



Revista Hambatu Science

Ambato – Ecuador / ISSN 3151-815X (en línea) / julio - septiembre 2026

Volumen 1, Número 3

<https://doi.org/10.63862/rhs-v1n3-345-369-2026>

Big Data para el Patrullaje Predictivo: Éxitos, Sesgos Algorítmicos y Protección de la Privacidad en la Seguridad Pública

*Big Data for Predictive Policing: Successes, Algorithmic
Biases, and Privacy Protection in Public Security*

Ricardo Cruz Vázquez
Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas



DOI: <https://doi.org/10.63862/rhs-v1n3-345-369-2026>

Big Data para el Patrullaje Predictivo: Éxitos, Sesgos Algorítmicos y Protección de la Privacidad en la Seguridad Pública

Ricardo Cruz Vázquez

Centro de Estudios Superiores en Ciencias

Jurídicas y Criminológicas

ricardocruzv081122@gmail.com

<https://orcid.org/0009-0008-3467-7470>

México

Recibido: 2026-07-20

Aceptado: 2026-07-23

Publicado: 2026-07-29

Resumen

La incorporación del Big Data y la inteligencia artificial ha transformado la seguridad pública al fortalecer la prevención del delito y la toma de decisiones policiales. El patrullaje predictivo utiliza algoritmos de aprendizaje automático y minería de datos para identificar patrones delictivos y optimizar la asignación de recursos. Sin embargo, su implementación plantea desafíos relacionados con los sesgos algorítmicos, la transparencia y la protección de datos personales. El objetivo de este artículo es analizar críticamente la aplicación del Big Data en el patrullaje predictivo, evaluando sus beneficios, limitaciones e implicaciones para la privacidad. Se realizó una revisión sistemática de literatura bajo los lineamientos PRISMA, considerando publicaciones científicas entre 2021 y 2026. Los resultados indican que estas tecnologías mejoran la inteligencia policial y la eficiencia operativa; no obstante, la calidad de los datos y la supervisión humana son factores determinantes para evitar decisiones discriminatorias y garantizar el respeto a los derechos fundamentales. Se concluye que el patrullaje predictivo requiere modelos de gobernanza de datos, transparencia algorítmica y mecanismos de auditoría para lograr una implementación responsable.

Palabras clave: Big Data; patrullaje predictivo; inteligencia policial; inteligencia artificial; sesgos algorítmicos; privacidad; seguridad pública.

Big Data for Predictive Policing: Successes, Algorithmic Biases, and Privacy Protection in Public Security

Abstract

The incorporation of Big Data and artificial intelligence has transformed public security by strengthening crime prevention and police decision-making. Predictive policing uses machine learning algorithms and data mining techniques to identify crime patterns and optimize resource allocation. However, its implementation raises concerns regarding algorithmic bias, transparency, and personal data protection. This study aims to critically analyze the application of Big Data in predictive policing by examining its benefits, limitations, and implications for privacy. A systematic literature review was conducted following the PRISMA guidelines, including scientific publications published between 2021 and 2026. The findings indicate that these technologies improve police intelligence and operational efficiency; however, data quality and human oversight remain essential to prevent discriminatory outcomes and safeguard fundamental rights. It is concluded that responsible predictive policing requires robust data governance, algorithmic transparency, and continuous auditing mechanisms.

Keywords: Big Data; Predictive policing; Police intelligence; Artificial intelligence; Algorithmic bias; Privacy; Public security.

Introducción

La transformación digital ha impulsado la incorporación del Big Data y la inteligencia artificial como herramientas estratégicas para fortalecer la inteligencia policial y la prevención del delito. El análisis de grandes volúmenes de información provenientes de registros criminales, videovigilancia, sensores urbanos y otras fuentes permite identificar patrones delictivos, optimizar la asignación de recursos y apoyar la toma de decisiones basada en evidencia.

En este contexto, el patrullaje predictivo surge como un modelo que emplea algoritmos de aprendizaje automático y análisis espacial para estimar la probabilidad de ocurrencia de delitos y orientar el despliegue operativo de las instituciones policiales. Su aplicación ha favorecido la transición de estrategias reactivas hacia enfoques preventivos sustentados en el análisis de datos.

No obstante, la creciente utilización de algoritmos también ha generado cuestionamientos relacionados con los sesgos algorítmicos, la falta de transparencia y la protección de datos personales. Los modelos predictivos pueden reproducir desigualdades presentes en los datos históricos y afectar principios como la igualdad, la privacidad y la rendición de cuentas, especialmente cuando no existen mecanismos de auditoría y supervisión adecuados.

Aunque el interés científico por el patrullaje predictivo ha aumentado en los últimos años, en América Latina persisten limitadas investigaciones sobre su implementación y evaluación. Esta situación evidencia la necesidad de analizar críticamente el potencial y los riesgos del Big Data en la seguridad pública desde una perspectiva tecnológica, ética y jurídica.

En este contexto, el presente estudio tiene como objetivo analizar la aplicación del Big Data en el patrullaje predictivo, evaluando sus beneficios, los desafíos derivados de los sesgos algorítmicos y las implicaciones para la privacidad, con el propósito de proponer lineamientos para una inteligencia policial responsable y respetuosa de los derechos fundamentales.

Estado de arte

Big Data aplicado a la seguridad pública

La acelerada transformación digital de las instituciones públicas ha convertido al Big Data en uno de los principales pilares de la seguridad pública contemporánea. Su incorporación en los sistemas policiales responde a la necesidad de procesar grandes volúmenes de información provenientes de fuentes heterogéneas, tales como registros criminales, llamadas de emergencia, sistemas de videovigilancia, dispositivos móviles, sensores urbanos, redes sociales, plataformas gubernamentales y bases de datos judiciales. A diferencia de los sistemas tradicionales de gestión de información, el Big Data permite integrar datos estructurados y no estructurados para generar conocimiento útil que fortalezca la inteligencia policial y facilite una toma de decisiones basada en evidencia.

Desde una perspectiva tecnológica, el Big Data se caracteriza por las denominadas cinco "V": volumen, velocidad, variedad, veracidad y valor. Estas dimensiones permiten comprender que el verdadero potencial del Big Data no radica únicamente en la acumulación masiva de información, sino en la capacidad de transformarla en conocimiento estratégico mediante herramientas de minería de datos, aprendizaje automático, inteligencia artificial y análisis predictivo. En consecuencia, las instituciones policiales han comenzado a sustituir modelos reactivos por sistemas analíticos capaces de anticipar riesgos delictivos y optimizar la asignación de recursos operativos.

El uso del Big Data ha fortalecido significativamente los procesos de inteligencia policial al facilitar la identificación de patrones espaciales y temporales del delito, detectar redes criminales, analizar vínculos entre personas y organizaciones, identificar tendencias emergentes y apoyar investigaciones complejas. Asimismo, la integración de información geoespacial con algoritmos predictivos permite elaborar mapas dinámicos de criminalidad y estimar probabilidades de ocurrencia delictiva en función de múltiples variables contextuales.

Diversas investigaciones coinciden en que el análisis masivo de datos representa un cambio de paradigma para la gestión de la seguridad pública. Sin embargo, este avance tecnológico también ha puesto de manifiesto importantes desafíos relacionados con la calidad de los datos, la gobernanza de la información y la transparencia de los algoritmos utilizados para apoyar la

toma de decisiones policiales. En este sentido, la eficacia de los modelos predictivos depende directamente de la representatividad, integridad y confiabilidad de las bases de datos que alimentan los sistemas analíticos.

Almasoud e Idowu (2025), en una revisión sistemática sobre equidad algorítmica en patrullaje predictivo, señalan: "Better data leads to better predictions." Esta afirmación sintetiza uno de los principios fundamentales de la ciencia de datos aplicada a la seguridad pública. La calidad del algoritmo nunca podrá superar la calidad de la información utilizada para entrenarlo. Bases de datos incompletas, desactualizadas o construidas sobre prácticas policiales históricamente sesgadas incrementan la probabilidad de generar predicciones erróneas y decisiones operativas injustas. En consecuencia, la gobernanza del dato constituye un requisito previo para cualquier estrategia de inteligencia policial basada en Big Data.

Desde otra perspectiva, la literatura reciente advierte que la utilización del Big Data no puede analizarse únicamente desde su capacidad tecnológica, sino también desde sus efectos institucionales y sociales. El desarrollo de modelos predictivos modifica la forma en que las organizaciones policiales priorizan recursos, seleccionan zonas de intervención y establecen criterios para la vigilancia preventiva. Esta transformación implica que los algoritmos dejan de ser simples herramientas informáticas para convertirse en instrumentos que influyen directamente en decisiones con impacto sobre los derechos fundamentales de las personas.

En este contexto, la discusión científica contemporánea sostiene que los sistemas de Big Data deben incorporar principios de transparencia, explicabilidad y supervisión humana. La inteligencia artificial aplicada a la seguridad pública no debe sustituir el juicio profesional de los analistas criminales, sino complementarlo mediante modelos que faciliten la interpretación de grandes cantidades de información y reduzcan la incertidumbre durante la planificación operativa.

Almasoud e Idowu (2025) concluyen igualmente que: "Police actions are the major driver of model discrimination." Esta conclusión representa uno de los hallazgos más relevantes de la investigación reciente sobre patrullaje predictivo. La discriminación algorítmica no se origina exclusivamente en el diseño matemático del modelo, sino en las prácticas institucionales reflejadas en los datos históricos utilizados para su entrenamiento.

Cuando determinados barrios reciben una vigilancia policial desproporcionada, los registros generados tienden a reforzar la percepción de mayor criminalidad, produciendo ciclos de retroalimentación que perpetúan el sobrepatrullaje y amplifican desigualdades preexistentes. Este fenómeno confirma que la implementación del Big Data debe acompañarse de auditorías algorítmicas, evaluación continua de la calidad de los datos y mecanismos de control institucional que permitan identificar y corregir sesgos antes de que afecten la toma de decisiones.

En consecuencia, el Big Data constituye una herramienta estratégica para modernizar la inteligencia policial y fortalecer la prevención del delito; sin embargo, su implementación responsable requiere combinar capacidades tecnológicas con principios éticos, supervisión humana, protección de datos personales y mecanismos permanentes de evaluación de la equidad algorítmica. Solo bajo estas condiciones será posible aprovechar el potencial analítico de estas tecnologías sin comprometer la legitimidad institucional ni los derechos fundamentales de la ciudadanía.

Patrullaje predictivo

El patrullaje predictivo constituye una estrategia de inteligencia policial basada en el análisis masivo de datos para anticipar la probabilidad de ocurrencia de eventos delictivos. A diferencia del patrullaje tradicional, cuyo despliegue responde principalmente a incidentes ya ocurridos o a criterios empíricos de los mandos policiales, este modelo utiliza algoritmos de aprendizaje automático, análisis espacial, minería de datos y sistemas de información geográfica para identificar patrones criminales y optimizar la distribución de recursos operativos.

Su desarrollo se encuentra estrechamente vinculado con el crecimiento del Big Data y de la inteligencia artificial, tecnologías que permiten procesar millones de registros provenientes de denuncias, llamadas de emergencia, antecedentes criminales, cámaras de videovigilancia, sensores urbanos y otras fuentes de información. Mediante el análisis de estas bases de datos es posible estimar zonas de riesgo (hot spots), horarios de mayor incidencia delictiva y modalidades criminales recurrentes, proporcionando información estratégica para la toma de decisiones preventivas.

Desde una perspectiva operativa, el patrullaje predictivo persigue incrementar la eficiencia institucional mediante una asignación más racional de los recursos policiales. La identificación anticipada de áreas con mayor probabilidad de incidencia delictiva permite focalizar la presencia policial, reducir tiempos de respuesta y fortalecer las capacidades de prevención situacional. Sin embargo, diversos estudios sostienen que la efectividad de estos modelos depende de la calidad de los datos utilizados para entrenar los algoritmos, así como de la supervisión permanente de sus resultados.

Asimismo, el patrullaje predictivo no debe entenderse como un mecanismo autónomo de toma de decisiones, sino como una herramienta de apoyo para la inteligencia policial. La interpretación de los resultados requiere la participación de analistas criminales y responsables operativos capaces de contextualizar la información generada por los modelos predictivos y valorar factores sociales, económicos y territoriales que los algoritmos no siempre logran representar adecuadamente.

"Evidence of effectiveness that can be used by policymakers still needs to be supported by more research." (Lee, Bradford, & Posch, 2024). La evidencia disponible muestra resultados prometedores, aunque todavía insuficientes para afirmar la eficacia universal del patrullaje predictivo.

Por otra parte, la literatura reciente enfatiza que la implementación de estos sistemas debe acompañarse de mecanismos de evaluación continua, transparencia y auditoría algorítmica. El uso indiscriminado de modelos predictivos puede generar decisiones automatizadas poco explicables y reproducir patrones históricos de vigilancia sobre determinados sectores de la población, afectando la legitimidad institucional.

"Predictive policing systems may reinforce historical patterns of policing." (Almasoud & Idowu, 2025). Esta afirmación evidencia la necesidad de revisar continuamente los datos de entrenamiento para evitar que los algoritmos reproduzcan sesgos históricos.

En consecuencia, el patrullaje predictivo representa una evolución significativa de la inteligencia policial hacia modelos preventivos basados en evidencia. No obstante, su implementación responsable requiere combinar innovación tecnológica, supervisión humana,

calidad de los datos y mecanismos de rendición de cuentas que garanticen el respeto a los derechos fundamentales y fortalezcan la confianza ciudadana.

Inteligencia Artificial en la Función Policial

La inteligencia artificial (IA) ha transformado los procesos de análisis de información dentro de las instituciones encargadas de la seguridad pública, al proporcionar herramientas capaces de procesar grandes volúmenes de datos con rapidez y precisión. En el ámbito policial, la IA permite identificar patrones delictivos, reconocer comportamientos anómalos, analizar redes criminales y generar modelos predictivos que apoyan la toma de decisiones estratégicas y operativas. Su integración con el Big Data ha favorecido el desarrollo de sistemas inteligentes orientados a fortalecer la prevención del delito y optimizar la distribución de recursos.

Los algoritmos de aprendizaje automático (Machine Learning) constituyen una de las aplicaciones más utilizadas en la función policial. Estos modelos aprenden a partir de datos históricos para identificar relaciones entre variables y estimar probabilidades de ocurrencia de eventos futuros. Dependiendo del problema de análisis, pueden emplearse algoritmos supervisados, no supervisados o de aprendizaje profundo (Deep Learning), los cuales ofrecen diferentes niveles de precisión para el reconocimiento de patrones criminales.

Otra aplicación relevante corresponde al procesamiento del lenguaje natural (Natural Language Processing), que facilita el análisis automatizado de denuncias, informes policiales, publicaciones en redes sociales y otras fuentes documentales. Asimismo, las técnicas de visión por computadora permiten analizar imágenes provenientes de sistemas de videovigilancia, detectar objetos, reconocer matrículas vehiculares y apoyar la búsqueda de personas desaparecidas o sospechosas, siempre bajo los principios de legalidad y protección de datos personales.

No obstante, la creciente automatización de los procesos de inteligencia policial también plantea desafíos relacionados con la transparencia, la explicabilidad de los modelos y la supervisión humana. La toma de decisiones basada exclusivamente en algoritmos puede afectar la confianza pública si no existen mecanismos que permitan comprender cómo se generan las predicciones y cuáles son las variables que influyen en los resultados.

"AI should augment, not replace, human decision-making." (UNESCO, 2021). La inteligencia artificial debe apoyar el trabajo policial, pero las decisiones finales deben permanecer bajo responsabilidad humana.

Asimismo, la literatura científica reciente sostiene que la adopción de sistemas inteligentes exige incorporar principios éticos desde el diseño de los algoritmos, garantizando transparencia, equidad y responsabilidad institucional durante todo su ciclo de vida.

"Trustworthy AI requires lawful, ethical and robust systems." (European Commission, 2021). La confianza en la IA depende no solo de su precisión técnica, sino también del cumplimiento de principios éticos y jurídicos. En consecuencia, la inteligencia artificial representa una herramienta estratégica para fortalecer la inteligencia policial y mejorar la capacidad de prevención del delito. Sin embargo, su implementación debe sustentarse en modelos transparentes, auditables y supervisados por especialistas que garanticen el respeto a los derechos humanos, la protección de datos personales y la rendición de cuentas institucional.

Teorías Criminológicas Aplicadas al Patrullaje Predictivo

El patrullaje predictivo encuentra su sustento científico en diversas teorías criminológicas que explican la distribución espacial y temporal del delito. Estas teorías permiten comprender por qué determinados lugares concentran una mayor incidencia delictiva y cómo las variables ambientales, sociales y situacionales influyen en la conducta criminal. En este sentido, el Big Data y la inteligencia artificial no sustituyen las teorías criminológicas, sino que fortalecen su capacidad explicativa mediante el análisis de grandes volúmenes de información.

Una de las teorías con mayor influencia es la Teoría de las Actividades Cotidianas (Routine Activity Theory), propuesta por Cohen y Felson, la cual sostiene que un delito ocurre cuando convergen un infractor motivado, un objetivo adecuado y la ausencia de un guardián capaz de impedir la conducta delictiva. Actualmente, los algoritmos de patrullaje predictivo utilizan variables relacionadas con movilidad urbana, horarios de mayor actividad, densidad poblacional y características ambientales para identificar escenarios donde dicha convergencia resulta más probable.

Complementariamente, la Teoría de los Patrones del Delito (Crime Pattern Theory) explica que los delincuentes desarrollan sus actividades dentro de espacios geográficos conocidos,

generando patrones relativamente estables que pueden identificarse mediante análisis geoespacial. Esta teoría constituye uno de los principales fundamentos para la elaboración de mapas de calor (hot spots) utilizados por los sistemas de patrullaje predictivo.

Otra aportación relevante corresponde a la Teoría de la Elección Racional (Rational Choice Theory), según la cual los delincuentes realizan una valoración entre los beneficios esperados y los riesgos asociados a la comisión del delito. Bajo esta perspectiva, la presencia policial focalizada en zonas de alta incidencia incrementa la percepción del riesgo y puede actuar como mecanismo de disuasión.

Las investigaciones recientes también destacan la importancia del enfoque de Hot Spots Policing, estrategia basada en la concentración de recursos policiales en áreas geográficas donde se registra una elevada frecuencia delictiva. La combinación entre Big Data, sistemas de información geográfica e inteligencia artificial ha incrementado la precisión para identificar estos puntos críticos y mejorar la eficiencia operativa de las instituciones policiales.

"Hot spots policing is among the most effective proactive policing strategies." (National Institute of Justice, 2021). La evidencia muestra que focalizar recursos en zonas críticas mejora la prevención cuando la intervención está sustentada en evidencia. No obstante, diversos autores advierten que las teorías criminológicas deben complementarse con el análisis de factores sociales y comunitarios para evitar interpretaciones reduccionistas del fenómeno criminal. El delito responde a múltiples causas que no siempre pueden explicarse únicamente mediante modelos espaciales o estadísticos.

"Crime is concentrated at very small places." (Weisburd, 2021). Comentario. La concentración espacial del delito justifica el empleo de análisis geoespacial, aunque no elimina la necesidad de comprender los factores sociales que lo originan. En consecuencia, las teorías criminológicas proporcionan el fundamento conceptual sobre el cual operan los sistemas de patrullaje predictivo. La integración de estos enfoques con herramientas de Big Data e inteligencia artificial permite mejorar la capacidad de anticipación de las instituciones policiales; sin embargo, la eficacia de dichos modelos depende de una adecuada interpretación criminológica de los datos y de estrategias preventivas que consideren tanto las variables espaciales como los factores sociales asociados a la criminalidad.

Sesgos Algorítmicos en el Patrullaje Predictivo

El crecimiento del Big Data y de la inteligencia artificial en la seguridad pública ha permitido desarrollar modelos predictivos con una elevada capacidad para identificar patrones delictivos y apoyar la toma de decisiones policiales. Sin embargo, el desempeño de estos sistemas depende directamente de la calidad, representatividad y neutralidad de los datos utilizados durante su entrenamiento. Cuando las bases de datos contienen errores, omisiones o reflejan prácticas institucionales históricamente discriminatorias, los algoritmos pueden reproducir e incluso amplificar dichos sesgos, afectando la objetividad del proceso de inteligencia policial.

Los sesgos algorítmicos pueden definirse como errores sistemáticos producidos por datos, modelos matemáticos o procesos de decisión automatizados que generan resultados desiguales para determinados individuos o grupos sociales. En el ámbito policial, estos sesgos pueden manifestarse mediante una vigilancia desproporcionada sobre determinadas zonas geográficas, perfiles sociodemográficos o comunidades históricamente sujetas a una mayor presencia policial.

Entre los principales tipos de sesgos identificados en la literatura científica destacan el sesgo histórico, derivado de registros policiales que reflejan prácticas pasadas de vigilancia selectiva; el sesgo de selección, ocasionado por muestras de datos incompletas o poco representativas; el sesgo de confirmación, cuando los operadores interpretan los resultados del algoritmo como evidencia suficiente para reforzar hipótesis previas; y el denominado feedback loop, fenómeno mediante el cual el incremento del patrullaje en determinadas áreas produce más registros policiales, fortaleciendo nuevamente la predicción de riesgo sobre los mismos lugares.

Estos problemas adquieren especial relevancia porque los algoritmos aprenden a partir de datos históricos. Si una comunidad ha sido objeto de una vigilancia policial intensiva durante años, es probable que exista un mayor número de registros delictivos en esa zona, independientemente de que la incidencia real sea superior a la de otros sectores. En consecuencia, el algoritmo interpreta esos datos como evidencia objetiva y recomienda incrementar nuevamente la presencia policial, generando un ciclo de retroalimentación difícil de romper.

Asimismo, diversos investigadores sostienen que la aparente neutralidad matemática de los modelos predictivos puede ocultar desigualdades estructurales. La objetividad de un algoritmo depende de la calidad de la información utilizada para entrenarlo y de los criterios empleados durante su diseño, validación y evaluación. Por ello, la equidad algorítmica constituye actualmente uno de los principales desafíos para la implementación responsable de la inteligencia artificial en la seguridad pública.

"Police actions are a major contributor to model discrimination." (Almasoud & Idowu, 2025). La principal fuente del sesgo suele encontrarse en los datos históricos y no exclusivamente en el algoritmo.

De igual manera, la literatura reciente enfatiza la necesidad de incorporar mecanismos permanentes de auditoría que permitan identificar posibles discriminaciones antes de que los modelos sean utilizados para apoyar decisiones operativas.

"Algorithmic fairness is not achieved automatically through technical improvements." (Kasy, 2024). La equidad requiere controles técnicos, jurídicos e institucionales durante todo el ciclo de vida del sistema. Frente a estos desafíos, organismos internacionales han promovido el desarrollo de principios de IA responsable, orientados a garantizar transparencia, explicabilidad, trazabilidad y supervisión humana significativa. La auditoría algorítmica, la evaluación continua del desempeño, la revisión periódica de las bases de datos y la participación de equipos multidisciplinarios constituyen estrategias fundamentales para reducir el riesgo de discriminación y fortalecer la legitimidad de los sistemas de patrullaje predictivo.

En consecuencia, los sesgos algorítmicos representan uno de los mayores retos para la implementación del Big Data en la seguridad pública. Si bien estas tecnologías ofrecen importantes ventajas para la prevención del delito, su utilización debe estar acompañada de mecanismos de gobernanza, control institucional y evaluación independiente que garanticen decisiones objetivas, transparentes y compatibles con los principios de igualdad, no discriminación y respeto a los derechos humanos.

Privacidad y Protección de Datos en el Patrullaje Predictivo

La implementación del Big Data y la inteligencia artificial en la seguridad pública implica el tratamiento de grandes volúmenes de datos personales, incluyendo información biométrica,

registros de geolocalización, imágenes de videovigilancia, antecedentes policiales y datos provenientes de dispositivos digitales. Si bien estos recursos fortalecen la capacidad de prevención e investigación del delito, también incrementan los riesgos asociados con la privacidad, la protección de datos personales y el ejercicio de los derechos fundamentales. En consecuencia, la eficacia tecnológica debe armonizarse con principios jurídicos y éticos que regulen el uso legítimo de la información.

El tratamiento masivo de datos exige que las instituciones policiales observen principios como la legalidad, finalidad, proporcionalidad, minimización de datos, transparencia y responsabilidad. Estos principios buscan garantizar que la recopilación y el procesamiento de información respondan exclusivamente a fines legítimos de seguridad pública y que no generen prácticas de vigilancia indiscriminada o utilización indebida de datos personales.

Uno de los principales desafíos consiste en evitar que la búsqueda de mayor eficiencia operativa derive en mecanismos de vigilancia masiva incompatibles con un Estado democrático de derecho. La utilización de tecnologías como el reconocimiento facial, la videovigilancia inteligente y los sistemas de monitoreo automatizado debe encontrarse sujeta a controles institucionales, supervisión judicial cuando corresponda y mecanismos efectivos de rendición de cuentas.

La protección de la privacidad también constituye un elemento esencial para fortalecer la confianza ciudadana en las instituciones encargadas de la seguridad pública. La transparencia respecto del tratamiento de los datos, la existencia de auditorías independientes y la implementación de políticas de ciberseguridad reducen el riesgo de uso indebido de la información y favorecen la legitimidad de los sistemas de inteligencia policial.

"Privacy should be protected throughout the AI system lifecycle." (UNESCO, 2021). Comentario. La protección de la privacidad debe incorporarse desde el diseño hasta la operación y evaluación de los sistemas de inteligencia artificial.

Asimismo, la regulación internacional reconoce que el desarrollo de sistemas inteligentes debe garantizar un equilibrio entre innovación tecnológica y protección de los derechos fundamentales.

AI systems should be human-centric and trustworthy." (European Parliament, 2024). La innovación tecnológica debe estar orientada al bienestar de las personas y sustentarse en principios de transparencia y responsabilidad.

En este contexto, la gobernanza de datos adquiere un papel estratégico para asegurar que las herramientas de patrullaje predictivo operen bajo criterios de legalidad, necesidad y proporcionalidad. La incorporación de evaluaciones de impacto, auditorías periódicas y supervisión humana permite reducir riesgos asociados con la privacidad y fortalece la legitimidad de las decisiones apoyadas por inteligencia artificial.

Panorama Internacional del Patrullaje Predictivo

Durante la última década, el patrullaje predictivo ha sido implementado en diversos países como una estrategia para fortalecer la prevención del delito mediante el uso de Big Data e inteligencia artificial. Estados Unidos ha liderado este proceso con el desarrollo de plataformas como PredPol, HunchLab y Risk Terrain Modeling (RTM), las cuales emplean algoritmos para identificar zonas de alta incidencia delictiva y optimizar la distribución de recursos policiales. Estas experiencias han servido como referencia para otras jurisdicciones interesadas en incorporar tecnologías predictivas en sus sistemas de seguridad pública.

En Europa, países como el Reino Unido, Alemania y los Países Bajos han impulsado proyectos orientados al análisis predictivo de la criminalidad, aunque bajo marcos regulatorios más estrictos en materia de protección de datos y derechos fundamentales. La entrada en vigor del Reglamento Europeo de Inteligencia Artificial representa un paso importante hacia la regulación de los sistemas algorítmicos utilizados por las autoridades públicas, estableciendo obligaciones específicas para aplicaciones consideradas de alto riesgo.

En Asia y Oceanía también se observa un crecimiento sostenido del uso de inteligencia artificial en funciones policiales, particularmente en el análisis de videovigilancia, reconocimiento facial y gestión inteligente de emergencias. Sin embargo, la evidencia científica coincide en que la eficacia de estas tecnologías depende tanto de la calidad de los datos como de los mecanismos de supervisión y control implementados por cada institución.

"Predictive policing remains an evolving field with mixed empirical evidence." (Lee, Bradford, & Posch, 2024). Los resultados disponibles muestran beneficios operativos, aunque la evidencia aún no es concluyente.

Por otra parte, la investigación internacional destaca la importancia de desarrollar modelos transparentes y auditables para fortalecer la legitimidad institucional.

"Algorithmic accountability is essential for public trust." (OECD, 2024). La confianza ciudadana depende de la transparencia y de la posibilidad de supervisar el funcionamiento de los algoritmos. En términos generales, la literatura internacional evidencia que el patrullaje predictivo ofrece importantes oportunidades para mejorar la eficiencia policial; no obstante, su implementación responsable requiere marcos normativos sólidos, supervisión permanente y mecanismos efectivos de evaluación de impacto.

Experiencias en América Latina

En América Latina, la incorporación del Big Data y de la inteligencia artificial en la seguridad pública se encuentra en una fase de desarrollo desigual. Países como Brasil, Chile, Colombia y México han impulsado iniciativas orientadas al análisis geoespacial del delito, sistemas de videovigilancia inteligente y plataformas de análisis criminal; sin embargo, la producción científica regional continúa siendo limitada en comparación con Europa y Estados Unidos.

Las principales experiencias latinoamericanas muestran avances en la integración de bases de datos policiales, sistemas de georreferenciación y centros de comando y control. No obstante, persisten desafíos relacionados con la interoperabilidad de la información, la calidad de los datos, la disponibilidad de personal especializado y la existencia de marcos regulatorios específicos para el uso de inteligencia artificial en seguridad pública.

Diversos estudios coinciden en que la adopción de estas tecnologías debe acompañarse de procesos de fortalecimiento institucional, capacitación continua y mecanismos de evaluación que permitan medir su impacto real sobre la reducción de la criminalidad y la protección de los derechos humanos.

"Artificial intelligence governance is a prerequisite for trustworthy public services." (UNESCO, 2021). La modernización tecnológica requiere instituciones capaces de garantizar un uso responsable de la inteligencia artificial. Asimismo, la evidencia disponible señala que la cooperación interinstitucional constituye un elemento clave para el éxito de las estrategias de inteligencia policial basadas en datos.

"Data sharing enhances evidence-based public decision-making." (OECD, 2024). Comentario. El intercambio seguro de información fortalece la capacidad analítica y mejora la coordinación entre instituciones. En consecuencia, América Latina enfrenta el reto de aprovechar el potencial del Big Data para fortalecer la seguridad pública sin reproducir desigualdades estructurales ni comprometer la protección de los derechos fundamentales. El desarrollo de políticas públicas orientadas a la gobernanza de datos, la formación especializada y la supervisión ética será determinante para consolidar modelos de patrullaje predictivo confiables y sostenibles.

Metodología

La investigación se desarrolló bajo un enfoque cualitativo, mediante una revisión sistemática de literatura siguiendo los lineamientos de la declaración PRISMA 2020. Se consultaron artículos científicos publicados entre 2021 y 2026 en las bases de datos Scopus, Web of Science, ScienceDirect, SpringerLink e IEEE Xplore, empleando palabras clave relacionadas con Big Data, predictive policing, artificial intelligence, algorithmic bias y privacy.

Se incluyeron investigaciones revisadas por pares, escritas en inglés y español, relacionadas con la aplicación del Big Data en la seguridad pública. Se excluyeron documentos duplicados, literatura gris y estudios sin revisión científica. La información obtenida fue organizada mediante análisis temático para identificar tendencias, beneficios, riesgos y desafíos del patrullaje predictivo.

Resultados

La revisión sistemática de literatura permitió identificar las principales tendencias científicas relacionadas con la aplicación del Big Data en el patrullaje predictivo durante el período comprendido entre 2021 y 2026. El análisis temático de los estudios seleccionados evidenció que las investigaciones pueden agruparse en cinco grandes ejes: (i) fortalecimiento de la

inteligencia policial mediante el análisis masivo de datos; (ii) optimización de la asignación de recursos policiales; (iii) impacto de los sesgos algorítmicos sobre la equidad de las decisiones; (iv) protección de la privacidad y gobernanza de datos; y (v) necesidad de mecanismos de transparencia, auditoría y supervisión humana.

En relación con el primer eje, la mayoría de los estudios coincide en que la integración de tecnologías de Big Data con herramientas de inteligencia artificial incrementa significativamente la capacidad analítica de las instituciones encargadas de la seguridad pública. La combinación de registros policiales, sistemas de videovigilancia, sensores urbanos, información geoespacial y bases de datos institucionales facilita la identificación de patrones espacio-temporales de la criminalidad, permitiendo elaborar modelos predictivos orientados a la prevención del delito y a una toma de decisiones sustentada en evidencia.

Respecto a la optimización operativa, la literatura revisada demuestra que los sistemas de patrullaje predictivo permiten distribuir de manera más eficiente los recursos policiales mediante la identificación anticipada de zonas de riesgo (*hot spots*), horarios de mayor incidencia delictiva y modalidades criminales recurrentes. Esta capacidad predictiva favorece una planificación estratégica del patrullaje, reduce tiempos de respuesta y fortalece los procesos de inteligencia policial. Sin embargo, los estudios también advierten que la efectividad de estos modelos depende directamente de la calidad, integridad y actualización permanente de las bases de datos utilizadas para entrenar los algoritmos.

Un hallazgo recurrente identificado en la revisión corresponde a la existencia de sesgos algorítmicos derivados de los datos históricos empleados durante el entrenamiento de los modelos predictivos. Diversos autores coinciden en señalar que la discriminación algorítmica no proviene exclusivamente del diseño matemático de los algoritmos, sino de las prácticas policiales históricas reflejadas en las bases de datos. Cuando determinadas comunidades han sido objeto de una vigilancia intensiva durante largos períodos, los sistemas predictivos tienden a reforzar dichas intervenciones, generando ciclos de retroalimentación (*feedback loops*) que pueden reproducir desigualdades territoriales y sociales.

Otro resultado relevante evidencia que la incorporación de inteligencia artificial en la seguridad pública ha incrementado el interés por desarrollar mecanismos de gobernanza de datos y protección de los derechos fundamentales. La mayoría de los estudios revisados destaca la

necesidad de implementar principios de legalidad, transparencia, proporcionalidad y minimización de datos para garantizar un tratamiento responsable de la información personal utilizada por los sistemas predictivos. Asimismo, se reconoce que la confianza ciudadana depende, en gran medida, de la existencia de políticas claras sobre privacidad, trazabilidad de la información y rendición de cuentas.

Finalmente, la revisión permitió identificar un amplio consenso respecto a que el patrullaje predictivo no debe sustituir el criterio profesional de los analistas criminales, sino constituirse como una herramienta complementaria para apoyar la toma de decisiones estratégicas. En este contexto, la supervisión humana, las auditorías algorítmicas, la evaluación continua del desempeño de los modelos y la explicabilidad de los algoritmos emergen como condiciones indispensables para una implementación responsable del Big Data en la seguridad pública.

En conjunto, los hallazgos obtenidos evidencian que el éxito del patrullaje predictivo depende no solamente del desarrollo tecnológico de los algoritmos, sino también de la calidad de los datos, la existencia de marcos regulatorios sólidos, la transparencia institucional y el respeto permanente de los derechos humanos.

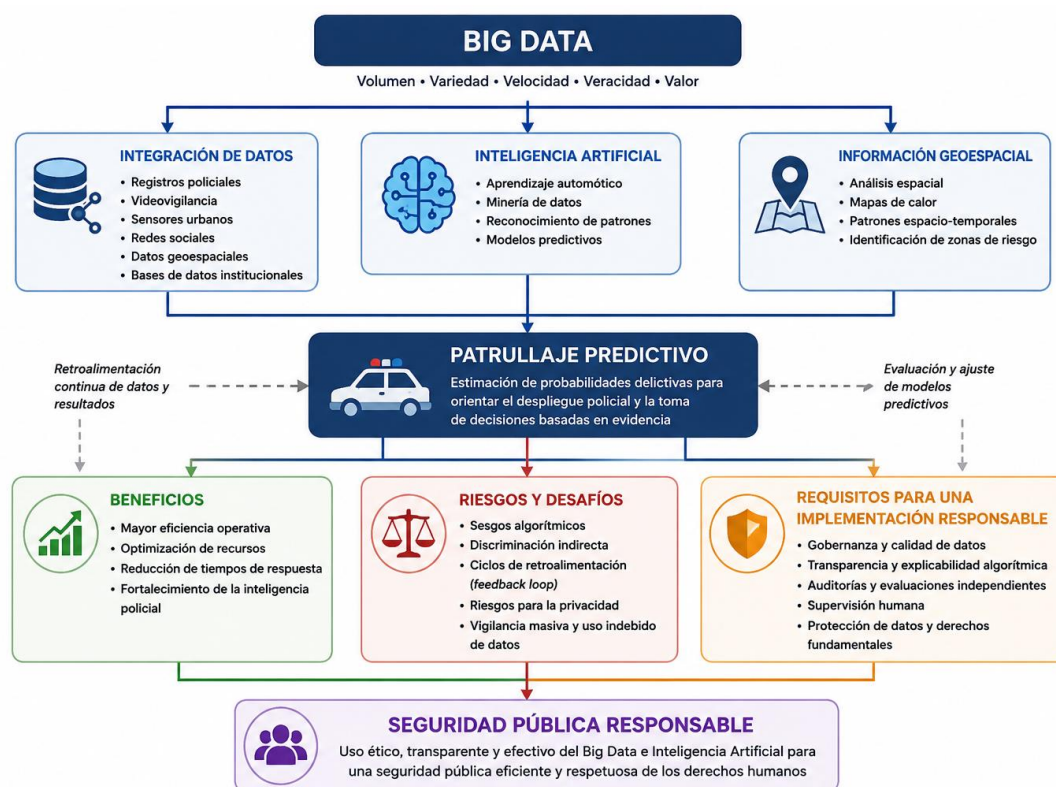
Tabla 1.
Síntesis de los principales hallazgos identificados en la revisión sistemática

Categoría de análisis	Hallazgos encontrados	Principales beneficios	Desafíos identificados
Big Data aplicado a la seguridad pública	Integración de información proveniente de registros policiales, videovigilancia, sensores urbanos, geolocalización y bases de datos institucionales.	Incremento de la capacidad analítica, mejor comprensión de patrones delictivos y fortalecimiento de la inteligencia policial.	Calidad de los datos, interoperabilidad entre sistemas y actualización permanente de la información.
Patrullaje predictivo	Utilización de algoritmos de aprendizaje automático para estimar probabilidades de ocurrencia delictiva e identificar zonas de riesgo.	Optimización del despliegue policial, reducción de tiempos de respuesta y focalización de recursos preventivos.	Evidencia empírica aún limitada respecto al impacto directo sobre la reducción de la criminalidad.
Inteligencia Artificial	Automatización del análisis criminal mediante técnicas de Machine Learning y minería de datos.	Apoyo a la toma de decisiones estratégicas y operativas con mayor rapidez y precisión.	Necesidad de explicabilidad de los modelos y supervisión humana permanente.
Sesgos algorítmicos	Reproducción de patrones históricos de vigilancia debido al entrenamiento con datos sesgados.	Impulso al desarrollo de metodologías de auditoría y evaluación de equidad algorítmica.	Discriminación indirecta, sobrepatrullaje de determinados sectores y ciclos de

			retroalimentación (<i>feedback loop</i>).
Privacidad y protección de datos	Tratamiento masivo de información personal, biométrica y geoespacial para apoyar procesos de inteligencia policial.	Mayor capacidad de prevención e investigación del delito basada en evidencia.	Riesgos de vigilancia masiva, vulneración de la privacidad y uso indebido de datos personales.
Gobernanza y regulación	Desarrollo progresivo de principios de inteligencia artificial responsable y marcos regulatorios internacionales.	Mayor transparencia institucional, fortalecimiento de la confianza pública y protección de los derechos fundamentales.	Implementación desigual entre países y ausencia de estándares homogéneos para la evaluación de sistemas predictivos.

Fuente: Elaboración propia con base en la revisión sistemática de literatura desarrollada en el presente estudio.

Figura 1.
Conceptual de síntesis de los resultados



La incorporación de esta tabla y de la figura conceptual permite sintetizar visualmente los resultados obtenidos durante la revisión sistemática y evidencia la relación existente entre las capacidades tecnológicas del Big Data, los beneficios operativos del patrullaje predictivo y los desafíos éticos, jurídicos y organizacionales que deben abordarse para garantizar una implementación responsable en los sistemas modernos de seguridad pública. Esta

representación facilita la comprensión de los hallazgos y aporta mayor solidez metodológica al artículo, al integrar en un esquema único las principales dimensiones identificadas durante el análisis de la literatura.

Discusión

Los resultados de la revisión sistemática permiten afirmar que el Big Data representa una de las principales transformaciones tecnológicas en la gestión contemporánea de la seguridad pública, al favorecer la transición desde modelos reactivos hacia estrategias preventivas sustentadas en el análisis masivo de datos. La evidencia científica analizada coincide en que la integración de inteligencia artificial, aprendizaje automático y análisis geoespacial fortalece significativamente la capacidad de las instituciones policiales para identificar patrones delictivos, estimar zonas de riesgo y optimizar la asignación de recursos operativos. En este sentido, el patrullaje predictivo constituye una herramienta con alto potencial para mejorar la eficiencia institucional y apoyar la toma de decisiones basada en evidencia.

Sin embargo, los hallazgos también demuestran que la efectividad de estos sistemas no depende exclusivamente del desarrollo tecnológico de los algoritmos, sino principalmente de la calidad, representatividad y gobernanza de los datos utilizados para su entrenamiento. La revisión evidencia que bases de datos incompletas, desactualizadas o construidas sobre registros históricos sesgados afectan directamente la precisión de las predicciones y pueden generar decisiones operativas poco confiables. Este resultado coincide con la literatura reciente, que identifica a los datos históricos como la principal fuente de discriminación en los sistemas de patrullaje predictivo, por encima de los propios modelos matemáticos. En consecuencia, la calidad de la información debe considerarse un requisito indispensable para el desarrollo de sistemas predictivos confiables y socialmente legítimos.

Otro aspecto ampliamente documentado durante la revisión corresponde a la persistencia de los sesgos algorítmicos como uno de los principales desafíos para la inteligencia artificial aplicada a la seguridad pública. Los estudios revisados muestran que los algoritmos pueden reproducir desigualdades existentes cuando son entrenados con información que refleja prácticas policiales históricamente selectivas. Este fenómeno genera ciclos de retroalimentación (feedback loops) que incrementan la vigilancia sobre determinados territorios y grupos sociales, afectando principios fundamentales como la igualdad, la no discriminación y la proporcionalidad. En

consecuencia, la literatura coincide en señalar que la equidad algorítmica requiere procesos permanentes de auditoría, evaluación independiente y revisión continua de los modelos predictivos.

La revisión también pone de manifiesto que la discusión científica ha evolucionado desde una perspectiva centrada únicamente en la precisión técnica hacia un enfoque multidimensional que incorpora aspectos éticos, jurídicos e institucionales. En la actualidad, la confianza en los sistemas de patrullaje predictivo depende tanto de su capacidad para anticipar eventos delictivos como de la transparencia en el funcionamiento de los algoritmos, la explicabilidad de los modelos, la trazabilidad de las decisiones y la existencia de mecanismos efectivos de rendición de cuentas. Bajo esta perspectiva, la supervisión humana continúa siendo un componente esencial para interpretar adecuadamente los resultados generados por la inteligencia artificial y contextualizarlos dentro de las realidades sociales, económicas y criminológicas que los algoritmos no siempre consiguen representar.

En materia de privacidad y protección de datos personales, los resultados evidencian que el incremento en la capacidad de procesamiento de información también incrementa la responsabilidad institucional respecto al tratamiento de datos sensibles. El uso de registros biométricos, sistemas de videovigilancia, información geoespacial y otras fuentes digitales exige la aplicación de principios de legalidad, necesidad, proporcionalidad, minimización de datos y seguridad de la información. De esta manera, la protección de la privacidad no constituye únicamente una obligación normativa, sino un elemento estratégico para fortalecer la legitimidad institucional y consolidar la confianza ciudadana en el uso de tecnologías de inteligencia artificial dentro de la seguridad pública.

Asimismo, la revisión sistemática permitió identificar diferencias importantes entre las experiencias internacionales y las desarrolladas en América Latina. Mientras que diversos países europeos y Estados Unidos han alcanzado mayores niveles de madurez tecnológica y regulatoria en la implementación del patrullaje predictivo, la región latinoamericana aún enfrenta limitaciones relacionadas con la interoperabilidad de los sistemas de información, la disponibilidad de infraestructura tecnológica, la capacitación especializada del personal y la consolidación de marcos regulatorios específicos sobre inteligencia artificial y gobernanza de datos. Estas diferencias evidencian la necesidad de fortalecer la investigación regional y

desarrollar modelos adaptados a las características institucionales y sociales de los países latinoamericanos.

Derivado de estos hallazgos, la presente investigación propone un Modelo Integral de Patrullaje Predictivo Responsable, concebido como una respuesta a las principales fortalezas y limitaciones identificadas durante la revisión sistemática. A diferencia de enfoques centrados exclusivamente en el rendimiento de los algoritmos, el modelo integra ocho componentes estratégicos: recolección ética de datos, integración de Big Data, limpieza y validación de la información, utilización de modelos de inteligencia artificial explicables, auditoría permanente de sesgos algorítmicos, supervisión humana especializada, protección de datos personales y evaluación continua del sistema. La articulación de estos elementos busca garantizar que la innovación tecnológica se desarrolle dentro de un marco de transparencia, responsabilidad institucional y respeto por los derechos fundamentales.

Desde una perspectiva científica, esta propuesta constituye un aporte conceptual al integrar dimensiones tecnológicas, organizacionales, jurídicas y éticas en un único marco de referencia para la implementación del patrullaje predictivo. Mientras gran parte de la literatura revisada aborda estos componentes de forma independiente, el modelo desarrollado en este estudio plantea una visión sistémica en la que la gobernanza de datos, la auditoría algorítmica y la supervisión humana actúan como mecanismos complementarios para fortalecer la confiabilidad de las decisiones apoyadas por inteligencia artificial. En consecuencia, el modelo no solo busca incrementar la eficiencia operativa de las instituciones policiales, sino también fortalecer su legitimidad democrática mediante procesos transparentes y auditables.

Desde el punto de vista práctico, la propuesta adquiere especial relevancia para las instituciones de seguridad pública que se encuentran en procesos de transformación digital, al ofrecer una guía para implementar tecnologías predictivas bajo criterios de legalidad, proporcionalidad y responsabilidad pública. La incorporación de mecanismos permanentes de evaluación y mejora continua favorece la adaptación del sistema a nuevos escenarios delictivos y reduce el riesgo de reproducir sesgos históricos, contribuyendo al fortalecimiento de una inteligencia policial basada en evidencia y orientada a la protección de los derechos humanos.

Finalmente, la revisión sistemática evidencia que el futuro del patrullaje predictivo dependerá de la capacidad de las instituciones para equilibrar innovación tecnológica y responsabilidad

ética. La consolidación de modelos de gobernanza de datos, el fortalecimiento de la transparencia algorítmica, la evaluación independiente de los sistemas de inteligencia artificial y la participación de equipos multidisciplinarios serán factores determinantes para garantizar que estas tecnologías contribuyan efectivamente a la prevención del delito sin comprometer los principios democráticos ni los derechos fundamentales de la ciudadanía. En este contexto, futuras investigaciones deberán profundizar en la validación empírica del modelo propuesto, evaluar su aplicabilidad en distintos entornos institucionales y desarrollar indicadores que permitan medir de manera objetiva tanto su eficacia operativa como su impacto en la equidad, la transparencia y la confianza pública.

Conclusiones

El Big Data representa una herramienta estratégica para fortalecer la inteligencia policial y optimizar el patrullaje predictivo mediante el análisis de grandes volúmenes de información. Sin embargo, su eficacia depende de la calidad de los datos, la transparencia de los algoritmos y la supervisión humana.

Los sesgos algorítmicos y los riesgos para la privacidad constituyen los principales desafíos para su implementación. En consecuencia, las instituciones de seguridad pública deben adoptar modelos de gobernanza de datos, auditorías algorítmicas y principios de inteligencia artificial responsable que garanticen la protección de los derechos fundamentales y fortalezcan la confianza ciudadana.

Referencias bibliográficas

- Almasoud, A. S., & Idowu, J. A. (2025). Algorithmic fairness in predictive policing. *AI and Ethics*, 5, 2323–2337. <https://doi.org/10.1007/s43681-024-00541-3>
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
- Kasy, M. (2024). Algorithmic bias and racial inequality: A critical review. *Oxford Review of Economic Policy*, 40(3), 530–546.

Lee, Y., Bradford, B., & Posch, K. (2024). The effectiveness of Big Data-driven predictive policing: A systematic review. *Justice Evaluation Journal*, 7(2), 127–160.

National Institute of Justice. (2021). Hot spots policing and crime prevention. U.S. Department of Justice.

Organisation for Economic Co-operation and Development. (2024). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD.

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO.
<https://unesdoc.unesco.org/ark:/48223/pf0000381137>

Weisburd, D. (2021). Hot spots of crime and place-based policing. *Annual Review of Criminology*, 4, 149–167. <https://doi.org/10.1146/annurev-criminol-061020-021407>

Declaraciones finales

Conflicto de intereses: Los autores declaran que no existe conflicto de interés posible.

Financiamiento: No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento: N/A

Nota editorial: El artículo no deriva de una publicación anterior ni se encuentra sometido simultáneamente a otra revista.