento Koban.

Entendiendo el sistema policial Koban, nos servirá de punto de partida para entender los valores japoneses comunidad, respeto, armonía y deber. Una cultura en donde la autoridad coexiste con la empatía, en donde no se requiere apelar a la confrontación y en donde los límites entre el bienestar personal y el bien común se difuminan deliberadamente por el bien común. El sistema policial Koban es un emblema del compromiso permanente de Japón por la paz, el orden y el mutuo respeto. El sistema Koban es algo más que una caseta policial con modesta estructura en una esquina o intersección de una calle residencial, ella es la piedra filosofal de la seguridad local y un símbolo de confianza serena en sus fuerzas del orden.

Los oficiales Koban en sus casetas policiales son llamados "señor patrulla"

Esa denominación "señor patrulla" transmite autoridad respetuosa y preocupación vecinal. El sistema Koban es el rostro amigable de la autoridad. Humaniza el rol del oficial de policía removiendo las barreras que pueden existir entre ciudadanos y la policía en otras culturas. El sistema Koban es parte de la cultura cívica en donde la seguridad es una responsabilidad colectiva. Los niños visitan desde los primeros años de escuela los locales Koban y reciben clases de educación cívica

inspiradas en el respeto mutuo, responsabilidad y cuidado comunitario. El sistema Koban es una cultura de servicio, no una vigilancia, el modelo Koban es un contraste de las estrategias policiales de la denominada "sociedad de vigilancia" que prevalece en otros países. A pesar de que Japón es un país experto en tecnología, sin embargo, sus estrategias de policiaimiento se caracterizan por ser de baja tecnología. La efectividad del sistema policial Koban no yacen en el reconocimiento facial a través de cámaras, la lectura de los datos de algoritmos o la medición de latidos del corazón, sino en la interacción cara a cara o en las visitas a los vecinos en sus domicilios.

Graduarse como oficial Koban implica no solo aprobar exámenes físicos y procesos de aprendizaje, los oficiales Koban reciben instrucción no solo en técnicas de aplicación de la ley. También son entrenados en comunicación interpersonal, resolución de crisis, sensibilidad cultural y participación comunitaria y aprenden a desactivar tensiones para una desescalada de conflictos, a leer el lenguaje no verbal y como mantener la calma en situaciones de alto estrés.

El sistema Koban implica un control policial a través de la familiaridad, previniendo el crimen a través de las relaciones sociales. La interacción constante tiene un efecto preventivo, cuando un bodeguero avisa de actitudes sospechosas de algún vecino o un maestro nota algo respecto a la conducta de un niño, o un vecino advierte de una actividad inusual de un residente puede ser una información clave. La interacción viene a

constituir la columna vertebral del policiaimiento proactivo.

El sistema Koban: piedra angular del bajo índice de criminalidad

No es una hipótesis afirmar que Japón es uno de los países más seguros del mundo. Ello se debe a las normas culturales, la estabilidad socioeconómica, el robusto sistema legal y el rol del sistema policial Koban basado en la integración en la comunidad y la filosofía de policiaimiento proactiva. El sistema Koban es visible, predictivo y está presente. Mientras otras fuerzas policiales tienen grandes recintos de unidades acuarteladas, el sistema Koban está enclavado directamente dentro de las comunidades donde prestan servicios. Se tiene más de 6,300 locales Koban en Japón en los centros urbanos y suburbanos los cuales son visibles y marcan una presencia policial constante. En Tokio hay 1,000 casetas Koban. Existen los Koban móviles o mini-Koban (en estaciones de tren, centros comerciales) y los Chuzashos en zonas rurales (6,200).

El sistema Koban enfatiza lo proactivo, no lo reactivo, en muchas latitudes de Occidente la filosofía del policiaimiento se centra en lo contrario. El patrullaje a pie, en bicicleta, a caballo o motorizado engancha con el público. El sistema Koban humaniza al oficial, construyendo familiaridad y confianza, normaliza las conversaciones del ciudadano con el policía. El oficial Koban reúne información de inteligencia a través de las relaciones, no utilizando necesariamente la vigilancia o tec-





Entre las principales actividades del Seminario Japón 2026 destacamos de (izq. a der.) a Masahito Kanetaka, presidente IPA Sección Japón, Tomio Kawabata, presidente IPA Japón - Filial Osaka y Ryogi Suzuki, coordinador del Seminario de la IPA de Japón.

nología permitiéndole desarrollar un mapa social en su jurisdicción. El sistema Koban focaliza la prevención sobre la represión, priorizando el orden y la rehabilitación, los oficiales Koban son entrenados en técnicas de mediación, conciliación y arreglo amistoso, buscan mediar y educar, ellos realizan visitas regulares en el vecindario. Los oficiales Koban no son bomberos que van a apagar incendios sino carteros, pero sin cartas, recorren el vecindario, tocan las puertas de los vecinos y dialogan cara a cara sobre los problemas de la comunidad.

La Agencia de la Policía Nacional de Japón revela que la criminalidad se ha reducido ostensiblemente en las dos últimas décadas. La tasa de homicidios es de 0.2 por cada 100,000 habitantes, una de las más bajas del globo. El número de asesinatos reportados en un año es menos de 100. Ello se debe a los valores de respeto mutuo, responsabilidad, orden, a la estabilidad económica, la educación, el ordenamiento jurídico del país y al sistema Koban que opera a través de su sistema físico de manera visible, funcional y efectiva.

Mecanismos de visitas a familias a domicilio y prevención comunitaria

En muchos países la idea de que un policía uniformado visite un domicilio sin anunciarse, generaría incomodidad, disconformidad y sospecha, en Japón sería al revés y sería siempre bienvenido. En Japón se denominan "visitas de enlace rutinarias" o "contacto de patrulla", este sistema Koban reafirma la idea de que la seguridad comunitaria se nutre de la relación interpersonal construyendo confianza, familiaridad y responsabilidad mutua. Los oficiales de patrullaje tocan cada puerta del vecindario y se presentan y entabla una breve conversación. No hay órdenes de arresto, ni investigaciones en curso, ni preguntas ni sospechas, la finalidad es obtener información sobre el número de miembros de la familia, si hay personas discapacitadas o adultos mayores, que luego será registrada en una ficha de datos del hogar, reparten folletos informativos sobre medi-

das de seguridad, que incluyen números telefónicos de emergencia. El objetivo no es vigilancia o control sino conexión.

El oficial Koban fomenta la confianza a través de la familiaridad. En muchos países los agentes de policía son percibidos como agentes reactivos, creando una distancia psicológica entre oficiales y ciudadanos, especialmente en comunidades que han experimentado abuso policial. En Japón estas visitas son estratégicas e introducen al policía en la vida de los ciudadanos ordinarios, no durante momentos de crisis sino durante momentos de calma. Ver un oficial con una sonrisa esfumará cualquier miedo al uniforme. Hay quienes consideran que estas prácticas son paternalistas y están en el límite de la vigilancia y el control, sin embargo, esta colección de información acerca de los hogares tiene propósitos benevolentes, pueden ser consideradas por sus críticos como medidas intrusivas que invaden la esfera personal, sin embargo, esta práctica en Japón se ha ido fortaleciendo por décadas y cuenta con el debido soporte institucional y social.

El oficial Koban es percibido como un vecino. Los residentes deben verlo como un aliado presto a rendir cuentas al vecindario. Ellos no solo mantienen el orden, sino que participan en el bienestar de la gente del vecindario, en otras latitudes los cuerpos de policía afrontan una crisis de legitimidad social.

La amplia gama de servicios del sistema Koban

En muchos países la palabra policía está asociada a vehículos policiales, esposas, varas de la ley, y aplicaciones de la normativa con importantes repercusiones. Los oficiales de policía responden a la actividad criminal, investigando los delitos y manteniendo el orden en tiempos de dislocaciones sociales. Sin embargo, en el Japón el sistema Koban va más allá del crimen, ellos son guías comunitarios, mediadores de conflictos, educadores de seguridad y guardianes de los ciudadanos más vulnerables. La armonía social no se preserva solo con la supresión o represión del

crimen sino a través del cultivo de la seguridad, confianza y la asistencia cotidiana.

Las casetas Koban, son navegadores en el laberinto urbano, ello no tiene que ver con el combate de la delincuencia, proporcionando direcciones domiciliarias, ya que el sistema de direcciones, en comparación con otros países, no es lineal, la conexión entre los números de inmuebles o edificios y su ubicación física a lo largo de las calles no son secuenciales, brindan especial atención a los turistas y personas foráneas ayudándolos a ubicar un domicilio, una estación de bus, un centro comercial., poseen conocimientos del idioma inglés. Los oficiales Koban están en la primera línea de las infracciones menores (robos de bicicletas, queja de ruidos molestos, disputas en el vecindario, etc.)

Los oficiales Koban son mediadores de conflictos, conciliadores y consejeros civiles solucionando las disputas vecinales, los malentendidos, las desavenencias sociales producto de ruidos molestos, los límites de propiedad. Ellos visitan como servidores imparciales de la comunidad a ambas partes y escuchan sus quejas y median para que no escale el conflicto. Se valen de la diplomacia personal para solucionar los problemas, ya que gozan de la confianza y respeto por parte de todos los ciudadanos. La intervención temprana de los oficiales Koban refuerzan la cohesión social y evita una escalada del conflicto. Los oficiales Koban son protectores de las personas vulnerables. La población del Japón tiene un 28% de población de adultos mayores de más de 65 años, en consecuencia, los oficiales Koban los protegen de la explotación, el olvido o ser víctimas de fraude. Igual sucede con personas con problemas mentales o alguna discapacidad física. La protección tiene una connotación emocional, las personas de edad viven por lo general aisladas y estas visitas policiales son muy reconfortantes para los ciudadanos mayores.

Los oficiales Koban son educadores, la educación pública es parte de su función. Visitan rutinaria-

mente escuelas, centros comunitarios, organizan seminarios de seguridad y campañas de concientización e imparten clases de educación vial en las escuelas a los niños a temprana edad. Durante los desastres o emergencias nacionales en caso de terremotos, ellos coordinan los esfuerzos de defensa civil, guían las evacuaciones, ayudan a localizar personas perdidas e imparten informaciones en tiempo real. Las casetas Koban sirven de un lugar de refugio, ya sea para un niño separado de sus padres en un centro comercial o una mujer víctima de violencia familiar o acoso sexual, o alguien que sufre un accidente, o que necesita algo de dinero urgente (préstamo), o desea hacer una llamada telefónica o ha encontrado un objeto valioso, todos los ciudadanos acuden a una caseta Koban para pedir ayuda. El sentido de santuario no es accidental ya que durante décadas los oficiales Koban han cultivado la interacción positiva con la comunidad (visibilidad, accesibilidad, transparencia y seguridad). El sistema Koban tiene un rol elástico y evolutivo hoy en día debido a que la sociedad japonesa ha cambiado demográfica, tecnológica y culturalmente.

Los oficiales Koban están envueltos en la educación de la ciberseguridad (protección de identidad digital, identificación de emails, phishing para eludir estafas online, etc.). El sistema Koban es el rostro de la policía comunitaria del Japón y representa el corazón de la comunidad: son navegadores, mediadores, educadores, protectores y vigilantes, en suma, servidores públicos en el estricto sentido de la palabra.

El sistema Koban refleja el principio arraigado de que la seguridad y el bienestar social están entrelazados. La prevención del crimen no comienza con sirenas y arrestos sino con conversaciones, direcciones, controles y cuidados. La prevención comienza conociendo a los vecinos y a la vez ser conocido por ellos. Este modelo de policiamiento comunitario se ejecuta no a través del poder sino a través del servicio, no a través de miedo, sino a través de la familiaridad y, por último; no a través del mandato, sino a través de la conexión.

El Chuzaisho: la contraparte rural al sistema Koban

Es una institución menos conocida, pero de igual importancia, ya que presta servicios de policiamiento en el Japón rural. Son subestaciones policiales residenciales que se encuentran ubicadas en las zonas más remotas de la sociedad japonesa, a pesar de ser menos en número que las casetas urbanas Koban, los Chuzaisho están dispersos más lejos geográficamente y se rigen por los mismos principios del sistema Koban (comunidad, familiaridad y un profundo sentido de cohesión social) siendo parte del tejido social. El modelo Chuzai-

sho tiene un concepto de residencia, el oficial vive entre la gente, su estructura es simple y tiene doble historia, en la parte anterior está la oficina y en la parte posterior es la casa cuartel en donde el oficial vive con su esposa e hijos. Mezcla el deber público con la vida privada generando una atmósfera genuina de integración. Las ventajas: el oficial está siempre presente y disponible, en casos de emergencia no hay pérdida de tiempo para su movilización, está siempre listo, su presencia 24/7 es invaluable en zonas remotas. La presencia no solo es física sino psicológica (familiaridad, cohesión social plena).

El sistema policial Koban: un modelo para el mundo

El sistema Koban del Japón no es un mero logro doméstico, es un concepto exportable ya que ha captado la atención de políticos, criminólogos e investigadores. En una era en que las relaciones policía-ciudadano se van tornado cada vez más tensas en virtud de los cambios vertiginosos, la reputación del sistema Koban fundada en accesibilidad, confianza y un compromiso proactivo con la comunidad, toma relevancia. Japón es conocido por ser un país exportador de automóviles, dispositivos electrónicos y cultura popular, hoy en día, recalca Masahito Kanetaka, ex presidente de la Agencia Nacional de Policía de Japón, se le conoce como un país exportador de una filosofía de policiamiento, una filosofía de proximidad y una filosofía de atención preventiva. La Agencia de Cooperación Internacional del Japón (JICA) ha llevado a cabo programas de cooperación bilaterales respecto al modelo de policía comunitaria del Japón, vale decir el sistema Koban con Singapur (en 1980 para sustituir los métodos

policiales tradicionales reactivos ante la expansión urbana y el crecimiento de la población con mayor diversidad étnica), con Brasil (Sao Paulo, en el año 2000 oficiales brasileños viajan a Japón para entrenamiento no solo de métodos tácticos sino para conocer el ethos cultural del sistema Koban), con Indonesia (implementación en toda la isla a mediados del año 2000) y con los EE.UU (Los Ángeles y Boston para contrarrestar el modelo policial militarizado de la "tolerancia cero")

Reflexión final

Pasar caminando por una caseta Koban es algo más que solo ver un edificio policial, es dar testimonio de un acuerdo social y entender que la preservación de la paz no es solo un trabajo policial sino de cada uno. Es un espacio donde la formalidad se une a la cordialidad, donde el deber se une a la buena vecindad y donde las fuerzas del orden no son un símbolo de miedo, sino de tranquilidad. El sistema Koban muestra lo que se puede lograr cuando una sociedad invierte no solo en infraestructuras o en inteligencia, sino también en la relación personal y la confianza mutua y; en ese trabajo cotidiano, a menudo invisible, de conocer y ser conocido.

En un mundo frecuentemente fracturado, adverso y de rápido movimiento, el recinto Koban se erige como un símbolo silencioso de algo perdurable, mostrando que la seguridad comienza no con el poder sino con la presencia. Quizá la medida más precisa del éxito de un cuerpo de policía no sea el número de delitos que resuelve, sino el número de comunidades que fortalece: un apretón de manos, una visita a domicilio, un humilde agente de policía, uno tras otro.



Javier Gamero Kinoshita
IPA, Perú



América Latina ante una disyuntiva estratégica: fronteras en disputa o territorios bajo control criminal

La seguridad regional atraviesa una paradoja: mientras los Estados preservan capacidades para disuadir amenazas externas y administrar controversias territoriales, organizaciones criminales disputan cotidianamente el control de barrios, fronteras, puertos, economías y poblaciones. La cuestión no consiste en abandonar la defensa nacional, sino en revisar qué amenazas demandan hoy mayor atención política, coordinación institucional y recursos.

La soberanía tiene una dimensión interior

Tradicionalmente, la soberanía se ha asociado con fronteras reconocidas, integridad territorial y capacidad de defensa frente a otros Estados. Esas funciones siguen siendo irrenunciables. Pero un país también ve limitada su soberanía cuando una organización criminal cobra extorsiones, impone horarios, decide quién circula, recluta jóvenes o condiciona a funcionarios. Allí aparece una autoridad de facto que compete con la ley.

No toda disputa territorial es artificial ni todo conflicto híbrido carece de gravedad. Existen controversias legítimas y amenazas estatales que requieren disuasión creíble. El problema surge cuando la retórica de confrontación absorbe la agenda y desplaza inversiones urgentes en inteligencia criminal, investigación patrimonial, justicia, prisiones y cooperación fronteriza.

La amenaza que ya está dentro

El balance regional de InSight Crime contabilizó al menos 108.838 homicidios en América Latina y el Caribe durante 2025. La cifra, aun con diferencias de registro entre países, ilustra la escala humana

de la violencia. El Fondo Monetario Internacional, apoyándose en estimaciones de UNODC, señaló en 2024 que los grupos criminales y las pandillas están vinculados con aproximadamente la mitad de los homicidios regionales. No todos los asesinatos responden al crimen organizado, pero su peso resulta estratégico.

Las organizaciones actuales no se limitan a transportar drogas. Convergen narcotráfico, tráfico de armas, trata de personas, extorsión, minería ilegal, contrabando, lavado de activos y corrupción. Las redes cambian de aliados, subcontratan servicios y aprovechan tanto pasos clandestinos como cadenas logísticas legales. Su ventaja no reside únicamente en el armamento: está en la flexibilidad, el dinero, la información y la capacidad de corromper instituciones.

El mapa criminal tampoco coincide con el mapa político. Una ruta puede comenzar en un territorio productor, atravesar varios países, utilizar un puerto del Pacífico o del Atlántico y terminar en mercados extrarregionales. Ninguna policía nacional puede desarticular por sí sola una arquitectura de esa naturaleza.

Chile: una advertencia desde el Pacífico

Chile ofrece un ejemplo significativo. El Informe de Crimen Organizado en Chile 2025 de la Fiscalía Nacional identifica mercados ilícitos interconectados en la macrozona norte, vinculados con pasos fronterizos, puertos, drogas, contrabando, armas y tráfico de personas. En la zona centro señala la diversificación criminal y el papel de nodos urbanos y portuarios. El informe también describe el crecimiento relativo de secuestros y extorsiones durante 2024.

Las investigaciones sobre células vinculadas al Tren de Aragua muestran que la amenaza no se agota en la violencia visible: requiere seguir flujos financieros, comunicaciones, facilitadores y conexiones internacionales. En junio de 2025, la Fiscalía chilena informó sobre una operación contra una red de lavado asociada a esa organización que movilizó millones de dólares. La lección es clara: detener ejecutores es necesario, pero insuficiente si el sistema económico criminal permanece intacto.

Defensa y seguridad: complementar, no confundir

Las Fuerzas Armadas y las policías poseen misiones, atribuciones, doctrinas y mecanismos de control diferentes. Convertir el crimen organizado en un problema exclusivamente militar puede producir resultados tácticos sin desmontar las redes financieras y políticas que lo sostienen. Del mismo modo, tratarlo como simple delincuencia común subestima su alcance transnacional y su capacidad de desafiar al Estado.

Se necesita una arquitectura integrada, con conducción civil, límites jurídicos precisos, control democrático y responsabilidades diferenciadas. La defensa aporta vigilancia del espacio marítimo, aéreo y terrestre, logística y capacidades especializadas dentro del marco legal; las policías investigan y actúan; las fiscalías sostienen los casos; las aduanas y unidades financieras rastrean el dinero; el sistema penitenciario impide que las cárceles se conviertan en centros de mando.

Cinco prioridades para una agenda regional

Primero, construir inteligencia estratégica compartida: identificar redes, liderazgos, facilitadores, rutas y economías ilícitas, con protocolos de protección de datos y supervisión. *Segundo*,

perseguir activos, empresas pantalla y circuitos de lavado, porque la organización se reproduce mientras conserve rentabilidad. *Tercero*, asegurar puertos, pasos fronterizos y cadenas logísticas mediante análisis de riesgo y controles focalizados, sin paralizar el comercio legítimo.

Cuarto, fortalecer fiscalías, cooperación judicial, extradiciones y mecanismos de intercambio probatorio; la información sin capacidad procesal rara vez se traduce en condenas sostenibles. *Quinto*, recuperar territorios con presencia estatal duradera: escuelas, servicios, protección de testigos, oportunidades económicas y policías confiables. Ocupar un barrio durante una semana no equivale a gobernarlo durante una década.

Estas prioridades exigen indicadores más exigentes que el número de detenidos o toneladas incautadas: reducción de homicidios y extorsiones, debilitamiento patrimonial de redes, disminución del reclutamiento, confianza ciudadana y continuidad del control estatal.

La verdadera disyuntiva

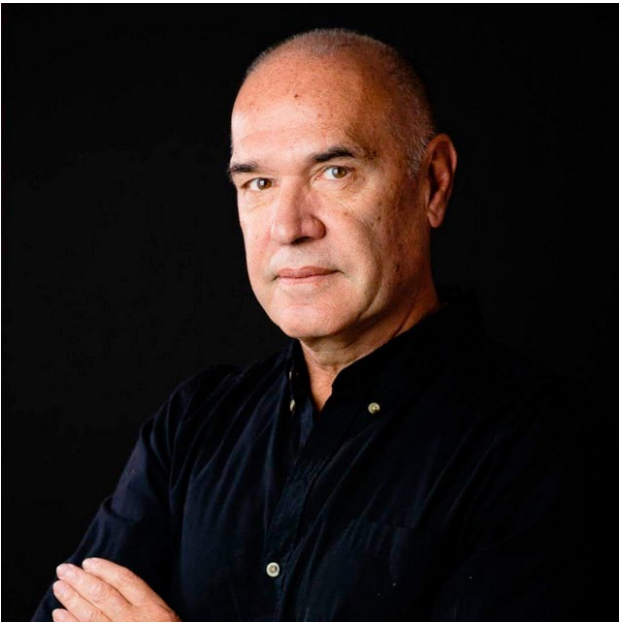
América Latina no debe elegir entre defender sus fronteras y proteger a sus ciudadanos. Debe evitar que las controversias interestatales —reales o magnificadas— oculten una erosión de soberanía

que ocurre a diario dentro de sus territorios. La inversión en defensa se justifica por amenazas evaluadas con rigor; la lucha contra el crimen organizado exige una prioridad igualmente estratégica, sostenida y regional.

La pregunta decisiva ya no es solamente dónde termina el territorio nacional. Es quién ejerce realmente la autoridad dentro de él. Una frontera protegida pierde parte de su significado si, detrás de ella, una estructura criminal impone sus propias reglas.

Fuentes de referencia:

Fiscalía Nacional de Chile, Informe de Crimen Organizado en Chile 2025; InSight Crime, Balance de homicidios 2025 (marzo de 2026); FMI, Violent Crime and Insecurity in Latin America and the Caribbean (2024); PNUD, Organized crime and human development (2025).



Fernando Vaccotti
Analista geopolítico y de
seguridad internacional

Cyber Security World Spain 4 al 5 de noviembre 2026, IFEMA, Madrid



Cyber Security World Madrid se consolida como el principal punto de encuentro para la ciberseguridad empresarial, corporativa e institucional. El evento reúne a las compañías y proveedores más relevantes del sector, que presentan sus soluciones y enfoques ante un panorama de amenazas y ciberataques en constante evolución.

La feria ofrece un entorno pensado para que organizaciones de cualquier ámbito identifiquen tecnologías clave, tendencias emergentes y partners estratégicos que les ayuden a reforzar su protección y anticiparse a nuevos riesgos digitales.

Safe Mining 2026, 30 de noviembre 2026, Riad, Arabia Saudita

¡La Fire Middle East Conference regresa en 2026 más grande y mejor que nunca!

Este evento exclusivo está dirigido a profesionales de todos los niveles en el ámbito de la protección contra incendios y la seguridad. La Conferencia Fire Middle East 2026 tiene como objetivo garantizar a sus altos funcionarios una agenda integral de debates de alto nivel, abordando los desafíos de seguridad más relevantes de la región en 2026 y más allá. Buscamos brindar amplias oportunidades de formación, creación de redes y preparación para el futuro, proporcionando a los asistentes las herramientas necesarias para convertirse en pioneros del sector y mantenerse alineados con la Visión Saudí 2030.



RESTCON 2026 8 al 12 de noviembre 2026, Fukuoka, Japón



RESTCON 2026 es la segunda Conferencia Internacional sobre Robótica, Ingeniería, Ciencia y Tecnología, que tendrá lugar del 18 al 20 de noviembre de 2026 en Fukuoka, Japón. Reúne a investigadores, expertos de la industria e innovadores para debatir sobre los avances emergentes en robótica y tecnologías de ingeniería. El evento ofrece una plataforma para presentar investigaciones, establecer contactos y explorar las futuras tendencias tecnológicas.

Tras el éxito de RESTCON 2024 en Pattaya, Tailandia, este evento contará con presentaciones de vanguardia, ponencias inspiradoras y excelentes oportunidades para establecer contactos.

AVAR CISO, 2 - 4 de diciembre 2026, Telangana, India

AVAR CISO Connect permite a los pioneros de la ciberseguridad perfeccionar sus habilidades, forjar relaciones clave y obtener la información esencial que necesitan para aumentar su valor para la junta directiva y otros grupos de interés de la empresa. Los CISO más destacados son reconocidos con los Premios CISO en las categorías de startups, organizaciones medianas y grandes empresas.

AVAR (Asociación de Investigadores Antivirus de Asia) se fundó en junio de 1998 con la misión de prevenir la propagación del malware y los daños que este provoca y está compuesta por destacados expertos de 17 territorios.





Revista
SEGURIDAD
& DEFENSA

NUEVA SECCIÓN PERMANENTE

SEGURIDAD MUNICIPAL

Análisis, prevención, innovación
gestión territorial y actualidad del
área de la seguridad municipal.



Un nuevo espacio editorial para visibilizar
desafíos, experiencias y soluciones en las
comunas de Chile.



ANÁLISIS
RIGUROSO



PREVENCIÓN
EFECTIVA



INNOVACIÓN
PÚBLICA



GESTIÓN
TERRITORIAL



ACTUALIDAD
MUNICIPAL

Porque la seguridad también se construye desde lo local
REVISTA SEGURIDAD AMPLÍA SU MIRADA

Acceda a través de nuestros dominios: revistaseguridad.cl y seguridadmunicipal.cl



Revista
SEGURIDAD
& DEFENSA

20 AÑOS

**GENERANDO CONOCIMIENTO
EN MATERIA DE SEGURIDAD**

La mayor plataforma de información en seguridad de Chile,
con una trayectoria de dos décadas.



Seguridad
Pública



Seguridad
Privada



Seguridad
Municipal



Seguridad
Minera

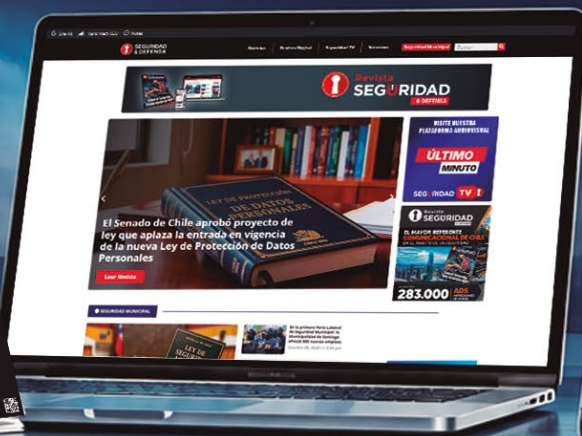


Ciberseguridad



Defensa

**MÁS QUE UNA REVISTA,
UNA COMPLETA PLATAFORMA INFORMATIVA**



YouTube
Canal
Seguridad
Televisión



200.000+

Impresiones mensuales en nuestro portal web

**4 CANALES
DE DIFUSIÓN**

Web · Revista · YouTube · Redes Sociales

**Conectamos a las empresas con los principales actores
y tomadores de decisiones del ecosistema de la seguridad y la defensa.**



info@revistaseguridad.cl



www.revistaseguridad.com