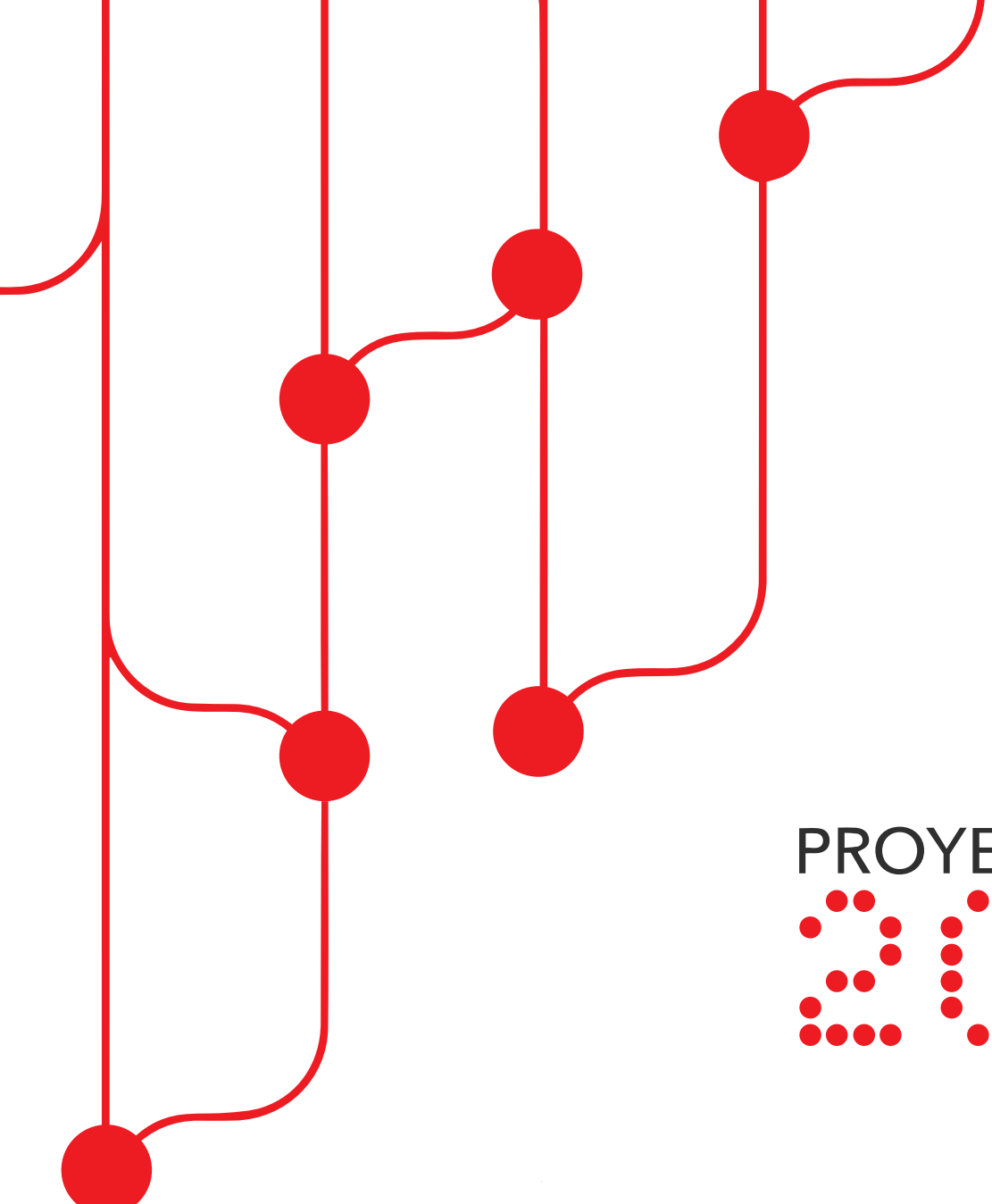




PROYECTACHILE

2050

Policy Brief

Mesa Seguridad e Inteligencia Artificial

Chile tiene futuro desde sus territorios:
Innovación tecnológica sostenible para
la seguridad pública



I. Resumen ejecutivo

La mesa de Seguridad Pública e Inteligencia Artificial (IA) fue concebida como un espacio de reflexión estratégica y colaboración intersectorial para anticipar los desafíos y oportunidades que traerá el desarrollo tecnológico en la seguridad del país. Con la coordinación general a cargo de Rodrigo Ramírez Pino, su trabajo se desplegó a través de cuatro submesas temáticas, con sus respectivos coordinadores:

1. *Ética, marco jurídico y derechos fundamentales en la era de la Inteligencia Artificial* (Carlos Reusser y María Isabel Cornejo).
2. *Gobernanza, coordinación interinstitucional, ecosistema de innovación pública y vinculación público-privado* (Patricio Urriola).
3. *Tecnologías emergentes aplicadas a la seguridad pública* (Juan Pablo Torres y Richard Weber).
4. *Infraestructura crítica, sostenibilidad tecnológica y ciberseguridad* (Hugo Durney).

Cada mesa abordó un ángulo complementario de la seguridad pública en la era digital, con el fin de generar una visión integrada para el Chile del 2050, que finalmente aportó más de 30 propuestas en esta materia.

Con este propósito, la mesa convocó a 116 participantes¹, provenientes de instituciones públicas, privadas, académicas y de la sociedad civil. Entre los actores involucrados, se encuentran: ministerios y organismos del Estado vinculados a la seguridad pública, la justicia y la innovación digital; universidades y centros de investigación; representantes del sector privado tecnológico; así como organizaciones ciudadanas con interés en derechos digitales, gobernanza democrática y seguridad ciudadana.

El objetivo central de la mesa fue deliberar sobre el uso responsable, ético y estratégico de la inteligencia artificial (IA) y de las tecnologías emergentes aplicadas a la seguridad pública, considerando tanto los riesgos como las oportunidades que estas plantean para la democracia, la cohesión social y la protección de derechos fundamentales. Con una mirada de largo plazo, se buscó identificar marcos de gobernanza, principios éticos, estándares técnicos y propuestas de política pública que permitan que Chile transite hacia un modelo de seguridad pública anticipatoria, inclusiva y legítima, apoyada en tecnología responsable.

La pertinencia de esta discusión para el Chile del 2050 es incuestionable. La acelerada transformación digital, la dependencia de infraestructuras críticas interconectadas y el uso creciente de algoritmos en la toma de decisiones exigen anticipar marcos

¹ Para ver el listado de participantes e instituciones convocadas en esta mesa, dirigirse al final del documento.

normativos y capacidades institucionales robustas para la seguridad pública. De no hacerlo, el país corre el riesgo de avanzar hacia un escenario inercial caracterizado por la vigilancia acrítica, la dependencia tecnológica externa y la erosión de la confianza ciudadana en las instituciones que no sean capaces de lidiar con la seguridad ni la tecnología. En contraste, un escenario transformador permitiría que la IA y la tecnología se conviertan en herramientas para fortalecer la seguridad pública, consolidar la democracia y proyectar a Chile como referente regional en innovación y gobernanza digital de bienes públicos tan importantes como estos.

Este trabajo, si bien está orientado al futuro, cobra especial vigencia en la agenda pública y electoral actual. Los resultados de la mesa ofrecen insumos estratégicos que pueden ser incorporados en los programas de gobierno y en las propuestas de candidaturas presidenciales para el periodo que se inicia en 2026. Al hacerlo, se contribuye a que las decisiones de política pública se dirijan hacia una visión prospectiva y responsable, capaz de anticipar riesgos y aprovechar oportunidades, con la convicción de que la seguridad pública del futuro debe construirse participativamente desde el presente.

II. Escenarios futuros contrastantes

A) Escenario inercial: en este escenario, Chile mantiene una senda marcada por la fragmentación institucional, la dependencia tecnológica externa y la descoordinación intersectorial. La gobernanza de la seguridad sigue erosionada por la falta de marcos normativos dinámicos y de coordinación entre instituciones clave, lo que debilita la legitimidad y confianza ciudadana.

La adopción tecnológica avanza de manera descoordinada, opaca y fragmentaria: proliferan sistemas de vigilancia basados en cámaras, drones, biometría y reconocimiento facial sin estándares comunes, armonización ni auditoría efectiva. Los modelos de inteligencia artificial presentan desarrollos por defecto, sesgos y baja explicabilidad, mientras que las decisiones automatizadas carecen de un control humano significativo. La interoperabilidad e integración entre Fiscalía, policías y Gendarmería es deficitaria, afectando la eficacia en prevención, investigación y persecución del delito.

A nivel ético y social, se profundiza la ausencia de estándares claros en la provisión privada de tecnologías, la discriminación algorítmica y la erosión de la licencia social. La baja alfabetización digital de la población incrementa la desconfianza hacia las instituciones. En el ámbito de la infraestructura crítica, persisten la vulnerabilidad, la dependencia de proveedores externos y la ausencia de capacidades soberanas, exponiendo al país a riesgos crecientes de ciberseguridad y a fallas sistémicas frente a crisis globales.

B) Escenario transformador: en esta trayectoria, Chile logra consolidarse como un referente regional en el uso responsable de las tecnologías emergentes para una mayor

seguridad pública, avanzando hacia un sistema robusto, transparente y centrado en derechos fundamentales.

La gobernanza se fortalece con marcos normativos dinámicos, mecanismos de rendición de cuentas y alianzas estratégicas público-privadas y regionales. Se promueve la soberanía tecnológica mediante el desarrollo de capacidades nacionales, el uso preferente de software abierto y soluciones auditables, y la formación de un capital humano altamente especializado.

El despliegue tecnológico se guía por criterios de interoperabilidad, explicabilidad y control humano significativo. Se implementan evaluaciones de impacto algorítmico, supervisión independiente y pilotos regulados (*sandboxes*) que permiten innovar con seguridad. Herramientas avanzadas como la forensia digital frente a *deepfakes* o el sistema SITIA, Sistema Integrado de Teleprotección con IA se escalan bajo estándares comunes de auditoría, fortaleciendo la prevención, la persecución penal y la gestión penitenciaria con legitimidad y eficacia verificables.

En el plano ético y social, la alfabetización cívico-digital masiva incrementa la confianza pública, reduce la discriminación algorítmica y fortalece la cohesión social. La cooperación regional para enfrentar riesgos transfronterizos permite a Chile insertarse en redes de seguridad digital más resilientes.

Finalmente, en materia de infraestructura crítica, el país logra consolidar sistemas soberanos, resilientes y descentralizados, con una gobernanza colaborativa que minimiza vulnerabilidades y asegura continuidad operativa.

III. Descripción del problema actual y tendencias emergentes

Para el Estado es fundamental avanzar en mejorar sus capacidades tecnológicas, se trata de un asunto estratégico, ya que existe suficiente evidencia que advierte que el crimen organizado en Chile está adoptando rápidamente herramientas tecnológicas avanzadas para fortalecer sus operaciones.

Para enfrentar la carrera tecnológica criminal urge mejorar las capacidades tecnológicas del Estado y de las instituciones facultadas por ley en materia de seguridad, con un ecosistema nacional tecnológico para la prevención del delito y la seguridad ciudadana, con inversiones estratégicas en infraestructura tecnológica, inteligencia artificial, análisis de datos, ciberseguridad y sistemas interoperables e integrados de información y de datos. El Estado está obligado a no quedarse atrás en capacidades, ya que la brecha tecnológica no sólo compromete la eficacia operativa, sino también la confianza ciudadana en la capacidad del sistema de seguridad para proteger a su población.

A) Desafíos para la ética, marco jurídico y derechos fundamentales en la era de la IA

Si bien Chile registra avances, persisten brechas normativas y éticas que exigen una visión estratégica de Estado a largo plazo. Para cerrarlas, la submesa propone fijar principios y valores claros para la relación entre IA y seguridad, acompañados de marcos jurídicos dinámicos, evaluaciones de impacto algorítmico antes del despliegue, transparencia y auditabilidad obligatorias y control humano efectivo sobre decisiones automatizadas. En paralelo, es clave desarrollar capacidades nacionales –incluido el uso de soluciones abiertas cuando corresponda– para reducir la dependencia tecnológica externa y resguardar la soberanía algorítmica.

Algunas de las tendencias consideradas por la submesa fueron: el impacto transversal de la tecnología, con la expansión de la vigilancia/teleprotección digital, la biometría y los sistemas algorítmicos; la soberanía tecnológica frente a la dependencia externa; las tensiones sobre derechos fundamentales (privacidad, igualdad, presunción de inocencia y debido proceso); la adaptación social, que demanda alfabetización digital y participación informada; la gobernanza global de riesgos transfronterizos, que requiere cooperación regional sin perder posición soberana; y el creciente protagonismo público-privado en seguridad, que demanda reglas claras para prevenir externalidades y resguardar garantías.

B) Desafíos para la gobernanza, coordinación interinstitucional, ecosistema de innovación pública y vinculación público-privado

El diagnóstico inicial de la submesa mostró un problema estructural de fragmentación institucional y regulatoria, más la ausencia de marcos de gobernanza claros en el uso actual de tecnologías para la seguridad, así como de la regulación de actividades que hasta la incorporación de IA no tenían un vínculo directo con problemas de seguridad. La dispersión de bases de datos, la falta de coordinación entre ministerios, policías, fiscalías y gobiernos subnacionales, la obsolescencia normativa, junto con una débil vinculación con el sector privado y académico, dificultan la generación de respuestas oportunas y la construcción de soluciones basadas en evidencia.

A partir de este análisis, la submesa reconoció megatendencias que condicionarán la gobernanza hacia 2050: la acelerada transformación digital, la crisis de confianza en las instituciones y la necesidad de resguardar la soberanía digital frente a la dependencia tecnológica.

C) Desafíos para tecnologías emergentes aplicadas a la seguridad pública

A diferencia de las demás submesas del ecosistema de seguridad pública, esta se centró en el análisis y fortalecimiento de medidas en torno a tres ámbitos centrales de la seguridad pública: prevención del delito, persecución penal y gestión carcelaria. A continuación, se desglosa parte del diagnóstico y los desafíos discutidos en estos tres ejes:

- **Prevención del delito:** ha pasado de ser una acción complementaria a convertirse en un eje estructural de la política pública, impulsando enfoques anticipatorios, territoriales y basados en datos. En este marco, la IA abre oportunidades para focalizar intervenciones y ganar eficiencia, pero también plantea dilemas de gobernanza de datos, resguardo de derechos y riesgo de vigilancia desproporcionada. La experiencia de Chile con el Sistema Integrado de Teleprotección con Inteligencia Artificial (SITIA) constituye un primer paso hacia la inteligencia territorial –al integrar múltiples fuentes, generar alertas tempranas y módulos predictivos–, aunque persisten limitaciones de interoperabilidad con instituciones clave y mecanismos insuficientes de retroalimentación ciudadana y control democrático. Las lecciones internacionales advierten sobre problemas de precisión y sesgos en tecnologías como *ShotSpotter* o el reconocimiento facial, y sobre amenazas emergentes como los *deepfakes*, lo que refuerza la necesidad de marcos ético-legales robustos, transparencia algorítmica y participación pública para legitimar y mejorar resultados.
- **Persecución del delito:** la IA ofrece un potencial transformador para la persecución penal al habilitar el análisis masivo de datos, la detección de patrones y redes criminales complejas y la priorización estratégica de investigaciones. Su desarrollo exige una secuencia rigurosa: definir el problema penal, aprovechar datos institucionales disponibles (carpetas investigativas, informes policiales, registros de llamadas), entrenar y validar modelos con metodologías científicas y, finalmente, apoyar decisiones del Ministerio Público y de las policías. Para un despliegue legítimo y eficaz, se requieren condiciones de explicabilidad, no discriminación, control institucional y supervisión independiente, así como marcos regulatorios específicos que establezcan límites, criterios de legalidad y responsabilidades. Hoy persisten brechas estructurales –capacidad operativa limitada, fragmentación, falta de interoperabilidad entre Fiscalía, Carabineros, PDI, Policía Marítima y Gendarmería– y déficits de adopción tecnológica por vacíos normativos, infraestructura insuficiente y carencias de capital humano, lo que afecta tanto la eficacia como la legitimidad ante la ciudadanía.
- **Gestión carcelaria:** la gestión penitenciaria enfrenta una tensión de base entre la función de custodia y el mandato de reinserción, en un contexto de hacinamiento, precariedad infraestructural y políticas fragmentadas con baja cobertura y eficacia de intervenciones psicosociales, educativas y laborales (menos del 15% accede a regímenes alternativos), lo que coadyuva a tasas altas de reincidencia. Las experiencias internacionales muestran caminos divergentes: debates sobre sesgos y predictibilidad en herramientas de evaluación de riesgo (como RisCanvi), modelos de “prisión inteligente” que promueven normalidad y acceso digital (Finlandia) y enfoques de gestión integral del caso (Canadá). En Chile, aún no existe una política penitenciaria digital integral; la interoperabilidad de Gendarmería con otras instituciones es deficitaria, el uso de IA es marginal y la regulación de datos penitenciarios sensibles es insuficiente. Avanzar requiere un enfoque de derechos, supervisión humana efectiva en decisiones automatizadas (clasificación, beneficios) y fortalecimiento de capacidades técnicas y éticas del

personal, para que la tecnología contribuya a la dignificación, la autonomía progresiva y la justicia restaurativa.

D) Desafíos para una infraestructura crítica, sostenibilidad tecnológica y ciberseguridad

Uno de los principales desafíos que discutió la submesa fue que el país presenta una alta vulnerabilidad en su infraestructura crítica, derivada de la fragmentación institucional, la dependencia de operadores privados, la insuficiencia de capital humano especializado y las brechas territoriales en inversión tecnológica. Estas debilidades comprometen no sólo la continuidad de servicios esenciales, sino también la seguridad pública y la confianza ciudadana en el Estado. A ello se suman bajos niveles de integración, interoperabilidad y redundancia entre sistemas clave –red eléctrica, agua potable, salud, transporte y comunicaciones–, que hoy operan de forma aislada y sin protocolos comunes de respaldo, lo que incrementa la exposición frente a amenazas naturales, tecnológicas e híbridas (incluidos ciberataques, interrupciones energéticas o sabotajes).

La excesiva dependencia de operadores privados en telecomunicaciones, energía, transporte, servicios digitales y almacenamiento de datos críticos limita el control estatal sobre estándares mínimos de continuidad e interoperabilidad y, además, se ve agravada por la concentración geográfica de inversión y gobernanza, que deja a regiones fuera de la Región Metropolitana con menor autonomía operativa ante eventos críticos.

Persisten brechas de ciberseguridad y obsolescencia tecnológica en instituciones públicas y servicios básicos; faltan protocolos sistemáticos de simulación y planificación prospectiva para orientar inversiones; y no existe aún una agencia nacional con mandato exclusivo para coordinar el ecosistema de infraestructura crítica, lo que perpetúa superposiciones normativas y desarticulación interinstitucional.

III. Implicancias para las políticas públicas

El diagnóstico realizado por la mesa de Seguridad, evidencia que la seguridad pública en Chile no puede abordarse sólo desde la perspectiva técnica, sino que requiere un replanteamiento político, institucional y prospectivo. La complejidad de las amenazas actuales obliga a fortalecer la gobernanza anticipatoria, la interoperabilidad de datos y la capacidad de prospectiva estratégica en las políticas públicas.

El Estado debe incorporar de manera sistemática metodologías de prospectiva y ejercicios de simulación de crisis para anticipar amenazas emergentes. Esto supone institucionalizar la vigilancia tecnológica, los escenarios de riesgo y el análisis de tendencias como insumos permanentes de la planificación en seguridad pública. La toma de decisiones no puede basarse únicamente en datos históricos, sino en proyecciones dinámicas que permitan diseñar políticas resilientes ante la incertidumbre.

Uno de los principales desafíos identificados es la fragmentación normativa y de sistemas de información. Para superar esta debilidad, se requiere construir un sistema nacional interoperable de datos críticos, que integre ciberseguridad, protección de datos, identidad digital y gestión de infraestructuras. La interoperabilidad no sólo aumenta la eficiencia, sino que habilita la respuesta coordinada entre distintos niveles de gobierno y actores privados frente a incidentes de seguridad.

El país necesita una institucionalidad especializada que articule de forma transversal a ministerios, gobiernos regionales, fuerzas de seguridad, empresas proveedoras de servicios esenciales, academia y sociedad civil. La coexistencia de marcos legales dispersos exige avanzar hacia un marco regulatorio unificado, flexible y adaptativo, alineado con estándares internacionales y con capacidad para actualizarse frente a innovaciones tecnológicas, y que, a su vez, resguarde la integridad de los derechos de las personas.

IV. Recomendaciones estratégicas

A) Propuestas estratégicas en relación a ética, marco jurídico y derechos fundamentales en la era de la IA

- 1. IA ética y centrada en la persona:** promover un marco ético-jurídico robusto que coloque los derechos humanos y principios éticos al centro del desarrollo y uso de la IA, especialmente en aplicaciones de seguridad pública. Se busca garantizar que las tecnologías de IA operen dentro de límites que respeten la dignidad humana, la privacidad, la no discriminación y las libertades fundamentales. Esto implica anticipar y mitigar los riesgos que la IA pueda suponer para derechos como la igualdad, el debido proceso o la libertad de expresión. Chile y la región ya han manifestado un compromiso con una IA que proteja los derechos humanos, las libertades fundamentales y la democracia. En línea con ello, este lineamiento refuerza la necesidad de actualizar marcos legales y principios rectores para la IA.
- ***Constitución 2050:*** la seguridad tecnológica como derecho constitucional de los chilenos: reforma constitucional que reconozca el derecho fundamental a la seguridad pública de cada persona, estableciendo la obligación estatal de garantizar entornos seguros apoyados en sistemas tecnológicos como herramienta garantista.
- 2. Transparencia algorítmica y rendición de cuentas (*accountability*):** instaurar la transparencia, explicabilidad, auditabilidad y *accountability* como pilares en el ciclo de vida de los sistemas de IA. En la visión al 2050, ningún sistema algorítmico que afecte a las personas debería operar como una “caja negra” inescrutable. Por el contrario, los ciudadanos tendrán derecho a conocer la base de las decisiones automatizadas que les conciernan (factores, lógica y métodos involucrados), lo que permite ejercer control democrático sobre la IA. Asimismo,

se aspira a mecanismos sólidos de rendición de cuentas: los desarrolladores y usuarios institucionales de IA deben ser responsables legal y socialmente por los efectos de sus algoritmos. En síntesis, una IA transparente y explicable aumentará la confianza pública y permitirá corregir oportunamente cualquier impacto negativo. Para lo cual, también se requerirá:

- **Justicia Aumentada 2050: IA para la Integridad de evidencias y testimonios:** desarrolla un Sistema Nacional de verificación de Medios Digitales, basado en inteligencia artificial para que policías, peritos forenses y tribunales puedan verificar la autenticidad de videos, audios e imágenes presentadas como evidencia judicial. El sistema busca detectar *deep fakes* y contenido manipulado digitalmente, complementándose con nuevas normas legales que penalicen el uso malicioso de estas tecnologías falsificadas en procesos judiciales.
- 3. Participación ciudadana y gobernanza multisectorial de la IA:** la participación activa de la ciudadanía y la colaboración de múltiples actores (gobierno, sector privado, academia, sociedad civil) deben ser principios clave en la gobernanza de la IA del futuro. Reconociendo que las decisiones sobre IA tienen profundas implicancias sociales, se propone un modelo de gobernanza inclusiva donde las políticas y proyectos de IA se diseñen con transparencia y con la intervención de diversos grupos de interés. La inclusión ciudadana es fundamental para legitimar el uso de IA en el sector público, combatir la desconfianza y anticipar impactos en comunidades específicas, con medidas como:
- **Establecer Mecanismo Nacional de Consulta Ciudadana para la gobernanza de la IA:** que sea obligatorio por regla general y aplicable al diseño, planificación, implementación y evaluación de políticas, marcos regulatorios e instituciones. Sus resultados, no vinculantes, deben dar respuesta fundada cuando no se acojan propuestas ampliamente respaldadas. Debe ser preferentemente virtual y accesible territorialmente (con identificación estatal), con excepciones acotadas por razones de seguridad nacional. Debe ser complementario de la consulta indígena conforme al Convenio 169, firmado por Chile ante la OIT², y desplegado en todos los sectores y regiones según el alcance de cada iniciativa, para legitimar decisiones, abrir espacio a iniciativas ciudadanas y fortalecer el debate público.
 - **Transformación educativa para la gestión del conocimiento, el desarrollo humano y la seguridad ciudadana en la era de la IA:** incorporar de manera sistemática contenidos sobre uso responsable de inteligencia artificial y humanismo digital en todos los niveles del currículum educativo nacional. Reconoce que la IA está transformando la interacción de niños, niñas y adolescentes con la tecnología en áreas como educación, entretenimiento y redes sociales, generando tanto oportunidades para el aprendizaje como riesgos para la privacidad y bienestar mental. Basándose en recomendaciones de UNESCO y UNICEF, la estrategia busca promover el pensamiento crítico y el uso

² El Convenio 169 de la Organización Internacional del Trabajo (OIT) es un tratado internacional ratificado por Chile en 2008, que reconoce y protege los derechos de los pueblos indígenas, garantizando su participación en las decisiones que los afectan y el derecho a sus tierras y territorios.

responsable de la IA desde edades tempranas, asegurando que los sistemas respeten los derechos de los menores.

- 4. Coordinación interagencial y soberanía tecnológica:** reforzar la coordinación institucional e interagencial en materia de IA, a la par de promover la soberanía tecnológica de Chile de aquí a 2050. Se parte del diagnóstico de que actualmente existen esfuerzos dispersos en distintos organismos del Estado, vacíos de liderazgo claro y vacíos normativos en la materia. Para responder a estos desafíos, se plantea crear una estructura de gobernanza unificada que alinee principios, estándares y acciones de IA en todo el aparataje público.
- **Ciudad Segura 2050:** crear la Red Nacional Inteligente de Prevención del Delito, que unifique cámaras, sensores y datos policiales de todo Chile en una plataforma centralizada con inteligencia artificial. El sistema analizará imágenes en tiempo real para detectar actividades sospechosas y generará alertas automáticas, mientras que algoritmos predictivos anticiparán dónde y cuándo podrían ocurrir delitos futuros para posicionar patrullas preventivamente.
 - **VIGÍA (Vigilancia Integrada con Gobernanza e Inteligencia Artificial):** se propone el diseño e implementación de una Plataforma Nacional de Coordinación y Analítica de Seguridad Pública basada en IA, como arquitectura integradora de datos, alertas, patrullajes y acciones de inteligencia de múltiples organismos (Ministerio del Interior, Carabineros, PDI, Ministerio Público, Fuerzas Armadas, ANCI, DGAC y gobiernos regionales y municipales). Esta plataforma operará bajo principios de gobernanza ética, con algoritmos auditables, datos anonimizados, interoperabilidad garantizada y órganos de supervisión. Su implementación deberá ser progresiva hasta el año 2030. VIGIA permitirá homologar y certificar que las tecnologías que se compren en materia de seguridad con IA sean adecuadas y con el estándar pertinente para sus fines y propósito (como la SEC de electricidad).
 - **Escudo Tecnológico 2030:** crear Sistema IA de Defensa contra Drones Delictivos, que detecta y neutraliza automáticamente drones no autorizados sobre centros urbanos y zonas sensibles en todo el territorio nacional, mediante sensores estratégicos (radiofrecuencia, radares, cámaras). Cuando identifica un dron hostil, despliega contramedidas automatizadas como interferencia de señales para forzar aterrizajes o drones interceptores que capturan físicamente las amenazas más peligrosas. El sistema incluye inteligencia predictiva que analiza patrones previos para anticipar posibles focos de lanzamiento de drones criminales.
 - **Centro nacional de entrenamiento de algoritmos para la seguridad pública - IA y Algoritmos eficientes, pertinentes y sin sesgos:** con el propósito que todo el sector tecnológico acceda a bancos de datos fiables que eviten el sesgo y la discriminación en su desarrollo y que permitan entrenar y diseñar algoritmos con pertenencia a los tipos del delito que se buscan predecir.

B) Propuestas estratégicas en relación a gobernanza, coordinación interinstitucional, ecosistema de innovación pública y vinculación público-privado

1. Interoperabilidad de plataformas y gobernanza de datos e IA: avanzar hacia un ecosistema de gobernanza de datos, tecnológica e inteligencia artificial (IA), que promueva la interoperabilidad entre plataformas digitales del Estado y del ecosistema público-privado, bajo criterios de responsabilidad, ética y respeto irrestricto a los derechos fundamentales. Esto requiere fortalecer el uso responsable de los datos y de la IA conforme a la normativa vigente, al tiempo que se impulsa la construcción de un marco normativo integral que regule el tratamiento de datos, garantice la protección de datos personales y salvaguarde la privacidad de las personas. Asimismo, se propone consolidar un sistema de identidad digital confiable, interoperable y centrado en el usuario, que permita facilitar el acceso equitativo a servicios públicos y privados. En este contexto, se enfatiza la necesidad de promover estándares abiertos y protocolos comunes que aseguren la compatibilidad técnica entre distintos sistemas y plataformas, contribuyendo a una arquitectura digital nacional resiliente, segura y escalable, a través de:

- **Gobernanza de datos:** se plantea la definición de una taxonomía de datos y fuentes autoritativas de información en función de criterios de priorización basados en la criticidad del dato.
- **Interoperabilidad y coordinación entre plataformas digitales del Estado y del ecosistema público-privado:** estandarización administrativa para la colaboración entre poderes del Estado, agencias, niveles de gobierno (municipal, regional, central) y con proveedores privados, perfilando roles claros en el diseño, operación y control.
- **Estándares abiertos y protocolos comunes:** definición normativa de estándares de interoperabilidad de datos en formato de repositorio colaborativo y abierto.

2. Coordinación entre policías, organismos de inteligencia, UAF, aduanas, municipios, DGAC, Agencia de protección de datos personales y otros actores estratégicos: impulsar un modelo robusto de coordinación interinstitucional que permita la integración efectiva entre policías, organismos de inteligencia, la Unidad de Análisis Financiero (UAF), sistemas de emergencia, municipalidades, aduanas, la Dirección General de Aeronáutica Civil (DGAC), gestores de eventos públicos y otras agencias estratégicas, tanto del sector público como privado. Esta articulación debe extenderse a entidades reguladas por la ley de seguridad privada y aquellas que manejan información financiera sensible, con el propósito de fortalecer la coproducción de seguridad pública en el país. Se propone establecer mecanismos formales y permanentes de comunicación y colaboración, tales como sistemas de alerta temprana interconectados, protocolos de intercambio seguro de información y un Centro Nacional de Operaciones Conjuntas. Este centro permitiría una respuesta coordinada, rápida y basada en datos frente a amenazas, emergencias y eventos de alto impacto, a través de implementar políticas públicas como:

- **Marco normativo para la coordinación interinstitucional:** el intercambio de datos en seguridad pública fortalece la gobernanza estatal, impulsa el uso estratégico del conocimiento, promueve la confianza ciudadana y permite abordar de forma integrada desafíos como por ejemplo la migración y el cambio demográfico.
- **Organismo articulador del sistema de seguridad:** crear un organismo articulador de los actores del sistema de seguridad que facilite la planificación conjunta, el uso compartido de datos, la trazabilidad ética de las decisiones y la implementación de políticas coherentes en los territorios. Además, se pretende que dicho organismo fortalezca la legitimidad democrática del sistema de seguridad al institucionalizar la participación de diversos actores, promoviendo una cultura de colaboración, transparencia y aprendizaje continuo.
- **Marco legal y técnico para el intercambio ético y seguro de datos entre el Estado de Chile y el sector privado:** creación de un marco legal y técnico que asegure el intercambio de datos seguro entre instituciones, con el objetivo de mejorar significativamente la capacidad del Estado para actuar de forma coordinada, anticiparse a amenazas y tomar decisiones basadas en evidencia. Se sugiere que dicho marco se base en tres pilares:
 - a) *Estándares técnicos comunes:* uso compartido de formatos y protocolos que permiten la integración entre sistemas.
 - b) *Seguridad y resiliencia digital:* protección robusta frente a ciberamenazas y continuidad operativa garantizada.
 - c) *Accesibilidad institucional:* sistemas fáciles de usar y adaptados a las capacidades de cada institución.

3. Modelos colaborativos público-privados para innovación en seguridad: fomentar modelos colaborativos público-privados orientados a la innovación en seguridad, mediante el establecimiento de entornos controlados (*sandbox* regulatorios) y laboratorios de innovación que permitan la experimentación con nuevas tecnologías, procesos y marcos regulatorios en contextos reales o simulados. Estos espacios deben facilitar la coproducción de soluciones tecnológicas de alto impacto, especialmente en materia de seguridad pública, fortaleciendo la confianza y la colaboración entre el Estado, el sector privado, la academia y la sociedad civil. Se propone la creación de espacios de datos compartidos, tanto públicos como privados, que habiliten la reutilización responsable de información para fines de investigación, desarrollo e innovación (I+D+i). Además, se sugiere fomentar la participación activa del sector privado —incluyendo grandes empresas, *startups* y pymes tecnológicas— en pruebas piloto, desarrollo y escalamiento de soluciones digitales de seguridad, incluyendo el entrenamiento de modelos de inteligencia artificial (IA), con datos públicos y privados anonimizados. Este enfoque busca posicionar al Estado como un habilitador estratégico de innovación colaborativa, orientada a responder proactivamente a los desafíos emergentes de seguridad en un entorno cada vez más digital y complejo.

- **Estructura de colaboración público-privada con modelos diversos:** diseñar y operar una estructura de colaboración público-privada con modelos diversos para crear soluciones a problemas nacionales, obteniendo aprendizajes que progresivamente den forma a una cultura de colaboración.

- **Programa Nacional de Retos abiertos de Innovación en Ciberseguridad:** generar retos nacionales con convocatorias mixtas público privados, desde donde se obtengan prototipos de soluciones tecnológicas que se puedan comercializar en el mercado.

4. Ciberseguridad a nivel nacional: fortalecer la ciberseguridad como eje estratégico de la seguridad pública y la lucha contra el crimen organizado y otras amenazas emergentes, mediante una gobernanza integrada, multisectorial y orientada a la prevención de amenazas digitales que afecten a personas, instituciones e infraestructuras críticas, que incluye:

- **Marco legal convergente en ciberseguridad:** actualizar y unificar la normativa nacional conforme a estándares internacionales (como ISO 27001 ó NIST), crear un marco legal convergente que regule la ciberseguridad en todos los sectores estratégicos, y establecer un organismo coordinador que supervise el cumplimiento y fomente la certificación.
- **Iniciativas de concientización y reportería:** desarrollar campañas nacionales de concientización en ciberseguridad dirigidas tanto a ciudadanos como a empresas, con el fin de instalar una cultura preventiva y proactiva frente a los riesgos digitales.
- **Formación y certificación en ciberseguridad:** programas de formación masiva y planes de inversión estratégica para reducir la brecha de talento y capacidades tecnológicas para la operación de un ecosistema nacional de ciberseguridad.

C) Propuestas estratégicas para tecnologías emergentes aplicadas a la seguridad pública

1. Estrategia Nacional de Gobernanza Algorítmica para la Seguridad Pública (ENAGAS): Esta propuesta de política pública estructural busca modernizar la seguridad pública mediante la integración responsable de tecnologías emergentes en los ámbitos de prevención del delito, persecución penal y gestión penitenciaria. La estrategia contempla cinco componentes principales:

- **Desarrollo de una plataforma de interoperabilidad de datos:** entre Fiscalía, Carabineros, PDI, Policía Marítima, Gendarmería y Poder Judicial.
- **Creación de un marco normativo específico para regular el uso de IA:** datos personales sensibles y decisiones automatizadas en seguridad pública.
- **Establecimiento de estándares éticos y técnicos:** para el diseño, implementación y monitoreo de tecnologías predictivas y de vigilancia.
- **Implementación de un programa de formación para funcionarios públicos:** en competencias técnicas, jurídicas y éticas vinculadas al uso de IA.
- **Accountability y trazabilidad integral del ciclo algorítmico:** creación de un régimen de responsabilidad y control que incluya Registro público de sistemas de

alto impacto (finalidad, bases de datos, versiones, responsables institucionales); Asignación explícita de responsables humanos por cada uso, con bitácoras auditables (logs) que vinculen decisiones, accesos y temporalidad de uso; Evaluaciones de impacto algorítmico (ex ante y periódicas) y declaración de finalidad con limitación de propósito y cláusulas de caducidad (sunset) para sistemas y datos; Deber de explicación a las personas afectadas, canales de reclamo y reparación, y notificación obligatoria de incidentes (fallas, sesgos, brechas); y auditorías independientes y mecanismos sancionatorios para proveedores y organismos usuarios cuando se incumplan estándares o se cause daño.

El alcance de esta propuesta es nacional, con pilotos iniciales en las regiones Metropolitana, Biobío y La Araucanía, territorios críticos por la presión delictual y la necesidad de respuestas innovadoras. Su implementación contempla una gobernanza multiactor que involucra al Estado, el Congreso, la Corte Suprema, universidades con experiencia en derecho, informática y criminología, organizaciones de la sociedad civil y organismos internacionales como la OCDE, la Unión Europea e INTERPOL.

D) Propuestas estratégicas para infraestructura crítica, sostenibilidad tecnológica y ciberseguridad

- 1. Fortalecimiento de la infraestructura digital nacional:** abordar la necesidad de consolidar una red de infraestructura digital pública, soberana y de alta disponibilidad, que contemple redes troncales de fibra óptica, centros de datos regionales y un Centro Nacional de Supercómputo. Se debatió sobre la propiedad, financiamiento y gobernanza de estos sistemas, así como la urgencia de garantizar estándares de ciberseguridad y resiliencia frente a cortes o ataques, lo que implica:
 - **Actualización y ampliación del marco legal relativo a infraestructura crítica:** establecer, mediante una ley y reglamentos unificados, qué es infraestructura crítica y su relación con servicios esenciales. Para esto, se debe revisar, complementar e integrar la normativa vigente (incluida la Ley N°21.542 y la Ley Marco de Ciberseguridad), establecer criterios sectoriales de criticidad y crear un registro nacional en línea con entidades críticas obligadas a planes de resiliencia y continuidad.
 - **Generación de Estrategia nacional de formación técnica para una infraestructura crítica digital segura y resiliente:** creación de un plan nacional de formación técnico-profesional, con programas descentralizados, laboratorios especializados y un fondo de becas, para contar con una fuerza laboral certificada capaz de operar, mantener y fiscalizar infraestructuras críticas en todo el país.

2. Infraestructura energética nacional como pilar de seguridad operacional: sobre el rol estratégico de la infraestructura energética para sustentar servicios críticos (salud, seguridad, comunicaciones, transporte). Se propone la modernización de redes mediante tecnologías inteligentes (*smart grids*), almacenamiento distribuido, y sistemas de respaldo en territorios vulnerables, a través de:

- **Plataforma Nacional de Integración Tecnológica para la Seguridad y Resiliencia de Infraestructuras Críticas:** diseño de un sistema tecnológico unificado que integre monitoreo, alerta temprana y comando en tiempo real, con protocolos comunes, IA para análisis predictivo, arquitecturas de ciberseguridad de confianza cero y respaldo en nube soberana con nodos regionales. Además, se propone sistematizar acciones de simulacro de ciberataques a nivel nacional para prevención y análisis de capacidades de reacción.

3. Integración y resiliencia de infraestructuras y servicios críticos: plantea la necesidad de una visión integrada del ecosistema de servicios esenciales (agua, energía, salud, transporte, comunicaciones), avanzando hacia su interoperabilidad, coordinación en emergencias, y planificación territorial. Se relevaron prácticas de redundancia y respaldo (físico y digital), como criterios fundamentales de diseño, para lo cual se propone:

- **Ventanilla Única Nacional para comunicación de emergencias y seguridad pública:** contar con número universal y canales multimodales; teléfono, web, tótems urbanos y recepción y analítica de imágenes, que integren en tiempo real la geolocalización de dispositivos y la coordinación interinstitucional. Se espera lograr un sistema único 24/7, inclusivo y multilingüe, con reducción significativa de los tiempos de respuesta y disminución del mal uso de las líneas de emergencia. Asimismo, busca facilitar acceso automático a datos de posicionamiento y otros en caso de activación o acceso a sistemas de comunicación por emergencia mediados por sistemas digitales en red.
- **Plataforma de acceso centralizado 911:** Chile contará con una plataforma de gestión con un sistema integrado tecnológico de numeración única, garantizando un entorno colaborativo, integrador y unificador entre quienes concurren con facultades en materia de prevención del delito y la seguridad pública. Las alertas ciudadanas y los reportes de incidentes se podrán gestionar de manera centralizada mediante la disposición de un número único para la comunicación de incidentes.

4. Gobernanza, regulación y capital humano para la ciberseguridad nacional: frente a las deficiencias normativas, la dispersión institucional y la falta de recursos para operar con estándares adecuados de ciberseguridad. Se discutió la creación de nuevas instituciones o agencias, la armonización entre distintas leyes (ciberseguridad, protección de datos, transformación digital) y la urgencia de formar capital humano técnico, profesional y especializado. Se propuso:

- **Sistema georreferenciado de puntos críticos para la Seguridad Pública:** creación de una base nacional de datos georreferenciados que permita

identificar y monitorear áreas de alto riesgo, facilitando la coordinación entre policías, SENAPRED y operadores de telecomunicaciones para mejorar la prevención y búsqueda de personas.

- **Plan nacional de ciberciudadanía:** Chile, país con cultura de IA y ciberseguridad, generación de una estrategia o plan nacional renovados de mediano plazo (4 años) y largo plazo (12 años), que apunte a la educación y creación de cultura para habilitación y empoderamiento digital de personas, con especial énfasis en infancia y adultos mayores.
- **Estrategia nacional de formación de capital humano avanzado en IA y ciberseguridad:** Se propone generar una estrategia o plan nacional de mediano plazo (4 años) y largo plazo (12 años) con foco en la promoción y potenciamiento de una oferta de formación y/o educación técnico profesional (ETP) de excelencia en áreas relacionadas con el despliegue, operación y mantenimiento de las infraestructuras críticas asociadas a servicios de comunicación digital y datos, así como a energías (generación, transporte, distribución y almacenamiento).

5. Prospectiva tecnológica y adaptabilidad institucional: capacidad del Estado y de sus instituciones para adaptarse a la disrupción tecnológica. Se analizaron tecnologías emergentes como la inteligencia artificial, la computación cuántica, la automatización laboral y la biometría. Se propuso fortalecer capacidades de vigilancia tecnológica, regulación anticipatoria y reconversión profesional ante la obsolescencia de oficios y saberes, a través de:

- **Estrategia nacional de prospectiva tecnológica y adaptabilidad institucional para infraestructuras críticas:** habilitar hojas de ruta actualizables y métricas públicas de preparación, mediante vigilancia y prospectiva sobre IA, biometría, automatización y computación cuántica, pruebas reguladas en *sandboxes* (entornos de pruebas), programas de formación y reconversión de talento con nodos regionales y la creación de un Observatorio Nacional. Se debe involucrar a ministerios sectoriales, agencias de ciberseguridad y ciencia, universidades, centros de I+D, empresas estratégicas y gobiernos regionales, para anticipar riesgos, orientar inversiones y sostener la continuidad de servicios esenciales.

V. Conclusión

El trabajo de la mesa de Seguridad Pública e Inteligencia Artificial ha permitido consolidar una visión estratégica compartida para Chile al 2050: un país que concibe la seguridad pública no sólo como un deber del Estado, sino como un bien común sustentado en la ética, la protección de derechos fundamentales, la gobernanza democrática y el uso responsable de las tecnologías emergentes. Asimismo, es capaz de ver el potencial que puede tener la IA para la seguridad pública.

Cada submesa aportó diagnósticos y propuestas complementarias que, en conjunto, delinean un marco integral de acción. La submesa de *Ética* puso en el centro la

necesidad de resguardar los derechos fundamentales frente al uso de la IA. La de *Gobernanza* abordó las bases institucionales, normativas y de coordinación intersectorial para anticipar amenazas y fortalecer la seguridad digital. La submesa de *Tecnologías Emergentes* enfatizó el potencial y los riesgos de su aplicación en seguridad pública, mientras que la de *Infraestructura Crítica* destacó la urgencia de contar con regulación, institucionalidad y sistemas resilientes y sostenibles, que protejan los bienes y servicios esenciales y estratégicos del país.

Los consensos alcanzados permiten trazar una hoja de ruta clara hacia 2030, 2040 y 2050, con acciones concretas que incluyen marcos normativos convergentes, programas de formación masiva en ciberseguridad, desarrollo de *hubs* de innovación territorializados, campañas de sensibilización ciudadana y mecanismos de interoperabilidad que garanticen confianza y transparencia. Estas medidas buscan responder a amenazas crecientes como los ciberataques, la desinformación y el uso indebido de tecnologías, al mismo tiempo que aprovechan las oportunidades de la IA para fortalecer la seguridad y la cohesión social.

La urgencia del problema radica en que mantener un enfoque inercial significaría perpetuar la fragmentación normativa, la dependencia tecnológica y la vulnerabilidad de infraestructuras críticas. En cambio, avanzar hacia el escenario transformador requiere decisión política, cooperación público-privada y compromiso ciudadano.

Los tomadores de decisión, en especial los candidatos presidenciales de 2026, deben reconocer que la gobernanza digital y la seguridad pública no son temas técnicos de segundo orden, sino ejes estratégicos para el futuro del país. Chile tiene hoy la oportunidad de anticiparse, innovar y liderar en la región, construyendo un modelo de seguridad pública digital que refuerce la democracia, proteja los derechos fundamentales y asegure un desarrollo inclusivo y sostenible para las próximas generaciones.

En síntesis, hubo tres ideas fuerza que guiaron este proceso:

1. **Ética y derechos:** como base de toda innovación en seguridad pública.
2. **Gobernanza colaborativa:** que articule Estado, sociedad civil, sector privado y academia.
3. **Ciberseguridad e innovación:** como motores para anticipar riesgos y fortalecer la confianza ciudadana.

Con esta visión, la mesa deja a disposición un conjunto de propuestas y lineamientos estratégicos que constituyen insumos esenciales para las agendas políticas, legislativas y sociales de los próximos años. El futuro de la seguridad pública en Chile se construye desde hoy, con la convicción de que sólo un enfoque integral, inclusivo y prospectivo permitirá enfrentar los desafíos de un mundo crecientemente interconectado.

Participantes mesa Seguridad e IA

Coordinación general: Rodrigo Ramírez Pino

Coordinación de submesas:

- Carlos Reusser y María Isabel Cornejo (*Ética, Marco Jurídico y Derechos Fundamentales en la Era de la IA*)
- Patricio Urriola (*Gobernanza, Coordinación Interinstitucional y Ecosistema de Innovación*)
- Juan Pablo Torres y Richard Weber (*Tecnologías Emergentes Aplicadas a la Seguridad Pública*)
- Hugo Durney (*Infraestructura Crítica, Sostenibilidad Tecnológica y Ciberseguridad*)

Comité editor: Carlos Reusser, Christian Schmitz, Claudia Gutiérrez, Cristián Barría, Daniel Inzunza, Darwin Muñoz, Héctor Torres, Hugo Durney, John Castro, Jorge Vergara, José Luis Lagos, Juan Pablo Torres, Kilian Vargas, María Isabel Cornejo, Mario Durán, Milton Sazo, Nicolás Ojeda, Richard Weber, Sergio Contreras y Sergio Miranda

Miembros del comité técnico convocado por la mesa:

Alejandro Inzunza	Gabriela Arriagada	Mylena Álvarez
Álvaro Soto	Gregory Toledo	Nicolás Muñoz
Ana Landaeta	Guillermo Puebla	Nicolás Ojeda
Bastián Felipe	Héctor Torres	Óscar Cartagena
Blanca Aída Villalobos	Isabel Riofrancos	Pablo Ignacio Pizarro
Camilo Sanhueza	Joaquín Carrasco	Patricia Reyes
Carla Vairetti	John Castro	Patricio Cofré
Carola Figueroa	Jonathan Vásquez	Paulina Etcheberry
Carolina Bonacic	Jorge Martinez	Pedro Huichalaf
Christian Belmar	Jorge Vergara	Pía Ignacia Corral
Christian Schmitz	José Luis Lagos	Rachel Grez
Claudia Gutiérrez	José Luis Riffo	Roberto Cippitani
Cristián Barría	José Manuel Muñiz	Rodrigo Zigante
Claudia Bañados	Juan Carlos Gutierrez	Rossana Ponce de León
Claudio Bravo	Juan Carlos Parra	Sandor Abad
Cristián Medina	Juan Jorge Faúndez	Sebastián Ortega
Daniel Barrientos	Juan Pablo González	Sergio Contreras
Daniel Inzunza	Kilian Vargas	Sergio Miranda
Darwin Muñoz	Lorayne Finol	Tamara Oyarce
Elizabeth Gutiérrez	Manuel Bozo	Víctor Escobar
Felipe Miranda	Marcelo Farr	Víctor Manuel Díaz
Fernando Contreras	María Isabel Cornejo	Víctor Manuel Mora
Francisco J.	Mario Durán	Vladimir Riffo
Bedecarratz	Martín Müller	Waldemar Méndez
Francisco Ortiz	Milton Sazo	