ACADEMIA NACIONAL DE
ESTUDIOS POLÍTICOS Y
ESTRATÉGICOS

IMPLICANCIAS DEL USO DE LA INTELIGENCIA ARTIFICIAL EN EL CRIMEN ORGANIZADO: DESAFÍOS PARA CHILE

Por

Francisca Muñoz Soto

Informe de Asesoría Profesional presentado al programa de Postgrados de la Academia Nacional de Estudios Políticos y Estratégicos para optar al grado académico de Magíster en Seguridad, Defensa y Relaciones Internacionales

Profesor Tutor:

Alejandro Arévalo Sarce

Noviembre, 2025

Santiago, Chile

ÍNDICE

Índice de Gráficos

Índice de Tablas

Resumen

El uso de inteligencia artificial por parte de organizaciones criminales es una amenaza emergente que ha comenzado a manifestarse a nivel global, pero cuya comprensión y respuesta en Chile sigue siendo incipiente.

A pesar de la creciente digitalización de procesos sociales y económicos, el país no cuenta con marcos normativos, capacidades técnicas ni protocolos de inteligencia suficientes para anticipar o enfrentar escenarios en que estas tecnologías sean utilizadas para cometer delitos complejos, como el narcotráfico, el lavado de activos o la trata de personas.

Esta carencia de herramientas plantea interrogantes urgentes sobre las brechas en las políticas de seguridad y la necesidad de una aproximación interinstitucional e interdisciplinaria que permita una respuesta eficaz ante esta nueva configuración del crimen organizado.

Palabras claves: Inteligencia Artificial – Crimen Organizado – Chile – Desafíos

Abstract

The use of artificial intelligence by criminal organizations represents an emerging global threat, one that remains insufficiently understood and addressed in Chile.

Despite the country's ongoing digital transformation across social and economic sectors, it still lacks robust legal frameworks, technical capabilities, and intelligence protocols to anticipate or counteract scenarios in which these technologies are exploited for complex crimes such as drug trafficking, money laundering, and human trafficking.

This institutional and regulatory gap raises urgent questions regarding Chile's security policies and highlights the necessity of an interinstitutional and interdisciplinary approach to ensure an effective response to the evolving dynamics of organized crime.

Keywords: Artificial Intelligence – Organized Crime – Chile – Challenge

1. INTRODUCCIÓN

La Inteligencia Artificial (IA) constituye una tecnología que amplía las capacidades humanas para la resolución de problemas, facilita el análisis de grandes volúmenes de información, favorece la toma de decisiones fundamentadas y genera recomendaciones de valor. Más que sustituir a las personas, la IA actúa como una herramienta que incrementa la eficiencia y la precisión en múltiples ámbitos, desde los asistentes virtuales hasta los sistemas de apoyo para el diagnóstico médico (Ministerio De Ciencias, Tecnología, Conocimiento E Innovación de Chile [MinCiencias], s.f).

En Chile, la IA desempeña un papel fundamental en la modernización del Estado y en la creación de soluciones innovadoras orientadas a mejorar la calidad de vida, promoviendo un desarrollo sostenible y equitativo. Su implementación en áreas como la salud, la educación y la seguridad está contribuyendo de manera significativa a la transformación positiva de la gestión tanto pública como privada (Ministerio De Ciencias, Tecnología, Conocimiento E Innovación de Chile, s.f).

No obstante, estos rápidos cambios y avances generan también grandes problemáticas en su uso, como, por ejemplo, su utilización como una herramienta criminal. Bajo este contexto, el objeto del presente estudio corresponde a las formas en que el crimen organizado puede utilizar herramientas de IA para expandir o sofisticar sus actividades delictivas en Chile. En consecuencia, se examina este fenómeno desde una perspectiva de seguridad pública, explorando sus implicancias en el contexto chileno.

El desarrollo de la presente investigación resulta relevante en el contexto actual de transformación tecnológica y seguridad pública en Chile. El avance acelerado de la inteligencia artificial ha generado tanto oportunidades como amenazas, especialmente en el ámbito del crimen organizado, que comienza a explorar y adaptar estas herramientas a sus fines ilícitos. Aunque el uso criminal de la IA en el país aún presenta manifestaciones incipientes, los antecedentes analizados demuestran un escenario de riesgo creciente, caracterizado por la sofisticación de las modalidades delictivas, la automatización de

procesos criminales y la posibilidad de manipular información o vulnerar infraestructuras críticas.

Bajo este escenario, se plantean como objetivo general analizar las implicancias del uso de inteligencia artificial por parte del crimen organizado en Chile, lo cual se realiza a través de la exploración de las formas actuales y emergentes en que las organizaciones criminales están utilizando inteligencia artificial a nivel global y regional, con énfasis en los delitos asociados al ciberespacio y crimen organizado, identificando posibles manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile, conociendo las experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública, para extraer aprendizajes útiles para el contexto chileno y finalmente identificando los principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile. Todo esto, se logró a través de la metodología de la investigación cualitativa, específicamente empleando el análisis de contenido cualitativo para textos académicos seleccionados y para las entrevistas que se realizaron a 03 expertos en la materia.

La motivación que dio origen a esta investigación, surge de la creciente preocupación por el impacto que la inteligencia artificial está teniendo en los distintos ámbitos de la seguridad pública, especialmente en relación con su potencial uso por parte de redes criminales. Frente a ello, Chile se encuentra en una etapa temprana de exposición a este fenómeno, lo que representa tanto un desafío como una oportunidad para la formulación de políticas preventivas y el fortalecimiento institucional.

Finalmente, el presente estudio se estructura a través de seis capítulos, el primero de ello corresponde al Planteamiento del Problema, para dar paso al Marco Teórico-Conceptual y la Metodología del estudio. Luego, se presentan los resultados del estudio, dando paso de esta forma a las Conclusiones y finalmente a las Recomendaciones. Los apartados finales del estudio, corresponden a las Referencias Bibliográficas y los Anexos del estudio.

2. PLANTEAMIENTO DEL PROBLEMA

Naciones Unidas (s.f) explica que, desde mediados del siglo XX, hasta el día de hoy, la Inteligencia Artificial (IA) ha evolucionado rápidamente, transformando diversos aspectos de la vida cotidiana. Hoy en día, los seres humanos interactuamos de manera constante con la IA, desde el uso de buscadores en internet, videojuegos, asistentes digitales presentes en teléfonos y dispositivos inteligentes, hasta sistemas de control de crucero automatizado en automóviles (Federal Bureau of Investigation [FBI], s.f).

Mientras que Internet necesitó más de dos décadas para alcanzar al 90% de los usuarios, la inteligencia artificial logró ese mismo nivel de adopción en apenas tres años, mostrando un crecimiento más acelerado tanto en la inversión como en la disminución de sus costos. Estos progresos constituyen una oportunidad para que los beneficios de la IA se extiendan a todos los sectores de la sociedad, evitando su concentración en los países del Norte Global. No obstante, alcanzar este objetivo exige un esfuerzo conjunto de todas las naciones para facilitar y fortalecer la adopción de esta tecnología (Naciones Unidas y Comisión Económica para América Latina y el Caribe [ONU y CEPAL], 2025).

A nivel regional es posible ubicar al Índice Latinoamericano de IA (ILIA), el cual presenta una visión general sobre el progreso de la inteligencia artificial en 19 países de América Latina y el Caribe, y expone un panorama de los elementos esenciales para que su desarrollo se oriente al beneficio de las personas (ONU y CEPAL, 2025). Este Índice fue elaborado desde el año 2023 en conjunto con el Centro Nacional de Inteligencia Artificial (CENIA) de Chile y con el respaldo de múltiples instituciones académicas, así como de entidades públicas y privadas. En consecuencia, el ILIA tiene como finalidad

> Contribuir con la transferencia de conocimiento y difusión de buenas prácticas para promover el desarrollo de la IA al servicio de las personas, además de una comprensión exhaustiva de los ecosistemas nacionales de IA en cada país para orientar el diseño de políticas públicas basadas en evidencia. (ONU y CEPAL, 2025, p. 21)

El ILIA es un instrumento analítico, único en su tipo en América Latina y el Caribe, el cual facilita la evaluación, comparación y comprensión del progreso de los ecosistemas nacionales de IA mediante tres dimensiones esenciales: A) Factores Habilitantes, B) Investigación, Desarrollo y Adopción, y C) Gobernanza. El índice agrupa a los países en tres categorías, según su grado de madurez:

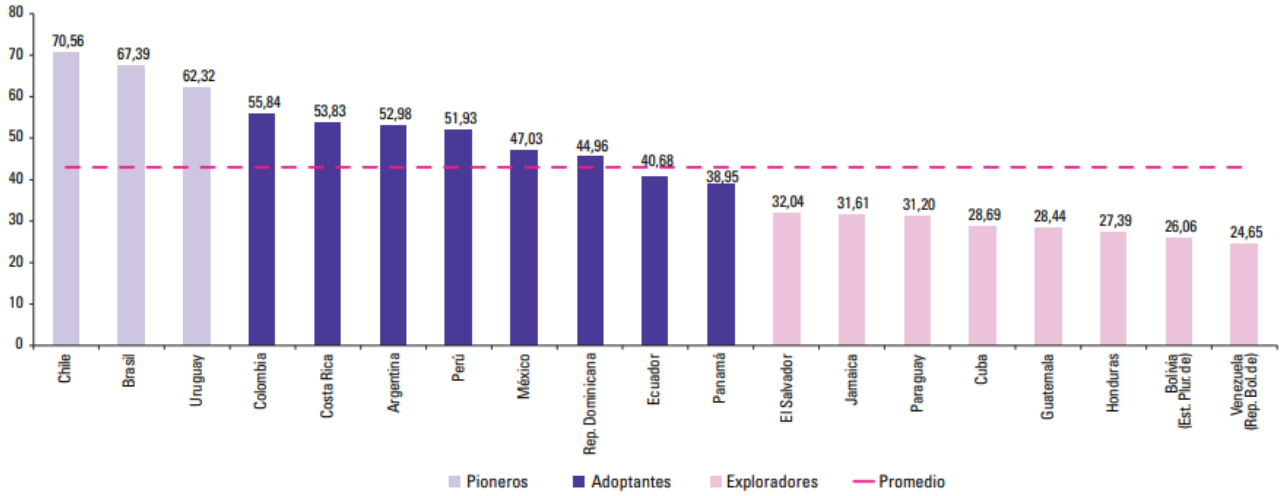
- Pioneros: superan los 60 puntos y destacan por sus esfuerzos en infraestructura tecnológica, talento especializado, investigación, innovación y gobernanza.
- Adoptantes: con puntajes entre 35 y 60, muestran avances intermedios, pero aún enfrentan brechas críticas que restringen el desarrollo y adopción de IA, particularmente en cuanto a su capacidad de investigación y de innovación.
- Exploradores: por debajo de 35 puntos, con ecosistemas incipientes y limitada capacidad para desplegar IA. (ONU y CEPAL, 2025)

A partir de los datos del ILIA, expresados en el Gráfico 1 se puede visualizar que los tres países con las más altas puntuaciones son Chile, Brasil y Uruguay. En este contexto, Chile, con 70,56 puntos, se posiciona como pionero en la escala de medida, lo que se traduce en que es un líder regional y el país con el mayor nivel de desarrollo en IA. Esto refleja la existencia una infraestructura consolidada en tecnología, formación de talento, investigación, innovación y gobernanza. Luego, en segundo puesto se encuentra Brasil con 67,39 puntos, país que también se ubica en el grupo de los pioneros, mostrando una sólida capacidad en investigación, desarrollo tecnológico y políticas nacionales orientadas a la IA. Su gran economía y actividad constante, le permiten mantener un liderazgo en la región, gracias a una estrategia que combina inversión, formación de personas y desarrollo de nuevas ideas.

Finalmente, el último país pionero según la escala de medida del ILIA, corresponde a Uruguay con 62,32 puntos, el cual se destaca por su infraestructura digital robusta y su modelo de gobernanza inclusiva. A pesar de ser una economía de menor escala, ha logrado posicionarse a la vanguardia mediante políticas efectivas en educación digital, conectividad y regulación responsable de la IA.

Gráfico 1

Puntaje total ILIA



Nota: Fuente ONU y CEPAL (2025)

Por otro lado, en cuanto a los principales hallazgos del informe ILIA 2025 (ONU y CEPAL, 2025), en las tres categorías que mide el Índice son:

a) Factores Habilitantes:

- Mejora la conectividad digital, aunque 11 de 19 países aún no superan los 50 puntos en infraestructura.
- La inclusión de contenidos de IA en la educación escolar aumentó de 2 a 6 países, lo que representa un avance hacia el desarrollo de capacidades locales y mayor equidad.
- Costa Rica lidera en habilidades profesionales en IA, demostrando el impacto de políticas de talento bien planificadas.
- Brasil concentra la capacidad de cómputo regional, mientras que Uruguay y Colombia destacan en GPU per cápita, favoreciendo una distribución más equitativa del desarrollo.

b) Investigación, Desarrollo y Adopción:

- La participación femenina en investigación en IA aumentó del 19,8% al 23,6%, aunque aún no alcanza la paridad.
- Perú encabeza la intensidad de uso de IA, evidenciando que la adopción no depende exclusivamente del nivel de desarrollo productivo.
- La inversión y la innovación en IA siguen concentradas en pocos países, representando solo el 1,12% de la inversión mundial.
- La IA generativa emerge como motor transversal de adopción, especialmente en educación, servicios públicos y MIPYMES.

c) Gobernanza:

- Existen dos escenarios paralelos: países con estrategias consolidadas (Brasil, Chile, Uruguay) y otros que aún no cuentan con una hoja de ruta definida.
- La mayoría de las estrategias nacionales carece de mecanismos de implementación efectivos.
- La región tiene baja participación en organismos internacionales de estandarización, lo que limita su influencia en la regulación global.
- Aunque hay avances legales en ciberseguridad y protección de datos, persisten debilidades técnicas para su aplicación.

Dentro de las principales conclusiones, se reflejan avances significativos en el desarrollo de la inteligencia artificial en la región, abriendo nuevas oportunidades en materia de productividad, inclusión y sostenibilidad. A diferencia de transformaciones tecnológicas previas, “su adopción no depende de matrices productivas sofisticadas, lo que permite que países de distinto tamaño y estructura económica puedan beneficiarse” (ONU y CEPAL, 2025, p. 18). El principal desafío consiste en vincular las políticas de digitalización con las de desarrollo productivo, de modo que la IA impulse la innovación, la productividad y la integración regional, al mismo tiempo que promueva una mayor inclusión social, sostenibilidad ambiental y fortalecimiento institucional.

Por otro lado, se plantea la reducción de las brechas de infraestructura, talento y gobernanza, incorporando enfoques de sostenibilidad y equidad de género, junto con fomentar la cooperación regional, lo cual será esencial para que la IA se consolide como un

motor de transformación estructural. En este contexto, el ILIA 2025 se presenta como "una guía para definir políticas de desarrollo, en el que la inteligencia artificial esté al servicio de un futuro más productivo, inclusivo y sostenible para América Latina y el Caribe" (ONU y CEPAL, 2025, p. 18).

No obstante, también existen aspectos positivos, entre ellos, que a nivel regional se presenta un fortalecimiento de los ecosistemas de investigación básica, los cuales constituyen la base sobre la que se sustentan las demás estructuras vinculadas a la inteligencia artificial. Este avance se refleja en el aumento de programas de doctorado y magíster en la mayoría de las economías. Asimismo, se observa una consolidación en la penetración de internet, lo que ha favorecido el rápido crecimiento del uso de aplicaciones de IA, con una participación regional estimada entre el 15% y el 20% del mercado mundial (ONU y CEPAL, 2025).

Como se ha visto hasta ahora, en la actualidad la inteligencia artificial es una de las tecnologías más disruptivas de las últimas décadas, transformando prácticamente todas las áreas de la vida humana. Su expansión ha traído consigo notables beneficios en materia de eficiencia, análisis de datos y automatización de procesos; sin embargo, también ha generado nuevos escenarios de riesgo que desafían las estructuras tradicionales de control y prevención del delito. En este contexto, la interacción entre IA y criminalidad emerge como una problemática de creciente preocupación, al evidenciar cómo las mismas herramientas diseñadas para el progreso pueden ser utilizadas con fines ilícitos.

Las organizaciones criminales transnacionales y cibercriminales pueden adaptar tecnologías de IA emergentes para sofisticar sus operaciones, planteando escenarios como el uso de sistemas de armas autónomas, *deepfakes*[1], robo de identidad y secuestro virtual. Asimismo, se ha explorado la relación entre el carácter dual de la IA y la necesidad de alianzas entre agencias de seguridad, academia y sector privado para anticipar respuestas estratégicas (Peters, 2019).

Como consecuencia de este escenario, algunos organismos han implementado iniciativas que buscan combatir este fenómeno. Es el caso de la Universidad de Chile, la

[1] Videos falsos generados con inteligencia artificial.

Universidad de Los Andes y la Universidad del Biobío, quienes firmaron un acuerdo con el Ministerio Público para el licenciamiento oficial del ecosistema de inteligencia artificial HeredIA. Esta herramienta, tiene como objetivo asistir a fiscales en la identificación de redes delictivas complejas (Universidad de Chile, 2025).

HeredIA, corresponde a "un sistema basado en *machine learning*[2] que permite analizar grandes volúmenes de información no estructurada como reportes policiales, denuncias ciudadanas y publicaciones en redes sociales" (Universidad de Chile, 2025, párr. 2). Desde que se implementó, en el año 2022, HeredIA ha posibilitado la identificación de organizaciones criminales, la anticipación de áreas de riesgo y una notable agilización en los procesos de análisis. En el caso de las estafas, por ejemplo, el tiempo de procesamiento disminuyó de 30 días a solo uno. Asimismo, ha tenido un papel fundamental en más de 30 investigaciones de gran relevancia, relacionadas con delitos como extorsión, homicidios, robos y secuestros. Debido a esto, en la cuenta pública 2025 del Ministerio Público, el fiscal nacional, destacó a HeredIA como uno de los pilares de la modernización tecnológica de la institución, señalando que "esta solución ha madurado en confiabilidad, seguridad e integración regional, consolidándose como esencial para abordar delitos complejos" (Universidad de Chile, 2025, párr. 4).

Con base en esta revisión bibliográfica, se determina que el problema de investigación se centra en comprender las implicancias del uso de la inteligencia artificial por parte del crimen organizado en Chile, considerando tanto las potenciales adaptaciones de estas tecnologías por redes criminales locales como la capacidad institucional del país para prevenir, detectar y responder a dichas amenazas. Este estudio se contextualiza en un escenario de creciente digitalización y sofisticación delictual en América Latina, donde las lecciones aprendidas a nivel internacional pueden orientar el diseño de estrategias nacionales de seguridad y defensa frente a la criminalidad potenciada por IA.

En base a esto, Hernández et al. (2014) explican que la justificación de una investigación recae en el para qué y el porqué del estudio, estableciendo ciertos criterios que evalúan la relevancia investigativa. Bajo este contexto, la justificación del presente estudio

[2] Rama de la inteligencia artificial que se centra en que las computadoras aprendan por sí mismas a partir de datos, sin necesidad de ser programadas.

se sustenta en la relevancia de comprender los riesgos que la IA representa para la seguridad pública y los derechos ciudadanos, al ser empleada para fines ilícitos como manipulación de información, suplantación de identidad, o generación de contenidos falsos.

2.1 Objetivos del estudio

2.1.1 Objetivo general:

Analizar las implicancias del uso de inteligencia artificial por parte del crimen organizado en Chile.

2.1.2 Objetivos específicos:

1. Explorar las formas actuales y emergentes en que las organizaciones criminales están utilizando inteligencia artificial a nivel global y regional, con énfasis en los delitos asociados al ciberespacio y crimen organizado.
2. Identificar posibles manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile.
3. Conocer experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública, para extraer aprendizajes útiles para el contexto chileno.
4. Identificar los principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile.

3. MARCO TEÓRICO-CONCEPTUAL

El presente capítulo, tiene como finalidad abordar la perspectiva teórica del objeto en estudio por medio de investigaciones y teorías científicas. Para estos fines, en un primer momento se presenta el concepto de Inteligencia Artificial, para luego conceptualizar el fenómeno delictual del crimen organizado. Posteriormente, se explica la el vínculo de la IA con el crimen organizado. Finalmente, se desarrolla el marco conceptual para el análisis del caso chileno desde el punto de vista de ambos fenómenos.

3.1 Conceptualización de la inteligencia artificial

La IA contempla una amplia gama de tecnologías, las que pueden definirse como "sistemas adaptativos de autoaprendizaje" (Naciones Unidas [ONU], s.f, párr. 2). Esta, a su vez, puede clasificarse según las tecnologías empleadas, los objetivos perseguidos (por ejemplo, el reconocimiento facial o de imágenes), las capacidades desarrolladas (como la interpretación del lenguaje o la resolución de problemas) o las clases de agentes involucrados (entre ellos, los robots y los vehículos autónomos).

Por su parte, el FBI (s.f) utiliza la definición establecida en la Ley de Autorización de Defensa Nacional del año fiscal 2019 (FY19 NDAA), que establece que la inteligencia artificial incluye, entre otras cosas, "cualquier sistema artificial que realiza tareas en circunstancias variables e impredecibles sin una supervisión humana significativa o que puede aprender de la experiencia y mejorar el rendimiento cuando se expone a conjuntos de datos" (FBI, s.f, párr. 3), así como también "un sistema artificial desarrollado en software de computadora, hardware físico u otro contexto que resuelve tareas que requieren percepción, cognición, planificación, aprendizaje, comunicación o acción física similares a las humanas" (FBI, s.f, párr. 4). En este contexto, para maximizar los beneficios de la Inteligencia Artificial resulta fundamental considerar cuidadosamente sus posibles riesgos, entre ellos, la protección de la privacidad de los datos, la mitigación de sesgos y la transparencia en la toma de decisiones (Chief Executives Board [CEB], s.f).

En esta perspectiva, Sutton (2019) señala que la reducción de costos constituye un elemento fundamental en la expansión del uso de la IA. De acuerdo con la ley de Moore y

sus extensiones, el precio por unidad de cómputo ha disminuido de manera exponencial, lo que ha vuelto la tecnología de IA más accesible y económica para distintos tipos de usuarios, desde investigadores hasta empresas. Esta caída en los costos ha favorecido el desarrollo e implementación de soluciones de IA más avanzadas y potentes, impulsando así la innovación y la experimentación en múltiples ámbitos.

Otro aspecto relevante a considerar, es que la enorme cantidad de información disponible en la actual era del capitalismo digital ha actuado como un factor determinante en el impulso y desarrollo de la inteligencia artificial, "que depende en gran medida de grandes conjuntos de datos para el aprendizaje y la mejora de sus modelos" (Fallas-Vargas y Morales, 2024, p. 78). La masiva generación de datos provenientes de dispositivos conectados a Internet, redes sociales, transacciones digitales y diversas plataformas en línea ha constituido una fuente sumamente valiosa para el diseño y entrenamiento de algoritmos de IA. En consecuencia, "esta disponibilidad de datos ha permitido no solo refinar los modelos existentes, sino también explorar nuevas aplicaciones de la IA en diversos sectores" (Fallas-Vargas y Morales, 2024, p. 78).

Fahim y Bajpai (2020), explican que, desde la óptica del derecho comparado, existe un consenso general respecto a que, en un futuro cercano, la inteligencia artificial podría desarrollar habilidades funcionales similares (e incluso, según algunos autores, idénticas) a las del pensamiento, razonamiento e inteligencia humana.

Bajo este contexto, la Universidad Nacional Autónoma de México ([UNAM], 2023), indica que, en algunos países, para el año 2023, alrededor del 80% de las personas hizo uso de la IA muchas veces sin ser conscientes de ello; donde solo un tercio reconoció su utilización. Asimismo, el organismo destaca que ChatGPT "ha sido la innovación más rápidamente adoptada en la historia de la humanidad: un millón de usuarios en cinco días, 100 millones en dos meses, y actualmente se estima que son más de 200 millones" (UNAM, 2023, párr. 9). Según especialistas de la UNAM, esta tecnología representa (o ya constituye), una transformación disruptiva con efectos en todos los ámbitos de la actividad humana (UNAM, 2023).

Si bien la inteligencia artificial cuenta con un enorme potencial para generar beneficios a las personas, la falta de una adecuada regulación podría hacer que estos se concentren únicamente en unos pocos Estados, empresas o individuos pioneros en el área, donde ya muchas naciones presentan "dificultades para acceder a las herramientas de la inteligencia artificial, lo que pone de relieve la necesidad de cooperación y solidaridad internacionales para cerrar la brecha de la IA en los países en desarrollo" (ONU, s.f, párr. 7). Dentro de esta materia, la ONU (2024) expresa una gran preocupación por las formas en que la IA puede utilizarse para trasgredir los derechos humanos de las personas. Debido a esto, diversos expertos de las Naciones Unidas, declararon la necesidad "irrefutable" de una regulación mundial de la IA, con la finalidad de evitar la brecha digital y la desigualdad (ONU, 2024).

Sin embargo, las diferencias de representación resultan evidentes, donde amplias regiones del mundo han sido excluidas de los debates internacionales relacionados con la gobernanza de la inteligencia artificial. Por ejemplo, sólo siete países (Canadá, Francia, Alemania, Italia, Japón, Reino Unido y EE.UU.) forman parte de siete iniciativas relevantes sobre IA fuera del marco de la ONU, en tanto que 118 países, en su mayoría pertenecientes al Sur Global, no participan en ninguna de ellas (ONU, 2024).

Con la finalidad de dar respuesta a estas inquietudes, un grupo de expertos de la ONU plantea diversas recomendaciones orientadas a regular el uso de la inteligencia artificial. Entre las propuestas, se incluyen la creación de un panel científico internacional independiente sobre IA, la instauración de un diálogo político intergubernamental y multisectorial y la implementación de un fondo mundial para la IA destinado a reducir la brecha digital (ONU, 2024). Asimismo, la organización enfatizó que todo uso de la inteligencia artificial en contextos militares debe ajustarse al derecho internacional humanitario y a los estándares de derechos humanos, instando a los Estados a establecer marcos jurídicos y mecanismos de supervisión sólidos. Conjuntamente, "estas recomendaciones instan a los Estados miembros de la ONU a sentar las bases de la primera arquitectura global inclusiva para la gobernanza de la IA basada en la cooperación internacional y la transparencia" (ONU, 2024, párr. 16).

3.2 Conceptualización del crimen organizado

El crimen organizado no es un fenómeno nuevo, existiendo durante décadas (Linares, 2008). Armienta, et. al (2015) señalan que, como consecuencia de las actividades criminales de nivel internacional, han surgido nuevas alianzas de grupos organizados que unen sus capacidades, replicando un modelo similar al de la asociación de empresas que operan en la economía legal.

Por otro lado, la UNODC (2012, citada en Cajiao et al., 2018) plantea la dificultad para caracterizar al fenómeno del crimen organizado, debido a que "la transformación de crimen transnacional es constante y la variedad y las diferencias entre los actores son tales que aún las propuestas más innovadoras se quedan cortas a la hora de caracterizar el crimen transnacional" (p.4).

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Naciones Unidas, 2004) define como grupo delictivo organizado a:

> Un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material. (Naciones Unidas, 2004, p. 5)

En las últimas décadas, las actividades que contempla del crimen organizado transnacional se han expandido a diversas áreas (Linares, 2008). En este contexto, existen grupos criminales que se dedican a la difusión de pornografía infantil, al tráfico de flora y fauna, de obras de arte, antigüedades, material intelectual, órganos humanos, para ser llevados a otros países. Sin embargo, el narcotráfico es considerado la actividad delictual que mayores ingresos entrega al crimen organizado (Rivera, 2011).

Por otra parte, existe una estrecha conexión entre el crimen organizado y el fenómeno de la globalización, ya que la tendencia de las organizaciones criminales "será hacia la intensificación de estos fenómenos, puesto que la tecnología continuará expandiéndose y las

redes criminales explotarán estas tecnologías de una manera más efectiva que los gobiernos" (Linares, 2008, p.375). En este sentido, Kessler (2015) plantea que, como consecuencia de la globalización, el concepto mismo de fronteras el que cambia, pues "hay nuevas fronteras cibernéticas y tecnológicas que no coinciden con las geográficas, reconfigurando las actividades del crimen organizado" (Kessler, 2015, p. 46). En consecuencia, el tráfico ilícito de drogas se beneficia en dimensiones como la facilidad de las transferencias electrónicas de dinero o el seguimiento satelital de los cargamentos que atraviesan fronteras.

Cajiao et al. (2018) indican que el crimen organizado se encuentra estructurado por medio de redes sociales "más fluidas, flexibles y con un alto grado de adaptación, que evoca el comportamiento de las corporaciones transnacionales que operan a través de redes y nodos que funcionan a nivel global" (p.5). Para Williams (2008, citado en Cajiao et al., 2018) el funcionamiento del crimen organizado transnacional por medio de redes facilita las interacciones entre estructuras, lo que permite una mayor adaptabilidad a la acción de las autoridades, permitiéndoles ser más adaptables a los cambios.

Como resultado de la exploración documental, se pudo dar cuenta de que diversos autores consultados establecen que el crimen organizado funciona bajo una estructura jerárquica con rasgos del tipo empresarial (Cajiao et al., 2018; Rivera, 2011). En este contexto, la estructura organizacional del crimen organizado es rígida, cuenta con un alto grado de burocratización, códigos de conducta que contempla a todos sus miembros y una cúpula directiva que concentra el poder y liderazgo dentro de la organización (Cajiao et al., 2018).

En cuanto a su estructura, las redes delictuales de cualquier tamaño suelen contar con un núcleo y una periferia, lo que refleja asimetrías de poder, influencia y control dentro de la organización criminal. El núcleo de la red "es donde se toman las decisiones, dirigen las operaciones y proporcionan mecanismos de dirección para la organización" (Cajiao et al., 2018, p.6) por lo que esta esfera cuenta con fuertes vínculos entre sus miembros, quienes se respaldan a través de mecanismos que los vinculan con la finalidad de crear altos niveles de confianza, cohesión y liderazgo, por lo que muchas veces los vínculos entre estos individuos son de tipo familiar. Mientras que, en la periferia de la organización criminal, las relaciones

entre los individuos son menos proxémicas y más flexibles, por lo que la relevancia de esta esfera "no radica en los vínculos entre individuos, sino en que la interacción con otras estructuras permite ampliar sus operaciones tanto geográfica como socialmente, facilitando operaciones más extensas, actividades más diversas y aumentando su capacidad de recolección de información" (Cajiao et al., 2018, p.6).

Debido a esto, Rivera (2011) destaca que el control del crimen organizado y la reducción de su capacidad para dañar a la sociedad no dependen únicamente del aparato estatal, ya sea desde la acción policial, la administración de justicia o la creación de leyes, sino también del compromiso y la participación activa de la ciudadanía frente a esta amenaza. Es necesario que la sociedad exija la aplicación rigurosa de la ley y el uso legítimo de la fuerza del Estado para enfrentarla, puesto que "las mafias o el crimen organizado prosperan en el abismo que separa el Estado de la sociedad pero, si se consigue unir ambos, se puede luchar en contra del Crimen Organizado" (Rivera, 2011, p. 3).

La investigación del crimen organizado presenta diversas problemáticas, puesto que es un fenómeno difícil de investigar por la dificultad que implica medir esta tipología delictual (Salinero, 2015). En este sentido, el autor declara la existencia de cuatro obstáculos en la investigación de este delito. El primero de ellos, es relativo al concepto de crimen organizado, ya que, a lo largo de la historia, su definición y existencia ha generado debates e imprecisiones, estableciéndose un consenso internacional en la década de los 2000 sobre la definición de este concepto, basado en una definición concreta desde el enfoque criminológico. La segunda dificultad, corresponde a la medición de los denominados "delitos complejos", ya que la medición de estos es diferente a los delitos convencionales. En este aspecto, la medición de un delito de homicidio es distinta a la del crimen organizado, ya que el delito de homicidio "constituye un acto singular y ejecutado individualmente y, en el segundo, la acción se realiza bajo la actuación de grupos criminales que desarrollan actividades ilícitas de las que […] necesitan de actividades instrumentales" (Salinero, 2015, p.32). El tercer problema y en relación con lo anterior, es la disponibilidad y el acceso a los datos propios del crimen organizado, puesto que, tanto en el contexto internacional como en el nacional, las fuentes de información carecen de datos sobre este tipo de criminalidad. Finalmente, la cuarta problemática, es que el crimen organizado se trata de un delito

transnacional, debido a esto, se dificulta la medición del mismo, ya que una ramificación de la organización no es representativa en función del volumen total que representa la organización completa desde un punto de vista global, además que su medición contempla la intervención de diversos actores, países y Estados (Salinero, 2015).

3.3 Inteligencia Artificial y Crimen Organizado

Uno de los principales desafíos para el aprovechamiento adecuado de la IA, radica en su carácter de herramienta, susceptible de emplearse tanto para el beneficio de la humanidad, como para fines opuestos (Fallas-Vargas y Morales, 2024). En el ámbito de la seguridad ciudadana, la inteligencia artificial ofrece herramientas avanzadas que fortalecen la vigilancia y la prevención del delito (Rejas et al., 2024). Los sistemas de videovigilancia dotados de IA son capaces de identificar conductas sospechosas y alertar de inmediato a las autoridades (Sarabia, 2023). Asimismo, los algoritmos de predicción delictual permiten a las fuerzas policiales anticipar posibles incidentes mediante el análisis de patrones y tendencias (Barragán-Huamán et al., 2023). En situaciones de emergencia, la inteligencia artificial facilita la gestión de datos provenientes de diversas fuentes, optimizando la coordinación y respuesta operativa. Del mismo modo, la aplicación del reconocimiento facial y biométrico en espacios públicos contribuye a reforzar la seguridad al posibilitar la identificación temprana de amenazas potenciales (Correa-Mende et al., 2023).

Sin embargo, si los sistemas basados en IA son programados o entrenados de manera incorrecta, las decisiones resultantes pueden generar consecuencias negativas, especialmente en ámbitos críticos como la medicina, el transporte o la seguridad, donde “específicamente en la seguridad y justicia la IA puede ser explotada para fines perniciosos, como es el caso de los ciberataques, la guerra cibernética, vigilancia invasiva o focalizada en determinados grupos o personas, manipulación de información, entre otros casos (Fallas-Vargas y Morales, 2024, p. 82).

Un ejemplo evidente es el empleo de la inteligencia artificial para diseñar ataques automáticos que se vuelven más complejos conforme acumulan y procesan información. Nica y Tănase (2020) explican que, durante la fase de preparación de un ataque cibernético,

el motor de IA, gracias al volumen de datos disponibles, puede detectar nuevas vulnerabilidades en la infraestructura objetivo y generar campañas de phishing dirigidas.

Otín (2025) explica que "la inteligencia artificial está incidiendo en el crimen, potenciando y facilitando la comisión de actos delictivos, lo que plantea retos inéditos para la política criminal" (p. 29). Entre estos, se ubican dificultades para saber quién es responsable, probar los hechos y seguir el rastro tecnológico, junto con el peligro de que se impongan castigos demasiado severos.

Diversos informes señalan que actores malintencionados están utilizando la inteligencia artificial para facilitar la comisión de delitos como hackeos, fraudes, campañas de desinformación y ciberataques de gran magnitud (Organización para la Cooperación y el Desarrollo Económicos, 2024, citada en Otín, 2025). Esta problemática reviste especial relevancia por la capacidad de la IA para ampliar el alcance, la sofisticación y el anonimato de las actividades ilícitas. La literatura (Blauth et al., 2022; Brundage et al., 2018; Caldwell et al., 2020; Easttom, 2025) confirma un creciente interés académico e institucional en analizar y clasificar estas amenazas, desarrollando tipologías y estudios de caso que aportan elementos para su comprensión y mitigación.

Blauth et al. (2022) presentan una tipología que distingue entre abuso y uso malicioso de la IA, identificando categorías como ataques a la integridad, resultados no intencionados, ingeniería social, desinformación y sistemas de armas autónomas. Estos autores destacan que la colaboración entre gobiernos, industria y sociedad civil es un factor clave para fortalecer la resiliencia frente a dichas amenazas. Otros estudios ofrecen un análisis interdisciplinario de las amenazas plausibles de la IA para el crimen, basándose en experimentos teóricos que muestran su uso para fraudes en redes sociales y manipulación de mercados. La literatura confirma que la ausencia de marcos normativos específicos limita la capacidad de prevención y respuesta en materia de *AI-Crime* (King et al., 2019).

Choraś y Woźniak (2022) introducen el concepto de *Ethical Adversarial Attacks* (EAA) como estrategia defensiva para contrarrestar sistemas de IA maliciosos. En esta línea, varios estudios han examinado métodos para engañar a sistemas de inteligencia artificial, considerándolos no solo como un riesgo, sino también como una posible herramienta de

protección cuando se utilizan de forma legal y ética. Asimismo, otros autores estructuran el panorama de amenazas en tres dominios: digital, físico y político. La IA puede expandir amenazas existentes, como el *spear phishing*, ataque cibernético que consiste en el envío de mensajes fraudulentos altamente personalizados y dirigidos a una persona o entidad específica; introducir amenazas inéditas, por ejemplo, enjambres de drones y modificar la naturaleza de los ataques, haciéndolos más difíciles de atribuir y más efectivos (Brundage et al., 2018).

Esa capacidad de autoaprendizaje y adaptación, torna a la IA particularmente peligrosa: "puede evadir los mecanismos de seguridad tradicionales más fácilmente y ser más efectiva en sus ataques" (Fallas-Vargas y Morales, 2024, p. 82). Al operar de forma autónoma y continua, los sistemas inteligentes pueden perpetrar ataques a gran escala con una eficiencia y sofisticación sin precedentes.

Por otro lado, en el ámbito del tráfico de drogas ilícitas, las organizaciones criminales también han incorporado el uso de la inteligencia artificial. Según señalan Aggarwal et al. (2019), el tráfico de drogas de punto a punto representa una amenaza creciente debido al empleo de vehículos no tripulados por parte de los delincuentes. Estos dispositivos utilizan sistemas de planificación basados en IA para identificar las rutas más seguras (evitando controles o presencia policial) y se apoyan en tecnologías de navegación autónoma que aumentan de manera significativa las tasas de éxito del contrabando.

A pesar de esta situación alarmante, la tecnología de inteligencia artificial posee un gran potencial para transformar la manera en que se previene y combate el crimen (Guzmán y Casteleiro, 2022). Sin el apoyo de herramientas avanzadas, como el análisis predictivo, la identificación de patrones y la automatización de procesos, los organismos encargados de la aplicación de la ley se encontrarán en desventaja frente a las tácticas cada vez más complejas de las organizaciones criminales (Calderón et al., 2021).

La incorporación de la inteligencia artificial en la seguridad pública puede generar múltiples beneficios, incluyendo una mayor eficiencia en la recopilación y análisis de datos, la detección temprana de amenazas y la optimización de recursos (Tuesta et al., 2024). No obstante, la ausencia de infraestructura tecnológica adecuada, la limitada comprensión sobre las aplicaciones prácticas de la IA y la posible resistencia al cambio, son obstáculos que

deben abordarse para modernizar y fortalecer las estrategias de combate al crimen organizado (Guttman y Fong, 2016).

3.4 Marco Conceptual para el Análisis del Caso Chileno

En cuanto al marco regulatorio de la Inteligencia Artificial en Chile, en un primer momento, es necesario mencionar a la Política Nacional de Inteligencia Artificial, la cual busca "que la Inteligencia Artificial (IA) se convierta en una herramienta clave para el desarrollo sostenible equitativo de nuestra sociedad" (MinCiencias, 2024, p. 5). En consecuencia, el objetivo de la Política es "fomentar el desarrollo y uso ético y responsable de la Inteligencia Artificial en Chile, para que esta tecnología juegue un rol promotor en el nuevo modelo de desarrollo y crecimiento del país" (MinCiencias, 2024, p. 19).

Reconociendo esta situación, el Consejo Nacional de Innovación para el Desarrollo (CNID) propuso en el año 2019 cinco áreas de acción fundamentales vinculadas a la IA: talento y empleo, capital tecnológico, capital social, modernización del Estado y marco ético-regulatorio. Del mismo modo, destacó cinco oportunidades estratégicas para el país: consolidar a Chile como un centro global de ciencia de datos, fortalecer el ecosistema de emprendimiento e innovación, promover una transformación tecnológica inclusiva, avanzar hacia un Estado digital y formar los talentos necesarios para el siglo XXI (MinCiencias, 2024).

En este contexto, Chile presentó en el año 2021 la primera versión de su Política Nacional de Inteligencia Artificial. Desde entonces, se han impulsado diversas iniciativas, entre ellas la creación del Centro Nacional de Inteligencia Artificial (CENIA) y del Núcleo Milenio *Futures of Artificial Intelligence Research* (FAIR), la asignación de becas de doctorado con foco en IA por parte de la Agencia Nacional de Investigación y Desarrollo (ANID), la implementación de redes 5G, el lanzamiento del primer doctorado en IA en Chile y Latinoamérica, así como la puesta en marcha del Proyecto "Algoritmos Éticos", destinado a promover la aplicación responsable de la IA y la ciencia de datos en el sector público. A esto se suma la emisión de una Circular Ministerial que regula el uso de la IA en el Estado, entre otras acciones. Gracias a estos avances, Chile se ha posicionado como líder regional en

el Índice Latinoamericano de Inteligencia Artificial (CENIA, 2023, citado en MinCiencias, 2024). En este último punto, dentro de los aspectos que destaca la Política Nacional de Inteligencia Artificial (MinCiencias, 2024) del Índice Latinoamericano de IA, son:

a) La investigación en IA es de las mejores a nivel regional, con publicaciones, investigadores y centros especializados, además de productividad e impacto altos.
b) La adopción de tecnologías de IA en el sector empresarial y el apoyo gubernamental en investigación y desarrollo superan los promedios regionales.
c) Chile ha hecho progresos significativos en la formulación de un marco regulatorio claro que aborde los desafíos éticos, legales y sociales asociados con estas tecnologías

Luego, como consecuencia del rápido avance de la inteligencia artificial a nivel mundial, durante los años 2023 y 2024 se optó por actualizar el contenido de la Política, con el propósito de abordar las nuevas oportunidades, desafíos y brechas surgidas en los últimos dos años. Esta revisión puso especial énfasis en el eje centrado en los aspectos de gobernanza y ética, por su influencia directa en la vida de las personas. Para estos fines entre enero y marzo de 2024 se llevó a cabo una consulta ciudadana en línea enfocada en estos aspectos de la política, en la cual participaron 640 personas de todo el país. Esto, "permitió identificar las inquietudes, opiniones y nivel de acuerdo de la ciudadanía con las acciones propuestas en el documento consultado" (MinCiencias, 2024, p. 12).

Bajo este contexto, la Política Nacional de Inteligencia Artificial, expone que el desarrollo de la IA debe orientarse al bienestar integral de todas las personas. Dado su creciente impacto en la vida cotidiana, es fundamental que esta tecnología se conciba y utilice de manera ética e inclusiva. Debido a esto, las acciones contempladas en esta Política buscan promover el uso de la IA para mejorar la calidad de vida de la población, garantizando que sus beneficios lleguen a todos, sin exclusiones ni discriminaciones, y que al mismo tiempo se enfrenten los riesgos e impactos negativos con pleno respeto a los derechos y la dignidad humana (MinCiencias, 2024).

Por otro lado, González (2017) plantea que, con el surgimiento, desarrollo y expansión desbordante de la era digital, el crimen organizado se ha visto obligado a adaptarse a este tipo de cambios, con la finalidad de evitar su obsolescencia, por lo que ha incorporado

nuevas modalidades a sus métodos tradicionales. En consecuencia, el ciber crimen ha constituido una nueva forma de operación en la web, generando importantes beneficios económicos a los grupos criminales.

Debido a esto, en el ciberespacio los sujetos aficionados han prácticamente desaparecidos, para así profesionalizarse en la comisión de los diversos ilícitos que se desarrollan en la web (González, 2017). Si bien estos delitos son llevados a cabo por individuos solitarios, muchas veces son cometidos de igual forma por grupos de expertos, los que se encuentran perfectamente organizados y dedicados de manera exclusiva a la comisión de ciberdelitos. En este contexto, Saldaña (2019) indica que el uso de la tecnología de la información ha cumplido el rol de "uno de los facilitadores para el crimen organizado para llevar a cabo sus actividades delictivas junto con la corrupción, el lavado de dinero, el fraude documental, el comercio online, la violencia y la extorsión" (p.3).

En consecuencia, la ciberseguridad no constituye un objetivo por sí misma, sino que es "una condición que, de existir, permite el uso pleno de Internet y de la web, herramientas habilitadoras y potenciadoras de las actividades humanas" (Comité Interministerial sobre Ciberseguridad, 2023, p. 8). En este este escenario, y considerando que los delitos informáticos no conocen fronteras, las respuestas policiales y penales pueden ser globales. Es por esto que, durante el año 2021 la PDI se integró a la Alianza de Ciberseguridad para el Progreso Mutuo (CAMP), una red de cooperación integrada por 47 países miembros, la cual se inició en el año 2015 por Corea del Sur (PDI, 2021). Entre los beneficios que significan para la persecución de los ciberdelitos en el país, se encuentran aquellos orientados a la entrega de información y conocimientos académicos relativos a la temática.

En este contexto, el marco legal e institucional dedicado a combatir el cibercrimen debe estar en constante adaptación y cambio, por lo que la PDI creó la Jefatura Nacional de Cibercrimen (JENACIBER). Asimismo, es de gran relevancia el proceso de transformación digital que desarrolla la PDI por medio de la Jefatura Nacional de Tecnologías de la Información y Transformación Digital (JENATID), así como también la seguridad de la información representada por medio de la creación del Centro Nacional de Ciberseguridad (CENACIB) durante el año 2019, el que tiene como objetivo principal "contribuir al

mejoramiento de la ciberseguridad de la institución enfrentando en la práctica, las amenazas informáticas que la puedan afectar" (PDI, 2022, p.18). Dentro de las áreas de análisis del CENACIB se encuentran: la seguridad informática, criptoanálisis, investigación e innovación y un observatorio de estudios y análisis.

Como consecuencia del avance de las nuevas tecnologías y la proliferación de la comisión de delitos cometidos vía *Internet*, tales como; amenazas; estafas; falsificación; pornografía infantil en internet; y delitos informáticos, entre otros, en año 2000 la Policía de Investigaciones de Chile crea las Brigadas Investigadoras del Cibercrimen (BRICIB). Actualmente dichas brigadas, se encuentran ubicadas en Santiago, Valparaíso y Concepción, y se crean como una "respuesta de la PDI al creciente desarrollo de la criminalidad informática en Chile y de la necesidad de contar con unidades dedicadas a la investigación y solución de los problemas que enfrenta la ciudadanía en el mundo virtual globalizado" (PDI, 2022, s.p).

La misión de las BRICIB se compone principalmente de tres dimensiones (Brigada Investigadora del Ciber Crimen, s.f):

a. Aportar los medios probatorios a los diferentes tribunales y fiscalías del país, cuando se detecta la utilización de herramientas y/o tecnologías de la información, en la comisión de delitos.
b. Detectar e investigar conductas ilícitas en Internet, referidas principalmente al comercio electrónico y hacking de sitios y servidores web.
c. Capacitar y formar investigadores especialistas en delitos informáticos

Mientras que el campo de acción principal de las BRICIB son los delitos informáticos, en sus diversas formas, las que se describen a continuación (PDI, 2022):

- **Sabotaje y espionaje informático:** Se asocian a acciones como el hackeo de cuentas de correo, redes sociales o cuentas bancarias[3], ataques DDOS, acceso indebido a

[3] Transferencias no autorizadas.

cualquier tipo de cuentas, extracción o eliminación de información desde bases de datos, entre otros.

- **Delitos asociados a la explotación sexual de menores a través de internet**: Como el almacenamiento, distribución, producción, difusión y comercialización de material pornográfico infantil, y el abuso sexual impropio. Este último se relaciona con el *Gromming*[4], en el cual se establece una amistad y luego, por medio de amenazas lo presiona para que le envíe fotografías con contenido erótico.

La BRICIB capacitan constantemente a sus Oficiales Investigadores, con el objeto de mantenerlos actualizados respecto al avance de las nuevas tecnologías. Además, cuenta con policías que mantiene estudios universitarios y técnicos en materias relacionadas con la informática, derecho, psicología, y cualquier disciplina relacionada con su ámbito de acción, lo que hace que sea una unidad profesional y científica.

En cuanto al marco legal, es posible mencionar que en el año 2022 se promulgó la Ley 21.459 (2022/2025), la cual establece normas sobre delitos informáticos y deroga la antigua Ley 19.223 (1993/2022) que tipificaba figuras penales relativas a la informática. Estos cambios se materializaron conforme al Convenio de Budapest, ya que Chile se comprometió a modificar su legislación en materias de delitos informáticos, en virtud de la promulgación del Decreto N°83 (2017) del Ministerio de Relaciones exteriores, el cual establece la suscripción al Convenio sobre la Ciberdelincuencia.

Las principales novedades de la Ley 21.459, recaen en la modernización de los tipos penales, para así adecuarlos a las nuevas formas de comisión de los delitos informáticos y a los avances de las tecnologías de la información y el *Internet*, considerando los nuevos riesgos y ataques sobre bienes jurídicos que no estaban contemplados en la anterior legislación (Aldoney et al., 2022).

En cuanto a la normativa internacional, el Convenio sobre la Ciberdelincuencia o Convenio de Budapest (2001) encabezado por el Consejo de Europa, es el primer tratado internacional que busca enfrentar a los delitos informáticos por medio de la armonización de

[4] Acción donde un adulto contacta a un menor de edad por medio de un perfil o cuenta real o falsa.

leyes entre naciones, tiene como objetivo que los países actúen coordinadamente en el combate contra la ciberdelincuencia, para contar con un sistema rápido y eficaz de cooperación internacional. Este Convenio resulta fundamental para establecer un marco legal internacional para combatir el ciberdelito, otorgando a los países adheridos un criterio base legislativo (ley modelo), para unificar y homologar la tipificación de estas conductas criminales. Cabe destacar que actualmente están suscritos 66 Estados, entre ellos; Chile, Argentina, Australia, Canadá, Cabo Verde, Colombia, Costa Rica, Estados Unidos de América (EUA), Filipinas, Ghana, Israel, Japón, Sudáfrica, entre otros (Consejo de Europa, 2001).

Becker y Viollier (2020) señalan que la ratificación del Convenio de Budapest para Chile tuvo como objetivo el "desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de los conceptos fundamentales y del tratamiento de la legislación penal, sustantiva y procesal, así como del establecimiento de un sistema rápido y eficaz de cooperación internacional" (p.77). En consecuencia, la naturaleza transnacional de los delitos informáticos requiere de una modificación de la legislación que cumpla con los estándares internacionales en la materia, para así mejorar la investigación y persecución de los delitos (Becker y Viollier, 2020).

El rápido avance de la tecnología ha provocado que las tecnologías de la información se utilicen como herramientas para la comisión de otros tipos de delitos como amenazas, estafas u otras defraudaciones, usurpación de nombre, delitos contra la vida privada, uso fraudulento de tarjetas de crédito y/o débito, entre otros. Sin embargo, este tipo de delitos no corresponden a delitos informáticos propiamente tal, sino que se utiliza un elemento tecnológico para su comisión. Además, pese a que estos ataques cibernéticos se han visto incrementados en los últimos años, la legislación chilena no ha ido avanzando conforme a esta situación, ya que la única herramienta disponible en Chile en materia legal es la Ley 21.459 (2022) la cual sanciona figuras de Ataque a la integridad de un sistema informático, Acceso ilícito, Interceptación ilícita, Ataque a la integridad de los datos informáticos, Falsificación informática, Receptación de datos y Fraude informáticos.

4. METODOLOGÍA

El presente capítulo, expone la vertebración metodológica del estudio. En este contexto, se define el tipo, el diseño y los procedimientos que permitan dar respuesta a los objetivos planteados, entre otros aspectos. En este capítulo, se describen las estrategias de recolección y análisis de la información, así como los criterios que guían la selección de fuentes y el tratamiento de los datos, asegurando la coherencia entre el problema de investigación, los objetivos y las técnicas aplicadas, garantizando la validez y confiabilidad de los resultados obtenidos. Para estos fines, se presentan siete subtítulos, fundamentando teóricamente cada uno de ellos.

4.1 Enfoque y diseño de investigación

Hernández-Sampieri et al. (2018) señalan que la investigación cualitativa se centra en comprender los fenómenos explorándolos desde la perspectiva de los participantes en su entorno natural y en relación con su contexto. Debido a esto, este enfoque se elige cuando el objetivo es analizar cómo ciertas personas perciben y experimentan los fenómenos a su alrededor, profundizando en sus puntos de vista, interpretaciones y significados.

La tipología cualitativa "resulta conveniente para comprender fenómenos desde la perspectiva de quienes los viven y cuando buscamos patrones y diferencias en estas experiencias y su significado" (Hernández-Sampieri et al, 2018, p.9). En este sentido, una de las características fundamentales de las investigaciones cualitativas, es que el investigador recopila información respecto a las percepciones, emociones, vivencias, significados y cualidades de los participantes del estudio, y mediante este proceso construye el conocimiento en base al fenómeno analizado (Hernández-Sampieri et al., 2018).

En consecuencia, el presente estudio se encuentra guiado bajo la tipología cualitativa, debido a que su principal objetivo es analizar las implicancias del uso de inteligencia artificial por parte del crimen organizado en Chile, lo que se realiza a través del diseño exploratorio, ya que este tipo de estudios "se llevan a cabo cuando el propósito es examinar un fenómeno o problema de investigación nuevo o poco estudiado, sobre el cual se tienen muchas dudas o no se ha abordado antes" (Hernández-Sampieri et al., 2018, p.106). Este diseño se selecciona

debido a que la inteligencia artificial, al ser una tecnología en constante evolución, mantiene su aplicación en el crimen organizado como un fenómeno aún en estudio.

4.2 Técnicas de recolección de datos

Las técnicas de recolección de datos empleadas en el presente estudio corresponden tanto al análisis documental como a la entrevista semiestructurada. En este contexto el análisis documental, se sustenta en un conjunto de técnicas y métodos orientados a localizar, procesar y organizar información contenida en diversos documentos. En una segunda etapa, dicha información se presenta de manera sistemática, coherente y argumentada en un nuevo texto (Tancara, 1993 citado Martínez et al., 2023). En consecuencia, el análisis documental, se dedica "no sólo en localizar y seleccionar, sino que se amplía el proceso en organizar y analizar los materiales para lograr encontrar esas respuestas" (Bermeo-Yaffar et al., 2016, citados en Martínez et al., 2023, p.69).

Por otro lado, respecto a la entrevista semiestructurada, en un primer momento, es necesario indicar que la entrevista cualitativa, a diferencia de la cuantitativa, es más íntima, flexible y abierta (Hernández-Sampieri et al., 2018). En consecuencia, se define como "una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados)" (Hernández-Sampieri et al., 2018, p. 449).

A su vez, Hernández-Sampieri et al. (2018) explica que las entrevistas se dividen en estructuradas, semiestructuradas y no estructuradas o abiertas. Por consiguientes, y para fines del presente estudio, la tipología de entrevista utilizada corresponde a la entrevista no estructurada, las que "las entrevistas semiestructuradas se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener mayor información" (Hernández-Sampieri et al., 2018, p. 449). Esta tipología, se fundamenta en la existencia de otra técnica de recolección de datos, por lo que se busca que ambas se complementen. En consecuencia, el número de entrevistados se mantiene acotado. A continuación, la Tabla 1 presenta la guía de preguntas, las que a su vez, al igual que el análisis documental, se encuentran basadas en los objetivos específicos del estudio:

Tabla 1

Entrevista semiestructurada

Objetivo específico	Pregunta
Explorar las formas actuales y emergentes en que las organizaciones criminales utilizan IA a nivel global y regional	En base a su experiencia, ¿Cuáles son las formas actuales y emergentes en que las organizaciones criminales utilizan a la IA, específicamente en los delitos asociados al ciberespacio y crimen organizado? ¿Podría mencionar algún caso específico que haya conocido o estudiado?
Identificar posibles manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile	¿Cuáles son los riesgos potenciales del uso de IA por parte de redes criminales en Chile? ¿Considera que Chile está preparado para enfrentar estos riesgos? ¿Qué aprendizaje podría sacar Chile de esto?
Conocer experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública, para extraer aprendizajes útiles para el contexto chileno	¿Conoce usted alguna(s) experiencia(s) internacional(es) que haya(n) abordado el fenómeno de la IA desde la seguridad pública? ¿Qué aprendizaje podría sacar Chile de esto? ¿Qué elementos de esas experiencias serían más urgentes de implementar en Chile?
	¿Qué rol juega la cooperación internacional en esta materia?
Identificar los principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile	¿Cuáles son los principales desafíos que el fenómeno de la IA representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile? ¿Qué actor institucional debería liderar esta respuesta?

Percepciones generales y elementos emergentes del fenómeno	Finalmente, ¿Hay algún aspecto relevante sobre IA y crimen organizado que no hayamos abordado y que considere importante mencionar?

Fuente: elaboración propia

4.3 Criterios para la selección de la muestra/ criterios de inclusión

Una muestra cualitativa se define como "el grupo de personas, eventos, sucesos, comunidades, etc., sobre el cual se habrán de recolectar los datos, sin que necesariamente sea estadísticamente representativo del universo o población que se estudia" (Hernández-Sampieri et al., 2018, p. 427).

En los estudios cualitativos el tamaño de muestra no es importante desde una perspectiva probabilística, ya que el interés del investigador no se enfoca en extender los resultados a un universo mayor, por lo que el objetivo de la indagación cualitativa es la profundidad. En consecuencia, el foco se encuentra en los casos o unidades, como participantes, organizaciones, manifestaciones humanas, eventos, animales, hechos, etc., lo que contribuye a entender el fenómeno de estudio y responder a las preguntas de investigación (Hernández-Sampieri et al., 2018).

Siguiendo el enfoque cualitativo y considerando la naturaleza compleja y multifacética del fenómeno investigado, de acuerdo con el tipo de muestreo del presente estudio, el criterio de inclusión de la investigación para el análisis documental se centra en el procedimiento de estudio estipulado en Martínez et al. (2023), el cual se divide en las siguientes etapas:

1. Localización de documentos como artículos científicos, libros o capítulos de libros en bases de datos como: Dialnet, SciELO, Redalyc y Google Académico.
2. Utilización de una combinación de palabras claves y complementarias al fenómeno de estudio.

3. Determinar un rango tiempo amplio de búsqueda de documentos, debido a la naturaleza exploratoria del tema, el cual se definió desde el año 1980 al 2025 (también por disposición de los documentos).
4. Son integrados al análisis los documentos que abordaran al menos 01 categoría de las propuestas en los objetivos específicos del estudio.

A los artículos resultantes de este proceso, les fueron aplicados criterios de inclusión y exclusión, donde se incluyeron los siguientes estudios: 1) textos en español, 2) que se vincularan con alguna de las categorías temáticas del estudio, 3) tuvieran links de accesos habilitados para visualizarlos de manera digital.

Por otro lado, la muestra del estudio, es de tipo cualitativa, específicamente se utiliza una muestra homogénea, donde "las unidades que se van a seleccionar poseen un mismo perfil o características, o bien comparten rasgos similares" (Hernández-Sampieri et al., 2018, p.431), estas muestras tienen la finalidad de centrarse en el tema a investigar. En consecuencia, la muestra se compone de 03 expertos en las áreas de cibercrimen y crimen organizado A continuación, para fines del análisis de la información, se enumeran y proporciona una breve descripción de cada uno de ellos:

1. **Entrevistado 1:** Subprefecto, jefe de la Brigada Investigadora de Crimen Organizado.
2. **Entrevistado 2:** Abogado, Fiscal Adjunto de Alta Complejidad y Contra el Crimen Organizado, fiscalía regional Metropolitana Sur.
3. **Entrevistado 3:** Abogado, Oficial de la Policía de Investigaciones de Chile, con especialidad en investigación de Cibercrimen.

4.4 Técnicas de análisis de la información

Como técnica de análisis de los datos, se realizó un análisis de contenido cualitativo, el que corresponde al contenido de los textos seleccionados y de las entrevistas realizadas. Se procedieron a dar análisis a las implicancias del uso de inteligencia artificial por parte del

crimen organizado en Chile, para lo cual se organizó el material en estudio a través de categorías y así dar respuesta a la pregunta de investigación desde

Dentro de una investigación cualitativa, el proceso de codificación sucede en aquel momento donde "el investigador considera segmentos de contenido, los analiza y compara" (Hernández-Sampieri et al., 2018, p.474). Bajo este contexto, si los contenidos son distintos en términos de significado y concepto, se induce una categoría de cada uno, mientras que si son similares, se induce una categoría común.

En consecuencia, las categorías cualitativas corresponden a "conceptualizaciones analíticas desarrolladas por el investigador para organizar los resultados o descubrimientos relacionados con un fenómeno o experiencia humana que está bajo investigación" (Hernández-Sampieri et al., 2018, p.474). Luego, en su fase selectiva, Gallicano (2013, citado en Hernández-Sampieri et al., 2018) explica que tiene como objetivo determinar la categoría o tema central que explica el problema de investigación, donde todas o la mayoría de las categorías se vinculan entre ellas y su relación es lógica y consistente. En consecuencia, se procedió a leer detalladamente cada uno de los textos y las respuestas proporcionadas por los expertos, a través de lo cual fueron confeccionadas las categorías temáticas, las que permiten establecer las implicancias del uso de inteligencia artificial por parte del crimen organizado en Chile.

4.5 Fuentes de información

Las fuentes de información analizadas en el presente estudio, corresponden a fuentes de información tanto primarias como secundarias. Estas fuentes corresponden a los textos académicos encontrados en las bases de datos web disponibles (de tipo secundarias), así como también las respuestas proporcionadas por los expertos en las entrevistas aplicadas (fuentes de tipo secundarias).

4.6 Consideraciones éticas

El desarrollo de la presente investigación se encuentra resguardado bajo un fuerte compromiso ético adoptado por la investigadora, lo que asegura la integridad del proceso investigativo y el respeto hacia todas las personas involucradas directa o indirectamente en

ella. En base a esto, la investigadora mantiene un acuerdo claro y transparente respecto a la propiedad intelectual a lo largo del estudio, por lo que todo uso de ideas, datos, publicaciones, tablas o cualquier otro tipo de contenido creado por terceros, es debidamente citado y/o referenciado, siguiendo los estándares académicos correspondientes.

Asimismo, toda recolección de datos que implique la participación de terceras personas, ajenas a la investigadora, se realiza únicamente bajo el principio del consentimiento informado, lo que significa que los participantes son informados de manera clara y trasparente sobre los fines del estudio y el uso que se le da a la información recopilada. Finalmente, cabe destacar que el acceso a los datos tratados en el estudio, se encuentran restringidos a la investigadora y se utilizan únicamente para fines académicos y de uso interno de la Academia Nacional de Estudios Políticos y Estratégicos.

4.7 Limitaciones metodológicas

Si bien la investigación aporta una aproximación relevante al fenómeno del uso de la IA por parte de redes criminales, presenta algunas limitaciones metodológicas que deben ser consideradas al interpretar los resultados. En primer lugar, la naturaleza emergente y dinámica del objeto de estudio, implica una disponibilidad limitada de estudios empíricos y bases de datos, especialmente en el contexto chileno, donde aún no existen registros sistemáticos ni casos judicializados vinculados directamente al uso criminal de IA. Esto restringe el alcance comparativo y obliga a tomar un enfoque principalmente exploratorio.

Otra limitación, corresponde a la heterogeneidad de las fuentes académicas empleadas. Los textos analizados provienen de distintos contextos geográficos y disciplinarios, lo que plantea una dificultad respecto a la comparación directa entre experiencias internacionales y la realidad nacional. Asimismo, la falta de documentación específica sobre políticas públicas chilenas relacionadas con la IA en el ámbito criminal impide un análisis integral de la respuesta estatal ante este fenómeno.

5. RESULTADOS

El presente capítulo expone los resultados obtenidos a partir de la aplicación de las metodologías empleadas en el desarrollo de la investigación. Con el propósito de responder a los objetivos planteados, fue ejecutado un análisis cualitativo de tipo documental complementado con el análisis de entrevistas a informantes clave. La utilización de ambos análisis permitió contrastar la información proveniente de fuentes secundarias con las percepciones, experiencias y conocimientos de actores directamente vinculados con la temática estudiada (fuentes primarias). La integración de ambos enfoques posibilita un examen más profundo y riguroso, favoreciendo la triangulación de la información y la validación de los resultados que se presentan a continuación.

En primera instancia, se presentan los hallazgos derivados del análisis documental, los cuales permiten identificar patrones, tendencias y antecedentes relevantes sobre el fenómeno en estudio. Posteriormente, se exponen los resultados del análisis de entrevistas, que aportan una visión basada en la experiencia y conocimiento técnico, enriqueciendo la comprensión de los datos, lo que permite contar con una interpretación más integral del fenómeno investigado.

5.1 Análisis cualitativo documental

Para la búsqueda y selección de la información documental, se llevó a cabo un proceso sistemático orientado a garantizar la pertinencia y calidad de las fuentes utilizadas. En primer lugar, se realizó la localización de documentos académicos, tales como artículos científicos, libros y capítulos de libros, en motores de búsqueda reconocidas por su rigor y fiabilidad, entre ellas Dialnet, SciELO, Redalyc y Google Académico. La búsqueda fue realizada mediante la combinación de palabras clave y términos complementarios relacionados con el fenómeno de estudio, lo que permitió ampliar el espectro de resultados y abarcar distintas perspectivas teóricas y empíricas.

Dado el carácter exploratorio del tema, se estableció un rango temporal amplio, comprendido entre los años 1980 y 2025, con el fin de incorporar tanto antecedentes

históricos como aportes contemporáneos, considerando además la disponibilidad de los documentos en las bases de datos. Finalmente, fueron integrados al análisis únicamente aquellos textos que abordaran al menos una de las categorías definidas en los objetivos específicos de la investigación, asegurando así la coherencia entre las fuentes seleccionadas y las dimensiones analíticas del estudio. Estas categorías, corresponden a:

1. Formas actuales y emergentes en que las organizaciones criminales utilizan IA a nivel global y regional.
2. Manifestaciones incipientes o riesgos potenciales del uso de IA por parte de redes criminales en Chile.
3. Experiencias internacionales que aborden a la IA desde la seguridad pública.
4. Desafíos que representa el uso de IA en contexto criminal para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile.

La exploración documental de fuentes secundarias, de manera inicial arrojó un total de 23.900 artículos académicos y científicos relacionados con las palabras claves utilizadas como filtro respecto al objeto de investigación. Luego, fueron seleccionados 9 artículos, los que se relacionaban tanto con el objeto como con el objetivo de investigación. A estos artículos, les fueron aplicados criterios de inclusión y exclusión, donde se escogieron estudios. La exploración documental realizada se documentó en una bitácora de trabajo, para lo cual el programa computacional Microsoft Excel a través del cual se utilizó una planilla de trabajo (Anexo A) con la finalidad de ordenar las fuentes bibliográficas encontradas.

En este contexto, la selección de los textos mediante la exploración de los sitios web fueron los siguientes:

Tabla 2

Cantidad de artículos encontrados en motores de búsqueda según categorías de investigación

Categoría de investigación	Dialnet	Redalyc	SciELO	Google Académico	Total
Formas actuales y emergentes en que las organizaciones criminales utilizan IA a nivel global y regional	1	1	0	0	**2**
Manifestaciones incipientes o riesgos potenciales del uso de IA por parte de redes criminales en Chile	0	0	0	1	**1**
Experiencias internacionales que aborden a la IA desde la seguridad pública	1	0	1	1	**3**
Desafíos que representa el uso de IA en contexto criminal para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile	1	1	1	0	**3**
Total	**3**	**2**	**2**	**1**	**9**

Fuente: elaboración propia

Finalmente, es importante señalar las limitaciones encontradas durante la selección de los artículos académicos. La primera de ellas se presentó con el uso del motor de búsqueda IEEE Xplore. Inicialmente, se consideró este recurso, pero la búsqueda con la palabra clave compuesta "organizaciones criminales e inteligencia artificial" no arrojó resultados. Al realizar las búsquedas por separado ("organizaciones criminales" o "inteligencia artificial"), los resultados obtenidos se desviaban significativamente del objeto de estudio.

Otra limitación relevante fue la necesidad de descartar algunos textos. Esto se debió a que no contaban con un enlace de acceso directo que permitiera la revisión detallada y completa de su contenido.

A continuación, se presenta el análisis cualitativo, el cual se realiza mediante subtítulos, los cuáles corresponden a las categorías temáticas que responden a los objetivos específicos del estudio.

5.1.1 Formas actuales y emergentes en que las organizaciones criminales utilizan IA a nivel global y regional

La presente categoría se basa en los textos de Fontalvo Herrera, et al. (2023) y De la Peña et al. (2024). En base a ambos textos, se pudo determinar que, en la actualidad, las organizaciones criminales están incorporando herramientas de IA como parte de sus estrategias operativas, tanto a nivel global como regional. Estas tecnologías, originalmente diseñadas para fortalecer la seguridad y la prevención del delito, presentan un riesgo de uso dual, ya que pueden ser aprovechadas por los propios grupos delictivos para optimizar sus actividades ilícitas, incrementar su capacidad de evasión y ampliar el alcance de sus operaciones. El estudio de De la Peña et al. (2024) "La Inteligencia Artificial en la Lucha Contra el Crimen Organizado" resalta que la IA se ha convertido en un instrumento clave dentro de la lucha contra la criminalidad, particularmente mediante el empleo de sistemas de videovigilancia inteligente, reconocimiento facial y análisis predictivo, los cuales permiten a las autoridades "aumentar la eficiencia en la recopilación y análisis de datos, la identificación temprana de amenazas y la optimización de recursos" (Rejas et al., 2024, p. 2.147). Sin embargo, esta misma capacidad de procesamiento y automatización puede ser utilizada por organizaciones criminales para monitorear entornos, seleccionar objetivos o anticipar acciones policiales, generando así un desequilibrio tecnológico entre las instituciones del Estado y las redes delictivas emergentes.

Los autores plantean interrogantes sobre los alcances de estas herramientas, preguntándose "¿cómo la detección y respuesta en tiempo real fortifica la lucha contra la criminalidad organizada?" y "¿cómo la automatización y eficiencia operativa fortalecen el combate frente a estas organizaciones?" (Rejas et al., 2024, p. 2.148). Estas preguntas

evidencian que la implementación de IA no solo implica ventajas operativas, sino también nuevos dilemas éticos y de seguridad, especialmente cuando la información recopilada no cuenta con salvaguardias adecuadas. En palabras del mismo estudio, “se debe abordar integralmente la protección de la información obtenida (…) garantizar la transparencia, imparcialidad y prevenir posibles impactos negativos que puedan vulnerar derechos fundamentales” (Rejas et al., 2024, p. 2.144).

En el contexto regional latinoamericano, el trabajo de Fontalvo-Herrera et al. (2023), titulado “Método de *clustering* e inteligencia artificial para clasificar y proyectar delitos violentos en Colombia”, evidencia la aplicación concreta de modelos de aprendizaje automático y análisis espacial para el estudio del crimen. Los autores proponen “clústeres de delitos violentos en Colombia por departamentos junto con una estructura de redes neuronales para su clasificación y proyección” (Fontalvo-Herrera et al., 2023, p. 551), demostrando la utilidad de la IA en la identificación de patrones territoriales y la predicción de comportamientos delictivos futuros. Sin embargo, estas mismas herramientas analíticas podrían ser aprovechadas por las organizaciones criminales para detectar áreas con menor presencia policial, planificar rutas seguras para el transporte de drogas o coordinar operaciones en función de zonas de oportunidad.

A nivel global y regional, el uso de técnicas de clustering, visión por computador, aprendizaje profundo y automatización de procesos se está consolidando tanto en la prevención como en la ejecución del delito. En este sentido, el potencial de la IA para procesar grandes volúmenes de datos, generar alertas en tiempo real y anticipar eventos, si bien resulta esencial para la seguridad pública, también puede ser empleado de manera inversa por grupos delictivos transnacionales. Esto incluye desde la manipulación de datos y la creación de *deepfakes* para fraudes o extorsiones, hasta el uso de algoritmos predictivos para evaluar riesgos operacionales en actividades ilícitas.

En síntesis, ambos estudios analizados reflejan que la IA, aunque es concebida como un instrumento de fortalecimiento institucional, se ha transformado en un recurso de poder en disputa entre Estados y organizaciones criminales. Tal como advierte Rejas et al. (2024), su implementación “apoya efectivamente en la lucha contra la criminalidad organizada” (p.

2.144), pero exige una regulación ética y técnica que impida su uso indebido. A nivel regional, la investigación de Fontalvo-Herrera et al. (2023) muestra cómo las metodologías de clasificación y proyección de delitos pueden ser reproducidas fuera del ámbito estatal, entregando a los grupos criminales herramientas para anticipar, adaptar y perfeccionar sus estructuras operativas.

En consecuencia, el análisis evidencia que las formas actuales y emergentes del uso de IA por parte de las organizaciones criminales no solo incluyen la automatización de procesos delictivos y la explotación de sistemas predictivos, sino que también la apropiación de capacidades tecnológicas originalmente destinadas a la seguridad pública. Esto, plantea la necesidad de marcos regulatorios, estrategias de ciberseguridad y mecanismos de cooperación internacional que limiten el potencial de la IA como instrumento para el crimen organizado.

5.1.2 Manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile

El análisis de la presente categoría, se realiza en base al texto de Jordán y Rosas (2024). Este, señala que el desarrollo acelerado de la IA ha comenzado a transformar de manera significativa el campo de la seguridad y la defensa en Chile. Sin embargo, las mismas capacidades tecnológicas que fortalecen la gestión estatal pueden, en su reverso, ser empleadas por redes criminales para optimizar su accionar, evadir la vigilancia institucional y ampliar su campo operativo. Tal como señalan Jordán y Rosas (2024) “aparte de las amenazas tradicionales (…) existen las ‘nuevas amenazas multidimensionales’ (…) que incluyen el crimen organizado, el terrorismo, la inmigración ilegal, el contrabando…” (Jordán y Rosas, 2023, párr. 2). Esta afirmación, evidencia que el propio marco de defensa chileno ya reconoce al crimen organizado como un actor emergente dentro del espectro de riesgos asociados a las tecnologías disruptivas.

Los autores destacan que la expansión de la IA se debe a factores estructurales, entre ellos “un aumento exponencial de los datos disponibles, la aparición de nuevas tecnologías computacionales (…) y la creación de cada vez más sofisticados algoritmos de aprendizaje

automático (machine learning y deep learning)" (Jordán y Rosas, 2023, párr. 6). Esta disponibilidad masiva de datos y capacidad analítica constituye un potencial de uso dual, ya que mientras el Estado la aplica en defensa, vigilancia o predicción, las organizaciones criminales podrían utilizar los mismos mecanismos para la identificación de objetivos, el monitoreo de entornos y la planificación estratégica de sus actividades ilícitas.

Uno de los principales riesgos advertidos en el texto, es la posibilidad de que la velocidad de innovación tecnológica deje a las instituciones nacionales rezagadas frente a actores no estatales. En este sentido, "la aparición de amenazas que utilizan proactivamente el potencial de la IA, el aprendizaje automático, la IoT, la realidad aumentada, la robótica avanzada (...) podrá enfrentar a la Defensa Nacional de Chile a ciclos de obsolescencia tecnológica" (Jordán y Rosas, 2023, párr. 16). Si se proyecta esta idea hacia el ámbito criminal, la obsolescencia estatal se traduce en ventaja operacionales para las redes delictivas, las cuales pueden adoptar antes o con mayor flexibilidad tecnologías emergentes para la gestión de información, comunicación cifrada o manipulación de entornos digitales.

Asimismo, los autores señalan que la IA ofrece "un amplio espectro de aplicaciones que pueden transformar radicalmente nuestras capacidades" (Jordán y Rosas, 2023, párr. 19), destacando su uso para: analizar grandes volúmenes de datos a una velocidad increíble e identificar patrones, amenazas, tendencias y anomalías en tiempo real. Estas capacidades, que en el marco institucional permiten anticipar delitos o prevenir ataques, podrían ser igualmente explotadas por organizaciones criminales para predecir estrategias policiales, coordinar operaciones de contrabando o diseñar estrategias de evasión basadas en el análisis de fuentes abiertas (OSINT) y datos obtenidos de manera ilícita.

Otro ámbito relevante es el uso de IA en el análisis financiero, donde los autores reconocen que permite "detectar casos sospechosos de lavado de activos o enriquecimiento ilícito" (Jordán y Rosas, 2023, párr. 29). Sin embargo, este mismo conocimiento puede ser replicado de otras formas: las redes criminales podrían entrenar algoritmos para ocultar flujos financieros, dispersar activos o generar patrones artificiales de transacciones, dificultando la detección por parte de los organismos de inteligencia económica.

El texto también advierte sobre la necesidad de garantizar un uso ético y regulado de la IA, señalando que se debe proteger la información privada de las personas en los análisis de datos masivos y adoptar medidas para asegurar que la IA será utilizada solo para fines lícitos (Jordán y Rosas, 2023). No obstante, en el escenario chileno, aún existe una debilidad normativa en materia de control y supervisión de estas tecnologías, lo que genera un vacío de gobernanza, el cual puede ser potencialmente aprovechado por organizaciones criminales que operan en los márgenes legales o en espacios digitales que no se encuentran regulados.

Finalmente, los autores subrayan el carácter transnacional de estas amenazas, destacando que

> La cooperación internacional será esencial en estos procesos, dada la naturaleza transfronteriza de algunas amenazas multidimensionales a enfrentar (ciberterrorismo, crimen organizado transnacional, pandemias, contrabando, etc.), facilitando el intercambio de información y promoviendo enfoques unificados para enfrentar desafíos comunes. Esto permitirá compartir inteligencia de las amenazas emergentes, incluyendo la aplicación de las lecciones aprendidas en el uso de nuevas tecnologías en estos ámbitos. (Jordán y Rosas, 2023, párr. 37)

Este elemento es particularmente relevante para Chile, puesto que las redes criminales pueden importar tecnologías de IA desarrolladas en otros países o asociarse con organizaciones que ya dominan técnicas de automatización y análisis de datos para la comisión de delitos complejos.

5.1.3 Experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública

El análisis del presente subtítulo, se realizó a través de los autores Machín (2023), García Falconí y Barona Pazmiño (2024), y Reyes (2025). En consecuencia, el análisis de contenido temático sobre las experiencias internacionales vinculadas al uso de IA en el ámbito de la seguridad pública, muestra una tendencia creciente hacia la incorporación de

tecnologías inteligentes en la prevención, investigación y persecución del delito. Los textos de Machín (2023), Reyes (2025) y García Falconí y Barona Pazmiño (2024) permiten identificar distintos enfoques desde el punto de vista institucional, así como también desafíos comunes respecto a la integración de la IA dentro de los sistemas de seguridad y justicia penal.

Bajo este contexto, Machín (2023) expone el caso Europeo, donde resalta que la IA se ha consolidado como un componente estratégico para la seguridad pública, particularmente en los ministerios del interior de países como España, Francia y Alemania. El autor sostiene que "la digitalización, la disponibilidad y el acceso a grandes volúmenes de datos, son elementos esenciales para el desarrollo de la IA" (Machín, 2023, p. 127). El enfoque del autor, contempla una visión institucional de la IA como herramienta de optimización operativa, orientada a la vigilancia inteligente y a la predicción de riesgos. Asimismo, Machín (2023) destaca que la implementación debe acompañarse de una gobernanza tecnológica sólida, la cual tiene el deber de garantizar la protección de los derechos fundamentales y la transparencia en la toma de decisiones automatizadas, destacando la necesidad de equilibrar eficacia y ética en el uso de estas tecnologías.

Por su parte, Reyes (2025) aborda el fenómeno desde la perspectiva de la criminalística y la investigación forense, destacando el potencial transformador de la IA en la obtención y análisis de evidencia. Para el autor, la inteligencia artificial representa una revolución tecnológica en la criminalística contemporánea, ya que permite procesar grandes volúmenes de información forense en tiempos mucho más reducidos (Reyes, 2025). Estas herramientas, aplicadas en la identificación facial, el análisis de ADN y la reconstrucción de escenas del crimen, fortalecen las capacidades de las instituciones de seguridad pública. Sin embargo, el texto también advierte sobre el riesgo de dependencia tecnológica y la necesidad de desarrollar marcos normativos que regulen la validez jurídica de las pruebas obtenidas mediante el uso de sistemas automatizados, lo que finalmente refleja un desafío ético y legal que atraviesa las experiencias internacionales.

En América Latina, la investigación de García Falconí y Barona Pazmiño (2024) examina la incorporación de la IA en el proceso penal ecuatoriano, destacando su papel en la

eficiencia procesal y la reducción de errores humanos. Los autores explican que la inteligencia artificial, aplicada al proceso penal, contribuye a optimizar la investigación judicial a través de algoritmos de análisis de patrones de comportamiento delictivo (García Falconí y Barona Pazmiño, 2024). No obstante, advierten que esta innovación también plantea retos relacionados con el debido proceso, la imparcialidad y la responsabilidad penal derivada de decisiones automatizadas. Las observaciones de los autores, reflejan una preocupación compartida en los sistemas judiciales de la región: el equilibrio entre eficiencia tecnológica y garantías procesales.

En conjunto, los 03 textos analizados permiten identificar una tendencia temática en torno a la IA como motor de modernización institucional en seguridad pública, con matices según el contexto sociopolítico y normativo de cada país. En este sentido, mientras Europa se centra en la consolidación de marcos regulatorios y estrategias estatales de innovación, América Latina se encuentra en una fase de adopción, en la que se destacan los debates sobre legitimidad, transparencia y derechos fundamentales. Esto, evidencia que las experiencias internacionales plantean advertencias sobre los riesgos potenciales de una implementación acelerada o sin control ético de la IA.

5.1.4 Principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile

El análisis temático de los textos de García Torres (2024), Morán (2021) y Ospina et al. (2025) permite identificar que el uso de la IA en contextos de seguridad y criminalidad plantea una serie de desafíos de índole estructural para los Estados, tanto en el ámbito de la seguridad nacional como en la adaptación institucional y el diseño de políticas públicas. Estas tensiones no son exclusivas del ámbito internacional, sino que proyectan implicancias directas para Chile, ya que el país se encuentra en un proceso de modernización tecnológica y digitalización de la gestión pública y de la seguridad.

García Torres (2024) advierte que la expansión de la ciberdelincuencia organizada, potenciada por la IA, constituye una amenaza directa para la seguridad nacional debido a la sofisticación técnica de los ataques y a la dificultad de rastrear a los responsables. Según la autora, “la ciberdelincuencia representa las acciones criminales que se apoyan en las

vulnerabilidades en esos sistemas y datos, todo ello con fines ilícitos" (García Torres, 2024, p. 17). Este diagnóstico cobra relevancia en el contexto chileno, donde dimensiones como el área energética, financiera y gubernamental, se han vuelto cada vez más vulnerable a ataques automatizados y coordinados. Asimismo, García Torres (2024) subraya que uno de los principales obstáculos recae en la ausencia de marcos normativos internacionales, los cuáles permiten contar con una persecución coordinada del delito digital, lo que expone la necesidad de cooperación internacional y de políticas públicas alineadas con estándares internacionales de ciberseguridad.

En el aspecto jurídico, Morán (2021) plantea un debate sobre la responsabilidad penal de la inteligencia artificial, que impacta directamente en la capacidad de los sistemas judiciales para imputar responsabilidad cuando los sistemas de IA participan en conductas ilícitas. La autora señala que se está en presencia de una frontera jurídica aún no resuelta, donde existe la posibilidad de atribuir responsabilidad penal a entidades no humanas cuando generan resultados delictivos (Morán, 2021). Este vacío normativo se traduce en un desafío para los Estados, que deben definir mecanismos de control, supervisión y atribución de responsabilidad tanto para los desarrolladores como para las instituciones que emplean IA en funciones elementales. En Chile, donde la adopción de tecnologías avanza en áreas como la vigilancia y la seguridad pública, este debate se vuelve cada vez más urgente, ya que la falta de regulación penal específica en la materia, podría limitar la capacidad estatal para sancionar conductas que se encuentran fuera de norma en el uso de sistemas automatizados.

El estudio de Ospina et al. (2025), aborda el papel de la IA "como herramienta para combatir la corrupción en organizaciones públicas, evaluando su capacidad para fortalecer dimensiones clave como datos, tecnología, recursos humanos y habilidades organizacionales" (p.7). En consecuencia, la inteligencia artificial puede fortalecer los sistemas de control institucional, siempre que exista una política pública orientada a la transparencia y al uso ético de la información.

Sin embargo, los autores advierten que el aprovechamiento de estas herramientas requiere capacidades técnicas y culturales dentro del Estado. En este sentido, señalan que la percepción social y la confianza institucional son elementos fundamentales para la aceptación

y efectividad del uso de la IA en la gestión estatal. En el caso chileno, esta idea implica que el éxito de las políticas de prevención del delito mediante IA depende tanto de la formación especializada de los funcionarios públicos como del establecimiento de mecanismos de rendición de cuentas y participación ciudadana, ya que "estas tecnologías han fortalecido la confianza ciudadana al transparentar las acciones del Estado y reforzar los controles internos y la rendición de cuentas" (Ospina et al., 2025, p. 13).

5.2 Análisis cualitativo de entrevistas

El presente apartado expone el análisis cualitativo de las entrevistas realizadas a 03 expertos en materia de cibercrimen y crimen organizado, cuyo propósito fue analizar las implicancias del uso de inteligencia artificial por parte del crimen organizado en Chile. A partir de sus perspectivas y experiencias, se logró identificar elementos relevantes sobre las características, dinámicas y particularidades de la utilización de IA en el contexto delictual, aportando una visión integral que contribuye a comprender mejor su alcance y complejidad. Asimismo, es importante destacar que en el apartado de Anexos (ver Anexo B), se ubican las respuestas textuales de los entrevistados mediante una tabla temática que ordena este material.

En consecuencia, a continuación, se presenta el respectivo análisis de la información, la cual se estructura en cinco categorías temáticas, las cuáles a su vez, responden a los objetivos de estudio. Luego, se presenta un análisis consolidado de las cinco categorías sumado al análisis documental mediante el análisis de los resultados.

5.2.1 Formas actuales y emergentes en que las organizaciones criminales utilizan IA a nivel global y regional

La presente categoría, contempla la visión basada en la experiencia de los expertos en torno a las formas en que las organizaciones criminales están incorporando (o bien podrían incorporar) IA en sus actividades ilícitas. De manera preliminar, las respuestas muestran un consenso respecto a que el uso de la IA representa una evolución en las capacidades

tecnológicas del crimen organizado**,** principalmente en el ámbito digital y financiero**,** aunque su presencia concreta en el contexto chileno aún es incipiente.

Bajo este contexto, los entrevistados señalan que la IA ha permitido aumentar la eficiencia, velocidad y alcance de los ataques digitales, generando de esta forma nuevas dinámicas de riesgo a nivel global. El Entrevistado 1 señala que "*las organizaciones criminales hoy en día están usando la IA para automatizar y escalar ataques como la generación de phishing, creación de deepfakes, y con este último a la clonación de audio y vídeo para extorsión o fraudes*". Asimismo, el Entrevistado 3 profundiza en este ámbito al describir la automatización de ataques cibernéticos, destacando que los grupos delictivos "*utilizan IA para escanear vulnerabilidades en sistemas, crear malware o programas malignos más sofisticados y automatizan ataques de phishing y ransomware*", enfatizando que esta tecnología adapta los ataques en tiempo real, aumentando su eficacia y complejidad.

Estos testimonios desde la experiencia de los expertos, exponen una tendencia hacia el uso instrumental de la IA como multiplicador de capacidades técnicas delictuales, especialmente en *phishing, ransomware* y manipulación de sistemas informáticos**.**

Otro aspecto destacable en esta categoría, dice relación con la utilización de IA generativa para crear contenido falso o engañoso, con fines de fraude, extorsión o desinformación. El Entrevistado 1 menciona la "*creación de deepfakes*" como uno de los usos más visibles, mientras que el Entrevistado 3 amplía esta idea señalando que los grupos criminales "*emplean deepfakes y generación de contenido sintético para engañar a víctimas, falsificar identidades o difundir desinformación*", destacando además que los delincuentes seleccionan como objetivo a "*personas de la tercera edad cuyo conocimiento de las tecnologías es mínimo*". Esta situación, evidencia un fenómeno global donde se aplica tecnología al engaño**,** donde la IA permite suplantar identidades, manipular percepciones y vulnerar la confianza digital, con consecuencias que van desde el ámbito económico hasta el psicológico de las víctimas.

Por otro lado, se observa una preocupación por la capacidad de la IA para ocultar rastros y dificultar la persecución penal. En consecuencia, el Entrevistado 3 describe que los delincuentes "*desarrollan técnicas de IA para evadir sistemas de detección y análisis en*

redes sociales, plataformas de comunicación y sistemas de seguridad, haciendo más difícil rastrear sus actividades". En este mismo sentido, el Entrevistado 2 anticipa que la IA podrá ser utilizada para "*ocultar el origen ilícito de recursos financieros, dificultar la trazabilidad de operaciones económicas, o manipular y encriptar información sensible que potencialmente podría constituir evidencia en procesos judiciales*".

La IA también aparece como un instrumento emergente en el ámbito del crimen financiero, de manera particular, en el lavado de dinero y la manipulación de mercados. El Entrevistado 2 plantea que la IA "*podría emplearse para optimizar mecanismos destinados a ocultar el origen ilícito de recursos financieros*", mientras que el Entrevistado 3 refuerza esta idea al señalar que "*la IA se usa para automatizar fraudes en plataformas de pagos, blanqueo de dinero mediante algoritmos que camuflan transacciones ilícitas y manipulan mercados financieros de manera ilegal*". Ambas visiones, coinciden en indicar una dimensión económica-tecnológica del crimen organizado, donde la IA facilita el manejo automatizado de datos financieros, reduciendo la exposición al control legal y ampliando de esta manera la sofisticación de las redes criminales.

Finalmente, surge el reconocimiento del uso de *bots* y algoritmos impulsados por IA con la finalidad de gestionar redes de comunicación ilícitas y desinformación. El Entrevistado 3 explica que "*los grupos criminales emplean bots impulsados por IA para administrar redes de cuentas falsas, promover actividades ilegales y coordinar operaciones sin ser detectados*". Esto muestra un uso estratégico de la IA no solo para ejecutar delitos, sino también para mantener unión y coordinación operativa dentro de las estructuras criminales**,** ampliando su alcance.

5.2.2 Manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile

La presente categoría se centra en identificar las formas iniciales, emergentes o potenciales en que la inteligencia artificial puede ser utilizada por redes criminales dentro del territorio chileno, así como los riesgos estructurales e institucionales que esto implica. Los testimonios de los entrevistados reflejan un consenso: aunque no existen casos masivos

detectados, el país enfrenta una vulnerabilidad creciente derivada de la rápida expansión de tecnologías basadas en IA y la limitada preparación institucional frente a ellas.

El Entrevistado 1 identifica que en Chile "*los riesgos se centran en fraude masivo mediante deepfakes, automatización de campañas de estafa, ataques dirigidos a infraestructura crítica, o uso de IA para organizar redes de tráfico, lavado u otros ilícitos complejos*". Esta afirmación, expone una percepción de amenazas en expansión, donde las tecnologías de IA se proyectan como herramientas de fraude, sabotaje y coordinación criminal digital, especialmente en sectores críticos. Además, el experto advierte que, si bien existen avances normativos (como la ley 21.663 de ciberseguridad), el país "*no está completamente preparado para el tipo de amenazas que plantea la IA al crimen organizado*" (Entrevistado 1). Esta situación, expone una brecha entre el desarrollo tecnológico y la capacidad regulatoria, lo que deja espacio a la vulnerabilidad que podría ser aprovechada por actores delictivos.

El Entrevistado 2 introduce un análisis sobre los riesgos operativos y de seguridad institucional. En este contexto, señala que "*a nivel nacional, aún no se ha dimensionado adecuadamente el impacto que puede tener la IA como instrumento facilitador del crimen organizado*", lo que incluye tanto su uso directo en delitos como en la exposición de datos dentro del sistema penal**.** Además, destaca la existencia de una herramienta nacional denominada HeredIA, de la cual ya se hizo mención al inicio de la presente investigación, y la que según el experto es descrita como "*un software de IA de carácter cerrado que opera exclusivamente con información interna del Ministerio Público*" (Entrevistado 2), cuyo objetivo es evitar vulneraciones. No obstante, advierte un riesgo paralelo: "*se ha observado que algunos funcionarios del sistema penal utilizan plataformas de IA abiertas, lo que constituye un riesgo operativo y de seguridad*". Esta visión, revela una debilidad institucional significativa: la falta de protocolos claros y formación especializada en el uso de IA dentro del ámbito judicial y policial, lo que podría eventualmente ser una falencia explotada por redes delictuales para acceder o interceptar información sensible. En consecuencia, el entrevistado alerta que una organización con capacidades tecnológicas adecuadas "*podría acceder a bases de datos institucionales o extraer información personal de fiscales y policías, comprometiendo incluso la integridad física de los funcionarios*". Esto, converge

en una doble vulnerabilidad: tecnológica (por el uso inadecuado de herramientas abiertas) y humana (por la falta de capacitación y conciencia de riesgo).

El Entrevistado 3 complementa esta visión al sostener que, si bien Chile presenta avances legislativos, "*existe muy poca información tanto en la ciudadanía como en los organismos policiales respecto al uso potencial y nocivo de la inteligencia artificial*", lo que dificulta la preparación y respuesta efectiva frente a este tipo de criminalidad. Reconoce además que "*en la actualidad existen muy pocos casos relativos al uso de estas tecnologías, por lo que es muy poca la información asociada al respecto*", evidenciando que la discusión sobre IA y crimen organizado se encuentra aún en una fase incipiente dentro del contexto nacional. Este testimonio, coincide con los anteriores al reflejar un vacío informativo y formativo que limita tanto la detección temprana de delitos basados en IA como la formulación de estrategias preventivas en el área.

De manera transversal, los tres entrevistados coinciden en que Chile no está plenamente preparado para enfrentar los riesgos que representa la IA utilizada por redes criminales. El Entrevistado 1 lo expresa claramente: "*podría decirse que no está completamente preparado para el tipo de amenazas que plantea la IA al crimen organizado*". De igual forma, el Entrevistado 2 refuerza esta idea señalando que "*dada la ausencia de directrices claras y un marco regulatorio sobre el uso de IA en el sector público, estimo que Chile no se encuentra plenamente preparado para enfrentar los riesgos derivados de la utilización de esta tecnología por parte del crimen organizado*". Ambas afirmaciones desde la experiencia de los expertos, reflejan una alerta sobre la necesidad de fortalecer el marco institucional, normativo y operativo, puntualmente en materia de ciberseguridad, protección de datos y protocolos de uso responsable de IA en las instituciones públicas.

5.2.3 Experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública

En la presente categoría, se examinan las percepciones y conocimientos de los expertos respecto a cómo otros países han enfrentado el uso de la IA desde el ámbito de la seguridad pública, especialmente en la prevención, detección e investigación del crimen organizado. Los expertos entrevistados, coinciden en que las experiencias internacionales

(particularmente de Estados Unidos y la Unión Europea) constituyen referentes primordiales para el diseño de políticas y marcos regulatorios en Chile. A su vez, se destaca la necesidad de cooperación internacional como consecuencia de la naturaleza transnacional del fenómeno criminal impulsado por la IA.

Bajo este escenario general, el Entrevistado 1 describe una experiencia relevante aplicada en el contexto chileno inspirada en modelos internacionales: "*Un ejemplo concreto en Chile ha sido el sistema ABIS utilizado por la PDI en el extremo norte del país, que aplica inteligencia artificial y biometría (rostro, huellas y voz) para identificar personas en los pasos fronterizos y comparar sus datos con bases criminales internacionales*". Esta práctica, en palabras del experto, permite "*detectar prófugos y mejorar el control migratorio*", evidenciando cómo la IA puede ser una herramienta eficaz para reforzar la seguridad fronteriza y la cooperación con bases de datos con otros países de la región y el mundo. Asimismo, señala que "*experiencias similares se han desarrollado en Estados Unidos y la Unión Europea, donde sistemas de IA apoyan la detección de sospechosos mediante reconocimiento facial y análisis predictivo delictual*". Esta mención introduce una comparación directa entre las prácticas internacionales y su adaptación local. El testimonio del experto concluye con una reflexión normativa: "*Chile podría aprender de estos casos la importancia de una regulación robusta sobre protección de datos*", destacando que la innovación tecnológica debe ir acompañada de garantías tanto éticas como legales.

Por otro lado, aunque el Entrevistado 2 reconoce no poseer conocimiento de casos específicos, sí enfatiza la existencia de avances regulatorios en otros países: "*sé que hay países que están avanzando en la implementación de políticas y marcos regulatorios destinados a normar el uso seguro de la IA*". Esta afirmación, hace entender que existen países que funcionan como referentes orientativos para el diseño de una política de seguridad nacional sobre IA. En este sentido, el experto sostiene que "*en el caso de Chile, considero urgente establecer una política de seguridad para el uso de la Inteligencia Artificial, que contemple lineamientos claros respecto de su aplicación en los procesos de investigación penal*", lo que incluye "*protocolos de manejo de información sensible, capacitación especializada y mecanismos que garanticen la integridad y confidencialidad de los datos*". Estas observaciones, exponen que las experiencias internacionales pueden reflejarse en el

contexto chileno, planteando la necesidad de institucionalizar buenas prácticas observadas en otros países que ya regulan el uso de la IA en seguridad pública.

Un eje transversal en los tres discursos es la relevancia de la cooperación internacional para enfrentar el carácter transnacional del delito asistido por IA. El Entrevistado 1 destaca que "*la cooperación internacional es clave porque el uso de IA por redes criminales trasciende fronteras, las plataformas, los datos, los ataques provienen o se ubican muchas veces en otros países, donde nosotros no mantenemos jurisdicción*". Agrega que es fundamental "*compartir inteligencia, estándares, buenas prácticas, capacidades de investigación forense digital e interoperabilidad de sistemas*", subrayando la interdependencia entre países en materia de ciberseguridad y persecución penal digital. Igualmente, el Entrevistado 2 sostiene que "*la cooperación internacional desempeña un rol esencial en la prevención, regulación y persecución de los delitos vinculados al uso indebido de la Inteligencia Artificial*". Menciona además que los avances tecnológicos y estándares de seguridad "*suelen estar determinados por prácticas y marcos regulatorios externos*", lo que exige fortalecer la articulación con organismos multilaterales como "*INTERPOL, Naciones Unidas y foros multilaterales sobre ciberseguridad*". Esta afirmación, realza la asimetría tecnológica entre países desarrollados y en vías de desarrollo, y la necesidad de colaboración para reducir brechas en capacidades de detección y respuesta. Finalmente, el Entrevistado 3 complementa esta idea señalando que "*el rol de la cooperación internacional es fundamental, toda vez que ayuda a integrar conocimientos de otras instituciones fuera del país, que ayudan a aportar experiencia y metodología práctica en aquellas materias y regulaciones que en Chile no se encuentren tan desarrolladas*". En este sentido, la cooperación se entiende no solo como intercambio de información, sino que también como mecanismo de transferencia de conocimiento técnico y metodológico, esencial para la consolidación de las capacidades locales.

El Entrevistado 3 menciona que "*Estados Unidos utiliza herramientas de inteligencia artificial y análisis de datos, para poder automatizar grandes volúmenes de datos provenientes de redes sociales, comunicaciones cifradas y transacciones financieras, facilitando la identificación de patrones delictivos y la localización de redes criminales*". Este ejemplo ilustra de qué manera la IA se ha integrado en las estrategias de seguridad

pública internacional como medio para anticipar, prevenir y desarticular redes criminales complejas, mostrando un enfoque de *inteligencia predictiva*. Dicha experiencia, evidencia que el uso de IA en seguridad pública puede incrementar la capacidad de análisis de los Estados, aunque también plantea disyuntivas sobre privacidad, vigilancia y uso ético de los datos.

5.2.4 Principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile

De manera general en esta categoría, los expertos entrevistados coinciden en señalar que Chile enfrenta importantes desafíos estructurales, normativos y de coordinación institucional frente al uso delictivo de la inteligencia artificial. La ausencia de marcos regulatorios específicos, la limitada preparación técnica del Estado y la falta de articulación interinstitucional debilitan la capacidad de respuesta ante amenazas que afectan directamente la seguridad nacional.

Uno de los puntos más reiterados por los entrevistados, es la ausencia de un marco legal claro que regule el uso y control de la IA, tanto en el ámbito público como privado. El Entrevistado 2 señala que *"la principal brecha que enfrenta Chile para abordar el uso delictivo de la Inteligencia Artificial radica en la ausencia de un marco regulatorio específico que establezca normas claras respecto de su desarrollo, utilización y control."* Agrega además que *"esta falta de regulación genera un vacío normativo que impide responder eficazmente ante los riesgos asociados al uso indebido de la IA, especialmente cuando es empleada por organizaciones criminales para ocultar información, manipular evidencias o vulnerar sistemas institucionales"*

De forma complementaria, el Entrevistado 3 menciona la necesidad de reforzar la actual legislación que protege los datos personales y de que la Agencia Nacional de Ciberseguridad (ANCI) asuma un rol activo frente a amenazas tecnológicas, lo que refuerza la idea de que Chile requiere fortalecer sus capacidades jurídicas y regulatorias en materia de IA. Los entrevistados coinciden en que uno de los principales desafíos es la coordinación entre organismos públicos y la definición de una institucionalidad que lidere la respuesta nacional frente al uso criminal de la IA. El Entrevistado 1 enfatiza la necesidad de crear una

instancia articuladora: *"Institucionalmente, el actor que debería liderar esta respuesta es un ente que coordine ciberseguridad, inteligencia, justicia y tecnología, por ejemplo, la Agencia Nacional de Ciberseguridad (ANCI) bajo la ley de ciberseguridad, en conjunto con el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación"* Asimismo, plantea que el desafío está en *"asegurar la cooperación entre defensa, interior, ciencia y justicia"*, lo cual revela que la IA necesita una gestión intersectorial y multidisciplinaria, que trascienda las fronteras tradicionales de la seguridad pública.

Otro aspecto recurrente es la necesidad de fortalecer las capacidades técnicas y humanas del Estado frente a la sofisticación de las herramientas de la IA.
El Entrevistado 1 identifica como desafío desarrollar capacidades institucionales (datos, IA, análisis, personal) para anticipar y contrarrestar ataques automatizados.
Por su parte, el Entrevistado 3 menciona una "brecha en el uso de la IA en Chile", asociada a la desinformación sobre su aplicación y potencial de mejora en los procesos investigativos. Esto demuestra que el fortalecimiento institucional no sólo depende de infraestructura tecnológica, sino que también de la capacitación y cultura organizacional que respecto a la IA.

Por otra parte, el impacto del fenómeno se extiende al ámbito de la seguridad nacional, especialmente en cuanto a la protección de datos estratégicos e infraestructuras críticas. El Entrevistado 1 advierte sobre la importancia de "*mantener la soberanía y seguridad frente a ataques automatizados"*, lo que refleja la percepción de que el uso indebido de la IA puede trascender la criminalidad común y afectar directamente la estabilidad del Estado.

5.2.5 Percepciones generales y elementos emergentes del fenómeno

En cuanto a las percepciones generales y los elementos emergentes de la utilización de la IA con fines criminales, los entrevistados expresaron percepciones que evidencian tanto una toma de conciencia sobre la creciente relación entre la IA y el crimen organizado, como la necesidad de anticipación institucional frente a riesgos emergentes. Las respuestas exponen una preocupación compartida por la autonomía de los sistemas que utilizan IA, la

capacidad de adaptación de las redes criminales, y las asimetrías tecnológicas entre países desarrollados y en desarrollo como Chile.

El Entrevistado 1 introduce una percepción crítica sobre los riesgos de una IA que opere sin supervisión humana: "*Un aspecto que merece atención es el riesgo de IA autónoma en manos de criminales, como, por ejemplo, agentes de IA que actúen sin supervisión humana, lo que puede cambiar la velocidad y escala del delito."* Esta reflexión apunta a un posible cambio en la naturaleza del crimen organizado, donde la automatización y el aprendizaje autónomo amplían la capacidad operativa de las organizaciones criminales, reduciendo los tiempos de ejecución y aumentando el alcance de sus actividades ilícitas.

Por otra parte, existe consenso entre los entrevistados en torno a la rápida capacidad de adaptación de las redes criminales frente a los avances tecnológicos. El Entrevistado 2 declara que: *"Sería un error subestimar la capacidad de las organizaciones criminales para incorporar la IA como herramienta en la comisión de ilícitos".* Además, advierte que pensar lo contrario sería *"una visión ingenua frente a la rapidez con que se adaptan a los avances tecnológicos"*, destacando que la criminalidad organizada no solo reacciona, sino que innova estratégicamente en el uso de tecnologías emergentes. De forma complementaria, el Entrevistado 1 ejemplifica esta adaptabilidad mediante usos concretos de IA: *"El crimen organizado en América Latina ya usa IA para planificar operaciones y para lavar dinero mediante perfiles y empresas falsas. También aprovecha datos filtrados en foros de la Deep y Dark web".* Este tipo de declaraciones introduce elementos emergentes basados en la experiencia de los expertos sobre cómo las organizaciones criminales ya integran la IA en sus estructuras operativas, especialmente en delitos financieros y cibernéticos.

El Entrevistado 3 plantea una lectura desde la geopolítica del fenómeno, destacando que los delitos vinculados a IA suelen originarse en países tecnológicamente más avanzados: *"La gran mayoría de casos investigados en donde existe un uso de inteligencia artificial en el país, tienen su origen fuera del mismo, más específicamente en Estados Unidos y/o países en donde la aplicación de la IA es más avanzada que en Chile".* Esta declaración, sugiere que Chile enfrenta una asimetría tecnológica que lo coloca en una posición de vulnerabilidad frente a amenazas globales, ya que la falta de desarrollo interno de capacidades en IA limita

la posibilidad de detección, persecución y prevención del delito. Igualmente, el entrevistado advierte que la criminalidad organizada local aún *"no mantiene un conocimiento vasto de este tipo de herramientas"*, lo cual puede interpretarse como una oportunidad para fortalecer las capacidades nacionales antes de que estas tecnologías se generalicen en el entorno delictivo chileno.

En consecuencia, los 03 expertos coinciden en la necesidad de cooperación internacional como respuesta clave frente al carácter transnacional del fenómeno. El Entrevistado 1 sostiene que: *"En Chile y la región urge anticiparse con más cooperación internacional, monitoreo de amenazas y control financiero digital por parte de los organismos encargados".* El Entrevistado 2 complementa esta idea al señalar que el abordaje del fenómeno requiere de *"voluntad política, fortalecimiento institucional y cooperación multisectorial",* demostrando que la respuesta debe ser coordinada y preventiva, más que reactiva ante este fenómeno que se encuentra en expansión.

5.3 Análisis de los resultados

El análisis de los resultados del estudio se realiza mediante el consolidado de los resultados que arrojaron tanto el análisis cualitativo de los estudios seleccionados y de las entrevistas aplicadas a los expertos. En consecuencia, respecto a las formas actuales y emergentes en que las organizaciones criminales utilizan IA a nivel global y regional, el análisis consolidado de entrevistas y textos académicos expone que las formas actuales y emergentes de uso de la inteligencia artificial por parte de organizaciones criminales se puede estructurar en dos dimensiones principales. La dimensión operativa-tecnológica, que abarca la automatización de ataques, el desarrollo de *malware* adaptable, la creación de *deepfakes* y las técnicas de evasión de detección, mientras que la dimensión estratégica-financiera se orienta a la comisión de delitos como el lavado de dinero, la manipulación de información y el uso de sistemas de comunicación cifrada. Estas prácticas reflejan una creciente sofisticación del crimen organizado, que se vuelve más autónomo, adaptable y difícil de rastrear.

En cuanto a la dimensión de manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile, los resultados se organizan

en tres dimensiones, las cuales se complementan. En primer lugar, la dimensión tecnológica-criminal se relaciona con la posibilidad de utilización de *deepfakes*, fraudes automatizados, ciberataques y manipulación de infraestructura, elementos que, según García Torres (2024) evidencian la necesidad de adaptar las herramientas procesales en base a las nuevas formas de criminalidad digital que superan la capacidad de respuesta actual del Estado. En segundo lugar, la dimensión institucional-operativa, se refiere a las vulnerabilidades en el manejo de información sensible y la ausencia de protocolos uniformes de ciberseguridad, lo que plantea interrogantes sobre la responsabilidad penal y la capacidad de los sistemas jurídicos para responder frente a decisiones autónomas de la IA.

En este aspecto, es relevante destacar a HeredIA, el cual es destacado por el Ministerio Público, como un pilar fundamental en la modernización tecnológica de la institución. Desde su implementación en 2022, HeredIA ha permitido detectar organizaciones criminales, anticipar zonas de riesgo y optimizar significativamente los procesos de análisis dentro del Ministerio Público. Esto, corresponden a una solución que ha impulsado la confiabilidad, seguridad e integración regional, consolidándose como esencial para abordar delitos complejos (Universidad de Chile, 2025). Asimismo, en base a lo declarado por el Entrevistado 2, HeredIA corresponde a un sistema de IA de uso restringido que funciona únicamente con datos internos del Ministerio Público. Su diseño excluye el uso de fuentes abiertas, con el propósito de prevenir eventuales filtraciones o vulneraciones de información. Cabe señalar que esta tecnología se encuentra todavía en fase de desarrollo, por lo cual no es posible contar con mayor información que la declarada en el presente estudio respecto a su funcionamiento, indicadores de gestión, entre otros.

Finalmente, la dimensión estructural-contextual se relaciona con el bajo nivel de conciencia pública e institucional sobre estos riesgos, la escasez de casos investigados y la limitada preparación técnica frente al avance tecnológico del crimen organizado. En conjunto, los expertos entrevistados coinciden en que Chile se encuentra en una etapa temprana de exposición a estos riesgos, pero que esta anticipación es una oportunidad para fortalecer la coordinación interinstitucional, desarrollar marcos normativos específicos y difundir la capacitación técnica de las policías y el sistema judicial. Tal como plantea Ospina Díaz et al. (2024), el aprovechamiento ético y transparente de la IA debe ir acompañado de

políticas de control y supervisión que impidan su captura por actores corruptos o delictivos. En este sentido, las manifestaciones incipientes del uso criminal de la IA son un riesgo actual derivado de la globalización.

En tercer lugar, respecto a las experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública, el análisis de las entrevistas permite identificar dos niveles complementarios de aprendizaje. En primer lugar, el nivel operativo-tecnológico, el cual se relaciona con la implementación de sistemas de reconocimiento facial, análisis predictivo delictual, biometría avanzada y procesamiento de datos masivos. Ejemplos de esta situación, según los entrevistados, son posible observarlas en Estados Unidos y en la Unión Europea, donde la IA ha sido integrada en las estrategias policiales para optimizar la vigilancia, anticipar patrones criminales y reforzar la toma de decisiones. Tal como plantea Machín (2023), la IA plantea nuevos desafíos éticos y jurídicos que deben ser asumidos desde una perspectiva de seguridad de manera integral. En segundo lugar, el nivel normativo-cooperativo se orienta al fortalecimiento de marcos regulatorios, políticas de seguridad y mecanismos de cooperación internacional que permitan prevenir, regular y perseguir los delitos facilitados por IA. En conjunto, los expertos coinciden en que la cooperación internacional y la regulación robusta son factores decisivos para enfrentar la criminalidad asistida por IA. Estas experiencias reflejan que la tecnología, sin un marco ético, puede derivar en prácticas invasivas o vulneraciones de derechos fundamentales, tal como advierte García Falconí y Barona Pazmiño (2024), quienes destacan la necesidad de alinear el uso de la IA con los principios del debido proceso y la tutela judicial efectiva.

Luego, los resultados de la categoría de principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile, indican que existe una visión compartida por parte de los entrevistados respecto a que la IA plantea desafíos multidimensionales para Chile, los que abarcan la seguridad nacional, las capacidades institucionales y la gobernanza tecnológica. Los expertos destacan la urgencia de contar con una legislación específica, una institucionalidad coordinada y especializada, y una política pública preventiva, la que debe ser capaz de anticipar riesgos antes de que se materialicen. En conjunto, las respuestas

muestran la necesidad de una estrategia nacional integral de IA y seguridad pública, que equilibre innovación, protección de derechos y defensa de los intereses soberanos.

Asimismo, los 03 textos analizados en esta categoría, coinciden en señalar que la IA, si bien ofrece oportunidades para fortalecer la seguridad, también plantea riesgos sistémicos que deben abordarse mediante políticas integrales. En el contexto de Chile, estos desafíos se expresan en tres planos: a) Seguridad nacional: vulnerabilidad frente a ciberataques y delitos digitales con proyección transnacional; b) Capacidades institucionales: existe una falta de marcos regulatorios claros y de competencias técnicas en ciber-inteligencia e investigación digital; c) Políticas públicas preventivas: hay una necesidad de diseñar estrategias que se basen en la transparencia, la ética digital y la colaboración entre el sector público y privado. Tal como lo sintetiza García Torres (2024), la lucha contra la ciberdelincuencia organizada no puede depender solamente de los Estados, sino que también requiere de una coordinación entre instituciones y del fortalecimiento de capacidades tecnológicas en todos los niveles institucionales.

Finalmente, la última categoría, correspondiente a las percepciones generales y elementos emergentes del fenómeno se basa en el análisis de las respuestas proporcionadas por los expertos, ya que esta dimensión fue elaborada en base a preguntas de cierre a los expertos, esto con la finalidad de sacar el mayor provecho a la instancia. En consecuencia, los resultados para esta categoría, muestran que los entrevistados comparten una percepción preocupación ante el avance de la IA en contextos delictivos, donde se destaca el riesgo de automatización y la capacidad de aprendizaje de los sistemas de IA desde el punto de vista criminalístico y la desigualdad tecnológica que expone a Chile frente a amenazas de nivel global. En suma, las respuestas reflejan que el fenómeno criminal de la IA, va más allá de las fronteras nacionales, lo que demanda respuestas integradas y cooperación internacional. La IA en el contexto del crimen organizado se configura, según los expertos, como un nuevo desafío para la seguridad pública**,** que exige políticas preventivas, inversión en capacidades técnicas y una visión estratégica de largo plazo.

6. CONCLUSIONES

El presente estudio, tuvo como finalidad analizar las implicancias del uso de inteligencia artificial por parte del crimen organizado en Chile. Esto, fue logrado a través de la metodología de investigación cualitativa, específicamente, ejecutando un análisis de contenido cualitativo para textos los académicos incluidos y para las entrevistas que se realizaron a 03 expertos en la materia. Para estos fines, se realizó la exploración de las formas actuales y emergentes en que las organizaciones criminales están utilizando inteligencia artificial a nivel global y regional, con énfasis en los delitos asociados al ciberespacio y crimen organizado, se identificaron las posibles manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile, se conocieron las experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública, para extraer aprendizajes útiles para el contexto chileno y finalmente se identificaron los principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile.

Respecto a la exploración de las formas actuales y emergentes en que las organizaciones criminales están utilizando inteligencia artificial a nivel global y regional, con énfasis en los delitos asociados al ciberespacio y crimen organizado, las conclusiones exponen que las formas actuales y emergentes pueden agruparse en dos grandes dimensiones. La primera, de carácter operativo-tecnológico, comprende la automatización de ataques, el desarrollo de malware con capacidad de adaptación, la generación de *deepfakes* y la implementación de mecanismos para evadir la detección. En este contexto, los expertos entrevistados coinciden en señalar que la IA ha aumentado la eficiencia, velocidad y alcance de los ataques digitales, generando de esta forma nuevas dinámicas de riesgo a nivel global. La segunda, de naturaleza estratégico-financiera, se relaciona con la ejecución de delitos como el lavado de activos, la manipulación de información y el uso de canales de comunicación encriptados. En conjunto, estas dinámicas evidencian una mayor sofisticación del crimen organizado, el cual se presenta cada vez más autónomo, flexible y difícil de

rastrear. En este aspecto, se podrían desarrollar futuras investigaciones, las que analicen en detalle la comisión de estos delitos mediante la utilización de IA.

Luego, respecto a la identificación de las posibles manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por parte de redes criminales en Chile, se determinó que, en un primer momento, las posibles manifestaciones o riesgos potenciales se estructuran en tres dimensiones complementarias. En primer lugar, la dimensión tecnológica-criminal se vincula con la posibilidad de utilizar *deepfakes*, fraudes automatizados, ciberataques y manipulación de infraestructuras, aspectos que, según García Torres (2024), exponen la urgencia de adecuar las herramientas procesales y penales frente a nuevas formas de criminalidad digital que actualmente superan la capacidad de respuesta del Estado. En segundo lugar, la dimensión institucional-operativa, aborda las vulnerabilidades en la gestión de información sensible y la falta de protocolos de ciberseguridad, lo que plantea problemáticas sobre la responsabilidad penal y la capacidad de los sistemas jurídicos para responder frente a decisiones tomadas por sistemas de IA. En este marco y en el ámbito nacional, se destaca la implementación de HeredIA, reconocida por el Ministerio Público como una herramienta clave en la modernización tecnológica institucional. Desde su puesta en marcha en 2022, esta plataforma ha contribuido a identificar organizaciones criminales, anticipar zonas de riesgo y optimizar los procesos analíticos internos, fortaleciendo la confianza, seguridad e integración regional (Universidad de Chile, 2025). HeredIA es un sistema de uso restringido que opera únicamente con datos internos, excluyendo deliberadamente el acceso a fuentes abiertas para prevenir eventuales filtraciones o vulneraciones de información. No obstante, dado que aún se encuentra en fase de desarrollo, no fue posible incluir mayor información sobre su funcionamiento o resultados de su gestión. En este aspecto también es posible ubicar un objeto de investigación para posibles estudios, los que analicen de manera profunda la gestión y contribución de HeredIA en materia de persecución penal en Chile.

Por último, la dimensión estructural-contextual se vincula con el bajo nivel de conciencia pública e institucional sobre los riesgos asociados, la escasez de investigaciones específicas y la limitada preparación técnica frente al rápido avance tecnológico del crimen organizado.

En cuanto a las experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública, para extraer aprendizajes útiles para el contexto chileno, se concluye la existencia de dos niveles de aprendizaje complementarios. El primero corresponde al nivel operativo-tecnológico, asociado a la aplicación de sistemas de reconocimiento facial, análisis predictivo delictual, biometría avanzada y procesamiento masivo de datos, herramientas que han sido incorporadas en Estados Unidos y la Unión Europea para optimizar la vigilancia, anticipar patrones criminales y fortalecer la toma de decisiones institucionales. El segundo nivel, de carácter normativo-cooperativo, se orienta al fortalecimiento de marcos regulatorios, políticas públicas y mecanismos de cooperación internacional que permitan regular, prevenir y sancionar los delitos facilitados por IA. Los expertos entrevistados coinciden en que la colaboración entre Estados y una regulación sólida resultan fundamentales para contener la criminalidad asistida por Tecnologías de la Información. En esta línea, García Falconí y Barona Pazmiño (2024) destacan que el uso de la IA en seguridad debe alinearse con los principios del debido proceso y la aplicación efectiva del sistema judicial.

Respecto a la identificación de los principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile, se concluye que existe una visión compartida entre los expertos: la IA plantea retos multidimensionales que exigen una respuesta coordinada y anticipada, por lo que además se plantea una urgencia de legislación específica, una institucionalidad especializada en la materia, y una política pública que sea capaz de identificar, prevenir y mitigar riesgos antes de su materialización

De forma complementaria, los textos académicos analizados sostienen que, aunque la IA ofrece oportunidades para fortalecer la seguridad, también introduce riesgos sistémicos que deben ser gestionados mediante políticas integrales. En el caso chileno, estos desafíos se expresan en tres niveles: la seguridad nacional frente a la exposición a ciberataques y delitos digitales transnacionales; las capacidades institucionales que son limitadas por la falta de marcos regulatorios claros; y finalmente las políticas preventivas, que requieren mayor transparencia, ética digital y cooperación público-privada. En este sentido, García Torres (2024) enfatiza que la lucha contra la ciberdelincuencia organizada no puede recaer

solamente en los Estados, sino que debe apoyarse en una coordinación interinstitucional y en el fortalecimiento de capacidades tecnológicas en todos los niveles de gestión pública.

Tal como se mencionó anteriormente, la categoría final, correspondiente a las percepciones generales y elementos emergentes del fenómeno, se elaboró a partir de las preguntas de cierre aplicadas a los expertos, con el objetivo de obtener una visión más amplia del tema. Los resultados revelan una preocupación común frente al avance de la IA en contextos delictivos, destacando riesgos como la automatización de procesos criminales, la capacidad de aprendizaje autónomo de los sistemas de IA y la brecha tecnológica que deja a Chile en una posición vulnerable ante amenazas globales. En síntesis, las percepciones de los expertos indican que el uso criminal de la IA trasciende las fronteras nacionales, por lo que requiere respuestas coordinadas e integradas a nivel internacional. Los expertos coinciden en que la IA aplicada al crimen organizado representa un nuevo desafío para la seguridad pública, que demanda políticas preventivas sólidas, inversión en capacidades técnicas y una planificación estratégica de largo plazo.

Uno de los principales hallazgos del estudio, corresponde a la constatación de que las organizaciones criminales están comenzando a incorporar tecnologías de IA para optimizar sus operaciones, particularmente en el ámbito digital. Esto incluye el uso potencial de *deepfakes*, fraudes automatizados, ciberataques y manipulación de información, entre otros, lo cual configura una nueva tipología delictual caracterizada por la automatización, el anonimato y la dificultad de rastreo. Por ende, se necesita con urgencia una nueva tipificación delictual basada en la IA. También, si bien la IA ofrece muchos beneficios y oportunidades para mejorar la seguridad pública, como por ejemplo la utilización del sistema HeredIA del Ministerio Público, también plantea riesgos, los cuáles se encuentran asociados a su uso indebido por actores criminales. Esta situación, refuerza la necesidad de un enfoque regulatorio, ético y preventivo en la aplicación de la IA tanto en el ámbito cotidiano como también en seguridad.

7. RECOMENDACIONES

A partir de los hallazgos obtenidos en la investigación, se establecen las siguientes recomendaciones en base a los resultados del estudio y pensando en fortalecer la capacidad del Estado chileno frente a los riesgos emergentes asociados al uso criminal de la IA. En consecuencia, se propone el desarrollo de un marco normativo que sea específico para la IA y el crimen organizado. En este sentido, se recomienda diseñar una legislación que regule el uso de sistemas de inteligencia artificial, tanto en el ámbito público como privado, estableciendo responsabilidades, mecanismos de supervisión y sanciones frente a su uso indebido o con fines delictuales.

Por otro lado, se propone que exista un fortalecimiento de las capacidades institucionales en ciber-inteligencia y análisis tecnológico, esto con la finalidad de invertir en la capacitación de personal especializado en análisis de datos, ciberseguridad e IA, especialmente en organismos como el Ministerio Público, cuerpos policiales y las unidades de inteligencia del Estado. Asimismo, es necesaria la creación de una estrategia nacional de IA y seguridad pública, la cual debe integrar innovación tecnológica, prevención del delito y protección de derechos fundamentales, la que incluya un énfasis en la cooperación entre el sector público y privado.

Un aspecto fundamental y que es mencionado tanto por los textos académicos analizados como por los expertos entrevistados, corresponde a la promoción de la cooperación internacional, ya que, debido al carácter transnacional del fenómeno, resulta esencial fortalecer los canales de colaboración con organismos internacionales, tanto para el intercambio de información como para la adopción de buenas prácticas en materia de regulación y persecución penal.

Finalmente, se propone que exista un fomento de la investigación científica en IA y su posterior aplicación en seguridad. Esto con la finalidad de incentivar proyectos de investigación que aborden el vínculo entre IA, criminalidad y gobernanza tecnológica, esto como base para la toma de decisiones basadas en evidencia, ya que como se constató en el presente estudio, el uso de IA en el ámbito de la criminalidad, es un fenómeno aún en estudio.

REFERENCIAS BIBLIOGRÁFICAS

Aggarwal N., Floridi, L., King, T., y Taddeo, M. (2019). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Science and Engineering Ethics, 95.

Aldoney, P., Albertz, P., Alcaino., E. (2022). Nueva Ley de Delitos Informáticos: aspectos penales y de compliance. *Carey*. https://www.carey.cl/nueva-ley-de-delitos-informaticos-aspectos-penales-y-de-compliance/

Armienta, G., Goite, M., Medina, A., Gambino, L., y García, L. (2015). *El lavado de dinero en el siglo XXI, una visión desde los instrumentos jurídicos internacionales, la doctrina y las leyes en América Latina y España*. México: Universidad Autónoma de Sinaloa. http://www.pensamientopenal.com.ar/system/files/2016/02/doctrina42906.pdf

Barragán-Huamán, H., Cataño-Añazco, K., Sevincha-Chacabana, M., y Vargas-Salas, O. (2023). La inteligencia artificial y la videovigilancia en la predicción y detección de delitos en espaciotiempo: una revisión sistemática. *Revista Criminalidad, 65*(1), 11-25.

Becker, S. y Viollier, P. (2020). La implementación del convenio de budapest en chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223. *Rev. derecho (Concepc.)* [online]. 2020, vol.88, n.248, pp.75-112. ISSN 0303-9986. https://www.scielo.cl/pdf/revderudec/v88n248/0718-591X-revderudec-88-248-75.pdf

Blauth, T. F., Gstrein, O. J., y Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *Ieee Access*, *10*, 77110-77122. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9831441

Brigada Investigadora del Ciber Crimen. (s.f). *Historia de la Brigada Investigadora del Ciber Crimen*. http://www.4law.co.il/ciber1.htm

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., y Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint.* arXiv:1802.07228. https://arxiv.org/pdf/1802.07228

Cajiao, A., González, P., Pardo, D., y Zapata, O. (2018). Una aproximación al crimen transnacional organizado: redes de narcotráfico Colombia-España. *Documento de trabajo*, *5*(15), 9. https://www.almendron.com/tribuna/wp-content/uploads/2018/03/dt5-2018-crimen-transnacional-organizado-redes-narcotrafico-colombia-espana.pdf

Calderón, G., Santillán, J., y Masias, Y. (2021). Plan de negocios para implementar un sistema de detección y alertas proactiva de inseguridad ciudadana con inteligencia artificial.

Caldwell, M., Andrews, J. T., Tanay, T., y Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1-13. https://link.springer.com/article/10.1186/s40163-020-00123-8

Chief Executives Board. (s.f). Artificial Intelligence. https://unsceb.org/topics/artificial-intelligence

Choraś, M., y Woźniak, M. (2022). The double-edged sword of AI: Ethical Adversarial Attacks to counter artificial intelligence for crime. *AI and Ethics*, *2*(4), 631-634. https://link.springer.com/article/10.1007/s43681-021-00113-9

Correa-Ménde, S., Méndez-García, A., y Varón-Meza, O. (2023). Modelo de reconocimiento facial basado en IA, Generador de alertas de intrusión.

De la Peña, A. F. R., Chavez, J. M. S., Salvador, J. L. A., Muñoz, E. H., y Salvatierra, E. R. D. (2024). La inteligencia artificial en la lucha contra el crimen organizado. *Ciencia*

Latina Revista Científica Multidisciplinar, *8*(4), 2144-2158. https://ciencialatina.org/index.php/cienciala/article/view/12455/18032

Decreto 83. (2017). Promulga el convenio sobre la ciberdelincuencia. https://www.bcn.cl/leychile/navegar?idNorma=1106936

Easttom, C. (2025). Malicious Use of Artificial Intelligence. In *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 00499-00507). IEEE. https://ieeexplore.ieee.org/abstract/document/10903787

Fahim, S., y Bajpai, G. S. (2020). AI and criminal liability. *Indian Journal of Artificial Intelligence and Law, 1* (1): 70-106 https://www.academia.edu/86155216/AI_and_Criminal_Liability

Fallas-Vargas, F., y Morales, C. (2024). Luces y sombras de la inteligencia artificial: ética, crimen organizado, justicia, industria cultural y minimalismo cognitivo. *Revista Estudios*, 75-101.

Federal Bureau of Investigation. (s.f). *Inteligencia Artificial*. https://www.fbi.gov/investigate/counterintelligence/emerging-and-advanced-technology/artificial-intelligence

Fontalvo Herrera, T. J., Vega Hernández, M. A., y Mejía Zambrano, F. (2023). Método de clustering e inteligencia artificial para clasificar y proyectar delitos violentos en Colombia. *Revista Científica General José María Córdova*, *21*(42), 550-572. https://revistacientificaesmic.com/index.php/esmic/article/view/1117

García Falconí, R. J., y Barona Pazmiño, K. F. (2024). Inteligencia artificial y proceso penal. *Revista San Gregorio*, *1*(58), 87-100. https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2808

García Torres, M. (2024). Ciberseguridad vs ciberdelincuencia: obstáculos procesales en la persecución de la ciberdelincuencia organizada. Propuestas para una más eficaz represión de los ciberdelitos. *Ciencia policial*, *182*, 15-69. https://revistas.usal.es/cuatro/index.php/2254-0326/article/view/31962/30000

González, M. (2017). La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado. *Grupo de estudios en seguridad internacional, Universidad de Granada*, 13-45. http://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen

Guttman y Fong (2016). Inteligencia Artificial como herramienta de estrategia y seguridad para defensa.

Guzmán, S., y Casteleiro, A. (2022). Acciones para combatir el impacto del crimen en el ciberespacio. Prevención y detección con la Inteligencia Artificial. *Studia Prawnicze: rozprawy i materiały*, *30*(1), 15-24.

Helm, P., y Hagendorff, T. (2021). Beyond the prediction paradigm: Challenges for AI in the struggle against organized crime. *Law and Contemp. Probs.*, *84*, 1. https://scholarship.law.duke.edu/lcp/vol84/iss3/2/

Hernández-Sampieri, R., y Mendoza, C. (2018). *Metodología de la Investigación: Las Rutas Cuantitativa, Cualitativa y Mixta*. McGraw Hill. https://bellasartes.upn.edu.co/wp-content/uploads/2024/11/METODOLOGIA-DE-LA-INVESTIGACION-Sampieri-Mendoza-2018.pdf

Jeong, D. (2020). Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues. *IEEE Access*, *8*, 184560-184574.

Jordán G., y Rosas, J (2024). Aplicación de la Inteligencia Artificial a la Defensa. *Revista de aeronáutica y astronáutica*, (559), 713-718.

https://revistamarina.cl/en/articulo/aplicacion-de-la-inteligencia-artificial-la-defensa-y-seguridad/

King, T. C., Aggarwal, N., Taddeo, M., y Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics*, *26*(1), 89-120. https://link.springer.com/article/10.1007/s11948-018-00081-0

Ley 21.459. (2022/2025). Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. https://www.bcn.cl/leychile/navegar?idNorma=1177743

Linares, J. (2008). Redes criminales transnacionales: principal amenaza para la seguridad internacional en la posguerra fría. *Revista criminalidad*, *50*(1), 371-384. http://www.scielo.org.co/pdf/crim/v50n1/v50n1a12.pdf

Machín, R. (2023). ANTECEDENTES PARA LA IMPLANTACIÓN DE LA IA EN SEGURIDAD A TRAVÉS DE EUROPA: La innovación tecnológica como factor clave para el Ministerio del Interior. *Logos Guardia Civil, Revista Científica del Centro Universitario de la Guardia Civil*, (1), 125-154. https://revistacugc.es/article/view/5834/6395

Martínez, J., Palacios, G., y Oliva, D (2023). Guía para la revisión y el análisis documental: propuesta desde el enfoque investigativo. *Revista Ra Ximhai*, *19*(1), 67-83. https://dialnet.unirioja.es/servlet/articulo?codigo=8851658

Mayorga-Sandoval, J. E., y Aldás-Benavides, A. M. (2025). La inteligencia artificial y su impacto en la seguridad del Estado ecuatoriano. *Revista Enfoques de la Comunicación*, (13), 226-260. https://revista.consejodecomunicacion.gob.ec/index.php/rec/article/view/242/788

Ministerio de Ciencias, Tecnología, Conocimiento e Innovación de Chile. (s.f). *Inteligencia Artificial.* https://www.minciencia.gob.cl/areas/inteligencia-artificial/Inteligencia-Artificial/

Ministerio de Ciencias, Tecnología, Conocimiento e Innovación de Chile. (2024). *Política Nacional de Inteligencia Artificial.* Actualización 2024.

Morán, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista ius*, *15*(48), 289-323. https://revistaius.com/index.php/ius/article/view/706/795

Naciones Unidas y Comisión Económica para América Latina y el Caribe. (2025). *Índice Latinoamericano de IA*. https://indicelatam.cl/wp-content/uploads/2025/10/Docuemnto-ILIA_WEB.pdf

Naciones Unidas, Oficina de Naciones Unidas contra la Droga y el Delito. (2004). *Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional y sus Protocolos*. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

Naciones Unidas. (2024, 19 de septiembre). *ONU: La regulación mundial de la IA es necesaria*. https://news.un.org/es/story/2024/09/1532941

Naciones Unidas. (s.f). *Inteligencia artificial* (IA). https://www.un.org/es/global-issues/artificial-intelligence#:~:text=Inteligencia%20artificial%20al%20servicio%20del%20bien%20com%C3%BAn&text=Adem%C3%A1s%2C%20la%20IA%20puede%20ayudar,el%20bien%20y%20salvar%20vidas.

Nica, C. y Tănase, T. (2020). Using weaponized machine learning in cyber offensive operations. *International Conference Knowledge-based Organization, 26* (1), 94-99. https://doi.org/10.2478/kbo-2020-0014

Oficina de las Naciones Unidas contra la Droga y el Delito. (s.f). *Definición en la Convención contra la Delincuencia Organizada*. https://www.unodc.org/e4j/es/organized-crime/module-1/key-issues/definition-in-convention.html

Ospina, M., Mora, R. M., y Maya, A. (2025). Percepción de la inteligencia artificial en la lucha contra la corrupción: una exploración al caso del Estado de Colombia. *Revista Opera*, (36), 7-45. https://www.redalyc.org/journal/675/67582020002/

Otín, J. M. (2025). Sumario QdC: Usos delictivos de la inteligencia artificial: Desafíos para la política criminal. *Quadernos de criminología: revista de criminología y ciencias forenses*, (65), 29-34.

Peters, K. (2019). 21st century crime: How malicious artificial intelligence will impact homeland security. *Homeland Security Affairs*. https://calhoun.nps.edu/server/api/core/bitstreams/7ccc8978-12ed-45a2-ab73-081f62b02c3b/content

Policía de Investigaciones. (2021 octubre 15). *Cooperación global para la Ciberseguridad*. https://www.pdichile.cl/centro-de-prensa/detalle-prensa/2021/10/15/cooperaci%C3%B3n-global-para-la-ciberseguridad

Policía de Investigaciones. (2022). *Brigadas Investigadoras del Cibercrimen*. https://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimen

Policía de Investigaciones. (2022). Cuenta Pública 2022. https://www.pdichile.cl/docs/default-source/default-document-library/cuentapublica2022.pdf?sfvrsn=9a0a6216_0

Rawat, R., Oki, O., Chakrawarti, R. K., Adekunle, T. S., Lukose, J. M., y Ajagbe, S. A. (2023). Autonomous artificial intelligence systems for fraud detection and forensics

in dark web environments. *Informatica*, *47*(9). https://www.informatica.si/index.php/informatica/article/view/4538/2501

Rejas, A., Salcedo, J., Alvarez J., Hoyos, E, y Diaz, E. (2024). La inteligencia artificial en la lucha contra el crimen organizado. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(4), 2144-2158.

Reyes, M. (2025). La inteligencia artificial en criminalística: revolución tecnológica en la investigación forense. *Perspectivas: Revista de ciencias jurídicas y políticas.* https://revistas.ucalp.edu.ar/index.php/Perspectivas/article/view/423/387

Rivera, J. (2011). El crimen organizado. *Instituto de Estudios em Seguridad. Guatemala*. https://www.galileo.edu/pdh/wp-content/blogs.dir/17/files/2011/04/EL_CRIMEN_ORGANIZADO-IES.pdf

Saldaña, P. (2019). ¿Por qué las organizaciones criminales utilizan criptomonedas? Los bitcoins en el crimen organizado. *El Criminalista Digital. Papeles de Criminología*, (7). https://scholar.googleusercontent.com/scholar?q=cache:UOZPEL7kvkIJ:scholar.google.com/+%C2%BFPor+qu%C3%A9+las+organizaciones+criminales+utilizan+criptomonedas%3F+Los+bitcoins+en+el+crimen+organizado.&hl=es&as_sdt=0,5

Salinero, S. (2015). El crimen organizado en Chile: Una aproximación criminológica al perfil del delincuente a través de un estudio a una muestra no representativa de privados de libertad por delitos de tráfico de estupefacientes. *Política criminal, 10* (19), 25-55. https://scielo.conicyt.cl/pdf/politcrim/v10n19/art02.pdf

Sarabia, E. (2023). *Sistema de videovigilancia comunitaria mediante visión artificial* [Tesis Magistral, Universidad Tecnológica Israel, Ecuador, Quito].

Sutton, R. (13 de marzo, 2019). *The Bitter Lesson.* http://www.incompleteideas.net/IncIdeas/BitterLesson.html

Tuesta, H., Mendo, H., Silva, O., Galecio, W., y Montoya, A. (2024). Crimen organizado y narcotráfico: retos actuales para el sistema penal peruano. *Epistemia, 8*(1), 71-78.

Universidad de Chile. (2025, 21 de julio). *U. de Chile y Fiscalía Nacional acuerdan licenciamiento de inteligencia artificial para enfrentar el crimen organizado*. https://www.dii.uchile.cl/2025/07/22/u-de-chile-y-fiscalia-nacional-acuerdan-licenciamiento-de-inteligencia-artificial-para-enfrentar-el-crimen-organizado/

Universidad Nacional Autónoma de México. (2023). *Cerca del 80 por ciento de las personas utiliza IA sin darse cuenta*. https://www.gaceta.unam.mx/cerca-del-80-por-ciento-de-las-personas-utiliza-ia-sin-darse-cuenta/

Anexos

Anexo A

Bitácora de trabajo

BUSCADOR	AUTOR	AÑO	CATEGORÍA TEMÁTICA CON LA QUE SE VINCULA	OBJETIVO DEL ESTUDIO	TIPO DE ESTUDIO	RESULTADOS	DOI /ISSN/WEBSITE
Dialnet	De la Peña et al.	2024	Formas actuales y emergentes	Examinar cómo la inteligencia artificial videovigilancia fortifica la lucha contra la criminalidad organizada	Cualitativa fenomenológica	la inteligencia artificial videovigilancia apoya efectivamente en la lucha contra la criminalidad organizada	https://cienciialatina.org/index.php/cienciala/article/view/12455/18032
Dialnet	Machín, R	2023	Experiencias internacionales	definición de los principios orientadores en materia IA para la seguridad.	Revisión documental	El esfuerzo que deben hacer todos los actores involucrados en el ámbito de la IA para la seguridad a nivel europeo y nacional es exigente	https://revistacugc.es/article/view/5834/6395
Dialnet	García Torres, M. L.	2024	Desafíos que representa el uso de IA	Analizar los obstáculos procesales en la persecución de la ciberdelincuencia organizada y proponer medidas para una represión más eficaz de los ciberdelitos	Revisión documental	Se concluye que, a pesar de los esfuerzos legislativos de la Unión Europea, los resultados en la represión de la ciberdelincuencia han sido escasos hasta el momento y la cooperación internacional es fundamental.	https://revistas.usal.es/cuatro/index.php/2254-0326/article/view/31962/30000
ScielO	García Falconí, R y Barona Pazmiño, K	2024	Experiencias internacionales	Analizar el papel de la inteligencia artificial como herramienta de mejora y optimización de los procesos penales en Ecuador.	Revisión documental	a IA mejora la eficiencia procesal, pero plantea desafíos relacionados con la privacidad, seguridad de datos y sesgos algorítmicos en la toma de decisiones judiciales.	https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2808
ScielO	Morán, A	2021	Desafíos que representa el uso de IA	Analizar la probable responsabilidad penal de la IA como “sujeto activo” de delitos	Revisión documental jurídico	Se concluye que se hace necesario crear marcos normativos específicos (incluida	https://revistaius.com/index.php/ius/

						la posibilidad de una “persona artificial”) para afrontar delitos cometidos por o con IA.	article/view/706/795
Redalyc	Ospina et al.	2025	Desafíos que representa el uso de IA	Analizar la percepción y efectividad de la IA como herramienta para combatir la corrupción en organizaciones públicas del Estado colombiano,	Cuantitativo	La IA tiene potencial, pero las capacidades actuales institucionales (infraestructura, talento humano, liderazgo) aún son débiles	https://www.redalyc.org/journal/675/6758202000 2/
Redalyc	Fontalvo-Herrera, J., Vega-Hernández, M., y Mejía-Zambrano, F	2023	Formas actuales y emergentes	Proponer clústeres de delitos violentos en Colombia por departamentos y diseñar una estructura de red neuronal (IA) para su clasificación y pronóstico	Cuantitativo	Los delitos más relevantes para el modelo fueron: secuestro, delitos sexuales, extorsión, amenazas, homicidios y terrorismo (en ese orden de importancia)	https://www.redalyc.org/journal/4762/476277508011/
Google Académico	Reyes Inca, M	2025	Experiencias internacionales	Analizar cómo la inteligencia artificial está transformando los métodos y técnicas de investigación forense, evaluando su impacto en la precisión, eficiencia y rapidez de los procesos criminalísticos.	Revisión documental jurídico	La IA permite automatizar y optimizar la recolección y análisis de evidencia forense.	https://revistas.ucalp.edu.ar/index.php/Perspectivas/article/view/423
Google Académico	Jordán, G y Rosas, J	2024	Manifestaciones incipientes o riesgos potenciales	Analizar cómo la IA puede integrarse en la seguridad y defensa de Chile,	Revisión documental	https://revistamarina.cl/en/articulo/aplicacion-de-la-inteligencia-artificial-la-defensa-y-seguridad/	

Fuente: elaboración propia

Anexo B

Tabla temática de entrevistas

CATEGORÍA	ENTREVISTADO 1	ENTREVISTADO 2	ENTREVISTADO 3
Formas actuales y emergentes en que las organizaciones criminales utilizan IA inteligencia artificial a nivel global y regional	*Las organizaciones criminales hoy en día están usando la IA para automatizar y escalar ataques como la generación de phishing, creación de deepfakes, y con este último a la clonación de audio y vídeo para extorsión o fraudes. Nosotros como PDI hemos alertados desde el año pasado este tipo de fraudes, sin embargo, a la fecha no se han detectado casos como estos en nuestro territorio.*	*En mi experiencia profesional, no he tenido aún la oportunidad de investigar casos en los que las organizaciones criminales hagan uso directo de herramientas de Inteligencia Artificial para la comisión de delitos. Sin embargo, resulta razonable anticipar que dicha tecnología comenzará a ser incorporada progresivamente por estas estructuras delictivas, especialmente en el ámbito de los delitos de carácter patrimonial.* *La IA podría emplearse, por ejemplo, para optimizar mecanismos destinados a ocultar el origen ilícito de recursos financieros, dificultar la trazabilidad de operaciones económicas, o manipular y encriptar información sensible que potencialmente podría constituir evidencia en procesos judiciales. Es previsible que las organizaciones utilicen la IA para la obtención y procesamiento de información, tanto sobre posibles víctimas como sobre instituciones*	*En base a mi experiencia las organizaciones criminales están encontrando diversas formas de utilizar la inteligencia artificial (IA) para potenciar sus actividades ilícitas, especialmente en el ámbito del ciberespacio y en la forma de ocupar las tecnologías de la información a su favor para desarrollar, idear y mejorar técnicas delictuales tales como;* *Automatización de ataques cibernéticos: Utilizan IA para escanear vulnerabilidades en sistemas, crear malware o programas malignos más sofisticado y automatizan ataques de phishing y ransomware. La IA permite adaptar los ataques en tiempo real y aumentar su eficacia, vulnerando las barreras que mantienen los distintos sistemas informáticos de manera más eficiente.* *Creación de contenido engañoso: Emplean "deepfakes" y Generación de contenido sintético para engañar a víctimas, falsificar identidades o*

		encargadas de su persecución penal, incrementando así su capacidad operativa y su nivel de sofisticación criminal.	*difundir desinformación y amenazar a personas cuya relación con las tecnologías no es tan cercana. Normalmente el público objetivo corresponde a personas de la tercera edad cuyo conocimiento de las tecnologías es mínimo.* *Evasión de detección: Desarrollan técnicas de IA para evadir sistemas de detección y análisis en redes sociales, plataformas de comunicación y sistemas de seguridad, haciendo más difícil rastrear sus actividades.* *Operaciones en ciberdelitos financieros: La IA se usa para automatizar fraudes en plataformas de pagos, blanqueo de dinero mediante algoritmos que camuflan transacciones ilícitas y manipulan mercados financieros de manera ilegal.* *Redes sociales y comunicación cifrada: Los grupos criminales emplean bots impulsados por IA para administrar redes de cuentas falsas, promover actividades ilegales y coordinar operaciones sin ser detectados.*
Manifestaciones incipientes o riesgos potenciales del uso de inteligencia artificial por	*En Chile los riesgos se centran en fraude masivo mediante deepfakes, automatización de campañas de estafa, ataques dirigidos a infraestructura crítica, o*	*Tal como señalé previamente, la utilización de herramientas de IA por parte de redes criminales representa un riesgo creciente,*	*Si bien, en Chile la legislación asociada a este tipo de medios tecnológicos va incrementando a través de diferentes leyes tanto en el ámbito de los*

parte de redes criminales en Chile	*uso de IA para organizar redes de tráfico, lavado u otros ilícitos complejos. Documentos nacionales señalan que la ciberseguridad aún presenta brechas. Aunque Chile ya cuenta con avances (por ejemplo, la ley de ciberseguridad Nº21.663), podría decirse que no está completamente preparado para el tipo de amenazas que plantea la IA al crimen organizado.*	*principalmente en cuanto a la dificultad para trazar operaciones económicas ilícitas y la manipulación o destrucción de evidencia digital. Considero que, a nivel nacional, aún no se ha dimensionado adecuadamente el impacto que puede tener la IA como instrumento facilitador del crimen organizado, no solo en la ejecución de delitos, sino también en las brechas de seguridad que afectan los procesos de investigación penal.* *En este sentido, si los organismos de persecución penal como la Fiscalía o la policía, no aplican protocolos estrictos en el manejo de datos mediante herramientas de IA, existe el riesgo de que información sensible se filtre y pueda ser accedida por actores externos o incluso por sistemas de inteligencia artificial interconectados.* *Actualmente, la Fiscalía Nacional dispone de una herramienta denominada HeredIA, un software de IA de carácter cerrado que opera exclusivamente con información interna del Ministerio Público, sin recurrir a fuentes abiertas, precisamente para evitar vulneraciones o fugas de información. Esta herramienta se*	*delitos informáticos y la ley de protección y tratamiento de datos informáticos la cual entra en vigencia en diciembre de 2026, existe muy poca información tanto en la ciudadanía como en los organismo policiales respecto al uso potencial y nocivo de la inteligencia artificial que hace difícil poder responder si nos encontramos preparados a este tipo de criminalidad delictual. En la actualidad existen muy pocos casos relativos al uso de estas tecnologías por lo que es muy poca la información asociada al respecto.*

		encuentra aún en etapa de desarrollo. *No obstante, se ha observado que algunos funcionarios del sistema penal utilizan plataformas de IA abiertas, lo que constituye un riesgo operativo y de seguridad. Una mala formulación de consultas o la entrega de datos sensibles podría generar respuestas erróneas o incluso exponer información confidencial. Además, es sabido que las IA abiertas pueden "intercambiar" o inferir datos a partir de sus bases de entrenamiento, lo que aumenta la posibilidad de brechas de seguridad institucionales.* *En consecuencia, una organización criminal con las capacidades tecnológicas adecuadas podría acceder a bases de datos institucionales o extraer información personal de fiscales y policías, comprometiendo incluso la integridad física de los funcionarios. Dada la ausencia de directrices claras y un marco regulatorio sobre el uso de IA en el sector público, estimo que Chile no se encuentra plenamente preparado para enfrentar los riesgos derivados de la utilización de esta*	

		tecnología por parte del crimen organizado.	
Experiencias internacionales que hayan abordado este fenómeno desde la seguridad pública	*Un ejemplo concreto en Chile ha sido el sistema ABIS utilizado por la PDI en el extremo norte del país, que aplica inteligencia artificial y biometría (rostro, huellas y voz) para identificar personas en los pasos fronterizos y comparar sus datos con bases criminales internacionales, permitiendo detectar prófugos y mejorar el control migratorio. Así como también el uso de otras tecnologías para reconocimiento facial y identificación de perfiles en las distintas redes sociales, obviamente con contenido público de perfiles, sin transgredir garantías. Experiencias similares se han desarrollado en Estados Unidos y la Unión Europea, donde sistemas de IA apoyan la detección de sospechosos mediante reconocimiento facial y análisis predictivo delictual. Chile podría aprender de estos casos la importancia de una regulación robusta sobre protección de datos, siendo urgente fortalecer estos marcos antes de ampliar el uso nacional de tecnologías IA en apoyo a la investigación y como indique anteriormente, capacitación de personal especializado en el ámbito. (…)*	*No poseo conocimiento experiencias internacionales específicas que hayan abordado el fenómeno de la Inteligencia Artificial desde la perspectiva de la seguridad pública. Sin embargo, sé que hay países que están avanzando en la implementación de políticas y marcos regulatorios destinados a normar el uso seguro de la IA.* *En el caso de Chile, considero urgente establecer una política de seguridad para el uso de la Inteligencia Artificial, que contemple lineamientos claros respecto de su aplicación en los procesos de investigación penal. Esta política debería incluir protocolos de manejo de información sensible, capacitación especializada para los funcionarios del sistema público y mecanismos que garanticen la integridad y confidencialidad de los datos (…)* *La cooperación internacional desempeña un rol esencial en la prevención, regulación y persecución de los delitos vinculados al uso indebido de la*	*Dentro del conocimiento que manejo respecto al tema, Estados Unidos utiliza herramientas de inteligencia artificial y análisis de datos, para poder automatizar grandes volúmenes de datos provenientes de redes sociales, comunicaciones cifradas y transacciones financieras, facilitando la identificación de patrones delictivos y la localización de redes criminales. (…)* *El rol de la cooperación internacional es fundamental, toda vez que ayuda a integrar conocimientos de otras instituciones fuera del país, que ayudan a aportar experiencia y metodología practica en aquellas materias y regulaciones que en chile no se encuentren tan desarrolladas*

	La cooperación internacional es clave porque el uso de IA por redes criminales trasciende fronteras, las plataformas, los datos, los ataques provienen o se ubican muchas veces en otros países, donde nosotros no mantenemos jurisdicción. Compartir inteligencia, estándares, buenas prácticas, capacidades de investigación forense digital e interoperabilidad de sistemas, es fundamental para el combate e investigación. Además, regular la IA ilícita exige acuerdos globales por la naturaleza transnacional del delito con IA.	*Inteligencia Artificial. Dado que el desarrollo y aplicación de esta tecnología tiene su origen en distintos países y empresas transnacionales, los avances tecnológicos, los mecanismos de control y los estándares de seguridad suelen estar determinados por prácticas y marcos regulatorios externos.* *Por ello, resulta crucial fortalecer los vínculos de cooperación con otros Estados y con organismos internacionales especializados, tales como INTERPOL, Naciones Unidas y foros multilaterales sobre ciberseguridad, a fin de compartir información, buenas prácticas y capacidades técnicas. Esta colaboración permitirá mejorar la respuesta investigativa y judicial frente al crimen organizado transnacional.*	
Principales desafíos que este fenómeno representa para la seguridad nacional, las capacidades institucionales y la formulación de políticas públicas preventivas en Chile	*Los desafíos mantener la soberanía y seguridad frente a ataques automatizados, desarrollar capacidades institucionales (datos, IA, análisis, personal); diseñar políticas públicas que anticipen usos ilícitos de IA (no sólo reaccionar), poder asegurar la cooperación entre defensa, interior, ciencia, justicia. Institucionalmente, el actor que debería liderar*	*La principal brecha que enfrenta Chile para abordar el uso delictivo de la Inteligencia Artificial radica en la ausencia de un marco regulatorio específico que establezca normas claras respecto de su desarrollo, utilización y control. Actualmente, el país carece de una legislación que delimite responsabilidades, defina estándares de seguridad tecnológica y*	*Los principales desafíos del fenómeno de la IA son principalmente el poder contrarrestar el avance de las tecnologías de la información a través de la utilización de IA, reforzando la actual legislación que contempla ciertas figuras que refuerzan la protección por ejemplo de los datos personales en la red de diferentes personas. Es en este*

	esta respuesta es un ente que coordine ciberseguridad, inteligencia, justicia y tecnología, por ejemplo, la Agencia Nacional de Ciberseguridad (ANCI) bajo la ley de ciberseguridad, en conjunto con el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación.	*determine mecanismos de fiscalización aplicables tanto al sector público como al privado. Esta falta de regulación genera un vacío normativo que impide responder eficazmente ante los riesgos asociados al uso indebido de la IA, especialmente cuando es empleada por organizaciones criminales para ocultar información, manipular evidencias o vulnerar sistemas institucionales.*	*mismo sentido, si bien la ANCI (Agencia Nacional de Ciberseguridad), mantiene un rol activo y preventivo ante las afectaciones provocadas a los sistemas informáticos o a la infraestructura critica del país ante ataques, puede ser un actor relevante en esta materia junto con el Ministerio Público quienes a través de la información que puedan aportar ambas entidades, pueda existir una concatenación que facilite la investigación de este tipo de fenómenos tanto de un carácter técnico como de un carácter legal. (...)* *La principal brecha en el uso de la IA en chile es la desinformación que existe relativa a su utilización y la posibilidad de mejoramiento que esta pueda aportar, tanto a los procesos investigativos como de gestión, que faciliten un resultado más exitoso en la investigación de casos en que se ocupe Inteligencia Artificial.*
Percepciones generales y elementos emergentes del fenómeno	*Creo que un aspecto que merece atención es el riesgo de IA autónoma en manos de criminales, como, por ejemplo, agentes de IA que actúen sin supervisión humana, lo que puede cambiar la velocidad y escala del delito. Además, un aspecto clave es que, se sabe que hoy en día, el*	*Considero que sería un error subestimar la capacidad de las organizaciones criminales para incorporar la IA como herramienta en la comisión de ilícitos. Pensar que estos grupos aún no están explorando o utilizando activamente este tipo de tecnologías*	*Creo que el aspecto más relevante que puede existir entre la IA y el crimen organizado que puede que no haya sido mencionado, dice relación al carácter internacional que hay de este tipo de fenómenos delictuales, los que comúnmente afectan a países más*

	crimen organizado en América Latina ya usa IA para planificar operaciones y para lavar dinero mediante perfiles y empresas falsas. También aprovecha datos filtrados en foros de la Deep y Dark web, como también el entrenamiento de modelos de IA abiertos para mejorar sus fraudes o mover capitales. En Chile y la región urge anticiparse con más cooperación internacional, monitoreo de amenazas y control financiero digital por parte de los organismos encargados.	*resulta una visión ingenua frente a la rapidez con que se adaptan a los avances tecnológicos. La IA representa un desafío técnico para las instituciones encargadas de garantizar la seguridad pública. Su abordaje requiere voluntad política, fortalecimiento institucional y cooperación multisectorial para enfrentar eficazmente su potencial uso delictivo.*	*desarrollados o que su conocimiento con la Inteligencia Artificial es superior, lo que afecta a países como Chile, en los que la criminalidad organizada todavía no mantiene un conocimiento basto de este tipo de herramientas para realizar delitos. Un ejemplo más claro, dice relación a que la gran mayoría de casos investigados en donde existe un uso de inteligencia artificial en el país, tienen su origen fuera del mismo, más específicamente en Estados Unidos y/o países en donde la aplicación de la IA es más avanzada que en Chile.*

Fuente: Elaboración propia en base a entrevistas