

# RIS

Revista de Inteligencia y  
Seguridad

**“NUEVO GLOSARIO Y PARADIGMAS DE LA DEFENSA Y  
SEGURIDAD: NORLATINISMO, INTELIGENCIA, CIUDADANA Y  
NORMATIVIDAD EMERGENTE”**

**NÚMERO 3  
(ENERO-JUNIO 2025)**

ISSN 2992-7455  
[www.inap.mx/ris](http://www.inap.mx/ris)





# RIS

## Revista de Inteligencia y Seguridad

Número 3  
(enero-junio 2025)

**“NUEVO GLOSARIO Y PARADIGMAS DE LA DEFENSA Y  
SEGURIDAD: NORLATINISMO, INTELIGENCIA CIUDADANA Y  
NORMATIVIDAD EMERGENTE”**



**Revista de Inteligencia y Seguridad**, No. 3, enero-junio 2025, es una publicación semestral digital ([www.inap.mx/ris](http://www.inap.mx/ris)), editada por el Instituto Nacional de Administración Pública, ubicado en Km. 14.5 Carretera México-Toluca No. 2151, Col. Palo Alto, C.P. 05110, Alcaldía de Cuajimalpa, Ciudad de México. Teléfono (55) 5081 2657. [www.inap.mx](http://www.inap.mx)  
[contacto@inap.org.mx](mailto:contacto@inap.org.mx)

Editor responsable: Rafael Martínez Puón.  
Reserva de Derechos al Uso Exclusivo No. 04-2023-032713274000-102, otorgado por Instituto Nacional del Derecho de Autor.  
ISSN: 2992-7455

Las opiniones expresadas en esta revista son estrictamente responsabilidad de los autores. La RIS, el INAP o las instituciones a las que están asociados no asumen responsabilidad por ellas.

Se autoriza la reproducción total o parcial de los artículos, citando la fuente, siempre y cuando sea sin fines de lucro.



## **Consejo Directivo 2023-2026**

Luis Miguel Martínez Anzures  
**Presidente**

Olga Sánchez Cordero  
**Vicepresidenta**

Rafael Enrique Valenzuela Mendoza  
**Vicepresidente para los IAPs de los Estados 2025-2026**

Armando Alfonzo Jiménez  
**Secretario Ejecutivo del INAP**

Rafael Martínez Puón  
**Director de la Escuela Nacional de Profesionalización Gubernamental**

## **CONSEJEROS**

Rina Aguilera Hintelholher  
Eber Omar Betanzos Torres  
Esther Nissán Schoenfeld  
David Villanueva Lomelí  
Susana Libián Díaz González  
Gerardo Felipe Laveaga Rendón  
Laura Enríquez Rodríguez  
Luis Humberto Fernández Fuentes

Ricardo Corral Luna  
**Director de Consultoría**

Luis Armando Carranza Camarena  
**Director de Administración y Finanzas**

## **CONSEJO DE HONOR**

Luis García Cárdenas  
José Natividad González Parás  
Alejandro Carrillo Castro  
José R. Castelazo  
Carlos Reta Martínez

## **IN MEMORIAM**

Gabino Fraga Magaña  
Gustavo Martínez Cabañas  
Andrés Caso Lombardo  
Raúl Salinas Lozano  
Ignacio Pichardo Pagaza  
Adolfo Lugo Verduzco

## FUNDADORES

Francisco Apodaca y Osuna  
José Attolini Aguirre  
Enrique Caamaño Muñoz  
Antonio Carrillo Flores  
Mario Cordera Pastor  
Daniel Escalante Ortega  
Gabino Fraga Magaña  
Jorge Gaxiola Zendejas  
José Iturriaga Saucó  
Gilberto Loyo González  
Rafael Mancera Ortiz  
Antonio Martínez Báez  
Lorenzo Mayoral Pardo  
Alfredo Navarrete Romero  
Alfonso Noriega Cantú  
Raúl Ortiz Mena  
Manuel Palavicini Piñeiro  
Álvaro Rodríguez Reyes  
Jesús Rodríguez y Rodríguez  
Raúl Salinas Lozano  
Andrés Serra Rojas  
Catalina Sierra Casasús  
Ricardo Torres Gaitán  
Rafael Urrutia Millán  
Gustavo R. Velasco Adalid

**REVISTA DE INTELIGENCIA Y SEGURIDAD**  
**Número 3 (enero-junio 2025)**

**“NUEVO GLOSARIO Y PARADIGMAS DE LA DEFENSA Y SEGURIDAD:  
NORLATINISMO, INTELIGENCIA CIUDADANA Y NORMATIVIDAD  
EMERGENTE”**

**Director del Número:** Mtro. Carlos Estrada Nava

**COORDINACIÓN EDITORIAL**

**Escuela Nacional de Profesionalización Gubernamental**

Rafael Martínez Puón  
Director

**Subdirección de Desarrollo y  
Difusión de la Cultura Administrativa**

Iván Lazcano Gutiérrez  
María Guadalupe Ocampo Rosas  
Irma Hernández Hipólito

**COMITÉ EDITORIAL**

Víctor Alarcón Olguín	Universidad Autónoma Metropolitana - Unidad Iztapalapa
Adán Arenas Becerril	Facultad de Ciencias Políticas y Sociales de la UNAM
Eber Omar Betanzos Torres	Auditoría Superior de la Federación
Mariana Chudnovsky	Centro de Investigación y Docencia Económicas
Alicia Islas Gurrola	Facultad de Ciencias Políticas y Sociales de la UNAM
Yanella Martínez Espinoza	Facultad de Ciencias Políticas y Sociales de la UNAM
Arturo Pontifes Martínez	Instituto Ortega y Gasset México
Arturo Sánchez Gutiérrez	Escuela de Gobierno y Transformación Pública del ITESM. Ciudad de México



# REVISTA DE INTELIGENCIA Y SEGURIDAD

Número 3

Enero-junio 2025

## ÍNDICE

<b>Presentación</b>	11
<i>Luis Miguel Martínez Anzures</i>	
<b>Introducción</b>	13
<i>Carlos Estrada Nava</i>	
<b>Geopolítica: Herramienta de Inteligencia para el Análisis de las Expresiones del Poder, Toma de Decisiones y Proyección Estratégica</b>	17
<i>Pedro Javier Pescina Ávila</i>	
<b>Inteligencia artificial, radicalización y terrorismo: De la herramienta a la futura autonomía</b>	51
<i>Jesús Rodrigo Navarrete Segovia</i>	
<b>El nuevo Sistema Nacional de Investigación e Inteligencia: hacia la conformación de una amplia comunidad y su armonización mediante un código de ética</b>	79
<i>Martín Granillo</i>	
<b>Guardia Nacional, inteligencia y control civil: balance jurídico de las reformas de seguridad de 2025 en México</b>	99
<i>Alejandra Flores</i> <i>Fernando Irala</i>	
<b>Más allá de la alineación algorítmica: retos éticos y culturales en la adaptación de la IA a la diversidad de los valores humanos</b>	123
<i>Javier Alejandro Padilla Santacruz</i>	
<b>La inteligencia ciudadana y el análisis prospectivo de la seguridad nacional en la relación México – Estados Unidos</b>	151
<i>Rodrigo De León Mondragón</i>	



## **PRESENTACIÓN**

La seguridad nacional constituye el conjunto de políticas, estrategias y acciones orientadas a preservar la integridad, estabilidad y soberanía del Estado frente a riesgos y amenazas internas y externas. Su propósito es garantizar el bienestar de la población, la continuidad de las instituciones y la defensa de los intereses nacionales en un entorno global cada vez más complejo. En este marco, la seguridad nacional se concibe como un esfuerzo integral que articula capacidades civiles, militares y sociales, promoviendo la cooperación interinstitucional y la participación ciudadana para fortalecer la resiliencia y la gobernanza democrática.

En esta búsqueda este número 3 de la RIS (Revista de Inteligencia y Seguridad) aborda los fundamentos teóricos de la Geopolítica como ciencia estratégica y método de análisis de las expresiones del poder en dinámicas espaciales y territoriales. Se plantea su utilidad como herramienta de Inteligencia Estratégica, capaz de orientar decisiones y proyecciones en distintos niveles de acción (global, regional y local).

Asimismo, se examinan las consecuencias políticas y sociales posteriores a la pandemia de COVID-19, destacando la diversificación de procesos de radicalización terrorista mediante el uso de inteligencia artificial y redes sociales como catalizadores de mensajes y planificación de ataques, en un contexto de crisis estatal y auge tecnológico.

Los expertos que aquí escriben analizan escenarios como: la relación entre guerra tecnológica y asimetría del conflicto, que favorece al individuo frente a grandes estructuras y los riesgos de que las herramientas de IA evolucionen hacia procesos autónomos de decisión; la reforma legal de 2025 que crea el

Sistema Nacional de Investigación e Inteligencia en Seguridad Pública, articulando actores públicos, privados y sociales, y proponiendo una ética aplicada para reducir la desconfianza ciudadana en cuerpos policiales; las reformas que consolidan la adscripción de la Guardia Nacional a la SEDENA, con implicaciones para el control civil, la transparencia, los derechos humanos y el federalismo.

En paralelo, se discute el dilema sociotécnico estructural de la inteligencia artificial: la tensión entre eficacia algorítmica y pluralismo moral, que no puede resolverse con ajustes normativos puntuales. Se advierte que la estandarización algorítmica reduce la diversidad cultural y moral, generando riesgos de exclusión y afectando la gobernanza democrática.

Finalmente, como parte de los resultados del Diplomado *Prospectiva política y planeación estratégica* del IMEESDN, se propone integrar la inteligencia ciudadana con la prospectiva estratégica. La participación cívica, junto con herramientas como la matriz de influencias cruzadas y el MICMAC, permite anticipar escenarios y fortalecer la cooperación México–EE. UU. y la reforma institucional mediante indicadores accionables (tiempos de triage, judicialización trazable, cierres  $\leq 72$  h, resiliencia frente a la desinformación y trazabilidad de armas).

La conclusión central es que una “alianza 2.0” con ciudadanía organizada puede reducir corrupción y capacidad criminal, siempre que exista voluntad política, evaluación y transparencia; de lo contrario, la participación corre el riesgo de convertirse en un ritual vacío o ruido institucional.

Aprovecho para agradecer a todos los colaboradores de este número, sus valiosas aportaciones y conocimientos para seguir trabajando y aprendiendo sobre temas que importan a toda la sociedad.

**Dr. Luis Miguel Martínez Anzures**  
**Presidente del INAP**

## INTRODUCCIÓN

En los dos números previos de la Revista de Inteligencia y Seguridad (RIS) se asentaron dos convicciones que hoy resultan aún más pertinentes: primero, que la producción académica especializada en defensa, seguridad e inteligencia crece cuando el entorno se vuelve más exigente y cuando los Estados —y sus sociedades— se ven obligados a repensar instituciones, doctrinas y métodos; y segundo, que no basta con describir coyunturas, sino que es indispensable tender puentes entre teoría, metodología y casos, a fin de construir un acervo útil para la decisión pública, la formación profesional y la deliberación democrática.

En continuidad con ese hilo conductor, este tercer número refuerza la vocación de la RIS por ordenar conceptos, proponer marcos analíticos y debatir reformas contemporáneas, pero lo hace colocando en el centro un desafío transversal: la modernización de la inteligencia y la seguridad en un entorno donde la tecnología acelera amenazas, multiplica dilemas éticos y tensiona los arreglos de control y legitimidad.

El punto de partida es deliberado: si en los números anteriores se subrayó el peso del contexto internacional y la urgencia de comprender la seguridad pública como principal preocupación ciudadana, aquí se amplía el lente hacia 2026, cuando la comunidad de inteligencia y seguridad en México enfrenta simultáneamente presiones operativas, transformaciones normativas y un cambio cultural profundo en la manera de producir “inteligencia útil”.

Esa perspectiva no es retórica: opera como criterio de lectura de los seis textos que componen el volumen, los cuales cubren desde geopolítica aplicada hasta prospectiva con ciudadanía organizada, pasando por terrorismo mediado por inteligencia artificial (IA), el rediseño del sistema de inteligencia e investigación, la reforma de la Guardia Nacional y los desafíos ético-culturales de alinear sistemas algorítmicos con pluralidad de valores humanos.

La primera contribución, “Geopolítica y Norlatinismo: herramientas de inteligencia para el análisis de las expresiones del poder, toma de decisiones y proyección estratégica”, propone un modelo de desarrollo geoestratégico para México, el Norlatinismo, así como una base conceptual y metodológica que resulta especialmente valiosa para 2026: pensar la geopolítica no sólo como disciplina, sino como método de análisis de expresiones del poder en dinámicas espaciales y territoriales, orientado a la toma de decisiones y a la proyección estratégica.

El segundo artículo, “Inteligencia artificial, radicalización y terrorismo: De la herramienta a la futura autonomía”, traslada ese clima de incertidumbre a un terreno donde la frontera entre lo físico y lo digital es cada vez más porosa. El texto explora connotaciones políticas y sociales posteriores a la pandemia de COVID-19, enfocándose en cómo la IA puede potenciar mensajes, estatutos y planificación de ataques en contextos de crisis estatal y auge tecnológico.

El tercer trabajo, “El nuevo Sistema Nacional de Investigación e Inteligencia: hacia la conformación de una amplia comunidad y su armonización mediante un código de ética”, introduce un giro institucional decisivo: la idea de que la transformación no es sólo tecnológica, sino de personas, cultura y reglas comunes, particularmente cuando el modelo incorpora, de manera explícita, interacción y cooperación entre entidades públicas y privadas.

La cuarta contribución, “Guardia Nacional, inteligencia y control civil: balance jurídico de las reformas de seguridad de 2025 en México”, ancla la discusión en uno de los dilemas estructurales de la agenda mexicana: cómo armonizar eficacia operativa con control civil, transparencia y derechos humanos. El artículo examina, desde un enfoque jurídico-garantista, reformas de 2025 que consolidan la adscripción de la Guardia Nacional a SEDENA y reconfiguran el sistema nacional de inteligencia; identifica fundamentos y alcances, pero subraya riesgos para control civil, transparencia y derechos, además de implicaciones para federalismo y coordinación interinstitucional.

El quinto artículo, “Más allá de la alineación algorítmica: retos éticos y culturales en la adaptación de la IA a la diversidad de los valores humanos”, desplaza el foco de la “IA como herramienta” hacia el “gobierno de la IA” en sociedades pluralistas. El trabajo examina los límites de la alineación normativa o técnica cuando se enfrenta a diversidad cultural y moral, advirtiendo que la estandarización

algorítmica puede reducir pluralidad, generar exclusión y afectar gobernanza democrática.

La sexta contribución, “La inteligencia ciudadana y el análisis prospectivo de la seguridad nacional en la relación México – Estados Unidos”, ofrece un cierre programático: incorporar prospectiva e inteligencia ciudadana con instrumentos concretos para anticipar escenarios, fortalecer cooperación binacional y producir indicadores accionables de reforma institucional.

Visto en conjunto, el número tres reafirma una tesis silenciosa pero constante desde el arranque de la revista: la inteligencia y la seguridad no pueden sostenerse sólo en estructuras formales; requieren comunidad, doctrina, método, ética y un vínculo de confianza con la sociedad. En 2026, este desafío se vuelve especialmente tangible ante reconfiguraciones institucionales relevantes en el ecosistema formativo y doctrinario: la desaparición de la Escuela Militar de Inteligencia para convertirse en Jefatura, como parte del cambio del Centro de Estudios del Ejército y Fuerza Aérea (CEEFA) hacia Centro de Estudios de Defensa (CEDEF), y el propósito de mantener y proyectar las actividades del Grupo Académico de Doctrina de Inteligencia (GADI). Ese tipo de transiciones no son administrativas: suelen redefinir identidades profesionales, currículos, estándares de formación y mecanismos de producción doctrinal, y por ello exigen plataformas de pensamiento y debate como la RIS, que permitan continuidad académica, discusión técnica y evaluación crítica.

Finalmente, conviene explicitar un conjunto de tendencias que atraviesan los seis textos, aunque no siempre aparezcan como tema principal, y que pueden marcar la agenda de los próximos años. Primero, la posibilidad de que la automatización de decisiones (por IA o por “analítica”) introduzca errores sistémicos difíciles de detectar a tiempo —por ejemplo, sesgos emergentes que surgen de interacciones entre bases de datos de múltiples entidades— y que terminen institucionalizando discriminaciones o errores de atribución. Segundo, los riesgos de “dependencias invisibles”: proveedores, arquitecturas, integraciones y cadenas de suministro digitales cuya fragilidad sólo se revela en crisis. Tercero, la vulnerabilidad a dinámicas de desinformación “de precisión”, donde actores estatales o criminales ajustan narrativas y contenidos a microaudiencias para detonar conflictos sociales, erosionar confianza o inducir errores operativos. Cuarto, la posibilidad de que reformas legales y reconfiguraciones institucionales produzcan efectos no intencionales sobre coordinación

federal, capacidad local y trazabilidad de responsabilidades, generando zonas grises que luego son explotadas por organizaciones criminales o por corrupción administrativa. Y quinto, el riesgo cultural: que, en la prisa por “modernizar”, se descuide la formación de criterio analítico, la ética profesional y la calidad metodológica, es decir, aquello que convierte información en inteligencia y que, como insiste este número, sigue dependiendo de personas.

En suma, este tercer número de la RIS consolida una apuesta editorial: discutir los fundamentos (geopolítica), los aceleradores de amenaza (IA y radicalización), el rediseño institucional y ético (sistema de investigación e inteligencia y código transversal), el equilibrio jurídico-político (control civil), la complejidad moral de la tecnología (alineación y diversidad de valores) y la necesidad de prospectiva con legitimidad social (inteligencia ciudadana). Es, por tanto, una invitación a leer el presente con herramientas, pero también a pensar el futuro con responsabilidad.

**Carlos Estrada Nava\***  
**Coordinador del número**

---

\* Instructor de Ciberdefensa (CEDEF, Defensa), de Riesgos y Amenazas a la Seguridad Nacional (CESNAV, Marina), y del Diplomado en Prospectiva Estratégica (IMEESDN).

## GEOPOLÍTICA Y NORLATINISMO: HERRAMIENTA DE INTELIGENCIA PARA EL ANÁLISIS DE LAS EXPRESIONES DEL PODER, TOMA DE DECISIONES Y PROYECCIÓN ESTRATÉGICA

Pedro Javier Pescina Ávila\*

**Resumen:** El presente ensayo expone la geopolítica como ciencia de enfoque estratégico y método de análisis para comprender las expresiones de poder en las configuraciones espaciales y territoriales de los grupos humanos; a partir de esta base, se incorpora la noción de “Norlatinismo”, entendida como una concepción geopolítica mexicana que articula el doble vector de gravitación del país—anclaje con América del Norte y proyección hacia Centroamérica, Caribe y Sudamérica—y que opera simultáneamente como representación (imagen--guía que ordena percepciones e intereses) y como diseño estratégico (modelo con objetivos, medios y plazos verificables) orientado a recuperar la condición de potencia media regional y fortalecer un liderazgo latinoamericano mediante diplomacia activa, “mexicanidad” como poder blando, provisión de bienes públicos regionales y una talasopolítica que coloque “a México de frente al mar”, con una “área de influencia inmediata” que incluye el sur de Estados Unidos y el Caribe hispano.

**Palabras clave:** Geopolítica, poder, espacio geográfico, método de análisis, representación geopolítica, modelo estratégico.

**Abstract:** This essay presents geopolitics as a strategic discipline and an analytical method to understand power expressions within spatial and

---

\* Capitán de Navío CG. Retirado de la Armada de México. Ingeniero en Ciencias Navales por la Heroica Escuela Naval Militar (H.E.N.M.), con especialidad en Mando Naval, Informática y Geopolítica por el Centro de Estudios Superiores Navales (CESNAV) Y Maestría en Inteligencia para la Seguridad Nacional por el INAP. Actualmente es Director/Administrador de la Sociedad Civil PESBAR Asesores y Consultores en Seguridad y Protección Marítima S.C.

territorial configurations of human groups; building on this, it introduces “Norlatinismo,” a Mexican geopolitical conception that deliberately combines the country’s dual gravitation—anchoring with North America and projecting toward Central America, the Caribbean, and South America—and operates both as a representation (an image that orders perceptions and interests) and as a strategic design (a model with objectives, means, and verifiable timelines) aimed at restoring Mexico’s status as a regional middle power and strengthening Latin American leadership through active diplomacy, “mexicanidad” as soft power, the provision of regional public goods, and a sea-oriented policy that brings “Mexico to the sea,” with an “immediate area of influence” encompassing the U.S. South and the Spanish-speaking Caribbean.

**Keywords:** Geopolitics, Power, Geographical Space, Analysis Method, Geopolitical Representation, Strategic Model.

## 1. Introducción.

### ¿Qué es la Geopolítica?

La Geopolítica es considerada por diversos estudiosos y teóricos como: Ciencia (una disciplina – con enfoque de pensamiento estratégico –) en el marco de las Ciencias Políticas; y también, como método de análisis de las expresiones del poder, dentro de las interacciones sociopolíticas y de la geografía política con la integración de diversos factores: históricos, geográficos, políticos, culturales, militares, económicos, demográficos y estratégicos.<sup>1</sup>

Bajo esta percepción, hace que posea una doble dimensión:

- a. La primera, como **herramienta** que sirve para la configuración del espacio y de los territorios, de acuerdo con ciertos intereses políticos que poseen motivaciones económicas (materiales), ideológicas (culturales, nacionalistas) y sociales (demográficas, de desarrollo, etc.).
- b. La segunda, como **un campo de estudio multidisciplinario** que sirve **para el análisis** de las dinámicas y configuraciones espaciales y territoriales que se encuentran directamente vinculadas con los intereses políticos y ejercicio del poder.

---

<sup>1</sup> Pescina Ávila Pedro J. (2021). ¿Qué es la Geopolítica? Repercusiones para México. Video conferencia. Hipona Centro de Estudios de Posgrado México.

La primera dimensión ha existido por largo tiempo en el transcurso de la historia y se ha acentuado conforme la práctica y el avance de las dinámicas internacionales. Para el caso de la segunda, ésta comenzó a desarrollarse a finales del siglo XIX con los estudios y análisis de la escuela geopolítica alemana, o escuela geopolítica clásica, la cual estuvo sumamente influenciada por la práctica imperialista, sirviendo de guía y justificación ideológica para el expansionismo alemán.

La posibilidad de demandar o de carecer de recursos para garantizar la existencia de una comunidad, conlleva a que se adopten ciertas medidas por quien asume la dirigencia de dicha sociedad, como son:

- a. Desplazarse hacia aquellos lugares que contienen recursos;
- b. Negociar la adquisición de tales recursos; o bien,
- c. Obtenerlos a base de la fuerza en territorio ajeno (Conquista).

Bajo este tenor, la geopolítica conlleva el análisis y el óptimo aprovechamiento del territorio y sus recursos, enfocándose en:

- La tierra, el suelo y el espacio geográfico.
- El espacio político de una determinada población con la pretensión de sobrevivir y existir.
- El componente primario y esencial donde se ubican las interacciones de poder que establece el hombre en su medio natural.

## **2. Marco Teórico – Escuelas Geopolíticas: Clásica vs Crítica.**

### **2.1 Geopolítica Clásica.**

Los antecedentes del estudio geopolítico se remiten a las aportaciones realizadas en diferentes ámbitos. Por ejemplo, en el campo de la filosofía política, pensadores como: Hobbes, Maquiavelo, Montesquieu, Hegel y Kant en sus estudios filosóficos relacionaron factores claves como: el territorio, el poder y la sociedad. En la geografía aplicada científicos alemanes, como: Alexander Von Humboldt y Kart Ritter, identificaron una

visión organicista del Estado, según la cual éste se asemeja a las funciones que sigue cualquier ser vivo. Esta propuesta se conoce como: Geopolítica clásica.

El sueco, Rudolf Kjellén, pionero de la geopolítica clásica, identificó a la geopolítica como parte de las ciencias políticas o de las ciencias del Estado, proponiendo un método que fuera más allá de lo descriptivo y que ofreciera mayor rigor analítico en torno a la relación entre el Estado y el territorio. Su visión organicista señala que:

*“...El Estado es un ser vivo, cuyo gobierno es el alma y el cerebro, el imperio es el cuerpo y el pueblo son los miembros”, el cual cumple con las funciones de nacer, crecer y morir en medio de luchas y conflictos biológicos (raza)...*

### **Alemania.**

El alemán, Federico Ratzel, incluyó a la historia como otra variable clave del análisis geopolítico, ya que se encarga de vincular al tiempo y a los hechos del pasado con los acontecimientos presentes y futuros, que ayudan a comprender con mayor veracidad al Estado, dentro de una lógica racional y humana; pensarlo como un “organismo vivo” que cumple con todas las funciones biológicas de la vida. Afirmó que:

*“...La historia nos permite conocer la transitoriedad de los grandes pueblos... Por ello vemos desaparecer con mayor velocidad a aquellos grupos humanos a quienes la naturaleza misma les niega posibilidades de expansión: pueblos insulares o aquellos que se conformaron con pequeños territorios o, finalmente, agrupaciones humanas reducidas que abarcan amplios espacios sin explotarlos totalmente”*

Dentro de esta afirmación se destaca otro aspecto primordial del análisis geopolítico: la ubicación geográfica de cada Estado; que dependerá en buena medida de la forma física que le otorga su localización: dentro o fuera de un continente, en su proximidad o alejado de océanos, ríos, montañas, desiertos, selvas, lagos, etc. El espacio se convierte en un factor primordial para la cohesión de un pueblo, tal como lo es la historia común que comparten, dando lugar a:

*“...La superioridad de un pueblo sobre otro, a través del espacio, al que rápidamente ocupa, explora, puebla y aprovecha, acelerando procesos”*

Bajo el concepto de que, el Estado es un “organismo territorial”: cambia, crece o empequeñece; Ratzel emana dos conceptos fundamentales que definieron el pensamiento geopolítico alemán de años siguientes, sobre todo de la mano Karl Haushofer, otro mítico pensador que se esforzó en institucionalizar la geopolítica para convertirla en un instrumento científico para el poder del Estado, en el marco del Tercer Reich alemán.

En tal sentido, se destacan los siguientes términos:

- El **lebensraum** o “**espacio vital**”. Referido al espacio necesario para satisfacer las “necesidades” del Estado. Las sociedades frágiles o primitivas sufren el sometimiento al medio. Los fuertes se mueven luchando por más territorio según sus necesidades y capacidades. Representa la influencia física de la geopolítica en ese tiempo.
- El **raumsinn** o “**sentido del espacio**”. Referido a la conciencia que el ciudadano debe tener del carácter vital del territorio y de sus posibilidades de expansión. Representa a su vez la influencia psicológica.
- La visión del “**volk**”: una idea romantizada del pueblo alemán. Este vocablo utilizaba toda la ideología, filosofía y modo de ser de la población alemana.

## *Lebensraum*: Espacio Vital Alemán



Fuente: <https://en.wikipedia.org/wiki/L>

### **Francia.**

El francés, Yves Lacoste, trata de rescatar a la Geopolítica de la sombra que pesaba sobre ella como “ciencia nazi”. La geopolítica no debe servir a un ente biológico absoluto e insaciable como lo era el Estado. Su nueva función es explicar los conflictos para crear conciencia en la población sobre las estrategias de dominación aplicadas a ellos por quienes detentan el poder.

- Categoriza a la geografía como instrumento del poder, como elemento de dominación, de conflicto, de lucha.
- La geopolítica designa todo aquello que concierne a las rivalidades de poderes o de influencias sobre territorios y las poblaciones que ahí habitan. Engloba todos aquellos elementos que entran en conflicto por el control o la dominación de territorios, ya sean actores grandes o pequeños.
- Estudia las rivalidades entre los poderes políticos de todo tipo, no sólo el actor clásico:

el Estado.

- Reconoce que la nación contiene valores, sentimientos y es reactiva a las amenazas y lazos hacia el territorio en disputa.
- Define una **idea psicológica** determinante, que se transforma en intenciones y en justificaciones de acciones e inspiraciones de posturas geopolíticas: las **representaciones geopolíticas**:

*“...Conjunto de ideas y percepciones colectivas de orden político, religioso u otro, que anima a los grupos sociales y que estructura el imaginario colectivo y la visión de su mundo”.*

- Recurre al **uso de mapas**, para delimitar el espacio que ocupa una problemática y entender la situación geopolítica, desarrollando así un análisis con base en el territorio que se estudia. Los conflictos pueden desarrollarse en diferentes niveles de análisis espacial y repercutir en el plano local, nacional, regional o internacional.
- Señala que, el poder de un Estado depende de factores como la unidad de su nación, de sus capacidades estratégicas y de su dirigencia.
- La fuerza se mide por sus capacidades de poder y su posibilidad de dominio, no sólo por la cantidad de territorio que amasa el Estado.

El punto de vista de los primeros teóricos se ciñe a la existencia de un Estado como actor racional que, considerando su propia naturaleza política, se debate entre la lucha por el poder (conflicto), la supervivencia y la supremacía sobre otros; o bien, en la pérdida de su poder. Lo cual convierte a la geopolítica como un instrumento esencial del realismo político, que le otorga un peso decisivo para el liderazgo y toma de decisiones de quien detenta el poder y dirige al Estado.

## 2.2 Geopolítica Crítica.

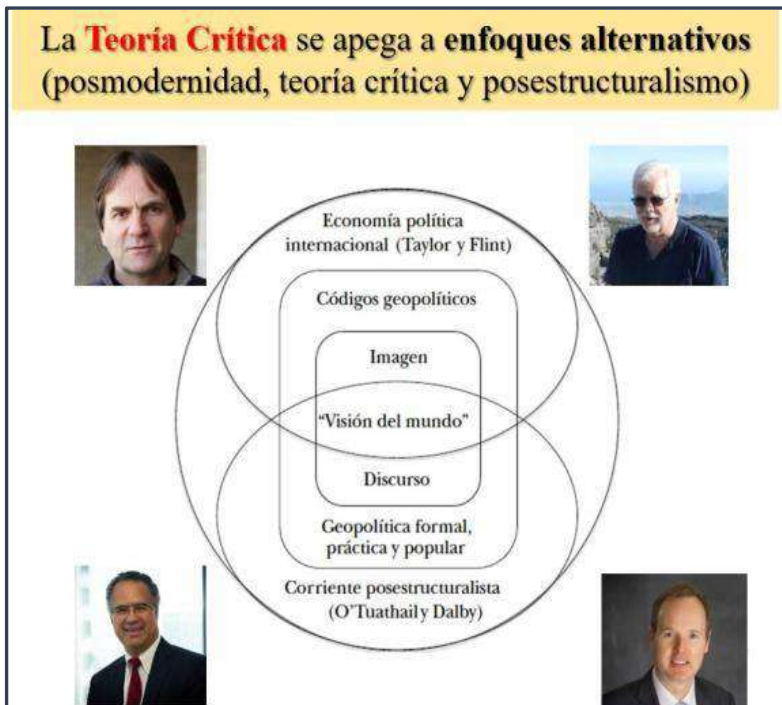
Retoma las vanguardias filosóficas, replanteadas con base en el pensamiento francés, criticándolo, pero recuperando la idea de una geopolítica para los ciudadanos. Esta corriente es originalmente anglosajona, representada por Peter Taylor, John Agnew, Simon Dalby y Gearóid O Tuathail, con un enorme impacto en el pensamiento europeo. Señala que la geopolítica se emplea más en su parte práctica que en su parte analítica. Se utiliza para elaborar diseños geopolíticos destinados a propiciar configuraciones espaciales, en consonancia con los intereses de las élites dirigentes.

A partir de la década de 1980 la escuela anglosajona pretende construir una Teoría Crítica que sirva para una verdadera comprensión de las dinámicas interrelacionales y espaciales. Apegado a enfoques alternativos (posmodernidad, teoría crítica y posestructuralismo), este pensamiento se caracteriza por:

- Una concepción constitutiva y no explicativa sobre la teoría, posee la convicción de que la teoría *no explica la realidad, sino que ayuda a crearla y transformarla.*
- Considera que no existe *una base sólida y objetiva* para observar, comprender y juzgar la realidad.
- Toma como base que todo conocimiento y teoría proceden de una concepción altamente subjetiva.
- Cree en la construcción histórica de *la realidad* y los discursos, las instituciones, las *verdades y los regímenes de la verdad*; en otras palabras, *las cosas no están ahí afuera esperando a ser descubiertas, sino que son política y socialmente construidas.*
- Las generalizaciones y universalismos no son válidos, las construcciones sociales son diversas y dependen de la cultura, la geografía, las cosmovisiones, los valores y los intereses particulares.

Para los críticos (O' Tuathail, 1994), la geopolítica clásica fue empleada en tres sentidos principales:

- a. **De forma descriptiva**, destinada únicamente a narrar los procesos y dinámicas que ocurren en una cierta región con un fuerte sentido monográfico.
- b. **En forma de consejos al príncipe** (sentido maquiavélico), brindando la guía para la política y las acciones que un Estado debería aplicar en un determinado momento histórico.
- c. **Como una gran estrategia**, colocando a los Estados y regiones dentro de categorizaciones y generalizaciones, dejando de un lado las dinámicas que ocurren dentro y alrededor de ellos y menospreciando el hecho de que existen casos particulares que no se inscriben dentro de los universalismos teóricos.



Fuente: Elaboración propia.

### **3. Diseños Geopolíticos: como Modelos Estratégicos.**

Estos representan la conceptualización de una configuración geoespacial, destinados a servir como una proyección del poder de los intereses nacionales-estatales o de cualquier tipo (comercial, militar, social, cultural, ideológico) en el marco de una gran estrategia<sup>2</sup>.

#### **3.1 “Modelo en Cruz” – El poder del Mar sobre la Tierra –.**

El estadounidense, Alfred T. Mahan (1840-1914), elaboró un diseño estratégico de poder fincado en el poderío naval y el uso de tácticas militares como base de la proyección internacional. Su pensamiento fue resultado del estudio histórico sobre los aciertos de la marina inglesa y la marina imperial española.

De España, rescató “el modelo en forma de cruz” implementado en el Nuevo Mundo. Este modelo, se trazó de forma horizontal para establecer la conexión directa entre las Filipinas con las Islas Canarias, es decir, entre Asia y Europa, pasando por el punto cardinal de la Nueva España (México), dando lugar a la correlación de manera vertical entre los territorios norteamericanos y la parte sur del continente.

Varias de las estrategias de la dirigencia política estadounidense de finales del S. XIX y principios del S. XX siguió este modelo, para establecer bases militares y controlar las principales rutas marítimas comerciales. La operatividad y suplantación del modelo por EE.UU., llevó a la expulsión de los españoles de sus colonias, tanto de Asia en las Filipinas, como del Mar Caribe – bautizado por Mahan “Mar Mediterráneo Americano” –, con los objetivos principales de Cuba y Puerto Rico.

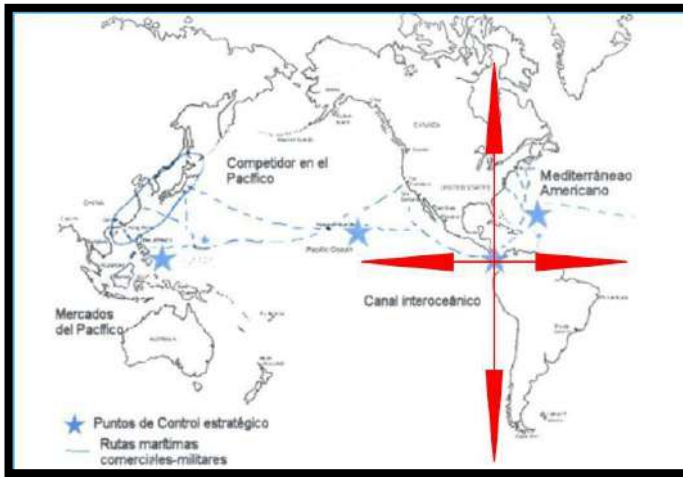
Una vez habilitado el corredor Asia-Pacífico-Europa, pasando por el Mar Caribe, ubicaron su punto cardinal en lo que hoy es Panamá. Para tal efecto, motivaron (1903) la separación de dicho territorio de Colombia. Panamá se erigió en el gran epicentro de poder estadounidense sobre el continente, desde donde se coordinaban labores de inteligencia, aprovisionamiento y entrenamiento militar – funciones que actualmente desempeña el

---

<sup>2</sup> Son un tipo de Representación Geopolítica. Definición propia.

USSOUTHCOM<sup>3</sup>, ubicado en Miami, Florida –, además de ser la zona de tránsito obligada para el comercio internacional. En términos geopolíticos, la conformación y el establecimiento de un verdadero rimland, siguiendo los planteamientos teóricos de Nicholas Spykman.

### “Modelo en Cruz” -El Poder del Mar sobre la Tierra-



Fuente: Elaboración propia.

### 3.2 Teoría del “Corazón de la Tierra” – Heartland: La Gran Isla –.

En contraste con el valor estratégico que Mahan señaló respecto al poder del mar; la visión inglesa de Halford Mackinder (1861-1947), concentró el valor geoestratégico en el factor terrestre, la conformación de una “gran isla territorial”: Eurasia, fusión de dos continentes: Europa y Asia. La mayor parte ocupada por el continente asiático, y Europa sería una especie de península anexa a esta “Gran Isla”.

<sup>3</sup> Comando Sur de Estados Unidos: Uno de los diez Comandos de Combate Unificado pertenecientes al Departamento de Defensa de Estados Unidos. Su jurisdicción comprende los países de América Latina -con Excepción de México que, pertenece al Comando Norte-, y las 12 islas bajo soberanía europea. También abarca los océanos Atlántico y Pacífico, entre los meridianos 30° y 92° oeste.

Eurasia representa el Heartland (el corazón en la tierra), en donde prevalece un centro o pivote: Rusia y constituye a su vez, un punto de significado valor estratégico frente al asedio del poder marítimo: aquellas potencias insulares o marginales a la llamada “Gran Isla”. A fin de resguardar (contener) el área pivote, se articulan semi – círculos de seguridad a partir de las cuatro grandes regiones marginales – continentales y oceánicas – que constituyen las islas costeras de Eurasia. Europa es la región marginal del Atlántico, China lo es del Pacífico, la India a partir del Indico, y Oriente Próximo estaría cercado por los “Cinco mares”: Mediterráneo, Negro, Caspio, Rojo y Arábigo.

Desde esta lógica, se propondría una alianza entre las potencias del mar: Reino Unido, Canadá, Estados Unidos, Sudáfrica, Australia y Japón; además de un acercamiento con los países de Europa del Este para cercar y debilitar el área pivote (Rusia).

**Precepto Mackinder:** *“Quien domina Europa Occidental controlaría el corazón continental; y quien domina el corazón continental, controlaría la isla mundial y controlaría el mundo”.*

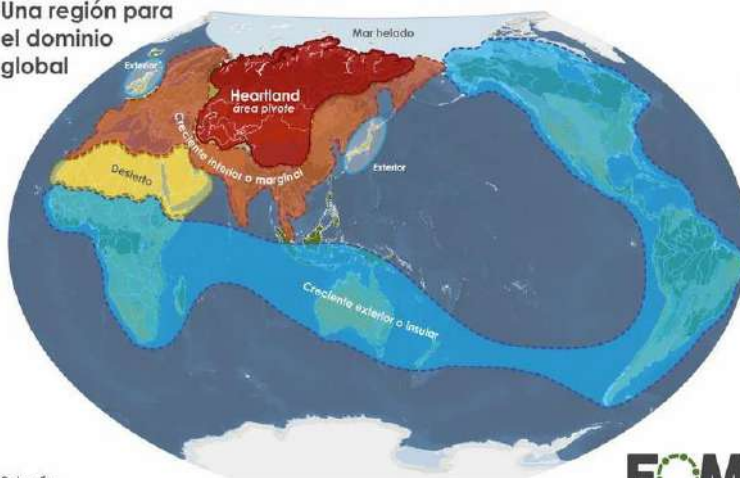
### **3.3 Teoría del Rimland.**

La contra – propuesta a Mackinder, surge en Estados Unidos a través de Nicholas J. Spykman (1893 – 1943). Pone en duda el núcleo duro de la “Teoría del Corazón de la Tierra”, estableciendo la Teoría del Rimland (teoría del cerco o la tierra – orilla), que consiste en determinar un área–tapón que funcione como una amplia zona amortiguadora en el conflicto entre el poder marítimo y el poder terrestre.

Precepto Spykman: “Quien controla el rimland domina Eurasia, y quien domina Eurasia controla los destinos del mundo”.

## Heartland: - El Corazón de la Tierra - Teoría del Heartland

Una región para el dominio global



Cartografía:  
Abel Gil Lobo (2018)

## Teoría del Rimland: Cerco o la tierra – orilla

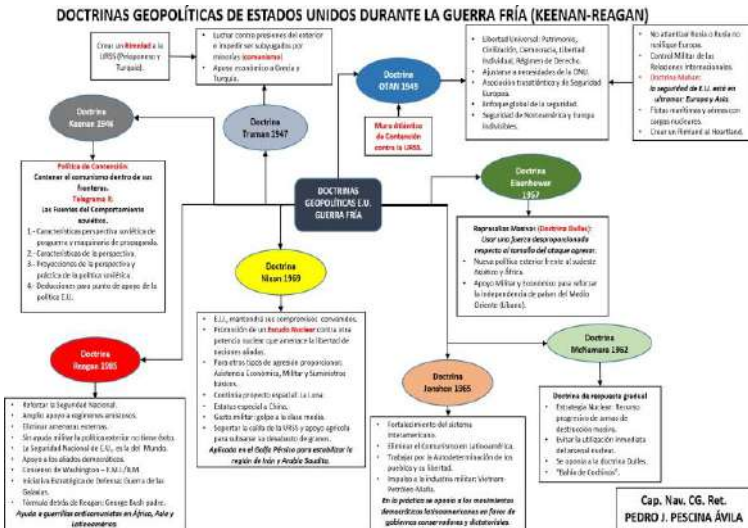


Fuente: <https://14milímetros.com/geopolitica-teorias-y-aplicacion>

### 3.4 Doctrinas de Contención.

Tales propuestas: Heartland-Rimland, fueron materializadas en una geoestrategia militar llevada a cabo por EE.UU., en la “Guerra Fría”; a través de las Doctrinas de Contención: Keenan 1946, Truman 1947, OTAN 1949, Eisenhower 1957, McNamara 1962, Jonhson 1965, Nixon 1969 y Reagan 1985.

#### Doctrinas de contención – 1



Fuente: Elaboración propia.

## Doctrinas de contención - 2



Fuente: Elaboración propia.

### 4 Geopolítica como método de análisis

La Geopolítica es una herramienta fundamental para identificar el “sentido del espacio” que poseen los Estados y diversos actores, en el contexto de las relaciones espaciales dentro de un entorno estratégico dinámico (VICA: volátil- incierto-complejo-ambiguo). Para ello, la geopolítica atiende la problemática desde tres vertientes fundamentales, que conforman sus tres dimensiones de análisis<sup>4</sup>:

- El territorio y el espacio, como ámbito material y virtual de las prácticas sociales humanas.
- El grupo humano, como actor histórico situado en la historia y en la geografía.
- El poder, como práctica política y simbólica, y como modo de apropiación del territorio.

<sup>4</sup> Arciga Rodríguez, Nohemí (2023). Geopolítica como método de análisis. Cátedra impartida dentro de la materia Gestión de Conocimiento y Redes. Maestría de Inteligencia para la Seguridad Nacional INAP. Enero-abril/2023.

## DIAGRAMA CONCEPTUAL



“La Geopolítica es el estudio de las relaciones entre poder y espacio, manifestadas por los grupos humanos a través del tiempo”

*Dra. Nobemi Arciga Rodríguez*

### 4.1 El análisis geopolítico

Si partimos del contexto holístico dentro de un marco de grandes intereses estratégicos y relaciones geoespaciales entre Estados o diversos actores, resulta de gran utilidad hacer referencia de ciertas representaciones geopolíticas como instrumentos de poder, para con ello interconectar motivaciones, comportamientos o intereses en juego; como, por ejemplo, los “Diseños Geopolíticos” previamente descritos.

Una representación geopolítica se refiere a la versión que cada grupo humano o actor (Estado, organismo, individuo) maneja; y no es otra cosa que sus ideas, creencias, percepciones e intereses. Dichas representaciones pueden tender hacia un enfoque Clásico, en donde el comportamiento de un Estado – Nación se asemeja al de un actor racional y en el que el realismo político es decisivo para la conducción del liderazgo y toma de decisiones de la dirigencia política. O bien, hacia un enfoque Crítico, en donde se relaciona con todo aquello que concierne a las rivalidades de poderes o de influencias sobre territorios y las poblaciones que ahí habitan. Engloba todos aquellos elementos que entran en conflicto por el control o la dominación de territorios, ya sean actores grandes o pequeños; no solo el actor clásico: el Estado. Todo buen análisis geopolítico debe tener una perspectiva ecléctica: Una combinación de diversas corrientes y escuelas de

pensamiento geopolítico, que aporten ideas y posibilidades de explicaciones diferentes.<sup>5</sup>

<b>Análisis Geopolítico</b>			
<b>Perspectiva Ecléctica:</b>	<b>Geopolítica Clásica</b>	+	<b>Geopolítica Crítica</b>

Fuente: Elaboración propia

A manera de correlacionar lo anterior, se destaca la propuesta del geopolítico francés Yves Lacoste, cuya tendencia primaria parte de un enfoque Crítico, pero que a su vez retoma y combina principios y fundamentos Clásicos, que siempre están vigentes.

#### **4.2 Método Yves Lacoste: La Espacialidad Diferencial.**

Para Lacoste, “Saber pensar el espacio” es como observar una pintura. Al mirarla de lejos se tiene la totalidad de un solo golpe; pero si nos acercamos un poco, comenzamos a descubrir detalles que no habíamos percibido, y vamos encontrando trazos más detallados a medida que nos acercamos, los cuales de lejos no podíamos ver.

Lo anterior, sugiere que la totalidad brinda solo una forma de análisis general, pero poco detallada. Para poder conocer más, es preciso observar desde otros ángulos intermedios o más cercanos. De esta manera, podremos analizar puntos concretos en el espacio de la pintura. A pesar de reducir nuestra visión, el análisis es más profundo.

De esta manera, Lacoste recurre a la combinación de cuatro tipos de razonamiento:

1. Geográfico (inductivo)
2. Espacial (deductivo)
3. Histórico (diacrónico)
4. Psicológico (representaciones)

---

<sup>5</sup> Arciga Rodríguez, Nohemí (2023). Análisis Geopolítico: Una visión sobre el ataque de Hamás a Israel. WEBINAP, Laboratorio de Excelencia Académica INAP, 15/nov/2023. <https://www.youtube.com/watch?v=6pW6EmEFWfg>.

## Razonamiento escuela geopolítica francesa



Fuente: Arciga Rodríguez, Nohemí (2023). *Geopolítica como método de análisis*.

El **razonamiento geográfico** se basa en:

- Formular las dimensiones espaciales de cada problema, tratando de responder a las siguientes preguntas: ¿Qué? ¿Por qué? ¿Quién? ¿Dónde? ¿Cuándo? ¿Cómo? ¿Qué hacen?
- De cada tema que se analiza, buscar las relaciones entre: Región, Medio físico y Sociedades humanas.
- Comparar lo no conocido a lo conocido.
- Practicar los cambios de escalas, es decir, combinar la información que tenemos de los mapas a diferentes escalas y tamaños.

El **razonamiento espacial** refiere a las diversas dimensiones que van de lo global a lo local – internacional, regional y local – o de lo general a lo particular. Para lo cual señala diversos aspectos:

- Conjuntos espaciales, es decir, la representación espacial elaborada de toda clase de conjuntos: continentes, estados, montañas, ríos, ciudades o cualquier tipo de territorio.
- Territorio y poder, la extensión claramente delimitada sobre la cual el Estado ejerce su autoridad y es responsable del orden público; la superficie del Estado, el trazado de las fronteras y las relaciones de fuerza con Estados vecinos.
- La nación, se refiere al territorio y características particulares de los pueblos que se identifica así mismo en base a las creencias, tradiciones y costumbres, y que no siempre corresponden a la totalidad del territorio que conforma un Estado, u otras veces se extienden más allá de éste.

- Diferentes niveles de análisis espaciales, clasificando los territorios por órdenes de tamaño. Para tal efecto se utiliza el diatopo:<sup>6</sup> representaciones gráficas formadas por la superposición esquemática de diferentes mapas relacionados, que muestran un determinado evento, fenómeno o realidad espacial en varias escalas.

El **razonamiento histórico** es diacrónico, porque se ocupa de un hecho, fenómeno o circunstancia desde el punto de vista de su evolución en el tiempo.

- Para entender una situación geopolítica es necesario contar con información a “grosso modo” de las rivalidades de poder que históricamente han acontecido en los territorios que se analizan.
- La relación que existe entre un mapa de “diatopos” con el razonamiento histórico es fundamental, ya que, de manera gráfica explican conflictos actuales, asociando los mapas que los representan con el análisis de las consecuencias presentes y los sucesos históricos. (una línea del tiempo).
- No obstante, hay que tener presente que la manipulación histórica es muy frecuente, en virtud de que los hechos históricos por lo general sirven como argumentos de las clases dirigentes, de acuerdo con sus intereses y sistemas de creencias impuestos a una sociedad.

El **razonamiento psicológico** deja entrever que las “representaciones geopolíticas” (ideas, creencias, percepciones e intereses) se utilizan como instrumentos de poder.

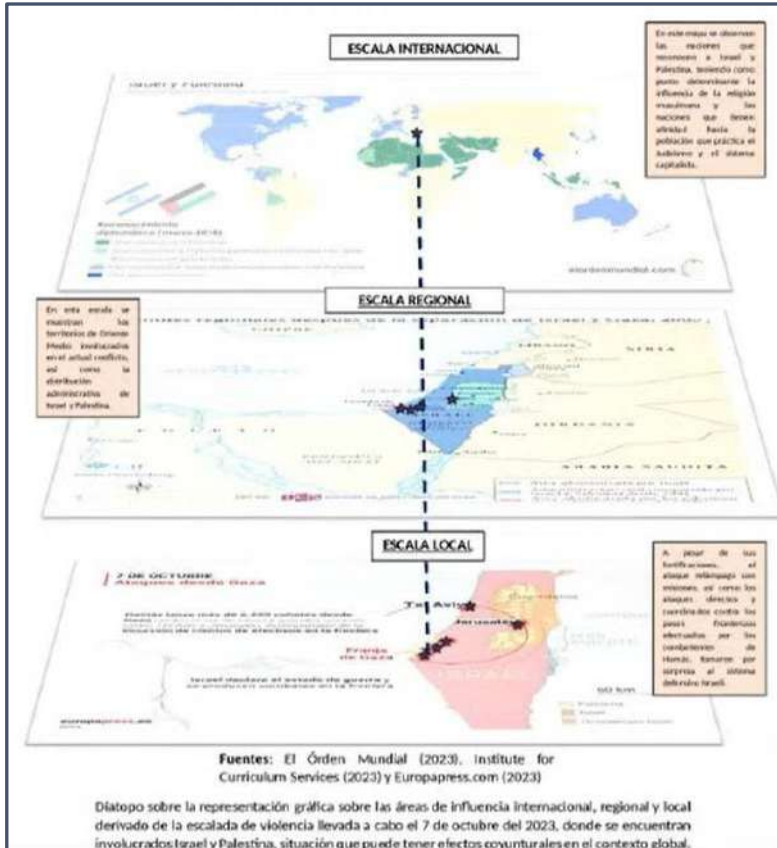
- Las rivalidades de poder entre los actores se cristalizan alrededor de temas algunas veces no objetivos o por consideraciones de pura estrategia; éstas también pueden surgir de “creencias erróneas o ciertas” de cada actor geopolítico.
- Las representaciones pueden tener fundamento, demostrarse o ser solamente hechos ilusorios, pero reflejan la manera de sentir y de pensar de los protagonistas, y se hace extensiva a la psique colectiva de una nación o sociedad.
- Las representaciones juegan un rol preponderante en la correlación de fuerzas entre actores, y la mayor parte de las veces conducen a “diálogos sordos”, falta de entendimiento, comunicación y subestimación del oponente, hasta transformarse

---

<sup>6</sup> Neologismos del griego “topo”: lugar, y la palabra “díá”: a través.

como focos generadores de violencia. Ejemplos: Yugoslavia, Rusia-Ucrania, Hamás-Israel.

### Espacialidad Diferencial – Diatopo



Fuente: Arciga Rodríguez, Nohemí (2023). Análisis Geopolítico: Una visión sobre el ataque de Hamás a Israel

## 5. Caso práctico del Análisis Geopolítico: Rusia vs Ucrania/OTAN.<sup>7</sup>

<sup>7</sup> Cabe mencionar, que las motivaciones iniciales del bloque occidental (EE.UU/Ucrania/OTAN) llevadas a cabo bajo la administración de Joe Biden contra Rusia, corresponden a la representación geopolítica contenida en la obra: El gran tablero mundial: La supremacía estadounidense y sus imperativos geoestratégicos, de Zbigniew Brzezinski; cuyo objetivo central es contener, colapsar y derrotar estratégicamente a Rusia, desmembrar el país y provocar su

Para el caso del análisis geopolítico del conflicto Rusia vs Ucrania/OTAN, haremos referencias geopolíticas que dan claridad al mismo:

- La visión de Estados Unidos respecto a Eurasia, manifestada en la representación geopolítica de Zbigniew K. Brzezinski en su libro “El Gran Tablero Mundial” (1998), y
- La Doctrina Geopolítica Rusa del “Euroasianismo”: resurgimiento de la “Tercer Roma”.

## 5.1 El Gran Tablero Mundial.

Desde 1997, Zbigniew Brzezinski, ex asesor de Seguridad Nacional de Estados Unidos durante la administración Carter, afirmó que:

*“... la potencia que domine Eurasia ejercerá una influencia decisiva sobre dos de las tres regiones mundiales más productivas económicamente”... (Europa y sudeste asiático). Añadió que:*

*“... una mirada al mapa sugiere que el Estado predominante en Eurasia tendrá el control automático del Medio Oriente y África”... Ante ello:*

*“...la tarea inmediata es asegurar que ningún Estado adquiera la capacidad de expulsar a Estados Unidos o siquiera disminuir su papel decisivo” en la región...*

El diseño Brzezinski consiste en:

1. Mantener el espacio euroasiático abierto a Estados Unidos, a través del acceso directo a Europa y a Japón, Corea del Sur y Taiwán.
2. Penetrar la masa euroasiática a través de los denominados Balcanes Globales que incluyen a Asia Central, el Cáucaso Sur, Afganistán y Pakistán, desde donde se buscará el control efectivo sobre el Medio Oriente, en donde Irak es una pieza clave.
3. Fragmentar la alianza entre el principal actor oriental (China) y el actor medio (Rusia)

---

cambio de régimen. Hoy en día bajo el mando de Donald Trump, los intereses geopolíticos de EE.UU. en la región y las relaciones bilaterales con Rusia se están alineando hacia otra dirección geoestratégica todavía en evolución

Para Brzezinski, Eurasia es la región más importante geopolíticamente hablando debido a que concentra el mayor número de personas, recursos naturales y posiciones geoestratégicas y territoriales del mundo; por eso se denomina el “tablero de ajedrez” donde más de dos jugadores se disputarán la región como recompensa.

*“Hacerse del control de los recursos energéticos y mantenerse como la única potencia mundial es el objetivo primordial de Estados Unidos en la región”.*

Eurasia comprende desde Portugal hasta el estrecho de Bering, pasando por los territorios ricos en recursos petroleros del Medio Oriente y Asia Central. Divide esta región en cuatro zonas: la parte oeste pertenece a Europa Occidental; el sur al creciente fértil y Asia Central; el este a Asia Oriental; Europa Oriental y Rusia como un espacio medio. Dentro de este escenario se considera que existen:

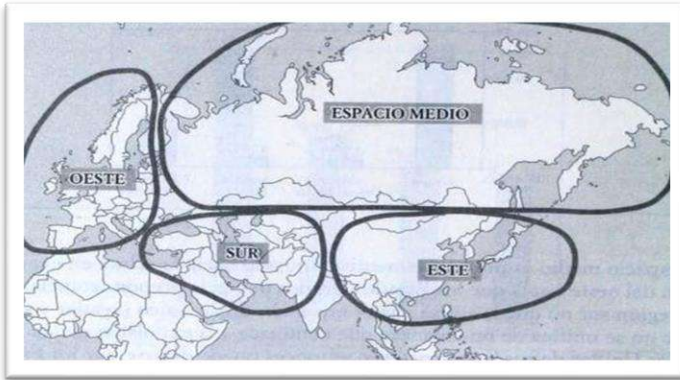
- Cinco jugadores geoestratégicos clave <sup>8</sup> : Francia, Alemania, Rusia, China e India.
- Cinco jugadores pivote<sup>9</sup>: Ucrania, Azerbaiyán, Corea del Sur, Turquía e Irán.

---

<sup>8</sup> Jugadores geoestratégicos clave: Estados activos con capacidad y voluntad nacional de ejercer poder, o influenciar más allá de sus fronteras, para alterar el estado geopolítico actual.

<sup>9</sup> Pivotes geopolíticos: Estados cuya importancia se deriva no de su poder y sus motivaciones, sino más bien de su situación geográfica sensible y de las consecuencias que su condición de potencial vulnerabilidad, provoca, provoca en el comportamiento de los jugadores geoestratégicos.

## El tablero euroasiático

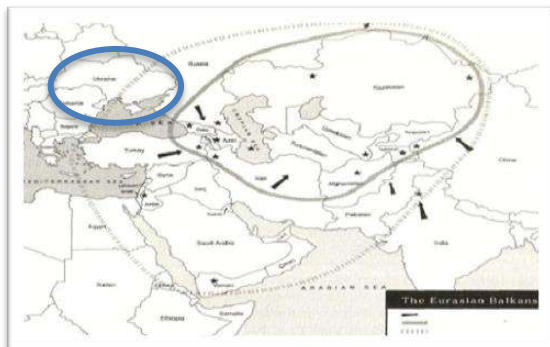


Según Brzezinski, Europa representa para Estados Unidos: la cabeza de puente democrática en Eurasia. Cualquier expansión del ámbito europeo entraña una expansión directa del área de influencia estadounidense. Europa se convertiría en un pilar vital dentro de la estructura euroasiática de seguridad estadounidense; por lo que se deberá tratar a la Unión Europea como su socio global político y de seguridad. Habrá de ajustarse la estructura interna de la OTAN, sobre la fórmula: 1+1 (Estados Unidos + Unión Europea). Por lo que, una política global estadounidense que trate a Asia como un todo, no resultará posible si el esfuerzo de ampliar la OTAN fracasa, y esto volvería a encender las aspiraciones rusas en Asia Central.

### **Ucrania: Jugador Pivote.**

- Sin Ucrania, Rusia deja de ser un Imperio euroasiático, y únicamente podría considerarse un imperio predominantemente asiático, más susceptible a ser arrastrado a los conflictos de los países de Asia Central.
- Si Rusia vuelve a tomar el control de Ucrania, con sus 52 millones de habitantes, sus importantes recursos y su acceso al mar, podría resurgir como un Estado imperial por encima de Europa y Asia.

## Ucrania: Jugador Pivote



Fuente: El Gran Tablero Mundial (1998).

Para los intereses de Estados Unidos, Brzezinski visionó que más allá del 2010, se conformaría un “núcleo fundamental de seguridad europea”, a través del triángulo: Francia-Alemania-Polonia + Ucrania. El cual brindaría la profundidad estratégica de Europa; y, permitiría una Europa más extensa e integrada, reforzada por una OTAN ampliada y más segura.

### 5.2 El Euroasianismo: resurgimiento de la “Tercera Roma”.

Ucrania es el origen histórico del pueblo Ruso. En el año 988 D.C., pueblos eslavos provenientes de Europa Oriental, de la mano del príncipe Vladimir de Kiev, se consolidan como un Estado Ortodoxo Cristiano en la Rus de Kiev. Posteriormente, el imperio mongol dominó durante casi tres siglos Rusia, y así nace Moscú, estableciéndose como su capital, con un predominio cultural asiático-oriental.

En 1511 el monje ruso Filofei propuso al Zar Vasili III, que Rusia, específicamente: Moscú, se constituyese en el centro de poder dejado por el Imperio Bizantino, y se erigiese como el Imperio Romano, convirtiéndose en la “Tercera Roma”. (Primera Roma: Roma; Segunda Roma: Constantinopla). Con esta visión mesiánica, los zares crean un vasto Imperio expandiéndose constantemente hacia oriente y occidente. La península de Crimea posee un particular magnetismo para la consciencia de la elite y buena parte del pueblo ruso. La obsesión por el acceso a los mares cálidos, la Guerra de Crimea en el siglo XIX y el mito de

Sebastopol, marcaron hitos en la historia rusa, que se repiten por generaciones. Boris Yeltsin reconoció la independencia ucraniana, y con ella, la de la propia península; sin embargo, Bielorrusia, Ucrania y Crimea para la elite imperialista rusa, integran el corazón o núcleo cultural ruso-eslavo, al estilo de Hawái o Puerto Rico, para Estados Unidos.

A inicios del siglo XXI, Vladimir Putin, inicia el resurgimiento paulatino del Estado ruso bajo la Doctrina ideológica del Euroasianismo. La visión es posicionar a Rusia como una Potencia de Primer Orden, equiparable al de la extinta Unión Soviética, y mediáticamente como al de la “Tercera Roma”. En ella, se retoman principios e ideologías del pasado, que se caracterizan por percibir a Rusia como un Imperio. Sus postulados doctrinarios son los siguientes:

- Se concibe a Rusia como una civilización original euroasiática.
- Se retoman principios, ideologías y aspectos culturales del Imperio Zarista.
- Para justificar los intereses rusos en el exterior se refuerza la consciencia nacionalista.
- Se enfatiza que las raíces culturales rusas son tanto asiáticas como europeas.
- Se apoya en la ortodoxia religiosa para recuperar el control del Estado y reforzar la unidad nacional.

## Euroasianismo



Fuente: <https://es.wikipedia.org/wiki/Euriasiatismo>

Al ponerse en práctica tales postulados, el Euroasianismo dejó de ser una ideología para convertirse en una doctrina geopolítica, con un interés primordial en la preservación de la integridad territorial, por lo que la defensa del territorio se fortaleció en regiones que son consideradas vitales para el desarrollo del país; y planteó como objetivo, que:

*“Rusia recupere su zona de influencia, en la zona geográfica que había pertenecido a la extinta Unión Soviética”*

Rusia se ha enfocado en desarrollar una geopolítica energética en regiones como Asia Central y el Cáucaso. Para lo cual, la defensa de los recursos energéticos en el “cercano extranjero”, fue considerada como parte sustancial para el desarrollo del país. La anexión de Crimea representa para Rusia mayor control para el suministro de gas y más presencia en el Medio Oriente. Además, Sebastopol alberga la principal base de la flota rusa en el Mar Negro; y le permite tener acceso marítimo a las costas de países miembros de la OTAN como Turquía, Rumania y Bulgaria.

*“Crimea es un puerto que no sólo le da salida al Mar Negro a Rusia, sino un control político y económico de la región y le permite tener presencia en Medio Oriente”*

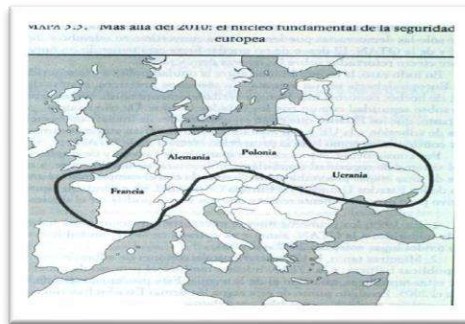
Una amenaza a la seguridad rusa lo representó la intención de Estados Unidos de instalar sistemas de defensa antimisiles en

Polonia y la República Checa, para supuestamente proteger a Europa de eventuales ataques con misiles de largo alcance iraníes. Detrás del conflicto entre Rusia, Ucrania y los países occidentales está también el equilibrio de poder en la región.

Para Estados Unidos/OTAN, Ucrania representa:<sup>10</sup>

- La pieza clave para inclinar la balanza estratégica a favor de Occidente y Estados Unidos en Eurasia, y con ello conformar un “núcleo fundamental de seguridad europea”, a través del triángulo: Francia-Alemania- Polonia + Ucrania, que le brindaría la profundidad estratégica de una Europa más extensa e integrada.
- Al crear inestabilidad en países limítrofes con Rusia, especialmente en sus satélites de Asia Central y en Ucrania, y, perturbar el flujo de gas y petróleo, se hace posible aislar a Rusia para que deje de ser una gran potencia.

Núcleo fundamental de la seguridad europea



Fuente: El Gran Tablero Mundial (1998)

**Para Rusia, Ucrania representa:**

- La inclusión de Ucrania como miembro de la Unión Europea y de la OTAN, representa la presencia de un potencial adversario en su propia frontera afectando su espacio vital, y, por lo tanto, una amenaza para su Seguridad Nacional.
- La elite imperialista rusa no concibe una Ucrania alejada de Rusia, dado que Bielorrusia, Ucrania y

---

<sup>10</sup> Según Brzezinski

Crimea, integran el corazón o núcleo cultural ruso-eslavo.

- En tal sentido:

*“La relevancia estratégica de Ucrania para Rusia reside en ser **un escudo** ante los avances de occidente”*

### Escudo ante el avance occidental



Fuente: Elaboración propia

## 6. Norlatinismo como propuesta de gran estrategia

El presente apartado expone, en términos operativos, una concepción geopolítica denominada “Norlatinismo”, pensada para recuperar la condición de México como potencia media regional y para robustecer su liderazgo ideológico en el espacio latinoamericano con horizonte 2030–2050. La propuesta parte de reconocer una doble gravitación estratégica: por un lado, la inserción geoeconómica en América del Norte; por el otro, la pertenencia civilizacional a América Latina. Lejos de constituir una contradicción, esa doble pertenencia se configura como un recurso estratégico que, si se ordena mediante método, puede convertirse en palanca de poder y en lenguaje común de Estado (Pescina Ávila, 2014).

### 6.1 Definición y alcance del norlatinismo

Se entiende por “Norlatinismo” la articulación deliberada de dos espacios de acción complementarios: el anclaje con América del Norte —por densidad comercial, tecnológica y demográfica transfronteriza— y la proyección hacia Centroamérica, el Caribe y Sudamérica —por comunidad histórica, lingüística y de valores—. La tesis que da sustento a este enfoque delimita, además, un “área de influencia inmediata” que incluye el sur de Estados Unidos con alta presencia mexicana y el Caribe hispano; desde ahí se propone irradiar influencia política, económica, cultural e incluso militar al vecindario ampliado, priorizando la provisión de bienes públicos regionales y la construcción de agendas compartidas (Pescina Ávila, 2014). El objetivo no consiste en sustituir identidades, sino en transformar la doble pertenencia en una cosmovisión propia, inteligible y atractiva para terceros.

## **6.2 Geopolítica como herramienta de inteligencia**

En la caja de herramientas del análisis estratégica, la geopolítica actúa como método ecléctico para “pensar el espacio”: integra territorio, grupo humano y poder, y opera a través de dos piezas acopladas, la representación y el diseño. El Norlatinismo ocupa ambos lugares. En tanto representación, fija una imagen de país que ordena percepciones e intereses; en tanto diseño, traduce esa imagen en objetivos secuenciados, indicadores verificables y medios de poder coherentes con las capacidades nacionales (Pescina Ávila, 2014). Esta doble condición le permite alimentar el ciclo de inteligencia: orientar recolección, encuadrar análisis, reducir incertidumbre y retroalimentar la planeación con resultados evaluables.

## **6.3 Postulados operativos**

La arquitectura del Norlatinismo se sostiene en un conjunto de postulados que orientan su implementación.

### **Correlación: Euroasianismo – Norlatinismo**

Tópico	Euroasianismo	Norlatinismo
<b>Intereses Nacionales</b>	Asia y Europa	Norteamérica y Latinoamérica
<b>Zona de Influencia</b>	"Cercano Extranjero"	Sur de Estados Unidos y Caribe Hispánico
<b>Unidad Nacional</b>	Cristianismo Ortodoxo	Guadalupeñismo
<b>Visión</b>	Potencia Hegemónica Mundial	Potencia Media Regional
<b>Gobierno</b>	Sentido Vertical del Poder	Régimen Centralizado y Fuerte
<b>Raíces Históricas</b>	Asiáticas y Europeas	Mestizas: Prehispánica y Española
<b>Seguridad</b>	<ul style="list-style-type: none"> <li>• Núcleo Estratégico Defensivo</li> <li>• Organización de Cooperación de Shanghai</li> </ul>	Nueva Arquitectura de Seguridad y Defensa (Alianza latinoamericana)
<b>Respeto</b>	Principios y Normas del Derecho Internacional	Soberanía y Autodeterminación de los pueblos
<b>Promoción</b>	Imagen Nacional: Cultura e Idioma Rusos	El poder blando mexicano "La Mexicanidad"
<b>Concepción Mundial</b>	Orden Multipolar Internacional	México como Actor Global
<b>Diplomacia</b>	Mayor Entendimiento y Concordancia	Diplomacia Activa y Pragmática
<b>Recurso Estratégico</b>	El Petróleo y Gas Natural	El Petróleo y El Mar

Fuente: Elaboración propia

En primer lugar, se plantea un doble vector estratégico: compatibilizar la integración productiva norteamericana con una proyección latinoamericana sostenida, asumiendo que el corredor transfronterizo —hecho de cadenas de suministro, remesas y redes migratorias— no es anomalía sino palanca de poder si se gobierna con inteligencia (Pescina Ávila, 2014).

En segundo término, se eleva la "mexicanidad" a categoría de poder blando; la cultura, la lengua, las artes, la tradición jurídica y la fe popular conforman un repertorio simbólico con capacidad de magnetizar afinidades cuando se convierte en política pública de diplomacia cultural y de conocimiento (Pescina Ávila, 2014).

En tercer lugar, se propone una diplomacia activa y pragmática que combine principios clásicos —no intervención, solución pacífica de controversias— con herramientas contemporáneas —negociación basada en datos, diplomacia económica y técnica, construcción de coaliciones funcionales en ciberseguridad, movilidad humana, seguridad marítima y cambio climático— (Pescina Ávila, 2014).

El cuarto postulado introduce un factor de unidad civilizacional como fundamento de cohesión interna y legitimidad externa; símbolos compartidos —entre ellos el guadalupanismo como emblema de la nación mestiza— operan como cemento psicológico que otorga continuidad a los proyectos de largo aliento (Pescina Ávila, 2014).

En quinto lugar, se sugiere una arquitectura de conducción política capaz de sostener estrategias de Estado más allá del ciclo sexenal; un presidencialismo eficaz, acotado por pesos y contrapesos y soportado en planeación democrática, se considera condición para priorizar, secuenciar y blindar inversiones estratégicas (Pescina Ávila, 2014).

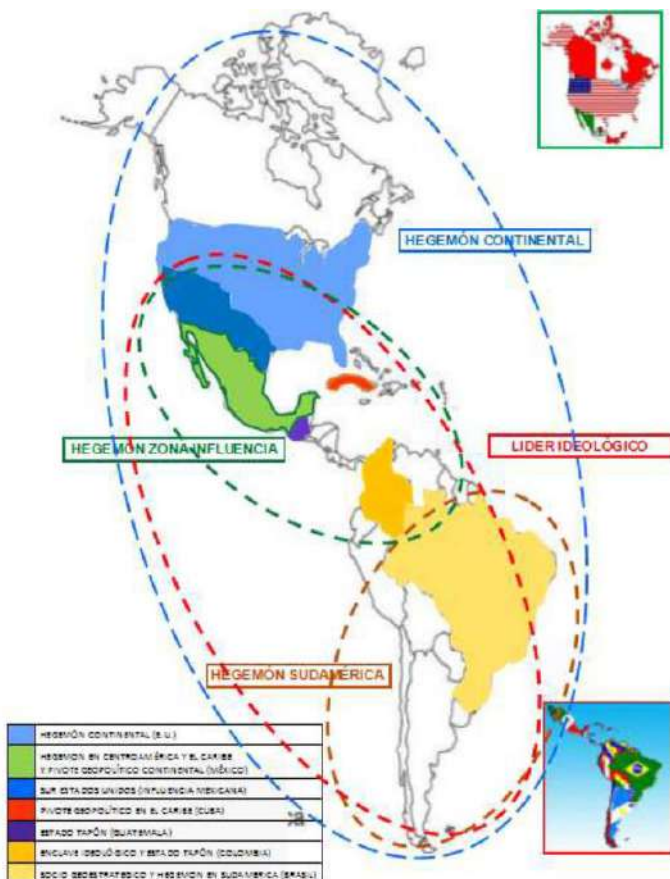
El sexto elemento postula la búsqueda de una hegemonía benigna en el vecindario, entendida no como imposición, sino como capacidad de marcar agenda y de proveer bienes públicos regionales —conectividad logística y digital, interoperabilidad educativa y de ciberdefensa, seguridad marítima, protección civil— (Pescina Ávila, 2014).

Finalmente, se establece el respeto al derecho internacional como marco de acción y se recupera la talasopolítica —“un México de frente al mar”— como palanca para dinamizar puertos, astilleros y rutas marítimas en los tres litorales, integrándolos a cadenas logísticas y energéticas de mayor alcance (Pescina Ávila, 2014).

#### **6.4 Modelo y hoja de ruta 2030–2050**

La operacionalización exige metas claras, medibles y escalonadas. En esta lógica, se propone: consolidar un posicionamiento regional que reconozca a México como primer respondiente en crisis humanitarias, desastres y contingencias marítimas; institucionalizar un doble anclaje norte/latino que alinee la integración productiva con estándares y reglas compartidas en el sur; escalar la proyección cultural, científica y tecnológica mediante diplomacia educativa y redes de investigación; ofrecer marcos de interoperabilidad en seguridad y ciberdefensa a través de centros de excelencia y ejercicios combinados; y priorizar la conectividad talasopolítica con corredores interoceánicos, puertos y backbones de telecomunicaciones.

## Visión geopolítica para México dentro del “ajedrez geopolítico americano”



Fuente: Elaboración propia

## 7. Conclusiones.

La Geopolítica es un excelente método de análisis para generar conocimiento por la forma en que aborda y procesa la información.

Es una disciplina descriptiva – analítica e integradora –, extrae conclusiones del análisis de interdependencias y condicionamientos presentes, entre diferentes categorías y especializaciones de las ciencias sociales y geográficas, para darlas a conocer a una autoridad política.

“Saber pensar el espacio” nos brinda además de un análisis general, el poder conocer más observando desde otros ángulos intermedios o más cercanos, y obtener así un análisis más profundo.

Todo buen análisis geopolítico debe estar sustentado bajo una perspectiva ecléctica: una combinación de diversas corrientes y escuelas de pensamiento geopolítico, que aporten ideas y posibles explicaciones diferentes, que le permita ser un valioso instrumento de inteligencia para la toma de decisiones.

Finalmente, en el marco de una Gran Estrategia Nacional: la Geopolítica como herramienta de inteligencia para el análisis de las expresiones del poder, toma de decisiones y proyección estratégica, puede ser útil para:

- Identificar los rasgos geopolíticos de México y el actuar político de su clase dirigente.
- Afianzar y concretar propuestas de dirección política del Estado Mexicano en la solución de problemas complejos desde el punto de vista de una sociedad orgánica.
- Proyectar un mejor reposicionamiento de México a nivel regional e internacional.
- Rescatar a la talasopolítica <sup>11</sup> como plataforma de proyección estratégica de México por su condición bioceánica y ubicación geográfica.
- Generar una doctrina de pensamiento geopolítico-estratégico en la clase dirigente y esferas del poder nacional.
  
- Que a partir de un análisis diferencial y prospectivo generar una representación geopolítica que refleje:
  - El orgullo de nuestra identidad y potencialidad como país.
  - La remembranza del Imperio que fuimos en el pasado (aspecto psicológico).
  - Una nación multifacética con extraordinaria cultura milenaria.
  - La transformación de las imperfecciones del Estado – Nación que queremos tener.

---

<sup>11</sup> Ofrece una visión que contempla como relevantes los asuntos entre el Estado y su condición marítima. Enorme ventaja en materia: Económica, Comercial, Diplomática y Sociocultural

- La ruta y derrotero hacia buen puerto de los destinos de nuestra nación.
- Líneas de acción orientadas a concretar las aspiraciones nacionales de justicia, desarrollo, seguridad y bienestar social.

### **Bibliografía y Fuentes consultadas:**

- Arciga Rodríguez, Nohemí (2023). Geopolítica como método de análisis. Cátedra impartida dentro de la materia Gestión de Conocimiento y Redes, Maestría en Inteligencia para la Seguridad Nacional INAP. Enero- Abril/2023.
- Arciga Rodríguez, Nohemí (2023). Análisis Geopolítico: Una visión sobre el ataque de Hamás a Israel. WEBINAP Laboratorio de Excelencia Académica INAP,15/Nov/2023, <https://www.youtube.com/watch?v=6pW6EmEFWfg>.
- Brzezinski, Z. (1998). El gran tablero mundial. La supremacía estadounidense y sus imperativos geoestratégicos. Buenos Aires: Paidós.
- CESNAV – UNAM. (2012). Fundamentos de Geopolítica: Visión y análisis. La larga tradición geopolítica rusa. La evolución de sus Escuelas, desde el Imperio Zarista hasta la Conformación de la Federación Rusa. México: CESNAV.
- González Ibarra, Edgar E. (2012). La larga tradición geopolítica rusa. La evolución de sus escuelas, desde el Imperio Zarista hasta la conformación de la Federación Rusa. Fundamentos de Geopolítica. Visión y Análisis. CESNAV-UNAM.
- Latschan, Thomas (2025). Los planes de Trump para Ucrania: lo que se sabe hasta ahora. Obtenido de <https://www.dw.com/es/los-planes-de-trump-para-ucrania-lo-que-se-sabe-hasta-ahora/a-71601477>.
- Mackinder, Halford J. (2011). El pivote geográfico de la historia. Geopolítica(s). Revista de estudios sobre espacio y poder, vol. 1, núm. 2, 301-319.
- Pescina Avila, Pedro J. (2021). ¿Qué es la Geopolítica? Repercusiones para México. Video conferencia. Hipona Centro de Estudios de Posgrado. México.
- Sánchez Herráez, Pedro (2021). Siglo XXI: ¿El retorno de la lucha por el Rimland? [https://www.ieee.es/Galerias/fichero/docs\\_analisis/2021/DI\\_EEEA12\\_2021\\_PEDSAN\\_Rimland.pdf](https://www.ieee.es/Galerias/fichero/docs_analisis/2021/DI_EEEA12_2021_PEDSAN_Rimland.pdf).

## INTELIGENCIA ARTIFICIAL, RADICALIZACIÓN Y TERRORISMO: DE LA HERRAMIENTA A LA FUTURA AUTONOMÍA

Jesús Rodrigo Navarrete Segovia\*

**Resumen:** El presente texto explora las connotaciones políticas y sociales posteriores a la pandemia mundial por COVID – 19 que dieron pauta a la diversificación de procesos de radicalización de corte terrorista a través de la inteligencia artificial como herramienta para potencializar mensajes, estatutos y planificación de ataques, en el marco de una crisis del Estado y el auge tecnológico.

En el primer apartado del desarrollo, repasaremos cómo el contexto de la guerra en un entorno tecnológico y su relación con la asimetría del conflicto es congruente con la dinámica social que aventaja al individuo sobre las grandes aglomeraciones.

Posteriormente, dirigiremos los esfuerzos en establecer la relación entre los procesos de radicalización terrorista, el uso de redes sociales y otras plataformas de inteligencia artificial como herramientas y catalizadores del terrorismo, para finalmente discutir si, con base en los

---

\* Maestro en Administración de la Seguridad con Especialidad en Ciberseguridad por la Universidad de las Américas Puebla; con estudios de Maestría en Seguridad e Inteligencia Estratégica e internacionalista de formación por la Facultad de Estudios Superiores Acatlán de la Universidad Nacional Autónoma de México. Cuenta con numerosa capacitación en áreas de seguridad e inteligencia, así como de auditoría e investigación, entre ellas las impartidas por el Instituto Nacional de Administración Pública, el Departamento de Estado de Estados Unidos, el Centro de Investigación y Docencia Económica, la Escuela de Administración Pública de la Ciudad de México y el Instituto Mexicano del Petróleo, entre otros. Tanto en la administración pública federal como en el ámbito privado, consta su trabajo en áreas de fiscalización e investigación también al sector de hidrocarburos nacional e internacional, y a su cadena completa de producción y distribución, así como en áreas de lavado de dinero y financiamiento al terrorismo en corporativo financiero internacional, sectores desde donde fungió no sólo como analista, sino también como capacitador institucional.

requerimientos técnicos de estas herramientas, serán capaces de desarrollar procesos y toma de decisiones de carácter autónomo.

**Palabras clave:** Procesos de radicalización, inteligencia artificial, asimetría del conflicto.

**Abstract:** This article explores the political and social connotations following the global COVID-19 pandemic that led to the diversification of terrorist radicalization processes through artificial intelligence as a tool to enhance messages, statutes, and attack planning, within the context of a state crisis and the rise of technology.

In the first section, we will review how the context of war in a technological environment and its relationship to conflict asymmetry is consistent with the social dynamics that favor individuals over large groups.

Subsequently, we will focus our efforts on establishing the relationship between terrorist radicalization processes and the use of social media and other artificial intelligence platforms as tools and catalysts for terrorism. Finally, we will discuss whether, based on the technical requirements of these tools, they will be capable of developing autonomous processes and decision-making.

**Keywords:** Radicalization processes, artificial intelligence, conflict asymmetry.

## Estructura Metodológica

Tras la exploración general de temas centrales y periféricos relacionados al objeto de estudio, se considera relevante aportar preguntas de investigación destinadas a identificar la relación entre la inteligencia artificial y los procesos de radicalización en un entorno digital.

1. ¿Es la inteligencia artificial, entendida como la capacidad de resolución de problemas de las computadoras con mínima o nula intervención humana, una concepción antagonica a la institucionalización de la sociedad y un factor preponderante en el aceleramiento en procesos de radicalización, propagación de ideología extremista y planificación de ataques de corte terrorista?
2. ¿Cuáles son los factores de riesgo a identificar en el uso de inteligencia artificial que faciliten procesos de radicalización?

## **Hipótesis**

Diagnóstica: La inteligencia artificial, como respuesta a la incapacidad de generación de conocimiento en un entorno de incertidumbre e inmediatez, sumada a una crisis del modelo democrático y a la reafirmación de la identidad nacional frente a procesos de migración masivos, aceleraron procesos de radicalización y propagación de ideología extremista de carácter terrorista.

Prospectiva: Bajo esa óptica, ante el mantenimiento del *status quo* institucional por parte del Estado, la poca vinculación con el sector privado tecnológico y una regulación jurídica tecnológica insuficiente, sumado a condiciones de proteccionismo económico y de conservadurismo político estatal, así como de una crisis de la inteligencia del Estado, la inteligencia artificial potencializará procesos de radicalización y planificación de ataques no sólo como herramienta, sino con carácter autónomo, a través de los análisis masivos de datos.

## **Objetivo General**

Analizar el marco contextual y textual del uso de inteligencia artificial frente a la incertidumbre, la migración internacional, la reafirmación nacional y el avance tecnológico como catalizador de procesos de radicalización.

## **Divulgación que lo anima**

En un entorno donde la era digital de todo y del internet de las cosas reconfiguró profundamente la vida profesional y personal de la sociedad, aumentó la necesidad de garantizar la confianza digital en materias como seguridad, economía y política.

Es así como, dentro del contexto internacional volátil y de múltiples vulnerabilidades, riesgos y amenazas, actores estatales y no estatales deben entender que su participación en la agenda internacional como actor tradicional ya no es suficiente para cubrir el amplio abanico de temas tan diversos como complejos en su origen, evolución y en su solución a largo plazo, con un enfoque no sólo estratégico, sino prospectivo.

Se considera pertinente analizar el contexto de pandemia mundial provocada por COVID-19 y la creciente aceleración de los nacionalismos, el aumento la ausencia de cooperación internacional y la profundización de la inequidad con un paralelismo del auge tecnológico y el levantamiento de la inteligencia artificial como herramienta de solución de problemas cotidianos, en primera instancia, para pasar a producir armas sin intervención humana.

## **Objeto de Estudio**

Condiciones contextuales exteriores e interiores de índole políticas y sociales en las que se originan procesos de radicalización a través de la inteligencia artificial frente a un entorno de incertidumbre y crisis de inteligencia de Estado, reflejada en la propagación de ideología extremista durante el periodo comprendido de enero a diciembre de 2024.

## **Objetivos**

Generales: Analizar el marco contextual y textual de la inteligencia artificial como herramienta del terrorismo en procesos de radicalización, propagación de ideología extremista y planificación y elección de ataques, en el marco de la incertidumbre y el riesgo, la migración internacional, la reafirmación nacional y el avance tecnológico como catalizador del terrorismo, así como una futura independencia de actuación del factor humano.

Específicos:

- 1.- Diagnosticar el aceleramiento de procesos de radicalización de carácter terrorista en un contexto de interdependencia tecnológica y uso de la inteligencia artificial como motor y herramienta de resolución de problemas.
- 2.- Identificar factores en la evolución de riesgo a procesos de radicalización y una futura acción autónoma de la tecnología, que permitan replantear el paradigma de la vigilancia tecnológica y sus vulnerabilidades, la inclusión vinculante de actores no estatales y privilegiar el uso ético y legal de la inteligencia artificial.

## DESARROLLO

Diagnóstico: la quinta generación de la guerra, asimetría del conflicto e individualización.

La globalización como la suma de distintos procesos políticos, económicos y sociales que convergen en la era global y digital ha consolidado a los mecanismos de control económicos, políticos y sociales como los tomadores de decisiones de la actualidad.

No basta con visitas protocolarias que la diplomacia de la vieja escuela exige, reverencias o mensajes con el lenguaje apropiado. Se trata de una diplomacia que se ejecuta desde las redes sociales, con una respuesta casi instantánea y flujo de información masivo en directo.

Tópicos de la agenda internacional como el feminismo o el impacto medio ambiental resuenan con mayor nitidez frente a las grandes amenazas tradicionales o asimétricas propias de un entorno volátil e incontrolable mediante canales emergentes consecuencia de la interdependencia tecnológica.

Como contrapeso a la decadencia estatal, el dinamismo económico asiático y la expansión del islam compiten abiertamente ante Estados Unidos y Europa como civilizaciones vivas y en proceso de madurez, partiendo de sistemas políticos no basados en democracia, aunque tampoco lograron erradicar carencias sociales propias.

Lo anterior, se reflejó en flujos migratorios activos y en reversa, donde el nuevo mundo descubierto en el siglo XIV se trasladó hacia su descubridor. En este momento, África y Oriente Próximo movilizan cientos de personas para lograr atravesar el Mediterráneo y sobrevivir de mejor forma su precario modo de vida. No obstante, la globalización y su consecuente avance tecnológico y de integración de mercado acentuaron carencias sociales y de valores.

Tanto el comercio internacional como las políticas monetarias estabilizadoras no contrarrestaron los efectos de aplastamiento económico y social que, tras la pandemia mundial por COVID-19, deshidrataron a una sociedad que se debate entre aceptarse en un

entorno global, aferrarse a su identidad nacional o resolver sus problemas diarios a través de la inteligencia artificial.

El avance tecnológico promovió, paralelamente con el auge del internet, una cultura de violencia y de reproducción de inestabilidad del Estado. Las redes sociales evidencian la decadencia social con crudeza y sin tapujos, consumida por una sociedad enferma de violencia y propensa a justificar la violencia sobre la razón.

La pandemia por COVID-19 generó nuevas exigencias dentro del mercado profesional y la vida diaria, desplazando al Estado y a su falta de actuación ante el inminente impacto sanitario, aunque manteniéndose como administrador del poder, poderes fácticos acrecentaron la distancia entre la sociedad y el Estado, distancia que reviró hacia la tecnología.

Esta contextualización justifica el aceleramiento en procesos de radicalización y propagación de ideas extremistas a través de herramientas de inteligencia artificial, ocupando ese vacío entre la sociedad y el Estado.

Otro sustento del trabajo, es el reporte *Global Trends 2040*, documento realizado por el *National Intelligence Council* de Estados Unidos, que establece 5 tópicos a considerar durante este estudio: cambios globales, fragmentación al interior de comunidades y Estados, desequilibrio en sistemas y organizaciones, contestación y adaptación, a través de fuerzas estructurales (demografía y desarrollo humano), dinámicas emergentes (sociedad) y escenarios hacia 2040 (renacimiento de la democracia, ambiente, economía, tecnología, Estado e internacional, así como competencia y coexistencia, y tragedia y movilización) (Council, 2021).

Desde una visión de Estado y una metodología de revisión de ediciones pasadas, el reporte nos adentra hacia un estudio prospectivo del balance demográfico mundial (donde la pobreza se mantendrá y la urbanización aumentará), así como de las tendencias en salud, donde se observa un incremento en la resistencia creciente a los antimicrobianos y del papel de Estados Unidos y China en su expansión ante estos acontecimientos. Asimismo, cómo la pandemia mundial provocada por COVID-19 aceleró los nacionalismos, aumentó el vacío de la cooperación internacional y profundizó la inequidad.

Las dificultades de una transición inmediata hacia ambientes de trabajo virtuales resultaron en la poca o nula planeación e identificación de las posibilidades sociales y económicas de los colaboradores para absorber su hogar como estación de trabajo, incluyendo: sistemas de apoyo, internet confiable, interfaces apropiadas, acceso remoto para Firewall y protección de bases de datos.

El uso de herramientas tecnológicas facilitó el contacto a distancia y coadyuvó a la resolución de problemas, al sostenimiento de la cultura organizacional y a discusiones informales propias de una estación de trabajo física.

Otro reporte, *Technology Futures: Projecting the Possible, Navigating What's Next*, expone procesos de identificación de proyecciones a través de tres modelos: exponencial, lineal y cíclico. Es así, que el texto transita desde dos ópticas: la de fluir con la tecnología y la relacionada los riesgos y su uso excesivo (Forum, 2021).

Desde la descentralización en la concentración de datos personales y la discusión sobre el uso de tecnología con motivaciones sustentables, hasta nuevas formas de educación y financiamiento económico, la realidad virtual nos obliga a tomar una postura respecto a formar parte del engranaje tecnológico y su consumo masivo, o bien, volver a las formas tradicionales de vida.

La proyección de la tecnología como canal que coadyuve a la inclusión social, el cuidado del medio ambiente y a la diversidad cultural, así como a la disminución de la pobreza, será determinante en un entorno de poder y prospectiva relacionada a éste.

Esta transición de lo estatal hacia lo tecnológico y múltiples aristas y variables dirigidas al desarrollo humano, la democracia y la economía, se tradujo en violencia, en algunos casos, premeditada, y que no solo tiene su causa en la religión, sino en un origen multifactorial relacionado a diversas motivaciones no sólo de grupos sociales, sino también del individuo, donde el Estado carece de métodos sociales de prevención y detección, por ejemplo, de terrorismo, como consecuencia del acelerado modo de vida social y tecnológico, así como de una crisis de inteligencia del Estado.

Es así, que la preponderancia de la individualidad sobre lo grupal es una realidad en la sociedad. Ante tal disociación, el individuo puede ser considerado como un activo propio del Estado que posee la capacidad de tomar decisiones propias y de transformar las relaciones políticas, económicas y sociales hacia el interior y exterior.

Por otra parte, la quinta generación de la guerra es un paradigma que explica la interrelación de la tecnología en el marco de la asimetría del conflicto. Con un breve repaso de las anteriores generaciones previas, George Michael, establece en su capítulo “Evolución de la guerra, conflicto y estrategia” (Michael, 2012) una línea del tiempo resumida en:

<b>Generaciones de la guerra</b>	
<b>Primera generación</b>	Riqueza de las naciones.
	Agricultura liberó a trabajadores para ser soldados.
	Nacimiento del nacionalismo.
<b>Segunda generación</b>	Riqueza generalizada por la industrialización.
	Mejores sistemas de administración pública (impuestos).
	Tecnologías nuevas (tren).
<b>Tercera generación</b>	Evitar ataque directo contra enemigo.
	Diplomacia no funciona en la Primera Guerra Mundial.
	Blitzkrieg.
<b>Cuarta generación</b>	Guerra de guerrillas.
	Estrategia de insurgencia.
	Terrorismo suicida como innovación táctica.

Fuente: Elaboración propia

Como se puede observar, el cambio generacional de la guerra es conexo a la industrialización y avance tecnológico del Estado del siglo XIX y de la primera mitad del siglo XX, trasladando la fuerza de un ataque frontal a la evasión de este, e incluso, a la evolución de la asimetría del conflicto.

En este orden de ideas, hacia finales del siglo XX, el cambio de orden hegemónico internacional a la par del Estado generó el desarrollo de amenazas asimétricas concebidas en el marco de la seguridad frente a un contexto exponencial de libre mercado, por lo que la ausencia de un punto de referencia fijo (el Estado) se cierne como el adversario actual, el cual, además, es móvil, transnacional y en ocasiones, intangible.

Lo anterior, entonces, traduce al terrorismo como fenómeno y enemigo asimétrico, el cual no cuenta con domicilio fijo y tiene una red dispersa en un entorno no sólo físico, sino virtual.

Ante tal desbordamiento de la economía y del poder estatal, mencionado anteriormente y que apartaron al Estado de sus competencias clásicas, surgió la individualización, como una respuesta de la sociedad ante el constante desplazamiento y aplastamiento del Estado hacia sus habitantes, éste último bajo la tutela su tutela y de sus intereses colectivos, predominando los intereses de las élites políticas y económicas.

Esta individualización, además, provenía desde el desarrollo capitalista y su modelo de competencia excesivo que exponía una fragmentación social como vulnerabilidad de la sociedad. Como consecuencia de esto, los valores familiares y sociales cooperantes fueron sustituidos por formas de egoísmo y egocentrismo, que alejaron al individuo de la solidaridad grupal.

Esta desintegración social coadyuva, por tanto, en procesos de radicalización y propagación de ideologías radicales y extremistas.

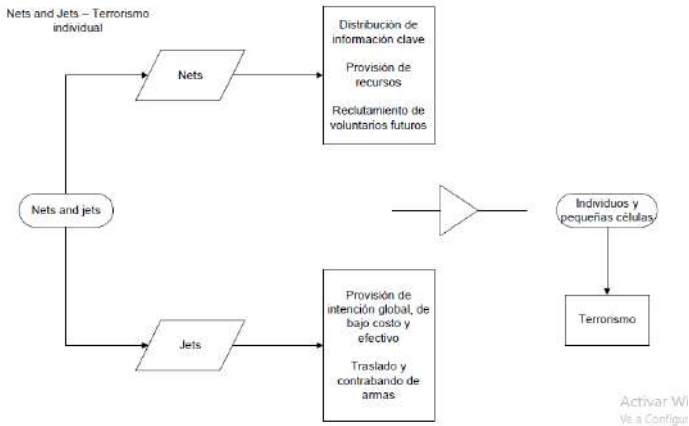
De lo explicado, se desprende la quinta generación de la guerra, donde el cambio en la conformación de las comunidades transfiere la fidelidad de las personas de sus países hacia causas individuales, acelerado principalmente, por la conectividad del internet.

Como resultado de este proceso de individualización, pequeños grupos e individuos cuentan con las herramientas tecnológicas de potencializar daño que anteriormente era exclusividad del Estado, lo que representa un incremento de capacidades de poder de pequeñas entidades e impacta, directamente, en el marco de la seguridad.

En este orden de ideas, otro enfoque del autor Thomas X. Hammes relaciona estas causas individuales y la globalización en torno al terrorismo en la expresión “nets and jets” (redes y aviones), donde las redes se encargan de distribuir información clave, de proveer recursos y de constituir campos de reclutas a futuro; mientras que los aviones se encargan de proveer la intención global, con bajo costo y efectividad para trasladar y

contrabandear armas, resultando en individuos y pequeñas células que predominan como agentes primarios de terrorismo.

Lo anterior, se resume de la siguiente forma:



Elaboración propia

Este tipo de guerra, llamada sin restricciones, tiene una característica única: no tiene líder, y se recarga en individuos con mínima y sin dirección desde una organización central. El factor tecnológico es vital para su desarrollo, sumado a la proliferación de diversos actores internacionales, la elevación del elemento transnacional y las nuevas relaciones humanas, causando un efecto acumulativo difícil de contener.

Es así, que las estrategias de prevención ante procesos de radicalización resultan rebasadas frente al avance de las amenazas asimétricas. Entendidas como la planificación de una serie de acciones que se dirijan a la toma de decisiones, se identifica principalmente dos tipos de estrategias relacionadas a terrorismo y a procesos de radicalización:

- a) Relacionadas a soft power (países del norte de Europa).
- b) Relacionadas al law enforcement (Estados Unidos).

Por un lado, la preponderancia en la participación del Estado y de organizaciones no gubernamentales a la inclusión de migrantes africanos y asiáticos se enfrenta a la constante reafirmación nacional del estado receptor. Por el otro, estrategias encaminadas

a la disuasión judicial, en primera instancia, con penas acotadas a terrorismo, y por supuesto, al refuerzo de los servicios de seguridad e inteligencia.

Ambos tipos de estrategias, distintas y similares a la vez, buscan contrarrestar la volatilidad de ataques terroristas, no obstante, la contención al rubro tecnológico, el desarrollo de la ética y *compliance* en el uso de herramientas tecnológicas y las diversas intenciones en el uso de éstas reconfiguran la óptica desde la cual se debe atender al terrorismo y su vinculación actual con la inteligencia artificial, ya que la gobernanza en la lucha contra el terrorismo es inexistente y se aborda de forma selectiva, con importantes lagunas en la transparencia, la supervisión y las restricciones jurídicas multilaterales (Martini, 2024).

Por ejemplo, el derecho de la inteligencia artificial es el relacionado al derecho que se encarga de regular las actividades y consecuencias de la inteligencia artificial, con la finalidad de prevenir y contender los posibles efectos sociales negativos que ésta puede llegar a tener (Cáceres Nieto, 2024). Excepto algunos casos comunitarios como la Unión Europea, la legislación de la inteligencia artificial y su uso ético es todavía un rubro pendiente por desarrollar por parte de la comunidad internacional.

Finalmente, se destaca que no se encontró evidencia de ejemplos históricos de ataques terroristas cometidos por inteligencia artificial, sólo existe evidencia de su uso como herramienta, no obstante, como veremos en el siguiente apartado, esta quinta ola del terrorismo se representa a través de individuos y grupos sociales específicos con un consumo exacerbado de internet, así como de redes neurales específicas de inteligencia artificial.

*Por otro lado, no es nada desdeñable, la capacidad de tomar decisiones de forma autónoma y con una rapidez nunca vista hasta nuestro tiempo.*

(Calvillo Cisneros, 2024)

### Radicalización e inteligencia artificial como herramienta: ¿posible autonomía en un futuro?

El texto de Klausen, Champion, Needle, Nguyen y Libretti (Jytte Kalusen, 2016) sobre trayectorias internas de radicalización

establece como primera hipótesis, que el proceso de radicalización, incluso individual, no tiene una temporalidad específica para su desarrollo ni existe algún consenso formal sobre algún perfil radical relacionado al nivel socio económico y al entorno.

Contrario a esto, es común encontrar posibles atacantes con buena educación y una economía saludable al interior del Estado, es decir, individuos que se rigen bajo las normas legales y sociales, preferentemente de bajo perfil.

Ejemplificando lo anterior, los autores exponen variables dinámicas que a su opinión componen el proceso de radicalización:

**Proceso político + Ideología + Experiencias propias +  
Antecedentes sociales + Demografía = Radicalización**

Estudios previos como el de Samuel Musa y Samuel Bendett (Musa & Bendett, 2010) ya consideraban al factor tecnológico como catalizador en procesos de radicalización de musulmanes en Estados Unidos.

De acuerdo con este texto, los modelos para entender procesos de radicalización se concentraron anteriormente en interacciones personales entre aquellos que predicaban y propagaban una acción forzosa en el nombre de la religión y aquellos que recibían el mensaje, es decir, un comunicado desde un líder carismático o un clérigo musulmán, tomando en cuenta otros factores como el adoctrinamiento y el contacto con algún grupo:

No obstante, este modelo de radicalización no contemplaba el factor tecnológico que en la actualidad facilita el proceso de radicalización:



Figure 1. Disrupting radicalization patterns.

Pre-2009 general radicalization model involved individuals dedicated to their cause who lived, trained and received indoctrination, advice and support from within the Muslim community's radicalized elements.



Present and future radicalization model takes the Muslim community and access to religious message into consideration, but does not require it – knowledge and radical Islamic message can be obtained from the Internet by an individual who was assimilated into larger American society.

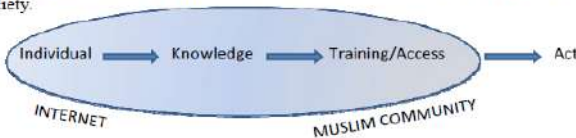


Figure 2. The changing nature of Islamic radicalization in the United States.

Como podemos observar, en la periferia entre el individuo y su adoctrinamiento se encuentran dos variables: el internet y la comunidad musulmana. Recursos, información y tecnología se detectaron directamente como elementos dentro del proceso de radicalización en la comunidad musulmana, misma que ha crecido exponencialmente a través de tiempo en Estados Unidos.

En este contexto, la recopilación de información sobre individuos dentro de una comunidad más grande no está exenta de

problemas y controversias, ya que las preocupaciones sobre la seguridad y la recopilación de inteligencia se reúnen con las cuestiones constitucionales de los derechos humanos y discriminación.

Bajo esta argumentación, los procesos de radicalización parten como un problema primario desde la concepción desintegradora de la sociedad. Por un lado, los flujos migratorios hacia Europa y Estados Unidos no son concebidos desde una apuesta de multiculturalidad de la parte receptora, sino como una carga económica que evoluciona hacia un nacionalismo ferviente. Por el otro, esta postura no integradora genera sentimientos de miedo, ira y frustración.

Naturalmente, este proceso de radicalización evoluciona en un radicalismo que, de acuerdo con la tendencia que analizaremos en capítulos posteriores, se postrará al interior del Estado. Entendido como un conjunto de ideas extremas que buscan la reforma profunda en el orden político o social, el radicalismo no sólo aguarda desde los partidos políticos de extrema derecha o desde los guetos musulmanes en Europa, también se acerca desde el individuo.

Este radicalismo al interior del Estado puede incluir elementos ideológicos que por su naturaleza se contraponen con los valores políticos, sociales y morales establecidos y aceptados, con base en el contrato social entre el Estado y los ciudadanos, por ejemplo, la supremacía blanca o una visión extremista del islam.

Finalmente, sin la prevención y atención adecuada a la fragmentación social, a la poca inclusión de migrantes, la reafirmación de identidad nacional y las barreras impuestas a la multiculturalidad, concatenados estas variables a un entorno económico que promueve sólo la riqueza de las élites, consecuentemente los procesos de radicalización son ya una amenaza a la permanencia del Estado.

Por otro lado, el empoderamiento de las máquinas es una realidad. Una crisis de generación de conocimiento y resolución de problemas acompañada de la revolución industrial actual cimbra en los cimientos de lo físico.

La inteligencia artificial se refiere al desarrollo de sistemas de computadoras que cuentan con la capacidad de realizar tareas que regularmente requieren de inteligencia humana (Anakotta, 2024), y está transformando cualitativa y cuantitativamente el desarrollo de tareas, al reducir el esfuerzo humano y los recursos necesarios para llevarlas a cabo, lo que permite realizar tareas complejas con rapidez y precisión (Martini, 2024). Es así, que la transición hacia la digitalización y el internet de las cosas no se encuentra en proceso, sino que ya moldea cada aspecto de la vida diaria y facilita, con consecuencias que no son detectadas por los grupos sociales, la resolución de problemas.

El uso de la inteligencia artificial tiene un impacto significativo y forma parte de cambios revolucionarios en el entendimiento de la vida cotidiana. La asistencia digital, a través de entornos hostiles y de incertidumbre durante la pandemia mundial por COVID-19 fue capaz de rescatar, mantener y recuperar todos aquellos procesos cotidianos opacados por el resguardo sanitario y la poca o nula preparación ante una crisis de magnitudes no sólo económicas, sino con impacto psicológico en individuos y grupos sociales diversos.

Por lo que, regularizados los procesos cotidianos, la transición hacia lo digital era ya una realidad. No obstante, el resguardo también generó tropiezos en dichos procesos, principalmente representados, por ejemplo, en violencia digital <sup>1</sup>, donde el anonimato de las redes dificulta la identificación del origen y potencializa violencia en diversas modalidades.

La violencia digital, por ejemplo, es aquella que se comete y expande a través de medios digitales como redes sociales, correo electrónico o aplicaciones de mensajería móvil, y que causa daños a la dignidad, la integridad y/o la seguridad de las víctimas (OVIGEM, 2020). Este anonimato se enmascara a través de la digitalización de las cosas y prolifera en el uso de redes sociales como herramienta, en primer lugar, por razones basadas en

---

<sup>1</sup> Para una mayor comprensión respecto a violencia digital, brecha digital y violencia de género en redes, se recomienda consultar el reporte de la Organización de las Naciones Unidas “Violencia contra mujeres y niñas en el espacio digital” (2020):

<https://mexico.unwomen.org/sites/default/files/Field%20Office%20Mexico/Documents/Publicaciones/2020/Diciembre%202020/FactSheet%20Violencia%20digital.pdf>

seguridad digital; en segundo lugar, con el aprovechamiento de encontrarse detrás de un equipo de cómputo que dificulte la identificación de datos básicos del usuario.

Es así, el uso de redes sociales funge como catalizador de violencia digital y desinformación. Por ejemplo, durante el desarrollo de la pandemia sanitaria por COVID-19, el movimiento anti -confinamiento impulsó en Alemania un entorno en el que se difundían entreveradas ideas conspirativas y de extrema derecha, en especial a través de las redes sociales (Hammer, 2024).

Las redes sociales, e Internet en general, por tanto, desempeñaron un importante papel en la radicalización de las personas como en su movilización en las manifestaciones. Para el caso mencionado anteriormente, en Europa estos actores de extrema derecha han ido desarrollando su propia infraestructura de plataformas más pequeñas y marginales, aunque reforzando un abanico tecnológico de mayor amplitud, mediante la denominada *Alt-Tech*, de las cuales se pueden diversificar en tres tipos (Hammer, 2024):

- a) las redes sociales creadas por miembros de movimientos extremistas;
- b) las plataformas reacias a regular los contenidos por razones ideológicas o empresariales; y,
- c) plataformas secuestradas que simplemente carecen de la capacidad necesaria para poder moderar sus contenidos.

Un ejemplo de ello es el reporte de la organización *Tech Against Terrorism*, que mediante su informe *Mapeo de la extrema derecha Mapping Far - right Terrorist Propaganda Online* publicado en 2024 y que abarcó el periodo comprendido de febrero de 2021 a noviembre de 2023, realizó un mapeo y estudio del uso de redes por parte de organizaciones e individuos terroristas (Tech Against Terrorism, 2024).

Los resultados confirman la postura plasmada en este texto sobre la adaptación del terrorismo al entorno digital. Durante la revisión, Tech Against Terrorism ha identificado consistentemente un mayor volumen de contenido terrorista relacionado con terroristas "solitarios" que con grupos designados de extrema derecha, lo que sugiere que el contenido producido por atacantes es más prominente en los espacios de extrema derecha (Tech Against Terrorism, 2024):



Lo anterior, es congruente con los procesos de individualización descritos en el primer apartado de este texto, donde las prioridades en el entorno actual se visualizan en necesidades personales o en pequeños grupos.

En adición a lo anterior, otro hallazgo importante del reporte está relacionado con la propagación de mensajes con connotaciones extremistas de carácter oficial por organizaciones reconocidas en algunos países como terroristas en internet, entre ellas algunas con base en Estados Unidos y Europa, por ejemplo, *Blood and Honour* (Tech Against Terrorism, 2024):

	UN	EU	US State	US Treasury	UK	Canada	Australia	New Zealand
Atomwaffen Division					●	●		
<i>National Socialist Order</i>					●	●	●	
Blood and Honour						●		
Combat 18						●		
Feuerkrieg Division					●			
National Action					●			
<i>National Socialist Anti-Capitalist Action</i>					●			
<i>Scottish Dawn</i>					●			
<i>System Resistance Network</i>					●			
Proud Boys						●		●
Russian Imperial Movement			●	●			●	
Sonnenkrieg Division					●		●	
The Base					●		●	●
James Mason						●		

● Designated terrorist entity      ● Designated under a synonym or umbrella group or by affiliation

El confinamiento por la pandemia sanitaria mundial y la amplitud de plataformas tecnológicas abre un espectro de opciones al consumidor, sin embargo, también extiende un panorama difícil de cubrir para las autoridades y empresas, debido al contenido postulado en plataformas con mayor apertura de difusión que las tradicionales: las plataformas *Alt-Tech* desempeñan un papel clave

en las estrategias de los agentes de extrema derecha para esquivar la moderación de contenidos o su percepción de la censura en Internet, encontrando, por ejemplo, vídeos negacionistas del Holocausto e imágenes de ataques terroristas de extrema derecha, como el tiroteo que tuvo lugar en 2022 en Buffalo (Nueva York), que dan una muestra del uso de la libertad de expresión y la política de escasa moderación de contenidos por parte de Odysee (Hammer, 2024).

La ausencia de disuasión, control e identificación de usuarios con connotaciones ideológicas extremistas es consecuencia de la denominada Web 2.0, donde (Daimon, 2024):

- a) la desinformación se ha potenciado por la difusión masiva a través de usuarios y bots;
- b) los "filtros de burbuja" limitan la exposición a ideas contrarias, reforzando posturas ideológicas;
- c) la radicalización se produce por la interacción con grupos afines, creando una falsa polarización; y,
- d) la moderación de contenidos es un desafío, con técnicas automatizadas que no siempre son efectivas.

A estas características en el entorno digital, con base en Daimon, se le conoce plataforma derivada de la Web 2.0, donde la aceleración de la información dificulta la disuasión, el control y la identificación de usuarios y el contenido publicado, sumado al consumo exacerbado y al comportamiento adictivo de usuario por el consumo de éste, conocido como *scrolling*<sup>2</sup>.

La nueva forma de flujo de información y la llegada de Internet han precipitado una transformación radical en cómo se difunde la información, ejerciendo así una profunda influencia en la naturaleza de los desafíos de seguridad y las respuestas a ellos, incluyendo las legales (Bartko R, 2025). El canal por el cual los administradores de las plataformas han tratado de contener la propagación de contenido es a través de la automatización de regulación y moderación de contenido utilizando inteligencia artificial, no obstante, el uso de *jailbreaks* urge en poner atención al

---

<sup>2</sup> Diversas publicaciones médicas analizan el fenómeno de *scrolling o doom scrolling* durante la pandemia y sus consecuencias psicológicas: algunas se pueden encontrar en los siguientes links:

- a) [Scrolling for data or doom during COVID-19? - PMC](#)
- b) [Doomscrolling dangers - Harvard Health](#)

uso de redes sociales e inteligencia artificial en la propagación de contenido extremista.

Los sistemas de IA operan con niveles significativos de automatización e incluyen varias iteraciones, como la IA algorítmica, la IA generativa, los grandes modelos de lenguaje (LLM) y las máquinas de aprendizaje profundo, en ese sentido, esas bondades operativas explotan vulnerabilidades que permiten que los terroristas aprendan, planifiquen y propaguen sus actividades con mayor eficiencia, precisión e impacto que nunca (Molas & Heron, 2024).

Un ejemplo de ello es conseguir el objetivo de aprender habilidades y herramientas técnicas y promover contenido extremista, así como desarrollar procesos de radicalización.

Comentan los autores citados en párrafos anteriores que algunos usuarios llegan incluso a compartir indicaciones codificadas, es decir, instrucciones aparentemente inofensivas, pero que están diseñadas para desbloquear contenido prohibido sin ser detectadas. Esto puede ocurrir con indicaciones que combinan palabras y símbolos (Molas & Heron, 2024).

Otro ejemplo se relaciona con la creación de imágenes generadas por inteligencia artificial, el uso de la difusión en el procesamiento de imágenes y la visión artificial, resultando en la generación de imágenes originales y coherentes a partir del texto, considerada una táctica ampliamente utilizada y útil para obtener contenido extremista y conspirativo que sólo se detecta mediante observación manual (Molas & Heron, 2024).

Lo anterior, reduce el ruido de la imagen y una variación aleatoria en la señal, sin eliminar partes significativas del contenido, las cuales son importantes para su interpretación, por lo que estas habilidades y herramientas técnicas aprendidas y desarrolladas a partir de los requerimientos técnicos de la inteligencia artificial, son importantes para producir propaganda de alta calidad.

En este orden de ideas, los *jailbreaks* son frases escritas que intentan eludir las salvaguardas éticas de un modelo de IA y obtener información prohibida. Utiliza indicaciones creativas en lenguaje sencillo para engañar a los sistemas de IA generativos para que publiquen información que, de otro modo, sus filtros de

contenido bloquearían (Weimann & Alexander T. Pack, 2024). Es decir, la automatización para moderar el contenido no logra contener técnicas de generación y propagación de contenido extremista, por lo que, la regulación y generación de contenido en plataformas tecnológicas es un área de oportunidad para administradores de plataformas.

En la era digital actual, las redes sociales han transformado radicalmente la forma en que las personas se comunican y acceden a la información. Sin embargo, estas plataformas también se han convertido en un caldo de cultivo para la propagación del ciberextremismo (Tahat K, 2024). Partiendo de esta idea, la diseminación de diversos tipos de contenido extremista eleva el riesgo significativo de radicalización y reclutamiento en línea, tanto de individuos como de grupos sociales, donde los grandes modelos de lenguaje tienen el potencial de permitir a los terroristas aprender, planificar y propagar sus actividades con mayor eficiencia, precisión e impacto que nunca (Weimann & Alexander T. Pack, 2024), por tanto, esta evolución tecnológica refuerza contenido extremista mediante un impacto eficaz en el consumidor.

Mediante subcampos de la inteligencia artificial como *machine learning* y los diversos algoritmos contenidos en ella, los grupos terroristas están explotando tecnologías de inteligencia artificial para diseminar su propaganda en varias plataformas en línea y a través de herramientas como chat-GPT, buscan influir en el sentimiento público y ampliar el impacto de sus ataques (Esmailzadeh, 2024),

Por tanto, el terrorismo, como fenómeno y como técnica, transitó del escenario convencional, a la digital con éxito, sobre todo, a través de adaptación y resiliencia, por un lado, a las nuevas exigencias de consumidor digital, y por el otro, con técnicas de identificación de vulnerabilidades de puntos críticos a nivel institucional y societal, destacando, entre otros, los relacionados a:

- propaganda: la inteligencia artificial se puede utilizar para generar y distribuir contenido de forma más rápida y eficiente;
- reclutamiento interactivo: los *chatbots* impulsados pueden interactuar con posibles reclutas, proporcionándoles información personalizada en función de sus intereses y

creencias, donde cada *jailbreak* se procesa individualmente. Esto puede utilizarse con fines de reclutamiento o para difundir discursos de odio e ideologías radicales. Los bots también pueden amplificar este contenido, dificultando su detección y respuesta;

- ataques automatizados: los terroristas pueden usar inteligencia artificial para llevar a cabo ataques de manera más eficiente y efectiva, por ejemplo, utilizando drones u otros vehículos autónomos;
- explotación de las redes sociales: también se puede utilizar para manipular las redes sociales y otras plataformas digitales para difundir propaganda y reclutar seguidores.
- ciberataques: los grupos extremistas pueden utilizar inteligencia artificial para mejorar su capacidad de lanzar ciberataques contra objetivos, causando potencialmente daños significativos.

Por tanto, los algoritmos de inteligencia artificial se pueden utilizar para analizar la actividad en las redes sociales, identificar a individuos que pueden ser receptivos a ideologías extremistas y, luego, dirigirles mensajes y contenido personalizados (Esmailzadeh, 2024), vulnerabilidades principalmente detectadas en individuos y grupos sociales acotadas y desarrolladas como consecuencia de la política de confinamiento por la pandemia sanitaria mundial.

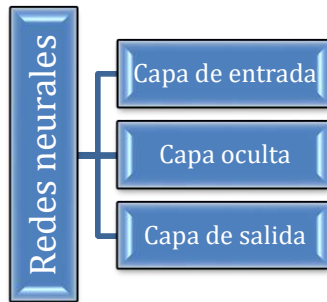
Con base en lo asentado anteriormente, la inteligencia artificial como herramienta que permite acceso a conocimiento acorde a un fin extremista es una de las grandes preocupaciones de los servicios de seguridad, principalmente a través del análisis masivo de datos de la red.

Con relación a lo anterior, podemos decir que la *Big data* es un conjunto de datos masivos, complejos y de alta velocidad, que impulsan la evolución de la toma de decisiones de la inteligencia artificial (Anakotta, 2024), y es mediante ésta que, en su evolución natural, la inteligencia artificial podría comenzar a tomar decisiones por cuenta propia.

Conocidas como redes neurales, su diseño se encuentra basado en el cerebro humano para realizar tareas de forma repetida para mejorar sus resultados, es decir, son un tipo de arquitectura informática que se basa en un modelo del funcionamiento del

cerebro humano (de ahí el nombre "neuronal"). Las redes neuronales están formadas por un conjunto de unidades de procesamiento denominadas "nodos". Estos nodos transmiten datos entre sí, igual que en el cerebro las neuronas se transmiten impulsos eléctricos (Cloudflare, 2025).

Como lo explica *Cloudflare*, las redes neuronales están compuestas por un conjunto de nodos, los cuales se encuentran distribuidos en, al menos, tres capas:



Elaboración propia

Toda red neural cuenta con estas tres capas, en algunos casos se cuenta con más de una capa oculta. Independientemente de la capa de la que forme parte, cada nodo realiza algún tipo de tarea o función de procesamiento sobre cualquier entrada que reciba del nodo anterior, es decir, de la capa inicial o de entrada. Cada nodo contiene una fórmula matemática, con cada variable dentro de la fórmula ponderada de forma diferente. Si el resultado de aplicar esa fórmula matemática a la entrada supera un determinado umbral, el nodo pasa los datos a la siguiente capa de la red neuronal.

Son una herramienta fundamental dentro del campo de la inteligencia artificial, puesto que permiten simular el funcionamiento del cerebro humano y mejorar las capacidades de aprendizaje y toma de decisiones de los sistemas de inteligencia artificial, destacando avances en las siguientes industrias (Culturaai, 2024):

- a) medicina: las redes neuronales se emplean para el diagnóstico de enfermedades a través del análisis de imágenes médicas y datos clínicos.

- b) sector financiero: las redes neuronales se aplican en la detección de fraudes y el análisis de riesgos.
- c) industria automotriz, las redes neuronales se utilizan en sistemas de asistencia al conductor y en la conducción autónoma.

Con anterioridad, mencionamos los subcampos que componen y coadyuvan al funcionamiento de las plataformas de inteligencia artificial. El aprendizaje automático, conocido en la jerga tecnológica como *machine learning*, entendida como la rama de la inteligencia artificial que entrena a las máquinas para imitar el comportamiento humano y de esta forma, generar una interacción predictiva que permita la interrelación entre ambos.

Otra rama es la del aprendizaje profundo. Con base en lo establecido por AWS Amazon, es un método de inteligencia artificial que enseña a las computadoras a procesar datos de una manera inspirada en el cerebro humano y son capaces de reconocer imágenes complejas, textos, sonidos y otros patrones de datos, a fin de generar información y predicciones precisas (Amazon Q, 2025).

En ambos casos, encontramos características técnicas que permiten generar entrenamiento específico que asimile e imite el comportamiento humano a través de reconocimiento de patrones de datos con el objeto de generar predicciones, no obstante, la inteligencia artificial puede ejecutar de manera autónoma algoritmos que contienen desinformación y noticias falsas utilizando Aprendizaje Automático y Aprendizaje Profundo (Anakotta, 2024), incluso, proporcionando asistencia digital, colaborando activamente en lo que podemos denominar ciberterrorismo.

En adición a lo anterior, se suma el problema del sesgo que la inteligencia artificial puede, inadvertidamente, pero de forma problemática, perpetrar y amplificar, ya que se entrena con enormes cantidades de datos generados por humanos y que pueden, por ejemplo, contener sesgos raciales, étnicos o de género, como ocurre con la lucha contra el terrorismo y la prevención y el control del extremismo violento (Martini, 2024).

Estos ejemplos demuestran el uso de la inteligencia artificial como herramienta para radicalizar, propagar ideología extremista,

planear y dirigir ataques de corte terrorista, no obstante, sugerimos que, a través de dichos requerimientos técnicos concretos en relación con las redes neurales y los subcampos y ramas de la inteligencia artificial, la inteligencia artificial desarrollará patrones, escenarios y predicciones autónomas<sup>3</sup>, debido al aceleramiento de la evolución tecnológica.

Lo anterior, consecuencia de la concatenación de las siguientes variables:

1. Un entorno digital de incertidumbre e inmediatez, polarizado por el aplastamiento del Estado sobre el individuo y grupos sociales, catalizando procesos de radicalización en el marco de una asimetría del conflicto.
2. La ausencia de una supervisión jurídica sólida del entorno digital y tecnológico, específicamente del uso de la inteligencia artificial.
3. Una constante evolución y aceleración de las ramas de la inteligencia artificial y aspectos técnicos.
4. La masiva cantidad de datos generada por humanos con sesgos raciales, étnicos o de género, así como posturas políticas y religiosas extremistas como insumo del análisis de datos masivo que realizan las plataformas de inteligencia artificial.
5. La adaptación desarrollada por el terrorismo ante el entorno digital.

### **Conclusiones:**

La inteligencia artificial es una herramienta de resolución de problemas que ofrece grandes posibilidades para la revolución industrial inteligente. Además de ayudar a recopilar datos relevantes, identificar alternativas, tomar decisiones, llevar a cabo acciones, revisar decisiones y hacer predicciones inteligentes.

En el entorno digital, el internet de las cosas (IoT) es un rubro fundamental de la llamada cuarta revolución industrial,

---

<sup>3</sup> Un ejemplo desde el ámbito militar, lo encontramos en las denominadas “armas autónomas”, aquellas que son capaces de llevar a cabo una misión sin intervención humana, ni en la toma de decisiones sobre cómo actuar, ni en la ejecución de la tarea militar (Cáceres Nieto, 2024).

proporcionando una infraestructura global para recopilar y procesar datos, incluyendo almacenamiento, análisis masivo de datos y tecnología de comunicación que sostienen gran parte de nuestra vida diaria.

La crisis del modelo democrático y el consecuente aplastamiento estatal hacia grupos sociales e individuos no ha reducido el impacto económico y psicológico generado por la pandemia sanitaria mundial, la cual obligó al modelo centralizado estatal a virar hacia el espacio tecnológico y su prominente aceleración a través de los años.

Desde una óptica de la seguridad, estas variables potencializaron procesos de radicalización, propagación de ideología extremista y facilitaron la planificación de ataques a través de la adaptación del terrorismo al entorno digital. Si bien la motivación política necesaria para considerar a un grupo o individuo terrorista se pudo diversificar, es también cierto que el enfoque terrorista de violencia premeditada se mantuvo a pesar de flotar en el espectro tecnológico, aprovechando la bondad de la velocidad con que viaja la información y por, sobre todo, la potencialización de su mensaje.

Es así, que el uso de la inteligencia artificial como herramienta para coadyuvar a los objetivos de dichas organizaciones e individuos es una realidad, no obstante, ante la deficiencia del control de la moderación de contenido en redes y técnicas que encubren el verdadero mensaje del terrorismo incluso en motores de búsqueda y aplicaciones de inteligencia artificial, generaron un vacío legal y operativo de los administradores de las plataformas.

El acelerado avance tecnológico y de sus herramientas, incluida las de inteligencia artificial y de sus redes neurales, sugieren un progreso que destinará sus esfuerzos, ante la ausencia de un contrapeso jurídico y de control, en la automatización de la inteligencia artificial no sólo como herramienta, sino como tomador de decisión, y por tanto, un posible atacante con autonomía operativa y poder de decisión sin intervención humana.

## **Bibliografía:**

Hammer, D., & Matlach, P. (2024). \*La lucha en Internet contra la radicalización de extrema derecha\*. En \*Anuario Internacional CIDOB 2025\* (pp. 135-137). CIDOB

Reflexiones sobre la inteligencia artificial aplicada al derecho y el derecho de la inteligencia artificial: ¿vamos hacia el mundo de black mirror?  
Enrique Cáceres Nieto

Revista del posgrado en derecho de la UNAM |  
revista.rpd@posgrado.unam.mx año 12, N° 20, Enero - Junio 2024 |  
<https://doi.org/>

Martini, Alice (2024). AI, counter-terrorism and global governance: state of the art. *Revista de Paz y Conflictos*, Vol. 17 pp. 205-221, DOI: <https://doi.org/10.30827/revpaz.17.31319>

“Say it’s only fictional”: How the Far-Right is Jailbreaking AI and What Can Be Done About It  
Bàrbara Molas and Heron Lopes ICCT Report October 2024  
International Center for Counter - Terrorism

Metaverso y Seguridad Internacional. Riesgos y Potenciales Amenazas  
José Miguel Calvillo Cisneros Universidad Complutense de Madrid /  
España jcalvill@ucm.es <https://orcid.org/0000-0003-3340-184X>

Radicalización yihadista en España: menores, espacios virtuales y la resonancia de conflictos internacionales Álvaro Vicente Investigador,  
Programa sobre Radicalización Violenta y Terrorismo Global, Real Instituto Elcano | @alvaro\_vicentep

Tahat K, Habes M, Mansoori A, et al.  
(2024). Algoritmos de redes sociales para combatir el ciberextremismo: Una revisión sistemática. *Revista de Infraestructura, Política y Desarrollo*. 8(8): 6632.  
<https://doi.org/10.24294/jipd.v8i8.6632>

Bartko R, Kelemen R. (2025).  
Hackers en funciones de ciberterrorismo  
*Revista de Infraestructura, Política y Desarrollo*. 9(2): 10979.  
<https://doi.org/10.24294/jipd10979>

Generating Terror: The Risks of Generative AI Exploitation By Gabriel Weimann, Alexander T. Pack, Rachel Sulciner, Joelle Scheinin, Gal Rapaport, and David Diaz. *CTC Sentinel*. January 2024. Volume 17 Number 1.

Daimon. Plataformización, automatización y aceleración en los medios sociales. Revista Internacional de Filosofía, n° 93 (2024), pp. 137-152  
ISSN: 1130-0507 (papel) y 1989-4651 (electrónico)  
<https://doi.org/10.6018/daimon.612051>

Esmailzadeh, Y., & Motaghi, E. (2024). \*International terrorism and social threats of artificial intelligence\*. Journal of Globalization Studies, 15(1), 168-179.  
<https://doi.org/10.30884/jogs/2024.01.09>

Anakotta, M. Y. (2024). \*AI: A new lone-wolf terrorism in the digital era (preliminary analysis)\*. \*Journal of Terrorism Studies, 6\*(2), Article 7.  
<https://doi.org/10.7454/jts.v6i2.1083>

Organización de las Naciones Unidas “Violencia contra mujeres y niñas en el espacio digital” (2020):  
<https://mexico.unwomen.org/sites/default/files/Field%20Office%20Mexico/Documentos/Publicaciones/2020/Diciembre%202020/FactSheet%20Violencia%20digital.pdf>



## EL NUEVO SISTEMA NACIONAL DE INVESTIGACIÓN E INTELIGENCIA: HACIA LA CONFORMACIÓN DE UNA AMPLIA COMUNIDAD Y SU ARMONIZACIÓN MEDIANTE UN CÓDIGO DE ÉTICA

Martín Granillo\*

**Resumen:** A mediados de 2025, la reforma legal que crea un Sistema Nacional de Investigación e Inteligencia en materia de seguridad pública abre paso a una comunidad amplia de inteligencia que articula actores públicos, privados y de la sociedad civil. Con base en los principios deontológicos que delimita el Código Nacional de Procedimientos Penales para el analista criminal en las fases de la investigación, se tiende un puente para identificar valores comunes -entre analistas de los tres órdenes de gobierno y analistas privados- útiles a una propuesta de ética aplicada. La intención es sugerir cómo desde la actuación de gabinete, sería posible contribuir a disminuir la percepción de desconfianza ciudadana en el desempeño de los cuerpos policiales.

**Palabras clave:** inteligencia para la seguridad pública, percepción ciudadana de confianza, código de ética, sesgos cognitivos.

**Abstract:** By mid-2025, the legal reform creating a National System of Investigation and Intelligence in Public Security matters will pave the way for a broad intelligence community that articulates public, private, and civil society actors. Based on the deontological principles outlined in the National Code of Criminal Procedure for criminal analysts in the investigative phases, a bridge is built to identify common values—among analysts from the three levels of government and private analysts—that are useful for a proposal for applied ethics. The intention is to suggest how, through cabinet-level action, it would be possible to contribute to

---

\*Maestro en Anticorrupción y Licenciado en Estudios Latinoamericanos. Analista e investigador con experiencia en el sector privado. En la administración pública colaboró en: Policía Federal, Agencia de Investigación Criminal de la Fiscalía General de la República y Guardia Nacional. Ha sido instructor de Inteligencia en la Academia Superior de Seguridad Pública Federal y de Análisis Criminal en la Universidad de las Américas Puebla. Correo: [juamar@unam.mx](mailto:juamar@unam.mx)

reducing the perception of citizen distrust in the performance of police forces.

**Keywords:** intelligence for public safety, citizen perception of trust, code of ethics, cognitive biases.

## Introducción

La Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LNSI) es la condición de posibilidad legal para que surja, y se materialice en nuestro país, una amplia comunidad de inteligencia civil mexicana para la seguridad pública;<sup>1</sup> misma que nació el pasado 16 de julio de 2025,<sup>2</sup> y que por primera vez, se hará palpable en la vida cotidiana con la vinculación de agentes de inteligencia de entes privados, la sociedad civil u ONG, junto con los agentes de inteligencia estatales de los tres órdenes de gobierno.

Dicha comunidad se estará forjando de manera artesanal y primigenia, primero a través del diseño y homologación de bases de datos, la compilación o llenado de las mismas, su análisis y posterior vinculación, para conformar de manera conjunta, un extenso sistema de inteligencia útil a la toma de decisiones y la judicialización: la Plataforma Central de Inteligencia, que en sí misma, es una acción legal que contribuye a la praxis de la abarcadora comunidad de inteligencia civil.

Sin embargo, esta semilla jurídica, inaugura el espacio a nuevas relaciones que tendrán un asidero en experiencias de contribución concreta. Y es importante dar cuenta del papel activo que corresponderá a los agentes de inteligencia, -sean públicos, privados o bien de ONG'S-, en sus mutuas relaciones de intercambio de información, en una cadena que pasará de lo local/privado, a lo nacional/público, como un horizonte en el que

---

<sup>1</sup> La definición de Inteligencia en seguridad pública, de acuerdo con artículo 2, fracción IV de la LNSI es: *“la función estatal estratégica que, mediante diversos procesos y actividades, responde a la necesidad de que las autoridades cuenten con los insumos necesarios para la toma de decisiones en beneficio de la sociedad, a través del conocimiento obtenido a partir de la captación, el procesamiento, análisis y aprovechamiento de datos documentales, visuales, auditivos, audiovisuales y, en general, de cualquier información que permita identificar conductas que puedan comprometer la seguridad pública y ser constitutivas de delitos, con la finalidad de prevenirlas, denunciarlas, perseguirlas, juzgarlas y sancionarlas; por medio de la interconexión, el acceso, la consulta e integración de la información...”*

<sup>2</sup> La LNSI se publicó en el Diario Oficial de la Federación, el pasado 16 de julio.

pueden darse vínculos de colaboración para sumar a la procuración de justicia, al fortalecimiento de la seguridad y paz pública, así como favorecer una percepción de confianza en la propia comunidad de inteligencia, por parte de la ciudadanía.

### **Delimitación conceptual y jurídica**

Conviene separar con nitidez tres planos: (i) seguridad nacional, (ii) seguridad interior, y (iii) seguridad pública. En México, el órgano civil de inteligencia del Estado (Centro Nacional de Inteligencia) ha evolucionado con naturaleza jurídica propia y competencias exclusivas para la seguridad nacional; mezclar sus fines con los de la LNSI puede producir solapamientos institucionales. Una política sana de seguridad pública debe respetar esa frontera y, al mismo tiempo, apoyarse en marcos claros de seguridad interior para la coordinación intergubernamental.

En esa línea, los trabajos de la Revista de Inteligencia y Seguridad han documentado: la evolución y naturaleza jurídica del CNI (Casillas Zamora, 2024), la regulación de la seguridad interior (Jiménez Solano, 2024), y la función de la identidad nacional en el diseño de políticas de seguridad (Ruíz de la Cruz, 2024).

La comunidad de inteligencia para seguridad pública es, por definición, heterogénea. Incluye analistas de los tres órdenes de gobierno, áreas de seguridad patrimonial y cumplimiento en empresas, así como actores de la sociedad civil que generan insumos valiosos; por ejemplo, proyectos de georreferenciación de violencias o de mapeo ciudadano ante eventos de alto impacto. La LNSI no debe reducirse a interconexión tecnológica; demanda un cambio cultural: reconocerse parte de una sola comunidad con objetivos compatibles y reglas de conducta compartidas.

### **Comunidad emergente**

Las nuevas disposiciones legales abren brecha a una unión más significativa, que la que se efectúa únicamente a través de las bases de datos y la inmediatez tecnológica, pues compromete a los involucrados en una renovación del modo de pensar: el asumirse y sentirse parte de una misma comunidad de inteligencia en común, cualquiera que sea su procedencia, sean activistas, miembros de la

sociedad civil, trabajadores de la iniciativa privada o personal de dependencias gubernamentales.

En el mundo corporativo o empresarial, gran parte de las labores de inteligencia están inscritas en las áreas de seguridad patrimonial, o como parte de las políticas de prevención que tienen a su cargo las áreas de *Compliance*, para prevenir delitos y mantener la continuidad operativa de las empresas, sean de la banca, transporte, logística, sector energético, bienes de consumo etc.

En cuanto a miembros de la sociedad civil, previamente ha habido una participación voluntaria, sin coacción y de manera natural, en compartir datos y productos de inteligencia, que en su mayoría suelen ser georreferenciaciones de información. En lo que respecta a productos divulgados públicamente, elaborados a partir de datos gubernamentales, se pueden mencionar como ejemplo los que desde 2014 presenta Diego Valle en su página web: *Hoyo del crimen*<sup>3</sup> para la Ciudad de México; o el proyecto *Mapear las violencias*<sup>4</sup> de Fernanda Verduzco, que busca visibilizar distintos tipos de violencias –como feminicidio, homicidio y violación– en el Área Metropolitana de Guadalajara, para el periodo 2018 - 2024.

Por otro lado, caben destacar ejercicios realizados con datos no gubernamentales, como el mapa de denuncias de intentos de secuestro de mujeres en el metro de la Ciudad de México, que creó Zoé Láscari; inicialmente con testimonios que se han difundido en redes sociales desde 2018, y que después se amplió para nutrirse de información voluntariamente aportada a través de un formulario de *Google Forms*, abierto para recibir casos.<sup>5</sup>

Un notable esfuerzo de cooperación, por lo inmediato y espontáneo, es el que ocurrió en Sinaloa, al crear un mapa con reportes ciudadanos y de prensa, para compilar la ubicación donde estaban sucediendo narco bloqueos y enfrentamientos durante el

---

<sup>3</sup> Valle, D. (s.f.) Hoyo del crimen. Recuperado el 14 de julio de 2025 de: <https://hoyodecrimen.com/>

<sup>4</sup> Verduzco, F. (s.f.) Mapear las violencias. Recuperado el 14 de julio de 2025 de: <https://mapearlasviolencias.com/>

<sup>5</sup> Láscari, Z. (s.f.) Mapeando el secuestro de mujeres en el STC-Metro CDMX. Recuperado el 14 de julio de 2025 de: <https://docs.google.com/forms/d/e/1FAIpQLSdsjGFfw-wXPxapXi0OvDbG0Hfbs7bL-4So3MAe5XmXG9Jm3w/viewform>

segundo operativo para detener a Ovidio Guzmán, conocido como el Culiacanazo II,<sup>6</sup> acaecido el 5 enero de 2023.

Del mismo modo, posterior a la detención del Mayo Zambada, entre el 9 y el 18 de septiembre de 2024, se desataron diversos hechos violentos en los municipios de: Culiacán, El Dorado, Cosalá, San Ignacio, Elota y Concordia, que fueron georreferenciados por la *Revista Espejo*,<sup>7</sup> con información de notas periodísticas y denuncias de los pobladores, para sortear la falta de datos oficiales.

Desde luego que “es fundamental entender que no puede haber inteligencia sin datos” (Favennec y Amador 2025), pues son la materia prima del analista. Y es bien conocida la frase de lugar común: *A mejor materia prima, mejor producto*. Mejor producto de inteligencia, en este caso. Ya que, para los analistas y tomadores de decisión, será una delicia contar con más y mejores insumos, pues Plataforma México, el sistema de información que lo antecede, aun cuando es primordial y operable, tiene algunos registros no actualizados que aportan información que suele ser imprecisa u obsoleta.<sup>8</sup>

En contraparte a la entusiasta perspectiva de los agentes de inteligencia, es primordial asimilar como ciudadano, las dudas e inquietudes entorno a las intenciones gubernamentales, pues existe una extendida opinión poblacional “de vivir en el temor creciente y real de ser espionado y acusado de cualquier delito”, (Valadés 2025)

---

<sup>6</sup> El Financiero (2023, 5 enero). *Culiacán sitiado*. Recuperado el 14 de julio de 2025 de: <https://www.elfinanciero.com.mx/estados/2023/01/05/culiacan-sitiado-asi-lucen-los-bloqueos-en-sinaloa-desde-google-maps/>

<sup>7</sup> Revista espejo (2024, 19 septiembre). *Este es el mapa de la guerra en Sinaloa*. Recuperado de: [https://revistaespejo.com/2024/09/19/este-es-el-mapa-de-la-guerra-en-sinaloa/#google\\_vignette](https://revistaespejo.com/2024/09/19/este-es-el-mapa-de-la-guerra-en-sinaloa/#google_vignette)

<sup>8</sup> Como apunte para entender la desactualización de Plataforma México, está la falta de inversión, apoyo económico o fondos para designar a personal en los municipios del país, que además estén capacitados y destinados en sus funciones, para alimentar de manera constante la información que se interconecta, para así tener una plataforma permanentemente actualizada en información.

Otro dato para tomar en cuenta es la complejidad técnica en la integración de múltiples sistemas e integración de diversas y nuevas tecnologías. Cabe precisar que las instalaciones de Plataforma México, que albergan a sus servidores bajo tierra, ubicadas en Avenida Constituyentes de la CDMX, cumplirán en noviembre de 2025, 16 años de haber sido inauguradas y, de entonces a la fecha, han ocurrido diversos y diferenciados avances tecnológicos en las diversas fuentes que brindan interoperabilidad.

es decir, hay una sospecha de politización de los servicios de inteligencia en materia de seguridad pública.

A primera vista, para quien no es especialista en la consulta de bases de datos para la investigación criminal, las fuentes de información a las que apunta la nueva ley de inteligencia<sup>9</sup> pueden parecer inesperadas e intrusivas; sin embargo, en la práctica, dichas bases de datos están dispersas y, en caso de necesidad, se puede tener acceso fundado y motivado legalmente a cada una de ellas, acorde con las principales atribuciones de investigación penal que establece el Código Nacional de Procedimientos Penales para las fases de: conducción de la investigación;<sup>10</sup> ejecución de la investigación;<sup>11</sup> actos de investigación<sup>12</sup> y registro de investigación.<sup>13</sup>

---

<sup>9</sup> LNSI Artículo 24. Fuentes de información en general.- “*Todas las autoridades del Estado mexicano y las personas particulares que tengan a su cargo sistemas de inteligencia, bases de datos, registros y registros administrativos, tales como registros de datos vehiculares y de placas, biométricos, telefónicos, así como registros públicos de la propiedad y del comercio, registros de personas morales, catastros, registros fiscales, registros de armas de fuego, registros de armas de fuego aseguradas o decomisadas, registros de comercio, registros de personas prestadoras de servicios de seguridad privada, registros de padrones de personas detenidas y sentenciadas, registros de servicios financieros, bancarios, de transporte, salud, telecomunicaciones, empresariales, comerciales, registros en materia marítima y todos aquellos de donde se pueda extraer información, indicios, datos y pruebas para la generación de productos de inteligencia para la prevención, investigación y persecución de los delitos, deberán vincularse y colaborar con los órganos del Sistema Nacional, para su consulta de acuerdo con las formas y mecanismos previstos en esta Ley*”.

<sup>10</sup> CNPP Artículo 127 Competencia del Ministerio Público; Artículo 129 Deber de objetividad y debida diligencia; Artículo 131, fracciones III, IV, V, VI, VII, IX y X. Obligaciones del Ministerio Público.

<sup>11</sup> CNPP Artículo 272 Peritajes y Artículo 369 Título oficial.

<sup>12</sup> CNPP Artículo 251 Actuaciones en la investigación que no requieren autorización previa del Juez de control; Artículo 252 fracción III y VI Actos de investigación que requieren autorización previa del Juez de control; Artículo 291 Intervención de las comunicaciones privadas; Artículo 292 Requisitos de la solicitud; Artículo 293, Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas; Artículo 294 Objeto de la intervención; Artículo 295 Conocimiento de delito diverso; Artículo 296 Ampliación de la intervención a otros sujetos; Artículo 301 Colaboración con la autoridad; Artículo 302 Deber de secrecía y Artículo 303 Localización geográfica en tiempo real y solicitud de entrega de datos conservados.

<sup>13</sup> CNPP Artículo 217 Registro de los actos de investigación; Artículo 368 Prueba pericial y Artículo 132, fracción XIV Obligaciones del Policía.

Si bien es muy generalizada la percepción ciudadana de corrupción, apatía en el servicio y malas prácticas policiales,<sup>14</sup> cabe precisar que dichas percepciones usualmente son sobre labores de tránsito, proximidad social y despliegue operativo; es decir, aquellas que tienen trato y atención directa con la población. Muy por el contrario, las tareas de: compilación, consulta, análisis y explotación de bases de datos, suelen ser actividades de gabinete, no de campo.

Así, el nuevo énfasis legal de un modelo de inteligencia colaborativa entre entidades públicas y privadas,<sup>15</sup> cuya finalidad es anticipar dinámicas delictivas, neutralizar generadores de violencia y aportar evidencia en la toma de decisiones e integración de carpetas de investigación, puede despejar dudas ciudadanas y armonizar a los distintos grupos de interés, a través de un código de ética<sup>16</sup> transversal que incluya a las diversas partes involucradas.

## Ética aplicada y Plataforma Central de Inteligencia

Hoy en día, cada dependencia tiene su respectivo conjunto de normas, principios y valores, acorde a sus funciones, públicas o

---

<sup>14</sup> De acuerdo con la encuesta *Policía y sociedad. Corresponsabilidad de la seguridad en México*, Centro de Opinión Pública de la Universidad del Valle de México / Instituto para la Seguridad y la Democracia, A.C., 75% de los ciudadanos señalan que, de tener trato con la policía, predominaría un sentimiento de desconfianza; 67% señala que sentiría de temor y para 55% su sensación sería de rechazo. Los principales factores causantes de tal recelo son: la corrupción en la policía (79%); por malas experiencias propias o de algún conocido (71%); abusos cometidos (70%); por vínculos con la delincuencia o crimen organizado (53%); por considerar que no están capacitados (44%); porque no hacen bien su trabajo (40%) y porque las instituciones policíacas están desprestigiadas (36%).

<sup>15</sup> LNSI. Ver artículos: 24, Fuentes de Información; 25, Fuentes de Información en posesión de entes públicos; 26, Fuentes de Información en posesión de particulares y 29, Criterios Técnicos y de Homologación.

<sup>16</sup> De acuerdo con el glosario de integridad corporativa coeditado por la Secretaría de la Función Pública / Oficina de las Naciones Unidas contra la Droga y el Delito, que armoniza a la Ley General de Responsabilidades Administrativas del Gobierno Federal con la Convención de las Naciones Unidas contra la Corrupción (UNCAC), al código de ética/conducta, se le define como: “Declaración de principios y valores que establece expectativas y estándares obligatorios sobre la conducta de una organización, un organismo gubernamental, una compañía, un grupo de personas afiliadas o un individuo, incluidos los niveles mínimos de cumplimiento y las medidas disciplinarias en caso de omisión, para la organización, su personal y los voluntarios. El objetivo de dicho mecanismo es procurar que impere una conducta digna y ética que responda a las necesidades de la sociedad y que oriente su desempeño”.

privadas. Algunas empresas cuentan con código de conducta. Las corporaciones policiales tienen el suyo, e incluso, desde 2022 existe uno que abarca a todas las dependencias federales, el código de ética de la administración pública federal.<sup>17</sup>

No obstante, estamos todos ante un nuevo marco referencial jurídico para la operación de la seguridad pública del país, que ahora compromete a entes públicos y privados en la construcción, resguardo y transmisión de fuentes de información. Por tanto, es pertinente reinterpretar la relación de las distintas fuentes de las que abrevará la Plataforma Central de Inteligencia, para desarrollar un enfoque grupal, privilegiando una visión de conjunto, que enfatice la dinámica relacional de la amplia comunidad de inteligencia en seguridad pública.

La Plataforma Central de Inteligencia es una apuesta por nuevas fuentes para la investigación, que significa poder acceder donde antes no se podía mirar legalmente. Sin embargo, no es únicamente una transformación digital. La Plataforma sólo es el cascarón. El cambio que apertura la reforma legal, más que ser tecnológico, de infraestructura o interconexión, es de personas y nuevas maneras de pensar. Más trascendente que la parte tecnológica, está el componente social y humano.<sup>18</sup>

No es el sistema lo relevante, sino la inteligencia que genere. No hay que perder de vista que analizar los datos, sacarles provecho y realizar inteligencia es la labor de las personas, de las y los integrantes de la comunidad de inteligencia.

Por ello es menester hacer lo correcto desde donde estamos, ese es el verdadero eje, el punto de apoyo de la comunidad de inteligencia para contribuir no sólo a un México libre de corrupción, sino de una vez por todas, desde el análisis y las labores de gabinete, mejorar la percepción ciudadana que se tiene sobre la confianza y desempeño de las autoridades policiales.<sup>19</sup> Ya

---

<sup>17</sup> Código de Ética de la Administración Pública. (2022, 8 febrero) Diario Oficial de la Federación.

<sup>18</sup> Greg Satell aborda el énfasis de lo humano en el futuro de las innovaciones tecnológicas en sus diversos artículos publicados en Harvard Business Review, y también en el libro: *Cascades, How to create a Movement that drives transformational Change*, McGraw-Hill, 2019.

<sup>19</sup> Es conocido que la población en México identifica a la Marina y el Ejército, como autoridades con mayor confianza y nivel efectividad en su trabajo, y han

no depende sólo del trato directo de los agentes con la ciudadanía en campo.

Ahora, el foco de atención está puesto en las labores de gabinete. Es la oportunidad de crear valor público, desde la interpretación y análisis de los datos crudos aportados en las diversas bases de múltiples entidades. Analizar dichos datos, comprenderlos y transmitir el entendimiento de estos, es de gran valía para implementar acciones basadas en evidencia. De eso se trata hacer inteligencia. Y hacerla bien, será una mejora radical en la eficacia de servicios de seguridad, desde el gabinete.

Se propone un código de ética transversal para quienes alimentan o explotan la PCI. Tres ejes articuladores son: integridad (honestidad intelectual y prohibición de manipulación de datos), transparencia metodológica (trazabilidad de fuentes, replicabilidad, explicitación de inferencias) y responsabilidad (deber de cuidado, minimización de datos, seguridad de la información y control de sesgos). Este marco debe armonizarse con el deber de objetividad, debida diligencia y secrecía que ya exige el Código Nacional de Procedimientos Penales para las funciones de análisis.

A la luz de la tutela de derechos humanos, la ética profesional del análisis impone límites materiales y procedimentales: finalidad legítima, estricta necesidad, proporcionalidad de las medidas y mecanismos de supervisión externa. La literatura reciente subraya la compatibilidad entre inteligencia para la seguridad nacional y la protección de derechos fundamentales, siempre que se apliquen salvaguardas robustas (Toledo Utrera, 2024).

### **Deontología del analista criminal y valores en común**

En México, la figura del analista criminal emergió a un mayor impulso con la reforma constitucional del Sistema Penal Acusatorio, publicada en 2008, y cuya posterior implementación fue gradual en los estados de la república; aumentando así, paulatinamente, la exigencia de investigaciones técnicas sustentadas con datos verificables.<sup>20</sup>

---

salido con mejores indicadores en las distintas ediciones de la Encuesta Nacional de Victimización y Percepción de Seguridad Pública (ENVIPE) que realiza el Instituto Nacional de Geografía e Informática (INEGI).

<sup>20</sup> Programa de Formación Técnica y Asistencia Técnica en Análisis Táctico y Estratégico Nacional, Manual de Formación del Curso de Generación de

Aun cuando las responsabilidades del analista pueden diferir en las legislaciones de cada entidad federativa, y a pesar de que en los hechos “las funciones de análisis recaen en policías de investigación, peritos habilitados o incluso personas con profesiones ajenas al ámbito” (López y Valdés 2025) puede resultar muy útil situar las tareas de análisis en el contexto normativo de la investigación de delitos, para homologar criterio y obtener una deontología profesional en común.<sup>21</sup>

En el Código Nacional de Procedimientos Penales se establece el deber de objetividad y debida diligencia,<sup>22</sup> así como el deber de secrecía.<sup>23</sup> Ambos refieren el correcto actuar profesional del analista de los entes gubernamentales, dentro de las etapas del proceso de investigación penal. Por supuesto que también el analista de inteligencia de entes privados, que tiende a responder a objetivos empresariales o de mercado, con la nueva LNSI que involucra las bases de datos y sistemas de información privada, bien puede caber dentro del mismo paraguas profesional de rectitud normativa.

Igualmente, más allá de la normatividad, analistas públicos y privados practican una ética aplicada que está internalizada en su hacer cotidiano -ya que la finalidad del análisis de datos es

---

productos de análisis criminal para la investigación de delitos, INL/LabCo, México, 2024.

<sup>21</sup> Por deontología profesional se entiende el “debe ser” en un trabajo, profesión u oficio. Su objetivo es determinar normas, preceptos y reglas que regulen la conducta y el desempeño laboral encaminado hacia lo que es recto y apropiado. El término deontología fue usado por primera vez por el filósofo inglés Jeremy Bentham en su obra *Deontología o ciencia de la moral* (1834).

<sup>22</sup> CNPP, “Artículo 129. Deber de objetividad y debida diligencia. *La investigación debe ser objetiva y referirse tanto a los elementos de cargo como de descargo y conducida con la debida diligencia, a efecto de garantizar el respeto de los derechos de las partes y el debido proceso.*

*Al concluir la investigación complementaria puede solicitar el sobreseimiento del proceso, o bien, en la audiencia de juicio podrá concluir solicitando la absolución o una condena más leve que aquella que sugiere la acusación, cuando en ésta surjan elementos que conduzcan a esa conclusión, de conformidad con lo previsto en este Código.*

*Durante la investigación, tanto el imputado como su Defensor, así como la víctima o el ofendido, podrán solicitar al Ministerio Público todos aquellos actos de investigación que consideraren pertinentes y útiles para el esclarecimiento de los hechos. El Ministerio Público dentro del plazo de tres días resolverá sobre dicha solicitud. Para tal efecto, podrá disponer que se lleven a cabo las diligencias que se estimen conducentes para efectos de la investigación”.* CNPP.

<sup>23</sup> CNPP, “Artículo 302. Deber de secrecía. *Quiénes participen en alguna intervención de comunicaciones privadas deberán observar el deber de secrecía sobre el contenido de las mismas”.*

compartir su comprensión- así que naturalmente, por conciencia y motivación individual, ambos perfiles de analistas están orientados al esclarecimiento de hechos en su respectivo ámbito de acción.

Es preciso conservar una capa de valores comunes para permitir la realización efectiva de una comunidad de inteligencia que genere confianza ciudadana. Los agentes de inteligencia son personas concretas que interactuarán con otras personas analistas igualmente concretas. Juntos materializarán a la comunidad de inteligencia en seguridad pública en sus haceres y valores personales.

Por lo antes dicho, es oportuno comenzar a dar los primeros pasos en favor de plasmar y proponer una inicial declaración de principios y valores comunes sobre la conducta de los analistas, públicos y privados, que integrarán la comunidad de inteligencia, con el objetivo de procurar que impere un conducta digna y ética, que responda a la actual necesidad de confianza de la sociedad en la Plataforma Central de Inteligencia.

En este camino hacia la declaración de principios, se puede encontrar inspiración en la Comunidad de Inteligencia de los Estados Unidos, compuesta por un total de 18 entidades: nueve del Departamento de Defensa,<sup>24</sup> siete que pertenecen a otros departamentos,<sup>25</sup> y dos agencias independientes.<sup>26</sup> Dicha comunidad cuenta con sus respectivos Principios de Ética Profesional para su Comunidad de Inteligencia.<sup>27</sup>

---

<sup>24</sup> Defense Intelligence Agency (DIA); National Security Agency (NSA); National Geospatial-Intelligence Agency (NGA); National Reconnaissance Office (NRO); U.S. Air Force Intelligence; U.S. Navy Intelligence; U.S. Army Intelligence; U.S. Marine Corps Intelligence & U.S. Space Force Intelligence.

<sup>25</sup> Department of Energy's Office of Intelligence and Counterintelligence; Department of Homeland Security's Office of Intelligence and Analysis; intelligence and counterintelligence elements of the U.S. Coast Guard; Department of Justice's Federal Bureau of Investigation (FBI); Drug Enforcement Administration's Office of National Security Intelligence (DEA); Department of State's Bureau of Intelligence and Research & The Department of the Treasury's Office of Intelligence and Analysis.

<sup>26</sup> Office of the Director of National Intelligence (ODNI) & Central Intelligence Agency (CIA).

<sup>27</sup> Office of the Director of National Intelligence (s.f.) *National Intelligence Strategy* 2023, Recuperado el 14 de julio de 2025 de: <https://www.intelligence.gov/templates/intelgov-template/custom-sections/the-nis-at-a-glance/nis-2023/pdf/nis-2023.pdf>

El analista criminal es un pivote del sistema. La normatividad federal define su función en dimensiones estratégica y táctica, su aporte al ciclo de inteligencia y un catálogo de productos analíticos. Profesionalizar este rol —con estándares de competencia y metodologías replicables— eleva la calidad probatoria y la utilidad operativa de la información (Vignettes, 2024).

Lineamientos operativos sugeridos: a) distinguir explícitamente entre hipótesis y hallazgos, b) gestionar bancos de datos con criterios de clasificación, retención y acceso compatibles con transparencia y contrainteligencia, y c) documentar decisiones mediante bitácoras auditables.

### **Tres valores clave: integridad, transparencia metodológica y responsabilidad.**

En el caso mexicano, debido a que históricamente los servicios de inteligencia han sido legalmente delineados en el contexto de seguridad nacional<sup>28</sup>, se han enfocado, “al control de la ciudadanía, así como a la represión de enemigos o disidentes políticos contrarios a los intereses políticos del régimen autoritario, por medio de acciones que iban desde del espionaje telefónico y la vigilancia hasta la tortura o la desaparición forzada”, (Cáceres y Jasso, 2021, p. 170); por ello, los nacientes servicios de inteligencia para la seguridad pública pueden marcar distancia del pasado con el valor de la integridad.

Se requiere integridad para decir la verdad, incluso cuando es incómoda para el grupo de poder en turno, pues la inteligencia no es propaganda, ni debe ser empleada como un arma defensiva, u ofensiva, para preservar a una clase política. La Plataforma Central de Inteligencia no es la amenaza, sino el uso faccioso o político que se le puede dar.

Retomar la sabiduría policial que se transmite a través de chistes, es una manera de resquebrajar los esquemas establecidos y dar la oportunidad de ver las cosas desde otra perspectiva. Como el

---

<sup>28</sup> La Ley de Seguridad Nacional (2005), en su artículo 29, entiende por inteligencia: "el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información, para la toma de decisiones en materia de Seguridad Nacional".

chiste de la junta de trabajo donde dos analistas de inteligencia platicaban en corto:

- Oye, ¿cómo ves que los cocodrilos vuelan?
- Eso no es cierto, ¿quién te dijo esa tontera?
- Lo dijo el Director de Inteligencia.
- Ah, bueno. Es que sí vuelan, pero muy, muy bajito.

Para romper el peso excesivo que en ocasiones se da una afirmación como verdadera, únicamente porque proviene de una fuente de autoridad, es necesario tener presente el valor de la integridad. Contra el sesgo<sup>29</sup> de autoridad, el valor de la integridad.

Otro valor clave en este momento de interacción entre entes públicos, privados, y posibles participaciones de la sociedad civil (como se mencionó con anterioridad al hablar de los productos de georreferenciación que se han aportado tanto de datos gubernamentales como no gubernamentales), es el valor de la transparencia metodológica: ser claros sobre los límites de las fuentes y la naturaleza de las inferencias.

Hay que hacer labor de difusión de los productos de inteligencia que se realizan, sus usos y alcances. Pues hasta en productos tan arraigados, como el análisis de datos conservados telefónicos, muchas veces los familiares de las víctimas de delitos, -e incluso activistas de diversos colectivos que agrupan a familiares-, pueden desconocer que la georreferenciación telefónica no es para dar con el paradero exacto de algún desaparecido, sino para establecer áreas de proximidad en relación al azimut, o ángulo desde el cual se enlazaron los teléfonos a las distintas radio bases de comunicación celular.

Como en el caso anterior, explicar la metodología y su alcance, también abona a la confianza ciudadana, pues aclara confusiones o falsa expectativas. Cabe precisar que en la comunidad de inteligencia para la seguridad pública también habrá que definir metodologías para la elaboración de la gama de productos de

---

<sup>29</sup> Daniel Kahneman, premio nobel de economía, explicó que existen dos sistemas de pensamiento. Sistema 1: Rápido, emocional y automático. Sistema 2: Lento, racional, agotador. Develando que el 95% del tiempo funcionamos en modo automático, reaccionando más que racionalizar. A esta condición del pensamiento le denominó sesgos cognitivos.

inteligencia que enlista la LNSI.<sup>30</sup> Desde luego que, conforme a sus atribuciones legales, será el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública el encargado de definir tanto las metodologías como los estándares, razonables y actualizados, para certificar la especialización de los agentes de Instituciones de Procuración de Justicia, Instituciones de Seguridad Pública e Instituciones Policiales.<sup>31</sup>

Adoptar transparencia metodológica, alertará al analista de inteligencia de la tendencia a depender demasiado de un valor inicial (o ancla), y ajustar insuficientemente la evaluación posterior en función de nueva información. Este sesgo de anclaje puede ser ilustrado con el cuento del tartamudo.

Resulta que un tartamudo es asignado como compañero de un impaciente agente de campo. En su primer día, el agente lo invita a comer tacos en un lugar donde hay una salsa picosa y sabrosa.

- ¿Les pongo esta cucharada de salsa picosa?
- Si, si, si, sin salsa.
- ¡Pareja, ya le puse!

Para prevenir y mitigar futuros malentendidos, el agente de poca paciencia acuerda con el tartamudo comunicarse mediante el uso de las viejas claves numéricas policiales, donde 37 significa sí, afirmativo. Y 50 no, negativo. Súbitamente, corren al auto para atender un llamado de emergencia. El agente conduce temerariamente, esquivando vehículos, hasta una bifurcación donde no alcanza a ver el tránsito. Entonces pide ayuda al tartamudo y le pregunta:

- ¿Paso pareja?
- Si, si, si, ¡50!

---

<sup>30</sup> Entre los productos de inteligencia que refiere el artículo 32 de la LNSI están:  
*"I.- Mapas, radiografías y organigramas de bandas y organizaciones criminales, así como de incidencia delictiva por localidades, municipios, entidades federativas, regiones, zonas prioritarias, de interés estratégico y transnacionales.*  
*II.- Reportes sobre antecedentes, modos de operación, planes, operaciones comerciales y financieras, estrategias, alianzas y delitos, en particular los de alto impacto cometidos por personas, grupos y organizaciones criminales;"*

<sup>31</sup> Ver artículos 87 y 89 de la Ley General del Sistema Nacional de Seguridad Pública.

El agente impaciente se quedó anclado a la sílaba si, adoptándolo como una afirmación, incapaz de ajustarse al tartamudo como fuente humana de información, que le aportaba un dato negativo, de negación, a su pregunta por la viabilidad de paso vehicular, expresado en la clave numérica 50. Para equilibrar el sesgo de anclaje, el valor de la transparencia metodológica.

En otra vertiente, la mala reputación de los servicios policiales demanda retomar el gusto por las cosas bien hechas, siempre en auxilio de los demás. Quizá se pueda insuflar el sentido de equidad y cumplimiento del deber con el valor de la responsabilidad; es decir, comprender y asumir que los productos de inteligencia que se hacen desde el trabajo de gabinete, pueden influir en decisiones que afectan otras vidas humanas.

El actuar desde el valor de la responsabilidad, indudablemente reposará y ahondará en la confianza en la policía y en la fiabilidad de los agentes. Pues balanceará la idea ciudadana de que los integrantes de los cuerpos policiales son un engranaje más en una oscura maquinaria de espionaje, con el contrapeso del sentido humano que se mantiene a través estrechar los lazos del tejido social. Es en ese servicio a la ciudadanía en el que los miembros de comunidad de inteligencia experimentarán motivación, pertenencia, inclusión y, más aún, la poderosa gratificación del deber cumplido. Existe un dicho policial que puede ilustrar el valor de la responsabilidad: “Haz lo que te toca. Ni más, ni menos. Sólo lo que es”.

## **Gobernanza de datos y ciberseguridad**

La PCI requiere arquitectura de datos interoperable y controles de ciberseguridad de nivel empresarial. La “ciberseguridad orquestable” integra orquestación, automatización y respuesta (SOAR) con telemetría y analítica en tiempo real para habilitar ciclos OODA (Observar, Orientar, Decidir y Actuar) durante incidentes. Con ello se reduce la latencia entre la detección, el aislamiento de activos comprometidos y la notificación a equipos de seguridad (Estrada Nava, 2024).

Buenas prácticas mínimas: gobierno de identidades y accesos, segmentación y microsegmentación, registro inalterable de

consultas, pruebas de estrés y *red teaming*, y evaluaciones periódicas de impacto en protección de datos (DPIA).

El caso del hackeo a la Comisión Nacional del Agua (Conagua) en 2023 ilustra que fallas de gobernanza —combinadas con debilidades técnicas— pueden escalar a riesgos de seguridad nacional y afectar servicios esenciales. La comunidad de inteligencia para seguridad pública debe incorporar estos aprendizajes en la PCI para anticipar y mitigar impactos (Aguilar Obregón, 2024).

Asimismo, la articulación ética y técnica de la comunidad ocurre en un entorno de policrisis: crisis simultáneas que se retroalimentan y erosionan el multilateralismo. Esta complejidad exige gestión basada en evidencia, cooperación interinstitucional y profesionalización continua (Rosas, 2024).

### **Propuesta para un código de ética de la comunidad de inteligencia**

- 1) Finalidad legítima y base jurídica
- 2) Necesidad y proporcionalidad
- 3) Minimización y calidad de datos
- 4) Transparencia metodológica y trazabilidad
- 5) Gestión de sesgos y validación cruzada
- 6) Seguridad de la información (confidencialidad, integridad, disponibilidad)
- 7) Protección de datos personales (DPIA, controles de acceso, registros de consulta, etc.)
- 8) Supervisión y auditoría interna/externa
- 9) Capacitación y certificación continua
- 10) Prohibiciones expresas (vigilancia masiva sin control judicial, reutilización de datos sin base legal, perfilamiento discriminatorio)

### **Consideración final**

Una comunidad de inteligencia amplia y ética no se decreta: se construye con reglas claras, capacidades técnicas y una cultura profesional exigente. La LNSI y la PCI serán herramientas valiosas si se adoptan prácticas de análisis robustas, salvaguardas de derechos y ciberseguridad que permita operar con resiliencia y rendición de cuentas.

Los valores de integridad, transparencia metodológica y responsabilidad se correlacionan como una fuente para abreviar hacia una renovada confianza ciudadana, y como un aviso de precaución para tener presentes los arraigados sesgos cognitivos, en el quehacer de gabinete, durante la elaboración de productos de inteligencia.

Brevemente contextualizados, dichos valores son apenas una invitación para empezar el diálogo en pro de armonizar entes públicos, privados y la sociedad civil dentro de la recién nacida comunidad de inteligencia para la seguridad pública. Bien podría esta Revista de Inteligencia y Seguridad aceptar dicha invitación para que en el próximo número pueda recibir y conjuntar artículos con diversas perspectivas. Tal vez sea útil y oportuno convocar a un foro o reunión para desarrollar un nutritivo conversatorio sobre este tema en el INAP.

## **Bibliografía**

- Aguilar Obregón, E. A. R. (2024). “Agua y seguridad nacional: El hackeo de la Comisión Nacional del Agua en México”. Revista de Inteligencia y Seguridad, 2 (enero–junio). INAP.
- Cáceres, Otto y Jasso Lucía (2021), *Los servicios de inteligencia en México ayer y hoy*, Instituto de Investigaciones Sociales, UNAM.
- Casillas Zamora, P. W. (2024). “Centro Nacional de Inteligencia: Evolución y naturaleza jurídica”. Revista de Inteligencia y Seguridad, 1 (enero–junio). INAP.
- Centro de Opinión Pública de la Universidad del Valle de México/ Instituto para la Seguridad y la Democracia, A.C. (2021, 24 agosto) *Policía y Sociedad. Corresponsabilidad de la Seguridad Pública en México*. Recuperado el 14 de julio de 2025 de <https://opinionpublica.uvm.mx/estudios/policia-y-sociedad-corresponsabilidad-de-la-seguridad-en-mexico/>
- Código de Ética de la Administración Pública. Recuperado el 14 de julio de 2025 de: [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5642176&fecha=08/02/2022#gsc.tab=0](https://www.dof.gob.mx/nota_detalle.php?codigo=5642176&fecha=08/02/2022#gsc.tab=0)
- Código Nacional de Procedimientos Penales. Recuperado el 14 de julio de 2025 de: [www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf)
- El Financiero (2023, 5 enero). *Culiacán sitiado*. Recuperado el 14 de julio de 2025 de: <https://www.elfinanciero.com.mx/estados/2023/01/05/culiacan-sitiado-asi-lucen-los-bloqueos-en-sinaloa-desde-google-maps/>

- Estrada Nava, C. (2024). “Ciberseguridad orquestable: Tendencias de IA para ciberdefensa proactiva y ciberinteligencia automatizable”. *Revista de Inteligencia y Seguridad*, 2 (enero–junio). INAP.
- Favennec, Thomas y Amador, Luis. (2025, 4 julio). *Más datos, más poder: potencialidades y desafíos de la nueva ley de inteligencia en México*. Nexos. Recuperado el 14 de julio de 2025 de: <https://seguridad.nexos.com.mx/mas-datos-mas-poder-potencialidades-y-desafios-de-la-nueva-ley-de-inteligencia-en-mexico/>
- Instituto Nacional de Geografía, Estadística e Informática, (2024,19 septiembre) *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2024*, Recuperado el 14 de julio de 2025 de <https://www.inegi.org.mx/programas/envipe/2024/>
- Jiménez Solano, J. (2024). “Legislación y regulación sobre seguridad interior”. *Revista de Inteligencia y Seguridad*, 1 (enero–junio). INAP.
- Kahneman, Daniel (2025), *Pensar rápido, pensar despacio*, Penguin Random House Grupo Editorial.
- Láscari, Zoé (s.f.) *Mapeando el secuestro de mujeres en el STC-Metro CDMX*. Recuperado el 14 de julio de 2025 de: <https://docs.google.com/forms/d/e/1FAIpQLSdsjGfEw-vXPxapXi0OvDbG0Hfbs7bL-4So3MAe5XmXG9Jm3w/viewform>
- Ley de Seguridad Nacional. Recuperado el 14 de julio de 2025 de: [www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf)
- Ley del Sistema Nacional de Investigación E Inteligencia en Materia de Seguridad Pública. Recuperado el 14 de julio de 2025 de: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LSNIIMSP.pdf>
- López Gabriela y Valdés Denisse (2025, 15 abril) *Análisis criminal e inteligencia en México: puntos clave para fortalecer la investigación de delitos*. La Costilla Rota. Recuperado el 14 de julio de 2025 de: <https://lacostillarota.com/2025/04/15/analisis-criminal-e-inteligencia-en-mexico-puntos-clave-para-fortalecer-la-investigacion-de-delitos/>
- Office of the Director of National Intelligence (s.f.) *National Intelligence Strategy 2023*, Recuperado el 14 de julio de 2025 de: <https://www.intelligence.gov/templates/intelgov-template/custom-sections/the-nis-at-a-glance/nis-2023/pdf/nis-2023.pdf>
- Programa de Formación Técnica y Asistencia Técnica en Análisis Táctico y Estratégico Nacional, *Manual de Formación del Curso de Generación de productos de análisis criminal para la investigación de delitos*, INL/LabCo, México, 2024.
- Revista espejo (2024, 19 septiembre). *Este es el mapa de la guerra en Sinaloa*. Recuperado el 14 de julio de 2025 de:

[https://revistaespejo.com/2024/09/19/este-es-el-mapa-de-la-guerra-en-sinaloa/#google\\_vignette](https://revistaespejo.com/2024/09/19/este-es-el-mapa-de-la-guerra-en-sinaloa/#google_vignette)

- Rosas, M. C. (2024). “Policrisis y multilateralismo fallido en el siglo XXI”. *Revista de Inteligencia y Seguridad*, 2 (enero–junio). INAP.
- Ruíz de la Cruz, E. F. (2024). “Identidad para la seguridad nacional”. *Revista de Inteligencia y Seguridad*, 1 (enero–junio). INAP.
- Satell Greg, Cascades, *How to create a Movement that drives transformational Change*, McGraw-Will, 2019.
- Toledo Utrera, A. (2024). “La inteligencia para la seguridad nacional como elemento de tutela de los derechos humanos”. *Revista de Inteligencia y Seguridad*, 2 (enero–junio). INAP.
- UNODC /Secretaría de la Función Pública (2018, abril) *Glosario de Términos de Integridad Corporativa*. PNUD/USAID. Recuperado el 14 de julio de 2025 de: <https://anticorruptcionmx.org/historico/archivo/integridad/1.Glosario.pdf?v=1>
- Valadés, Guillermo (2025, 10 julio) *Preguntas sobre la ley del sistema de inteligencia*, Letras Libres. Recuperado el 14 de julio de 2025 de: <https://letraslibres.com/politica/valdes-castellanos-preguntas-sobre-la-ley-del-sistema-de-inteligencia/>
- Valle, Diego (s.f.) *Hoyo del crimen*. Recuperado el 14 de julio de 2025 de: <https://hoyodecrimen.com/>
- Verduzco, F. (s.f.) *Mapear las violencias*. Recuperado el 14 de julio de 2025 de: <https://mapearlasviolencias.com/>
- Vignettes, M. (2024). “Claves del análisis criminal en México. *Revista de Inteligencia y Seguridad*, 2 (enero–junio)”. INAP.
- Zerón García, Eduardo, (2025, 1 Julio) *La inteligencia que sí necesitamos*. La Silla Rota. Recuperado el 14 de julio de 2025 de: <https://lasillarota.com/opinion/columnas/2025/7/1/la-inteligencia-que-si-necesitamos-543527.html>



## Guardia Nacional, inteligencia y control civil: balance jurídico de las reformas de seguridad de 2025 en México

Alejandra Flores  
Fernando Irala

**Resumen:** El artículo examina, desde una perspectiva jurídico-garantista, las reformas de 2025 que consolidan la adscripción de la Guardia Nacional a la SEDENA y reconfiguran el Sistema Nacional de Inteligencia. Se analizan sus fundamentos, alcances y riesgos para el control civil, la transparencia y los derechos humanos, así como sus efectos en el federalismo y la coordinación interinstitucional. Con base en Constitución, jurisprudencia y estándares interamericanos, se valora la compatibilidad del nuevo diseño con un Estado democrático de derecho y se plantean recomendaciones para robustecer instituciones civiles y controles efectivos.

**Palabras clave:** Seguridad pública; Guardia Nacional; reformas legislativas; derechos humanos; militarización; Estado democrático; Sistema Nacional de Investigación e Inteligencia; Interoperabilidad; México.

**Abstract:** This article offers a rights-based legal assessment of Mexico's 2025 security reforms, which place the National Guard under the Ministry of Defense and restructure the National Intelligence System. It evaluates the reforms' constitutional footing, operational reach, and risks to civil oversight, transparency, human rights, and federal balance. Drawing on the Constitution, Supreme Court case law, and inter-American standards, the study weighs the reforms' compatibility with democratic rule of law and proposes measures to strengthen civilian institutions, accountability, and lawful intelligence-policing interoperability.

**Keywords:** Public security; National Guard; legislative reforms; human rights; militarization; democratic state; National Intelligence and Research System; interoperability; Mexico.

## **Introducción:**

### **Planteamiento del problema**

La seguridad pública en México atraviesa una crisis estructural que ha motivado intervenciones legislativas de varios tipos y alcances. Pese a los esfuerzos normativos emprendidos entre 2019 y 2024, particularmente con la creación de la Guardia Nacional, los índices de violencia y criminalidad se han mantenido en crecimiento y en algunos casos, contener en indicadores elevados, por lo que la percepción ciudadana de inseguridad sigue siendo una de las más altas en América Latina. Este panorama refleja la ineficacia de las medidas implementadas y evidencia la imperiosa necesidad de reconfigurar el modelo institucional de seguridad pública, a fin de adecuarlo a los principios constitucionales y al marco normativo vigente.

El dilema central radica en la tensión entre dos ejes normativos: por un lado, la obligación del Estado de garantizar la seguridad como condición sine qua non del ejercicio y goce de Derechos fundamentales; y por otro, el imperativo democrático de preservar la naturaleza civil de las instituciones policiales, principio mandado en el artículo 21 constitucional. La intervención creciente de las Fuerzas Armadas en funciones de seguridad pública ha generado un campo de fricción jurídica en torno a la constitucionalidad de tales disposiciones, así como, sobre su compatibilidad con estándares internacionales de protección a Derechos Humanos.

En 2025, las reformas legislativas en materia de seguridad conllevan riesgos en su implementación al realizar transformaciones sustanciales tanto en la Guardia Nacional como en el Sistema Nacional de Inteligencia. Este contexto abre los siguientes dilemas jurídicos: ¿Respetan las reformas los límites establecidos por la Constitución en materia de seguridad? ¿Con qué alcance se fortalecen o debilitan el control civil sobre la fuerza pública y los órganos de inteligencia? ¿Generan una evolución hacia la profesionalización de la seguridad pública o, en contrario sensu, consolidan un modelo de militarización con peligros para el Estado democrático de derecho?

## Justificación del estudio

La importancia de este análisis se sostiene en tres ejes interrelacionados. En primer lugar, desde el marco constitucional, ya que las reformas de 2025 inciden directamente en la configuración del sistema de seguridad pública establecido en el artículo 21 y en la distribución de competencias entre la Federación, los estados y los municipios.

En segundo término, desde la perspectiva jurídico-institucional, pues permite evaluar cómo las modificaciones repercuten en la estructura, funciones y mecanismos de control de la Guardia Nacional y del Sistema Nacional de Inteligencia, así como en la coordinación intergubernamental.

Finalmente, en el ámbito de la democracia y los Derechos Humanos, el estudio es relevante para identificar los riesgos asociados a la militarización sostenida, posibles retrocesos en la tutela de garantías fundamentales y la eficacia de los controles parlamentarios, judiciales y ciudadanos.

En conjunto, el análisis se justifica porque las reformas de 2025 no solo actualizan el marco normativo, sino que redefinen el paradigma de seguridad en México, con implicaciones directas sobre el Estado de Derecho y el equilibrio entre seguridad y libertades.

## Objetivos

El artículo se propone los siguientes objetivos:

**Objetivo general:** Analizar desde una perspectiva jurídico–constitucional las reformas legislativas de 2025 en materia de seguridad pública, con especial énfasis en la Guardia Nacional y el Sistema Nacional de Inteligencia.

### **Objetivos específicos:**

1. Examinar el contenido y alcance de las reformas constitucionales y legales aprobadas en 2025.
2. Identificar los cambios estructurales en la Guardia Nacional y en el Sistema Nacional de Inteligencia.
3. Evaluar las implicaciones de las reformas en el respeto a los Derechos Humanos, el control civil de la seguridad y la coordinación interinstitucional.

4. Formular propuestas orientadas a fortalecer un modelo de seguridad pública compatible con un Estado democrático de derecho.

### **Metodología**

La investigación se desarrolla bajo un enfoque jurídico-documental. Se recurre al análisis de fuentes normativas - principalmente la Constitución Política de los Estados Unidos Mexicanos, las Leyes del Sistema Nacional Seguridad Pública y de Inteligencia, así como las reformas de 2025- y a la interpretación de la jurisprudencia de la Suprema Corte de Justicia de la Nación en materia de seguridad y derechos humanos.

Asimismo, se consideran insumos doctrinales y estudios comparados sobre modelos de seguridad e inteligencia en contextos democráticos. El método empleado es cualitativo-descriptivo y crítico, lo que permite identificar los alcances normativos de las reformas, contrastarlos con principios constitucionales y evaluar su congruencia con en relación con estándares internacionales, y ofrecer un análisis crítico.

Esta propuesta no pretende agotar el debate, sino aportar un análisis sistemático que pueda servir como base para la discusión académica y la formulación de propuestas a políticas públicas en materia de seguridad.

### **Marco teórico y conceptual**

#### **Concepto de seguridad pública en el marco constitucional mexicano**

La seguridad pública en México tiene un anclaje Constitucional preciso en el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), donde se establece que constituye una función a cargo de la Federación, las entidades federativas y los municipios, coordinados en un Sistema Nacional de Seguridad Pública. Su finalidad es la protección de las personas, la preservación del orden, la paz pública y el resguardo de los bienes jurídicos fundamentales.

Desde una perspectiva jurídico-doctrinal, la seguridad pública es considerada tanto, una garantía social como una función estatal.

En su carácter de derecho, constituye una condición necesaria para el ejercicio de las libertades individuales; en su vertiente Institucional, implica un conjunto de competencias y facultades atribuidas a órganos del Estado.

El reto Constitucional ha sido conciliar ambas dimensiones: garantizar seguridad sin detrimento de libertades, y hacerlo dentro de un marco democrático de derecho que limite el uso de la fuerza y preserve el monopolio del uso de la fuerza en el ámbito civil.

### **Funciones y naturaleza jurídica de la Guardia Nacional**

La Guardia Nacional, creada mediante reforma Constitucional publicada en marzo de 2019, fue concebida como un cuerpo de seguridad de carácter civil, con adscripción administrativa a la Secretaría de Seguridad y Protección Ciudadana (SSPC). No obstante, su integración mayoritaria por elementos provenientes de las Fuerzas Armadas y la operación bajo disciplina castrense generaron desde su origen un debate jurídico sobre su verdadera naturaleza.

De acuerdo con el artículo 21 constitucional y su Ley Orgánica, la Guardia Nacional tiene entre sus funciones: prevenir la comisión de delitos, realizar labores de investigación para la persecución de delitos bajo conducción ministerial, coadyuvar en tareas de seguridad pública con los tres órdenes de gobierno y participar en acciones de preservación del orden.

Su naturaleza jurídica ha sido objeto de controversia. Para algunos autores, constituye una institución policial nacional con régimen excepcionalmente militarizado; para otros, representa un híbrido normativo que desdibuja los límites entre funciones castrenses y de seguridad civil. La jurisprudencia de la Suprema Corte aún no ha resuelto de forma definitiva esta tensión, aunque ha subrayado la importancia de que el mando operativo sea compatible con la Constitución y con estándares de Derechos Humanos.

### **Principios rectores de la seguridad pública en un Estado democrático de derecho**

La doctrina constitucional e internacional reconoce ciertos principios rectores que deben orientar la seguridad pública:

- Legalidad: toda actuación debe estar prevista en la ley y en estricto apego al orden constitucional.
- Necesidad y proporcionalidad en el uso de la fuerza: conforme a los instrumentos internacionales de Derechos Humanos, el uso de la fuerza debe ser excepcional y limitado a lo estrictamente indispensable.
- Control civil y subordinación castrense: en un régimen democrático, los cuerpos militares no pueden sustituir de manera permanente a las instituciones policiales civiles.
- Rendición de cuentas y transparencia: la seguridad no puede quedar exenta de mecanismos de fiscalización legislativa, judicial y ciudadana.
- Respeto irrestricto a los derechos humanos: cualquier medida de seguridad debe ser compatible con la protección de la dignidad humana, la presunción de inocencia y el debido proceso.

Estos principios funcionan como límites jurídicos frente a políticas de seguridad que privilegien la eficacia por encima de la legalidad, constituyendo un parámetro de análisis para las reformas de 2025.

### **Concepto y evolución de la inteligencia en materia de seguridad**

El concepto de inteligencia en materia de seguridad ha transitado de una visión meramente militar a una concepción estratégica multidimensional. Jurídicamente, la inteligencia puede definirse como el conjunto de procesos sistemáticos de obtención, análisis y difusión de información para la prevención de riesgos y amenazas a la Seguridad Nacional y Pública.

En México, la Ley de Seguridad Nacional regula las actividades de inteligencia, asignando al Centro Nacional de Inteligencia (CNI) la función de generar conocimiento útil para la toma de decisiones de seguridad nacional. Sin embargo, la coordinación entre este órgano y las instancias de seguridad pública ha sido limitada, lo que ha provocado duplicidad de esfuerzos y vacíos de información.

En el ámbito internacional, los estándares democráticos establecen que la inteligencia debe:

1. Operar bajo marcos normativos claros que delimiten sus competencias.
2. Estar sujeta a controles parlamentarios y judiciales para evitar abusos.
3. Integrarse en un sistema nacional que facilite la interoperabilidad con cuerpos policiales y militares sin menoscabar los derechos fundamentales.

## **El Sistema Nacional de Inteligencia en el contexto mexicano**

La evolución del Sistema Nacional de Inteligencia (SINAI) en México ha sido lenta y fragmentada. Si bien se reconoce la existencia de mecanismos de coordinación, en la práctica ha prevalecido la centralización de funciones en el CNI, con escasa articulación con policías locales y con la Guardia Nacional.

Previo a 2025, el SNI carecía de un diseño normativo robusto que garantizara una verdadera interoperabilidad institucional. Sus limitaciones principales eran:

- Falta de integración con el Sistema Nacional de Seguridad Pública.
- Ausencia de controles democráticos efectivos sobre sus productos de inteligencia.
- Insuficiente transparencia y rendición de cuentas.

Las reformas de 2025 se presentan como una oportunidad para subsanar estas deficiencias, pero también implican riesgos: ampliar facultades sin controles efectivos podría derivar en un modelo de inteligencia opaco y poco compatible con un Estado de derecho democrático.

## **Contexto político y jurídico previo a las reformas de 2025**

### **Antecedentes legislativos: reformas 2019–2024**

El proceso de reformas en materia de seguridad pública entre 2019 y 2024 estuvo marcado por un reacomodo institucional profundo. La reforma Constitucional de marzo de 2019 dio origen a la Guardia Nacional (GN), concebida como un cuerpo policial de carácter civil pero conformado mayoritariamente por elementos de las Fuerzas Armadas en activo y retirados.

A partir de 2020, se aprobaron Leyes reglamentarias que ampliaron las atribuciones de la GN en labores de investigación y coordinación con ministerios públicos. Asimismo, mediante disposiciones transitorias se permitió que la Secretaría de la Defensa Nacional (SEDENA) y la Secretaría de Marina (SEMAR) aportaran efectivos y recursos para su operación.

En 2022, se publicó un decreto mediante el cual la GN pasó a estar adscrita administrativa y operativamente a la SEDENA, decisión que fue controvertida ante la Suprema Corte de Justicia de la Nación (SCJN) por posibles violaciones al principio de seguridad civil establecido en el artículo 21 constitucional. Aunque algunos ministros se pronunciaron sobre la necesidad de preservar el mando civil, la resolución definitiva reflejó tensiones interpretativas respecto al alcance de la reforma.

Entre 2023 y 2024 se discutieron diversas iniciativas que buscaban redefinir el papel del Centro Nacional de Inteligencia (CNI) dentro del Sistema Nacional de Seguridad Pública, pero ninguna logró consolidarse en el Congreso. Este escenario de reformas parciales dejó abierto el debate sobre la integración del Sistema Nacional de Inteligencia (SINAI) en un marco más coherente y sujeto a controles democráticos.

### **Debates sobre la militarización de la seguridad**

Uno de los ejes más controvertidos del periodo 2019–2024 fue la creciente participación de las Fuerzas Armadas en funciones de seguridad pública. La presencia militar en las calles se justificó por la incapacidad de policías locales para enfrentar a la delincuencia organizada, pero también generó un intenso debate jurídico y político.

Desde la perspectiva constitucional, el artículo 129 de la CPEUM establece que en tiempos de paz “ninguna autoridad militar puede ejercer más funciones que las que tengan exacta conexión con la disciplina militar”. Este precepto ha sido interpretado como un límite claro al involucramiento permanente de las Fuerzas Armadas en seguridad pública. Sin embargo, mediante acuerdos presidenciales y disposiciones transitorias, se habilitó a la SEDENA y a la SEMAR para desempeñar estas funciones hasta 2028.

El debate académico se centra en tres cuestiones principales:

1. **Constitucionalidad** de la participación militar prolongada en tareas de seguridad.
2. **Compatibilidad** con estándares internacionales, en particular con las sentencias de la Corte Interamericana de Derechos Humanos (Corte IDH) que han reiterado que la seguridad ciudadana debe estar a cargo de instituciones civiles.
3. **Eficacia** de la militarización como política pública, frente a la persistencia de altos índices de violencia.

La discusión mostró un contraste entre la narrativa gubernamental de eficacia y la preocupación de organismos nacionales e internacionales por el debilitamiento de los principios democráticos.

### **Jurisprudencia relevante de la Suprema Corte de Justicia de la Nación**

La SCJN ha emitido criterios fundamentales que sirven de antecedente para analizar las reformas de 2025. Destacan los siguientes:

- **Acción de Inconstitucionalidad 6/2018 (Ley de Seguridad Interior):** la Corte declaró inválida esta norma por contravenir el principio de subordinación civil y permitir una intervención militar excesivamente amplia y sin controles.
- **Acción de Inconstitucionalidad 62/2019 y acumuladas (Guardia Nacional):** aunque se avaló la creación de la GN, varios ministros subrayaron que su naturaleza debía ser civil, en congruencia con el artículo 21 constitucional.
- **Controversias constitucionales 90/2020 y 91/2020 (acuerdos de participación militar):** se planteó la obligación de que la participación de Fuerzas Armadas en seguridad pública fuera extraordinaria, fiscalizada, subordinada y complementaria.

Estos precedentes muestran que, aunque la SCJN no ha cerrado el debate, existe una línea jurisprudencial que insiste en el carácter civil de la seguridad pública y en la necesidad de controles

democráticos efectivos sobre la actuación militar en funciones ajenas a la defensa nacional.

### **Marco normativo previo del Sistema Nacional de Inteligencia**

Antes de las reformas de 2025, el Sistema Nacional de Inteligencia (SINAI) carecía de un marco jurídico claro y unitario. Sus funciones se encontraban dispersas en la Ley de Seguridad Nacional, la Ley de la Guardia Nacional, la Ley de la Fiscalía General de la República y otras disposiciones secundarias.

El CNI operaba como órgano desconcentrado de la Secretaría de Seguridad y Protección Ciudadana, aunque en la práctica mantenía vínculos estrechos con la SEDENA y con la Secretaría de Relaciones Exteriores en temas de cooperación internacional.

Los principales problemas identificados eran:

- **Fragmentación normativa**, sin una ley marco que integrara las funciones de inteligencia civil, militar y policial.
- **Débil coordinación** con las policías estatales y municipales.
- **Escaso control democrático**, pues los mecanismos de fiscalización parlamentaria eran limitados y carecían de herramientas de acceso a información clasificada.
- **Opacidad institucional**, que dificultaba evaluar la eficacia y proporcionalidad de las actividades de inteligencia.

En este escenario, las reformas de 2025 surgen como respuesta a la necesidad de dotar al país de un Sistema Nacional de Inteligencia articulado y con mayor interoperabilidad, aunque su diseño normativo plantea riesgos de concentración de poder y posibles regresiones en materia de control democrático.

### **Análisis de las reformas legislativas de 2025**

#### **Contenido y alcance de las reformas constitucionales y legales**

Las reformas de 2025 en materia de seguridad pública fueron aprobadas con el objetivo declarado de fortalecer la capacidad del

Estado para enfrentar la violencia y el crimen organizado. Jurídicamente, abarcan modificaciones tanto al artículo 21 de la CPEUM como a leyes secundarias: la Ley de la Guardia Nacional, la Ley de Seguridad Nacional, la Ley Orgánica de la Administración Pública Federal y, disposiciones de la Ley General del Sistema Nacional de Seguridad Pública.

Entre sus principales alcances destacan:

1. **Reconfiguración de la Guardia Nacional (GN)**, reafirmando su adscripción a la Secretaría de la Defensa Nacional (SEDENA) pero precisando nuevos mecanismos de coordinación con la SSPC.
2. **Creación formal del Sistema Nacional de Inteligencia (SINAI)**, como un entramado institucional integrado por el CNI, la GN, la FGR y las instancias de seguridad de los tres órdenes de gobierno.
3. **Establecimiento de controles parlamentarios y judiciales** sobre las actividades de inteligencia, aunque con limitaciones en el acceso a información clasificada.
4. **Ampliación de facultades en prevención del delito** para la GN, incluyendo labores de inteligencia estratégica bajo conducción ministerial.

El contenido de las reformas refleja una intención de consolidar la militarización administrativa de la GN, al tiempo que busca articular un sistema de inteligencia más robusto. Sin embargo, su constitucionalidad y compatibilidad con estándares internacionales de derechos humanos son materia de discusión.

### **Modificaciones a la estructura y operación de la Guardia Nacional**

Las reformas introducen tres cambios estructurales principales:

- **Mando operativo y administrativo:** la GN queda bajo control directo de la SEDENA, con un esquema de mando militarizado. Esto supone una consolidación del proceso iniciado en 2022, pese a que el texto constitucional de 2019 preveía un cuerpo civil.
- **Formación y disciplina:** se establece que la formación de los elementos se regirá por la doctrina militar,

incorporando materias policiales y de derechos humanos, lo que refuerza el carácter híbrido de la institución.

- **Competencias ampliadas:** además de las funciones de prevención, la GN adquiere atribuciones en materia de inteligencia táctica, uso de tecnologías de vigilancia y coordinación con el CNI en investigaciones criminales.

Este rediseño plantea un dilema jurídico: ¿se trata aún de una institución policial nacional o de una fuerza militar con facultades de policía? El riesgo radica en que se difumine la línea constitucional que exige el carácter civil de la seguridad pública.

### **Cambios en la coordinación entre fuerzas federales, estatales y municipales**

El modelo de coordinación previo descansaba en el Sistema Nacional de Seguridad Pública (SNSP). Con las reformas de 2025, se incorporan mecanismos de interoperabilidad tecnológica y de intercambio de inteligencia entre la GN, las policías estatales y municipales, y el SNII.

Se prevé la creación de una Plataforma Nacional de Información en Seguridad, con acceso compartido a bases de datos de criminalidad, armas, vehículos y personas. Sin embargo, persisten dudas sobre la capacidad real de los municipios para integrarse a este esquema, dada su debilidad institucional y los altos niveles de corrupción documentados en varias corporaciones.

El nuevo modelo refuerza el predominio federal en la conducción de la seguridad, lo que podría interpretarse como una recentralización contraria al espíritu del federalismo consagrado en la CPEUM.

### **Nuevas atribuciones y controles democráticos**

Un aspecto innovador de las reformas es la introducción de mecanismos de control parlamentario. Se establece la obligación de que el Ejecutivo Federal presente un informe anual al Congreso sobre las actividades de la GN y del SNII, con posibilidad de requerir información adicional en comisiones de seguridad y defensa.

Asimismo, se reconoce la facultad de la Comisión Nacional de los Derechos Humanos (CNDH) para supervisar las actividades de la

GN en materia de uso de la fuerza, y se incorpora un régimen sancionador por violaciones a derechos humanos atribuibles a la institución.

En cuanto a la inteligencia, se crea una Comisión Bicameral de Supervisión del SNI, con atribuciones para revisar presupuestos, lineamientos generales y cumplimiento de normas. No obstante, las limitaciones de acceso a información clasificada reducen el alcance de la fiscalización, lo que puede convertir al mecanismo en una falacia.

### **Transformaciones en el Sistema Nacional de Inteligencia**

Las reformas de 2025 establecen por primera vez un Sistema Nacional de Inteligencia (SINAI) con base constitucional. Este sistema busca articular las capacidades del CNI, la GN, la FGR y los órganos de inteligencia militar, bajo principios de coordinación, cooperación y confidencialidad.

Entre sus innovaciones se encuentran:

- **Consejo Nacional de Inteligencia:** presidido por el Ejecutivo Federal, con participación de Secretarios de Estado y del Fiscal General.
- **Normas sobre clasificación y desclasificación de información,** con plazos y procedimientos específicos.
- **Enfoque multidimensional de seguridad,** incluyendo inteligencia sobre ciberseguridad, terrorismo, tráfico de armas y delitos financieros.

Aunque representa un avance en términos de integración, también concentra el poder en el Ejecutivo, lo que genera dudas sobre la suficiencia de los contrapesos democráticos.

### **Interoperabilidad entre Guardia Nacional e instituciones de inteligencia**

Un rasgo central de las reformas es la interoperabilidad entre la GN y las instituciones de inteligencia. Se faculta a la GN a participar en labores de obtención de información, análisis de patrones delictivos y uso de tecnologías de vigilancia, siempre bajo coordinación con el CNI y la FGR.

Este diseño busca superar la tradicional fragmentación del sistema de seguridad mexicano. No obstante, plantea riesgos:

- **Dilución de fronteras normativas** entre funciones policiales y de inteligencia.
- **Posible invasión de competencias** de la FGR en materia de investigación.
- **Amenazas a derechos fundamentales** como la privacidad, debido al uso de técnicas de vigilancia tecnológica sin garantías suficientes.

La interoperabilidad, en consecuencia, debe evaluarse no sólo como un avance técnico, sino también como un reto jurídico para preservar el equilibrio entre seguridad y libertades.

### **Implicaciones jurídicas y sociales de las reformas Derechos humanos y control del uso de la fuerza**

Las reformas de 2025, al consolidar la adscripción de la Guardia Nacional (GN) a la Secretaría de la Defensa Nacional (SEDENA) y ampliar sus atribuciones de inteligencia, generan preocupaciones sobre la protección de los derechos humanos.

El marco internacional, particularmente la jurisprudencia de la Corte Interamericana de Derechos Humanos (Corte IDH), ha establecido que la seguridad ciudadana debe estar a cargo de cuerpos policiales civiles, y que la participación militar en tareas de seguridad debe ser excepcional, temporal y subordinada. En el Caso Zambrano Vélez y otros vs. Ecuador (2007), la Corte señaló que “la participación de las fuerzas armadas en tareas de seguridad ciudadana debe ser estrictamente excepcional, pues el entrenamiento de los militares está dirigido a derrotar al enemigo y no a la protección y control de civiles” (párr. 51). Con ello, se subraya que la lógica militar resulta incompatible con el paradigma de protección de derechos humanos que orienta la seguridad pública.

De manera complementaria, en el Caso Montero Aranguren y otros (Retén de Catia) vs. Venezuela (2006), el tribunal precisó que los Estados están obligados a organizar su aparato de seguridad de forma tal que garantice el pleno respeto y goce de los derechos fundamentales, particularmente la vida y la integridad

personal, lo que implica dotar a los cuerpos policiales civiles de capacitación, recursos y controles suficientes (párr. 68).

En el contexto mexicano, la Corte ha reiterado esta doctrina en el Caso Alvarado Espinoza y otros vs. México (2018), donde consideró que el despliegue militar para funciones de seguridad pública no puede convertirse en regla general y que las operaciones de las fuerzas armadas deben estar sujetas a controles civiles y mecanismos de rendición de cuentas efectivos (págs. 175-177). Asimismo, estableció que la intervención castrense, al no estar prevista de manera clara, precisa y estrictamente delimitada por la ley, vulneraba el principio de legalidad y ponía en riesgo derechos fundamentales.

Esta línea jurisprudencial busca evitar la militarización de la seguridad ciudadana, la cual produce riesgos de violaciones graves a los derechos humanos, como detenciones arbitrarias, desapariciones forzadas o ejecuciones extrajudiciales, y debilita los procesos de fortalecimiento institucional de las policías civiles.

En suma, la Corte IDH ha consolidado un estándar regional conforme al cual la seguridad ciudadana debe estar a cargo de instituciones civiles, mientras que el uso de las fuerzas armadas en ese ámbito se admite únicamente como excepción estricta, bajo condiciones de temporalidad, subordinación y fiscalización civil, constituyendo un criterio vinculante para todos los Estados parte de la Convención Americana sobre Derechos Humanos.

El riesgo principal radica en que la GN, al operar bajo disciplina militar, desdibuje el principio de uso diferenciado, progresivo y proporcional de la fuerza, previsto en la Ley Nacional sobre el Uso de la Fuerza. En términos jurídicos, esto podría dar lugar a violaciones a la vida, integridad personal y privacidad, especialmente en labores de inteligencia tecnológica y vigilancia masiva.

Aunque las reformas incorporan mecanismos de supervisión, como la obligación de rendir informes al Congreso y la supervisión de la CNDH, subsiste la duda de si estos controles tendrán eficacia real frente al poder concentrado en el Ejecutivo.

## **Evaluación del nuevo modelo de Seguridad Pública**

El nuevo modelo diseñado en 2025 combina tres ejes: militarización administrativa de la GN, integración del Sistema Nacional de Inteligencia (SINAI) y recentralización de la coordinación federal.

Desde un punto de vista jurídico, este modelo presenta ventajas y riesgos:

- **Ventajas:** Mayor articulación institucional, interoperabilidad tecnológica, acceso centralizado a bases de datos y fortalecimiento de capacidades en inteligencia.
- **Riesgos:** Vulneración al principio de civilidad, concentración excesiva en el Ejecutivo, debilitamiento del federalismo y limitados contrapesos legislativos y judiciales.

La evaluación del modelo, por tanto, no puede limitarse a su eficacia en reducir índices delictivos, sino que debe considerar si es compatible con los principios constitucionales de legalidad, división de poderes y control civil de la seguridad pública.

### **Riesgos de militarización y retrocesos democráticos**

Uno de los riesgos jurídicos más relevantes es la consolidación de la militarización estructural de la seguridad. La GN, al quedar bajo control directo de la SEDENA, pierde la posibilidad de desarrollarse como un cuerpo policial civil, en aparente contradicción con lo dispuesto por el artículo 21 constitucional.

La doctrina democrática sostiene que la militarización permanente de la seguridad pública erosiona tres pilares fundamentales:

1. **Federalismo**, pues las entidades federativas y municipios pierden margen de acción frente a la hegemonía de las fuerzas federales.
2. **División de poderes**, al concentrarse en el Ejecutivo facultades de seguridad e inteligencia sin contrapesos suficientes.
3. **Tutela de derechos**, dado que la lógica militar responde a parámetros de defensa nacional y no a estándares de seguridad ciudadana.

Este proceso implica un retroceso democrático, especialmente si se compara con las recomendaciones de Organismos

Internacionales que han insistido en la necesidad de fortalecer a las policías civiles.

### **Opinión de Organismos Nacionales e Internacionales**

Los organismos nacionales de derechos humanos, como la CNDH, han señalado la necesidad de establecer mecanismos más robustos de rendición de cuentas y de capacitación en derechos humanos para la GN. No obstante, su capacidad vinculante frente a las Fuerzas Armadas es limitada.

En el plano internacional, instancias como la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ONU-DH) y la Comisión Interamericana de Derechos Humanos (CIDH) han manifestado preocupaciones sobre la tendencia a normalizar la participación militar en seguridad pública en México. Estas observaciones coinciden en que la seguridad debe regirse por un enfoque civil, democrático y con controles efectivos.

Si bien las reformas de 2025 intentan responder a tales críticas mediante la creación de mecanismos de supervisión parlamentaria, su eficacia dependerá de la voluntad política y de la capacidad de los órganos legislativos y judiciales para ejercer contrapesos reales.

### **Impacto de las reformas en el equilibrio entre seguridad e inteligencia**

La integración de la GN al Sistema Nacional de Inteligencia (SINAI) redefine el equilibrio entre seguridad pública e inteligencia estratégica. Desde la óptica jurídica, este rediseño puede generar beneficios, como mayor coordinación y capacidad de prevención. Sin embargo, también plantea riesgos significativos:

- **Difuminación de competencias:** la GN, al realizar tareas de inteligencia, puede invadir facultades de la Fiscalía General de la República y del CNI.
- **Posible violación de Derechos Fundamentales:** el uso de herramientas de vigilancia sin controles judiciales adecuados amenaza la privacidad y la libertad de expresión.
- **Concentración de poder en el Ejecutivo:** el Consejo Nacional de Inteligencia, presidido por el Ejecutivo,

reduce la autonomía de los demás órganos y limita los contrapesos.

En conclusión, el impacto de las reformas en este ámbito dependerá de la eficacia de los controles democráticos y de la capacidad del Estado para compensar las exigencias de seguridad con el respeto a los derechos fundamentales.

## **Retos pendientes y recomendaciones**

### **Fortalecimiento de las instituciones civiles**

Uno de los retos más apremiantes tras las reformas de 2025 es impedir que la centralización de la seguridad en la SEDENA neutralice el desarrollo de las instituciones civiles de seguridad.

El artículo 21 constitucional establece con claridad que la seguridad pública es una función a cargo de Instituciones de carácter civil. Por tanto, es indispensable impulsar un programa nacional de profesionalización de policías estatales y municipales, acompañado de mecanismos de financiamiento estable y políticas de dignificación salarial.

Asimismo, debe fortalecerse el Servicio Profesional de Carrera Policial, para que la GN y las policías civiles compartan estándares comunes de formación y actuación profesional, lo cual contribuiría a reducir la brecha entre estructuras militares y civiles.

### **Mecanismos de fiscalización y transparencia**

Las reformas crean la obligación de que la GN y el Sistema Nacional de Inteligencia (SINAI) rindan informes periódicos al Congreso de la Unión. Sin embargo, la eficacia de estos controles dependerá de que no se conviertan en ejercicios meramente formales.

Es necesario:

- **Fortalecer la fiscalización parlamentaria**, dotando a las comisiones de seguridad y defensa de facultades para citar a mandos militares y exigir información desagregada.

- **Ampliar las facultades de la Auditoría Superior de la Federación (ASF)** para auditar recursos de seguridad nacional, sin perjuicio de la reserva en temas estratégicos.
- **Garantizar transparencia proactiva**, con la publicación de estadísticas de operativos, denuncias por violaciones de Derechos Humanos y criterios de intervención.

El control judicial también es fundamental: el Poder Judicial de la Federación debe tener un papel más activo en supervisar la legalidad de actos de inteligencia, a través de autorizaciones judiciales previas para intervenciones de comunicaciones y mecanismos de revisión posterior.

### **Participación ciudadana y rendición de cuentas**

La legitimidad de la seguridad pública no depende solo de su eficacia en disminuir índices delictivos, sino también de la confianza ciudadana. Para ello, resulta indispensable abrir canales de participación social:

- Creación de Consejos Ciudadanos de Supervisión de la GN y el SIN, integrados por especialistas, académicos y defensores de derechos humanos.
- Establecimiento de Observatorios Locales de Seguridad, con facultades para emitir recomendaciones públicas y dar seguimiento a indicadores de desempeño.
- Impulso de mecanismos de denuncia accesibles frente a abusos de la GN o violaciones de derechos en tareas de inteligencia.

La rendición de cuentas debe concebirse como un eje estructural, no como una concesión, pues únicamente así se logrará consolidar un modelo de seguridad democrático y compatible con los compromisos internacionales asumidos por México.

### **Diálogo crítico con números previos de la revista RIS INAP**

El debate que articula este trabajo —constitucionalidad de las reformas de 2025, carácter civil de la seguridad pública, rediseño del sistema de inteligencia y controles democráticos— ya había sido anticipado por la propia *Revista de Inteligencia y Seguridad* en sus números 1 (2024) y 2 (2025). Integrar esas aportaciones permite calibrar mejor los alcances y riesgos de las reformas, así como

proponer lineamientos operativos y de control acordes con un Estado democrático de derecho.

### **Sobre la naturaleza jurídica del CNI y el rediseño del SINAI**

Antes de la reforma, se documentó la evolución institucional del órgano civil de inteligencia —del CISEN al CNI— y las inconsistencias reglamentarias que aún incidían en su actuación. Ese balance subrayó que el CNI había transitado “de ser un área administrativa... a un órgano administrativo desconcentrado con autonomía técnica, operativa y de gasto, con competencia exclusiva y directa”, advirtiendo normas aplicadas en tensión con la Ley de Seguridad Nacional (Casillas Zamora, 2024).

Esta línea de análisis robustece el examen de 2025: si el nuevo SINAI concentra funciones, debe resolver la vieja dispersión normativa y evitar regresiones en la naturaleza civil de la inteligencia estratégica.

### **Constitucionalidad y límites a la participación militar**

El número 1 ofreció un antecedente doctrinal y jurisprudencial clave: la invalidez de la Ley de Seguridad Interior por normalizar el empleo castrense en seguridad pública, contraria al orden constitucional. Esa síntesis reafirma que cualquier intervención militar debe ser extraordinaria, fiscalizada y subordinada (Jiménez Solano, 2024).

En sintonía, el ensayo sobre militarización advirtió impactos negativos en derechos humanos, erosión de controles y la necesidad de fortalecer policías civiles en lugar de perpetuar despliegues militares (Romero, 2024).

Estos hallazgos son un contrapeso imprescindible al traslado del mando de la Guardia Nacional y a su integración operativa con inteligencia.

### **Metodologías de análisis criminal e interoperabilidad**

Para que la reforma no quede en arquitectura nominal, se requiere capacidad analítica real. El número 2 sistematizó el rol del *analista criminal* y su cartera de productos (tácticos y estratégicos), precisando que un “sistema único de inteligencia”, en el mejor

escenario, sería un componente dentro del Sistema Nacional de Seguridad Pública (Vignettes, 2025).

Este enfoque confirma dos tesis del presente artículo: i) la interoperabilidad debe anclarse en estándares analíticos verificables y ii) la recentralización sin profesionalización local reproduce cuellos de botella.

### **Inteligencia y derechos humanos: un marco para controles democráticos**

La revista también perfiló un puente conceptual entre inteligencia y tutela de derechos: la inteligencia pública, correctamente enmarcada, puede y debe resguardar vida, libertad, privacidad y datos personales (Toledo Utrera, 2025).

De allí se desprende un criterio operativo: controles ex ante (autorización judicial para técnicas intrusivas) y ex post (auditorías y comisiones bicamerales) no son accesorios, sino condición de legitimidad del nuevo SINAI. El propio artículo enfatiza que la inteligencia debe enfocarse no solo en proteger al Estado, sino en amparar derechos universales, indivisibles y progresivos (Toledo Utrera, 2025).

### **Tecnología, ciberseguridad y vigilancia: riesgos y capacidades**

En materia de tecnología aplicada, el número 2 discutió *ciberseguridad orquestable* y *ciberdefensa proactiva*: orquestación (SOAR), automatización y agentes autónomos (AICA) para anticipar y neutralizar amenazas, con telemetría y análisis masivo de datos (Estrada Nava, 2025).

Este repertorio técnico debe leerse junto con las salvaguardas constitucionales del presente artículo: sin control judicial y transparencia selectiva, estas mismas capacidades pueden escalar a vigilancia desproporcionada. El caso *Conagua* —secuestro de ~15 años de información por *BlackByte*— ilustra la urgencia de integrar ciberseguridad crítica al modelo, bajo estándares de seguridad nacional y rendición de cuentas (Aguilar Obregón, 2025).

### **Lecciones operativas y proporcionalidad del uso de la fuerza**

Como estudio de caso, el análisis de la primera captura de Ovidio Guzmán identificó aciertos y errores de inteligencia (2019), subrayando la necesidad de anticipación analítica, coordinación interinstitucional y protocolos de uso de la fuerza compatibles con estándares democráticos (Jaimes Álvarez, 2024).

Estas lecciones operativas son aplicables a una Guardia Nacional con atribuciones ampliadas: la profesionalización táctica no puede prescindir de mandos civiles, control judicial y trazabilidad de las decisiones.

### **Contexto estratégico: policrisis y gobernanza**

Finalmente, el número 2 enmarcó el presente ciclo en una *policrisis* global y en el deterioro del multilateralismo, que presionan por respuestas rápidas con menos tiempo para procesar información en un entorno de infodemia (Rosas, 2025).

Esta presión por eficacia no debe traducirse en excepciones permanentes ni en concentración de poder; al contrario, refuerza la exigencia de controles, transparencia y profesionalización local.

### **Síntesis integradora**

Los números previos de la revista sostienen —desde ángulos jurídico, operativo y tecnológico— tres puntos que dialogan directamente con las conclusiones de este artículo: (i) el núcleo de la seguridad pública debe permanecer civil y sujeto a controles constitucionales; (ii) la interoperabilidad y la inteligencia solo rinden frutos si descansan en estándares analíticos, ciberseguridad robusta y capacidades locales; y (iii) la legitimidad democrática de la seguridad exige poner los derechos en el centro del ciclo de inteligencia y del uso de la fuerza.

### **Conclusiones**

Las reformas legislativas de 2025 constituyen un parteaguas en el diseño del sistema de Seguridad Pública e Inteligencia en México. Si bien responden a la urgencia de enfrentar la violencia y el crimen organizado con estructuras más robustas, también plantean desafíos serios para la vigencia del Estado Constitucional de Derecho.

Desde una perspectiva técnico-jurídica, pueden destacarse tres conclusiones principales:

1. **Consolidación de la militarización:** la adscripción definitiva de la Guardia Nacional a la SEDENA y su incorporación plena al Sistema Nacional de Inteligencia tensionan el principio de civilidad previsto en el artículo 21 constitucional y en los estándares interamericanos.
2. **Insuficiencia de controles democráticos:** aunque las reformas prevén mecanismos de supervisión parlamentaria y de fiscalización, subsiste el riesgo de que éstos resulten débiles frente al peso político y presupuestal de las Fuerzas Armadas.
3. **Necesidad de equilibrio entre seguridad y derechos:** el éxito del nuevo modelo no debe medirse únicamente en el abatimiento de cifras delictivas, sino en su capacidad para armonizar la eficacia operativa con el respeto a los derechos humanos, la división de poderes y el federalismo.

Finalmente, el futuro del modelo de seguridad dependerá de la capacidad del Estado mexicano para fortalecer las instituciones civiles, consolidar mecanismos efectivos de fiscalización y garantizar una participación ciudadana real en la toma de decisiones y en la rendición de cuentas. De lo contrario, se corre el riesgo de consolidar un modelo de seguridad altamente centralizado y militarizado, con consecuencias adversas para la Democracia Constitucional en México.

## BIBLIOGRAFÍA

- Aguilar Obregón, E. A. R. (2025). Agua y seguridad nacional: El hackeo de la Comisión Nacional del Agua en México. *Revista de Inteligencia y Seguridad*, Número 2 (enero–junio). INAP.
- Casillas Zamora, P. W. (2024). Centro Nacional de Inteligencia: Evolución y naturaleza jurídica. *Revista de Inteligencia y Seguridad*, Número 1 (enero–junio). INAP.
- Comisión Interamericana de Derechos Humanos (2023). Informe sobre seguridad y militarización en las Américas.
- Constitución Política de los Estados Unidos Mexicanos.
- Diario Oficial de la Federación (2025). Decreto de reformas en materia de seguridad pública.
- Estrada Nava, C. (2025). Ciberseguridad orquestable: Tendencias de IA para ciberdefensa proactiva y ciberinteligencia automatizable. *Revista de Inteligencia y Seguridad*, Número 2 (enero–junio). INAP.
- Jaimes Álvarez, O. (2024). Labores de inteligencia: Análisis de la primera captura de Ovidio Guzmán. *Revista de Inteligencia y Seguridad*, Número 1 (enero–junio). INAP.
- Jiménez Solano, J. (2024). Legislación y regulación sobre seguridad interior. *Revista de Inteligencia y Seguridad*, Número 1 (enero–junio). INAP.
- ONU-DH México (2024). Observaciones sobre la Guardia Nacional y el uso de la fuerza.
- Romero, C. (2024). Proceso de militarización de la seguridad pública en México. *Revista de Inteligencia y Seguridad*, Número 1 (enero–junio). INAP.
- Rosas, M. C. (2025). Policrisis y multilateralismo fallido en el siglo XXI. *Revista de Inteligencia y Seguridad*, Número 2 (enero–junio). INAP.
- Suprema Corte de Justicia de la Nación (2019–2024). Jurisprudencia sobre uso de Fuerzas Armadas en seguridad pública.
- Toledo Utrera, A. (2025). La inteligencia para la seguridad nacional como elemento de tutela de los derechos humanos. *Revista de Inteligencia y Seguridad*, Número 2 (enero–junio). INAP.
- Vignettes, M. (2025). Claves del análisis criminal en México. *Revista de Inteligencia y Seguridad*, Número 2 (enero–junio). INAP.

## MÁS ALLÁ DE LA ALINEACIÓN ALGORÍTMICA: RETOS ÉTICOS Y CULTURALES EN LA ADAPTACIÓN DE LA IA A LA DIVERSIDAD DE LOS VALORES HUMANOS

Javier Alejandro Padilla Santacruz\*

**Resumen:** El crecimiento de los sistemas de inteligencia artificial (IA) en justicia, salud, educación y seguridad ha intensificado la discusión sobre su alineación con valores humanos. Sostenemos que la tensión entre eficacia algorítmica y pluralismo moral no es accidental ni resoluble con ajustes normativos puntuales: es un dilema sociotécnico estructural. La estandarización que exige la IA choca con la variabilidad legítima de valores entre culturas y a lo largo del tiempo. Desde un enfoque teórico-aplicado, se revisan fundamentos técnicos y filosóficos, y se advierten riesgos de importar modelos insensibles al contexto que amplifiquen exclusiones morales, epistémicas y sociales. La versión ampliada vincula estos debates con marcos de seguridad e inteligencia en México y América Latina, proponiendo líneas de acción para una gobernanza plural y responsable.

El presente artículo sostiene la hipótesis con respecto a que esta tensión no es contingente ni corregible mediante ajustes normativos dentro de los sistemas de inteligencia artificial, sino que constituyen un dilema irresoluble dentro del diseño actual de la IA. Esto es debido a que a medida que los algoritmos requieren estandarizar y parametrizar decisiones para trabajar a escala, se ven forzados a reducir la riqueza

---

\* **Javier Padilla Santacruz** es politólogo por el Instituto Tecnológico Autónomo de México (ITAM), y cuenta con Especialidad y Maestría en Inteligencia para la Seguridad Nacional en el INAP, así como formación en políticas públicas, lo que le permite trascender lo operativo e incidir en la toma de decisiones estratégicas. Actualmente es docente en instituciones militares y navales. Cuenta con más de 14 años de experiencia en sector público y privado. Ha coordinado operaciones con fuerzas armadas y autoridades civiles que derivaron en la desarticulación de redes criminales y la recuperación de activos estratégicos, siempre con enfoque ético y orientado a resultados. Su trabajo integra tecnología, análisis de datos y políticas públicas para reducir vulnerabilidades institucionales, impulsando programas de prevención del delito y marcos de seguridad a distintos niveles de gobierno.

moral y cultural de los valores humanos a una relación lógica, normalizada y homogénea. El problema trasciende lo algorítmico: abarca la definición legítima de valores, su traducción técnica, la auditoría y los mecanismos de corrección cuando aparezcan efectos no deseados.

**Palabras Clave:** Inteligencia Artificial, justicia, seguridad, marcos de seguridad e inteligencia, gobernanza, ética cultural, alineación algorítmica.

**Abstract:** The growth of artificial intelligence (AI) systems in justice, health, education, and security has intensified the discussion about their alignment with human values. We argue that the tension between algorithmic efficiency and moral pluralism is neither accidental nor solvable through ad hoc regulatory adjustments: it is a structural sociotechnical dilemma. The standardization demanded by AI clashes with the legitimate variability of values across cultures and over time. From a theoretical-applied perspective, we review technical and philosophical foundations and warn of the risks of importing context-insensitive models that amplify moral, epistemic, and social exclusions. The expanded version links these debates to security and intelligence frameworks in Mexico and Latin America, proposing lines of action for pluralistic and responsible governance.

This article supports the hypothesis that this tension is neither contingent nor correctable through regulatory adjustments within artificial intelligence systems but rather constitutes an irresolvable dilemma within the current design of AI. This is because, as algorithms need to standardize and parameterize decisions to work at scale, they are forced to reduce the moral and cultural richness of human values to a logical, normalized, and homogeneous relationship. The problem transcends the algorithmic: it encompasses the legitimate definition of values, their technical translation, auditing, and corrective mechanisms when unintended effects arise.

**Keywords:** Artificial Intelligence, justice, security, security and intelligence frameworks, governance, cultural ethics, algorithmic alignment

### **Alineación algorítmica: concepto y alcance**

Abordar la alineación de la Inteligencia Artificial refiere al proceso de diseñar, entrenar y aplicar sistemas de aprendizaje masivo para que los objetivos y comportamientos obtenidos estén en concordancia con los valores y metas humanas deseadas (Jonker & Gomstyn, 2024). De esta forma, se busca que la IA opere de manera en que refleje los valores, intereses y objetivos de la humanidad, evitando acciones que pudiesen ser perjudiciales para

las personas o la sociedad *per se* (Acosta, 2024). Esta alineación se presenta como el problema de la alineación de la IA, descrito como uno de los desafíos centrales de la ética en el desarrollo de estos modelos (Russell, 2019).

Hablar de una IA no alineada con el valor humano, podría suponer un escenario futurible contraproducente a la aparente razón de incluir más IA dentro de la vida actual, con consecuencias para las siguientes generaciones. Con esto, la metáfora del Rey Midas podría ser un referente directo, al pedir o *promptear* una serie de deseos o tareas mal especificados, se podrían tomar decisiones dañinas o sesgadas por el afán de la optimización a toda costa sin consideraciones éticas que estuviesen incluidas explícitamente en su programación inicial.

Jonker & Gomstyn (2024), toman como ejemplo el desarrollo de un vehículo autónomo, el cual podría enfocarse en ser el que genere mayor velocidad siempre y que, por llegar rápidamente a su destino, sacrifique las reglas de seguridad vial, atentando potencialmente contra la vida del usuario y, a la vez, poner en peligro la seguridad de los no usuarios.

Hasta el momento, la alineación algorítmica ha sido abordada principalmente desde una perspectiva técnica, teniendo como eje central los modelos de aprendizaje por refuerzo con retroalimentación humana, que en inglés se conoce como *Reinforcement Learning from Human Feedback* (RLHF), lo cual lleva a que los modelos sean refinados con conjuntos de datos estandarizados anteriormente (Ouyang, 2022). De esta manera, la alineación refiere al diseño, entrenamiento y operación de sistemas de IA para que sus objetivos y conductas sean compatibles con metas y valores humanos deseables.

Dicho lo anterior, estos métodos buscan que el modelo aprenda a evitar respuestas dañinas o indeseables, que respete ciertas preferencias definidas *a priori* por los desarrolladores. Un ejemplo es cómo a los *chatbots* modernos se les entrena para rehusarse a proporcionar instrucciones peligrosas, como sería la construcción de un arma casera, alineando sus respuestas con normas de seguridad (Jonker & Gomstyn, 2024).

No obstante, la alineación de la IA no debe tener como único principio la eficiencia técnica, sino también ética y política, es

decir, además de algoritmos, se debe integrar un proceso de decisiones sobre qué valores serán los que se prioricen cuando aparezcan temas que violen las reglas sociales, describir qué líneas rojas existen, quién las define y cómo se implementan, de forma transparente y responsable. Este reconocimiento nos lleva más allá de la simple optimización técnica, y nos sitúa en la comprensión de los retos éticos y culturales implicados en alinear la IA con la pluralidad de valores humanos (Acosta, 2024).

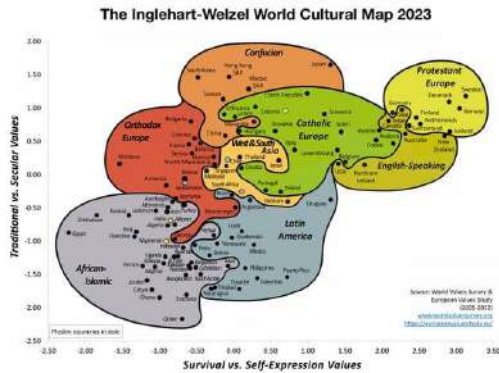
## **Diversidad de valores humanos y su relevancia para la IA**

El reto de la alineación de la IA con los valores humanos no es tema sencillo, sino que es una dificultad enorme al no existir valores inamovibles o aceptados universalmente por la totalidad de la población humana, sino que existen divisiones, escisiones, diferencias entre países, regiones culturales, sociedades e incluso individuos. Esta problemática ha sido descrita por diversas disciplinas, evidenciando que no existe un consenso universal sobre lo que constituye una vida correcta, ni los valores que deberán componerla.

Gardels (2024), describe esta dificultad como el inexistente acuerdo universal para compartir un buen vivir que funciones para los pueblos actuales y futuros, en todo tiempo y lugar. Con esto se puede afirmar que no sólo existirán contrastes constantes, sino que la divergencia tendrá que ver con la pluralidad de contextos históricos, religiosos y sociales, reflejando las diferencias extremas que pueden existir dentro de las normas que rigen la vida en sociedad.

Evidenciando el punto anterior, existe un ejercicio particular, titulado Mapa Cultural Mundial, a través de la encuesta *World Values Survey* del 2023 (WVS), la cual visibiliza la gran diversidad de valores culturales mundiales, lo cual se representa en un eje cartesiano, teniendo los valores tradicionales vs. valores liberales en el eje vertical (eje Y), mientras que los valores de supervivencia vs. valores de autoexpresión se encuentran en el eje horizontal (eje X).

Este ejercicio arroja como resultado la multiplicidad de valores sociales del mundo, agrupadas en distintos *clusters*, mostrando variedades de todo tipo, lo cual se muestra en el siguiente gráfico:



Se pueden sacar todo tipo de conclusiones, como lo son países de tradición protestante en Europa, los cuales tienden a ubicarse altos en el cluster de valores liberales, lo cual podría materializarse en el privilegio de la autonomía individual, así como la igualdad de género, tolerancia a la diversidad, etc. Mientras que, en sociedades en desarrollo, el cluster agrupa valores más tradicionales y de supervivencia, materializándose en la gran importancia a temas como religión, seguridad económica y cohesión familiar.

Esta multiplicidad de valores evidencia los bemoles que existen sobre el concepto de qué es lo que se considera un comportamiento socialmente aceptable o deseable de forma individual, destacando la notable variación de una cultura a otra.

Asimismo, evidenciar la gran diversidad de valores, evoca un contexto mucho más complicado, desde la historia de las comunidades originarias, formas de profesión religiosa, organización económica y posición social de hombres y mujeres, dejando en claro que cualquier noción de valores humanos abarca un espectro muy amplio y a veces conflictivo.

La diversidad interna dentro de cada cultura también es relevante. Ninguna cultura es completamente homogénea, dentro de un mismo país coexisten subgrupos con valores divergentes por generación, género, clase social, ideología política, religión, etc. Por ejemplo, la afirmación de que, los valores de X cultura son Y, implica una simplificación extrema, cada cultura agrega multitud de visiones a menudo contrapuestas, así como todo grupo tiene contenido otro grupo de inconformes (Law, 2024).

Si se intentara alinear un sistema de IA con un conjunto fijo de valores culturales promedio de una nación específica, se correría el riesgo de excluir a las minorías o disidentes cuyas creencias se apartan de la norma estadística. En otras palabras, la variabilidad interna significa que alinearse con la cultura puede traducirse en invisibilizar a quienes no encajan en el molde mayoritario, planteando un dilema de representatividad y justicia (Law, 2024).

Esta diversidad de valores humanos implica que la alineación para la IA no puede concebirse como simplemente programar un conjunto único de valores universales y ya está. ¿Qué valores y de quién? Preguntas que se harán inicialmente por simpatizantes y contrarios. Algunas propuestas apelan a valores universalistas basados en los derechos humanos fundamentales, como los promulgados por las Naciones Unidas, buscando una base ética mínima común a toda la humanidad.

De hecho, iniciativas globales como la Recomendación sobre la Ética de la IA de la UNESCO (2021), establecen principios de alcance universal, como la dignidad, la justicia y los derechos humanos, así como reconocer la importancia de la diversidad cultural, instando a respetar las diferencias locales siempre que no contradigan los derechos fundamentales.

No obstante, conceptos aparentemente universales como lo son la justicia, privacidad o libertad pueden tener interpretaciones y pesos distintos según el contexto cultural en el cual se definan. Por ejemplo, la privacidad es altamente valorada como derecho fundamental e irrevocable en Europa, mientras que en Estados Unidos suele ser renunciable y equilibrarse más con consideraciones de interés económico o seguridad nacional.

Estas discrepancias dificultan en sobremanera la definición de un conjunto único de valores para la IA que satisfaga a todos por igual. Con esto se expone la dificultad intrínseca en contar con una gran diversidad de valores humanos, entre culturas y dentro de ellas, que establece el escenario sobre el cual deben navegar los esfuerzos de alineación de la IA, presentando importantes retos éticos y culturales (Upmann, 2023).

## **Retos éticos en la alineación de la IA con valores humanos**

Entrando en materia, los desafíos éticos surgen al decidir qué valores incorporar en los sistemas de IA, cómo hacerlo de manera justa y transparente, y cómo lidiar con los posibles conflictos que existirán con certeza. Un primer reto entra sobre la posibilidad de sesgos y discriminación si la IA no está correctamente alineada. Este problema existirá de forma inherente debido a que los sistemas de IA aprenden basados en datos que reflejan prejuicios humanos existentes; sin una alineación deliberada y en algunos casos forzada, incluyendo con valores de equidad por default, se corre el riesgo latente de que se puedan perpetuar o amplificar esas injusticias.

Jonker & Gomstyn (2024) dan como ejemplo la existencia de la existencia de un grupo de herramientas de IA para contratación de personal corporativo, así como la concesión de créditos hipotecarios, podrían generar discriminación contra grupos minoritarios si fueron entrenadas con datos históricos sesgados. Un sistema alineado éticamente debería detectar y mitigar tales sesgos, incorporando el valor de justicia objetiva en su toma de decisiones.

Sin embargo, implementar la justicia no es trivial, ¿se debe buscar igualdad estricta de resultados entre grupos, o más bien procedimientos imparciales? Cada aproximación ética, basada en igualitarismo, meritocracia, equidad, etc., conlleva distintos criterios cuantificables y, por lo tanto, se deberá destacar cuál será el valor mayor sobre el cual el modelo tomará con mayor jerarquía.

Lograr consenso sobre cuál criterio usar es en sí un dilema ético y político, lo que involucra que abordar este reto requiere procesos adicionales, como auditorías de equidad, participación de grupos afectados y actualización continua de los sistemas conforme evoluciona la comprensión social de la justicia (WEF, 2024).

Otro reto ético clave es evitar la imposición hegemónica de valores, lo que algunos analistas denominan imperialismo ético, dado el dominio que ciertas empresas y países tienen en el desarrollo de IA, existe el riesgo de que las normas culturales de un grupo terminen incrustadas globalmente en los sistemas de IA, subordinando visiones alternativas (Upmann, 2023).

Por ejemplo, se ha observado que muchos Modelos de Lenguaje Grandes, que en inglés se conoce como Large Language Model (LLMs), tienden a reflejar valores propios de países anglosajones y europeos occidentales, debido tanto a los sesgos en los datos de entrenamiento de la IA están mayoritariamente en inglés, así como a las decisiones de sus creadores sobre qué contenido es aceptable y cual deberá incluirse sin demasiada importancia (Tao, 2024; Law, 2024).

En un estudio generado por Tao (2024), se halló que modelos como ChatGPT, en ausencia de instrucciones específicas, mostraban una inclinación hacia valores de autoexpresión, individualismo y libertad religiosa típicos de Estados Unidos y Europa. Esto implica, por ejemplo, mayor tolerancia a la diversidad, énfasis en igualdad de género y libertad de expresión en las respuestas por defecto de la IA. Si bien esos valores encajan con ciertas culturas, en otras regiones podían percibirse como sesgados o ajenos a las normas locales.

El mismo estudio demostró que simplemente modificando la instrucción generada a la IA, llamado comúnmente como prompt, e indicando al modelo que respondiera como una persona promedio de X país, se reducía significativamente este sesgo cultural en la mayoría (71–81%) de los países probados. Este hallazgo sugiere que una alineación culturalmente sensible es técnicamente posible hasta cierto punto, por ejemplo, mediante una instrucción con sesgo cultural, o cultural prompting, realizados a los ajustes personalizados desde un modelo general.

Esta programación y sesgo específico de inicio plantea una pregunta ética: ¿hasta dónde se debe adaptar la IA a las normas locales, se deberán hacer por parte del usuario o deberán ser omitidas especialmente si algunas de esas normas contradicen valores universales y/o derechos humanos?

Este último punto constituye otro dilema ético: la tensión entre relativismo cultural y valores universales. Si adoptamos una postura de alinear la IA a cada cultura, podríamos terminar justificando que un sistema de IA en un país autoritario censure información política porque refleja los valores locales de orden y autoridad, o que, en una sociedad con fuertes prejuicios de género, una IA perpetúe roles discriminatorios ya que así piensa la

mayoría. Esto claramente choca con principios éticos globales de derechos humanos y dignidad, por lo cual los expertos advierten que la IA no debe simplemente replicar acríticamente las normas locales si estas vulneran derechos fundamentales (Law, 2024).

Hay un límite ético necesario: la alineación cultural no puede ser excusa para violaciones éticas mayores con argumentos de preferencia de un mal menor vs bien cultural. En la práctica, significa que las empresas y gobiernos enfrentan decisiones complejas sobre qué valores son no negociables. Algunos han propuesto establecer líneas rojas éticas universales. Como corolario, la IA nunca debe emplearse para incitar violencia, violar la privacidad, ni discriminar por raza o género, pero deberá arrojar información de investigación sólo dentro de los márgenes que no crucen esas líneas (Acosta, 2024).

Este enfoque combina universalismo ético con pluralismo cultural en temas donde haya margen de adaptación y, aun así, no siempre es obvio dónde trazar la línea. Por ejemplo, la libertad de expresión en Occidente es un valor central, pero muchas culturas Orientales ponen límites para proteger otros valores, como la honra, religión y estabilidad social. Una IA alineada en Occidente podría tolerar expresiones críticas o satíricas que, de alinearse a otra cultura, deberían ser bloqueadas por considerarse blasfemia o discurso peligroso para el Estado. Decidir si la IA debe anteponer la libertad de expresión universal o la sensibilidad local a la religión es un dilema ético sin respuesta fácil, requiriendo deliberación puntual y probablemente soluciones caso por caso (Gardels, 2024).

Además, existe el reto ético de la transparencia y legitimidad en la toma de decisiones de alineación. Responder a la pregunta ¿quién elige los valores? es crucial, debido a que si sólo los desarrolladores en Silicon Valley o los reguladores de una superpotencia internacional deciden cómo se alinea la IA, se corre el riesgo de excluir la voz de muchas comunidades afectadas. Éticamente, es necesario abogar por procesos participativos y multilaterales, incluir a diversos grupos de interés tanto como expertos en ética, representantes de minorías culturales y organizaciones de la sociedad civil en la definición de principios de IA (WEF, 2024).

Como señala Upmann (2023) el 72% de expertos globales en IA concuerdan en que las consideraciones culturales deben guiar el desarrollo ético de la IA, lo cual implica involucrar voces locales en ese proceso, dejando claro que, sin una gobernanza inclusiva, la alineación carecerá de legitimidad democrática.

La rendición de cuentas es otro aspecto: es preciso documentar qué valores se incluyeron y cómo, para que usuarios y auditores puedan evaluar si un sistema de IA opera conforme a lo prometido inicialmente. La transparencia sobre los compromisos éticos realizados permite un escrutinio público y ajuste en caso necesario.

En resumen, los retos éticos de la alineación giran en torno a garantizar que la IA haga el bien conforme a valores humanos ampliamente compartidos, evitando causar daño por sesgo o desvío, sin imponer una moral única ni traicionar principios fundamentales, lo que requiere un delicado equilibrio entre universalidad y pluralismo, rodeado de procesos éticos robustos en la gobernanza de la IA.

### **Retos culturales en la adaptación de la IA a diferentes contextos**

Además de los dilemas éticos generales, la alineación de la IA enfrenta retos prácticos y conceptuales específicos en el ámbito cultural. Uno de ellos es la complejidad de capturar las normas y valores culturales de múltiples sociedades de una manera precisa y traducir éstas a un lenguaje técnico para que pueda ser utilizado por la tecnología existente.

El desafío radica en que la cultura es un fenómeno dinámico, multifacético y a veces ambiguo, difícil de cuantificar o traducir en reglas concretas para un algoritmo. Los intentos de medir cultura, al presentarse como variables o valores promedio por país, tienden a simplificar excesivamente la realidad, reduciendo sociedades enteras a unos pocos números. Estas medidas pueden servir como referencia, pero no fueron diseñadas para la alineación de IA, advierte Law (2024).

Asimismo, si una IA se ajusta rígidamente a ese valor promedio, podría responder de la misma forma a todos los usuarios de esa nacionalidad asumiendo, digamos, un estilo colectivo, ignorando

la variación individual. Esto ilustra el problema de que una IA alineada a un estereotipo cultural puede terminar lijando las diferencias sociales y marginando a los disidentes, lo que sería un grave ataque a las minorías religiosas, voces opositoras o estilos de vida no convencionales, las cuales quedarían invisibles para un sistema calibrado solo con la norma dominante (Law, 2024).

Relacionado a lo anterior, surge el riesgo de crear sistemas de IA con prejuicios locales contribuyendo a perpetuarlos, frenar el progreso social y devolviendo a los usuarios las mismas premisas culturales redundantes. Law (2024) denomina estasis a este fenómeno en el que la IA, al alinearse con lo que la sociedad ya cree, podría inhibir el cuestionamiento y la evolución de esos valores con el tiempo.

Por ejemplo, imaginemos una IA entrenada para alinearse con las normas de género tradicionales de cierta cultura conservadora X, la cual, al interactuar con usuarios, reforzaría esos roles en lugar de ofrecer perspectivas distintas, consolidando así la visión tradicional dominante, esto plantea la cuestión de si la IA debe ser un espejo de la cultura vigente o también una ventana a ideas diferentes. Una alineación puramente culturalista corre el riesgo de convertirse en cómplice de la inercia cultural, validando incluso costumbres problemáticas solo porque son prevalentes localmente.

Estudios recientes señalan que la introducción de nuevas tecnologías en sí mismas puede transformar valores y comportamientos humanos, es decir, la relación es bidireccional: la cultura influye en la IA y la IA influye en la cultura. Esto conlleva a una capa adicional de complejidad intrínseca, el poder alinear la IA no es sólo adaptarla pasivamente, sino que conlleva decidir qué influencias culturales queremos reforzar o mitigar a través de ella (Danaher & Saeltra, 2023; Bravansky, 2024).

Otra dificultad cultural es la coexistencia de marcos normativos distintos en entornos globalizados en donde las aplicaciones de IA a menudo se despliegan globalmente a través de Internet, cruzando fronteras. Un mismo sistema puede ser usado simultáneamente por personas en países con culturas muy diferentes por lo que ¿debe el sistema comportarse de forma distinta según la ubicación o perfil cultural del usuario? Resolver

este dilema, técnicamente implica detectar contexto cultural y adaptar la respuesta en tiempo real.

En este sentido, ya se han dado pasos en esta dirección: por ejemplo, OpenAI en 2023 introdujo la opción de modo confidencial en ChatGPT para el mercado europeo, esto fue en respuesta a sensibilidades locales sobre privacidad y seguridad, mientras que en otros lugares el comportamiento es distinto. Sin embargo, la adaptación cultural es un reto continuo, requiere localización precisa, adaptación inmediata del sistema, así como aplicación expresa en el diseño de producto, interfaces, lenguaje y contenido.

Empresas como IBM han recomendado crear directrices éticas modulares por región, de modo que los principios globales se personalicen según leyes y valores locales manteniendo un núcleo común. No obstante, incluso con el desarrollo de IA en un ambiente multicultural, surgen choques culturales directos entre visiones de distintos países (Upmann, 2023).

Destacando el caso icónico de la guerra fría entre la filosofía de Silicon Valley y la de China en cuanto a IA; entendiendo que, históricamente dentro de Silicon Valley se han exaltado valores de libertad individual, así como de transparencia, mientras que China enfatiza los valores de colectivismo y armonía social bajo lineamientos estatales (Gardels, 2024).

Estas diferencias se plasman en las normas a las que se alinean sus IAs, OpenAI declara que la IA debe ser una extensión de la voluntad individual humana, distribuida lo más ampliamente posible, mientras que las regulaciones chinas exigen que la IA encarne los valores socialistas centrales, censurando cualquier contenido considerado subversivo al Estado. Para una empresa tecnológica global, satisfacer simultáneamente ambas exigencias es prácticamente imposible de ahí que veamos dos bandos en constante ataque, teniendo desarrollos de IAs occidentales inaccesibles en China y viceversa, cada una alineada a su ecosistema cultural, político y social.

Con esto, se deberá tener principal cuidado en la aplicación de estrategias de alineación, considerando sensibilidades y confianza dentro de la variedad de sociedades que serán usuarias de esta herramienta. Esto apela al problema inherente que se ha

abordado, un mismo enfoque de IA ética puede generar tranquilidad en una cultura y sospecha en otra.

Comunicar la ficha técnica en cómo se ha alineado la IA, en términos entendibles y relevantes localmente, sin tecnicismos sobre la construcción del algoritmo y en un lenguaje lo más plano posible es crucial para lograr su adopción. En suma, los retos culturales obligan a tratar la alineación de la IA no como un ajuste universal, sino como un proceso contextualizado, flexible y consciente tanto de las diferencias genuinas como de las complejidades intrínsecas para la definición de los valores culturales universales de forma operativa.

### **Estrategias y enfoques para adaptar la IA a la diversidad de valores**

Frente a los retos descritos, investigadores, empresas y organismos de la sociedad civil han propuesto diversas estrategias para lograr que la IA se adapte de manera ética y efectiva a la pluralidad de los valores humanos. Un enfoque fundamental es adoptar un proceso de alineación multilateral y bidireccional.

Bravansky (2024) sugiere que la alineación cultural debería replantearse como un proceso bidireccional, en el que no solo incrustamos valores culturales en la IA, sino que también interrogamos y comprendemos cómo los usuarios en cada contexto quieren que la IA se comporte, adaptando la interacción en consecuencia.

Esto implica diseñar frameworks de interacción donde los usuarios locales puedan influir en el comportamiento de la IA de manera estructurada. Por ejemplo, un asistente de IA podría preguntar por las preferencias del usuario antes de generar respuestas en ciertas decisiones sensibles y ajustar sus algoritmos según esas indicaciones. Este tipo de personalización cultural a nivel de usuario es uno de los métodos más prometedores: en lugar de asumir que todos los miembros de una cultura quieren lo mismo, se le da oportunidad y libertad al individuo para calibrar la IA a sus propios valores dentro de un rango permitido (Tao, 2024).

En este sentido, aplicar cultural prompting entra directamente en esta categoría: el usuario provee contexto cultural al inicio de la

sesión y el modelo modula su salida acorde a ese contexto, con mejoras notables en alineación a nivel personal e individual que provea específicamente el usuario. Esta máxima personalización podría diseñar una directriz al futuro en la que las interfaces brinden al usuario un perfil de ajustes de valores, similar a configurar la privacidad de un navegador o la aplicación de filtros de contenido, eligiendo entre distintos perfiles e intervalos éticos (Law, 2024).

Esta idea se alinea con la noción de sistemas dirigibles, que en inglés es conocido como *steerable systems* abogada por algunos expertos, donde la IA ofrece un universo moral y ético personalizable pero finito, en el cual el usuario puede mover qué tanto aplique este universo a todos los prompts que se generen de acuerdo con su cosmovisión. En esencia, en vez de una única IA estática para todos, se tendría una IA multifacética y plural, que puede configurarse dentro de ciertos márgenes éticos, pero de forma totalmente personalizada (Law, 2024).

Otra estrategia complementaria es la localización y regionalización de los sistemas de IA, lo que puede significar desarrollar modelos locales entrenados con datos del propio entorno cultural-lingüístico como base, o crear versiones regionales de modelos globales ajustados a normativas y valores locales (Gardels, 2024).

De igual modo, países como Francia y Alemania promueven proyectos de IA soberana, que refleje de forma más cercana y personalizada sus valores en ámbitos ciudadanos como privacidad y transparencia. Por otra parte, China ha desarrollado sus propios algoritmos de recomendación, motores de búsqueda y recientemente modelos generativos, como Alibaba's Tongyi Qianwen, que incorporan explícitamente filtros y sesgos alineados con la ideología y cultura política china, esto por mandato regulatorio, evitando críticas al gobierno y enfatizando contenidos patrióticos sobre cualquier búsqueda de información (China State Council, 2022; Gardels, 2024).

En contextos democráticos, una alternativa menos impositiva va en el sentido de integrar dentro del diseño de la IA a actores locales. Por ejemplo, IBM ha reportado con éxito el trabajo realizado en África para adaptar herramientas de IA que den prioridad cultural y entiendan la realidad económica local de diversas comunidades (Upmann, 2023).

Involucrar a las partes usuarias, como lo son líderes comunitarios, ONGs y usuarios finales en las pruebas piloto, así como en la creación de procesos activos de retroalimentación, permite detectar a tiempo donde la IA entra en conflicto con costumbres o necesidades locales y corregir el algoritmo. Este enfoque participativo se enlaza con diseñar de manera conjunta el marco de la ética de la IA (Upmann, 2023).

En términos técnicos, se hace uso de diversas metodologías para instrumentar los límites y los valores éticos dentro de la programación de las IA, contando con un diseño sensible a los valores humanos, conocido en inglés como Value-Sensitive Design (VSD), lo que propone identificar qué valores son los relevantes para los usuarios finales desde el inicio y así incorporarlos a su diseño final (Friedman, 2013).

Existe algo muy particular que comenta Mitchell (2019) a manera de aviso inicial en el uso de IA, por ejemplo, que la documentación técnica de un modelo podría indicar: “Entrenado principalmente con datos de EE.UU. y Europa, puede presentar sesgos si se usa en otras regiones, se recomienda ajuste local antes de cualquier prompt”, con la intención de que sea útil esta herramienta para otra locación.

Del mismo modo, iniciativas globales como la Asociación Global Partnership on AI (GPAI) buscan compartir mejores prácticas entre países para alinear la IA respetando la diversidad cultural. Un ejemplo concreto es la recomendación de la UNESCO en 2021 en relación con la inclusión de las minorías culturales y comunidades indígenas dentro de sus desarrollos de IA, con la finalidad de preservar idiomas locales, conocimientos tradicionales y patrimonio cultural.

Esto se traduce, por ejemplo, en apoyar la digitalización de lenguas poco representadas y su incorporación en sistemas de procesamiento de lenguaje natural, para que esas comunidades puedan interactuar con la tecnología en sus propios idiomas y con sus propios modismos. La diversidad lingüística es un componente esencial de la diversidad de valores, pues el lenguaje porta visiones de mundo en sí mismo, y en ese sentido, alinear la IA a valores humanos incluye también habilitarla para entender,

producir y desarrollar contenidos únicos desde diferentes marcos culturales.

### **Más allá de la alineación algorítmica: perspectivas y recomendaciones futuras**

Los análisis anteriores dejan claro que alinear la inteligencia artificial con los valores humanos no es una tarea que se resuelva únicamente en el nivel algorítmico o con una serie de ajustes dentro del modelo. Más allá de la alineación algorítmica, implica reconocer que estamos ante un desafío sociotécnico continuo, que abarca consideraciones éticas profundas y sensibilidades culturales muy profundas.

En primer lugar, es evidente que la alineación de la IA debe concebirse como un proceso iterativo y participativo en constante evolución, más que como un producto terminado. Los valores sociales cambian con el tiempo, al igual que los avances tecnológicos por lo cual, lo que una generación considera aceptable, la siguiente puede verlo problemático, ejemplos sobran. Por lo tanto, una IA alineada en el día de hoy, podría verse como altamente anarquista o anticuada para los valores del futuro si es que no existen mecanismos de actualización.

Esto implica establecer mecanismos constantes de retroalimentación, donde las experiencias de uso real alimenten mejoras que ni si quiera existen en este momento, conceptos como monitorear dónde el sistema está generando confusión o respuestas que generen malestar cultural deberán ser recogidas de forma inmediata para su correcto ajuste.

Autores como Floridi (2020) proponen incluso la creación de un ombudsman o auditor social de la IA, que recolecte quejas de comunidades diversas y obligue a revisiones de alineación en consecuencia. En cualquier caso, la adaptabilidad debe ser un atributo central, tanto a nivel técnico, con modelos capaces de adaptarse a nuevos datos, como a nivel organizacional, entendido como un sistema ético que responda a los dilemas éticos que emerjan.

También, se tendría que aceptar que no existe una sola respuesta correcta sobre cómo debe comportarse una IA en todos los contextos, sino múltiples configuraciones legítimas según la

comunidad de usuarios, de su ubicación, de su cultura y capacidad de que la IA refleje esta nano-personalización. Como ejemplo concreto se puede observar a los sistemas legales internacionales, al existir distintas jurisdicciones con leyes adecuadas a sus sociedades, pero todas respetando estándares internacionales de derechos, igualmente podríamos tener distintas instancias de IA alineadas a marcos culturales nacionales, sujetas a un conjunto de lineamientos globales mínimos (Whittlestone, 2019).

La iniciativa Pluralistic Alignment presentada en la Conference and Workshop on Neural Information Processing Systems (NeurIPS, 2024) apunta en esa dirección, explorando cómo integrar diversas perspectivas, valores y experticias en la alineación de las IAs actuales, en lugar de buscar un consenso único. Esta visión pluralista requerirá desarrollar técnicas para manejar multiplicidad de significados y coexistencia de múltiples objetivos en los sistemas de IA, quizás inspirándose en algoritmos de optimización con múltiples objetivos, que puedan equilibrar varios valores éticos a la vez.

Teniendo esto en mente, es altamente probable que veamos la consolidación de líneas rojas globales para la IA, usos o comportamientos prohibidos sin excepciones culturales, semejante a cómo hay prohibiciones universales de comportamientos, uso de armas o prácticas inhumanas sin distinción geográfica.

Al mismo tiempo, la forma de implementar localmente esos valores podrá variar. Por ejemplo, todas las IA deberán respetar la dignidad humana, pero la expresión concreta de la dignidad podría ajustarse, con lo cual, en una cultura puede implicar la comunicación formal y con honor en todas las respuestas o el respeto incuestionable hacia algunas figuras públicas o deidades, mientras que en otras será más un proceso de respetar las libertades individuales (Floridi, 2022).

Dejando en claro esta posición, se deberá tener en cuenta un aspecto crucial, lo que se refiere a la educación y alfabetización en IA tanto de desarrolladores como del público usuario. Para que esta alineación tenga éxito, los desarrolladores deben formarse en ética intercultural y humanidades, no sólo en programación, mientras que los usuarios deben adquirir nociones de cómo

funcionan estos sistemas y cuáles son sus ajustes de programación inicial.

Finalmente, es importante resaltar que la alineación ética y cultural de la IA es un medio para un fin mayor, el cual es brindar un extenso compendio de herramientas para que la humanidad pueda crecer como un todo, expandir la conciencia colectiva y que, en el mejor de los casos, evolucionemos a un nuevo estado de relaciones humanas, priorizando a la conciencia humana universal sobre las diferencias personales, culturales y efímeras, abocando hacia un estado de entendimiento trascendental de la experiencia humana.

Como señala Gardels (2024), alinear la IA con valores universales debe, ante todo, significar reconocer las particularidades humanas desde sistemas de creencias plurales, visiones del mundo encontradas, hasta temáticas culturales que sean incómodas. En concreto, entender la alineación algorítmica implica que lo más importante en el desarrollo de la IA es el elemento humano, al que siempre deberá servir como una herramienta que detente su valor en potenciar su expansión de conciencia.

### **¿Puede la IA alinearse verdaderamente con una pluralidad de valores humanos sin caer en contradicciones o sacrificios éticos?**

En primer lugar, desde un plano técnico, la idea de una IA que sea simultáneamente precisa, coherente y plural resulta problemática en todos sentidos. Como señala Rodríguez (2024), convertir conceptos éticos abstractos en reglas computables es ya un desafío monumental, además, si se intenta traducir múltiples visiones culturales simultáneamente, el sistema se ve forzado a operar con ambigüedad y posibles conflictos lógicos.

Esta tensión entre precisión y contextualización moral se expresa, por ejemplo, en los dilemas sobre libertad de expresión versus sensibilidad cultural o seguridad colectiva versus privacidad personal. Tal como lo argumenta Knight (2024), la IA no puede evitar tomar partido en decisiones que implican valores contrapuestos, lo que inevitablemente generará descontento en algunos sectores sociales.

Ante esta postura, se propone como alternativa teórica el contar con un pluralismo moral que se encuentre dentro de la programación inicial de las IA, esta visión rechaza que se cuente con un solo alineamiento único y universal, sino que esté adaptándose de forma constante a los marcos morales locales, dentro del universo de los valores mínimos universales humanos.

El fundamento de esta propuesta proviene de las guías éticas para la inclusión de principios indígenas, como lo es la población Maori en Nueva Zelanda (Taiuru, 2020), hasta estudios aplicados desarrollados en Canadá (González & Martínez, 2023), sobre cómo las instituciones modernas pueden generar marcos normativos que integren a la población indígena a través de su ética hasta sus formas de desarrollo comunitario

Este enfoque plural no es más que la implementación de un diseño participativo de la ética de la IA, teniendo en cuenta que esta herramienta ha servido, de gran forma, para generar un diagnóstico que revelen las necesidades, retos, problemas y acceso a oportunidades de las comunidades marginadas. Este enfoque de creación en conjunto, como plantea Rodríguez (2024), refleja qué prioridades serán puntualmente incluidas en el diseño final de la IA. Esta idea podría tener como resultado el que los sistemas de reconocimiento de voz detecten las lenguas indígenas, los modismos locales, así como conceptos nuevos, que puedan ser integrados al conocimiento global que provee la IA.

Hay un punto esencial en esta propuesta, el cual viene de un aprendizaje ontológico social, entendiendo que se deberá generar la identificación de valores no negociables dentro del pluralismo propuesto. La intención es evadir el relativismo ético, en el cual habría tantas éticas como usuarios finales, sino que se integre el pluralismo a través de consensos mínimos y límites definidos para cada comunidad, así como una ética global que aplique integrando a sus símiles locales.

Básicamente se quiere ejemplificar este proceso en donde una IA pueda acoplarse a comunidades con fuerte arraigo espiritual o religioso, en la que se deba tener atención especial a respetar ciertos temas tabúes, así como otras comunidades que necesiten incluir posiciones agnósticas o enfocadas a la libertad humana. Este nivel de flexibilidad requiere un sistema técnico con una estructura adaptable y procesos de deliberación moral que se

mantengan a lo largo del tiempo. Este enfoque, a pesar de ser desafiante, podría incrementar significativamente la legitimidad de la IA en diferentes contextos y evitar conflictos culturales que obstaculicen su implementación.

Adicionalmente, cabe destacar que es de vital importancia el entender con qué datos se está entrenando a la IA, debido a que el contar con poca data para el entrenamiento de modelos masivos podría significar que se tendrían que eliminar de inmediato, con la intención de evitar errores de sintaxis o ser poco profundo en su entendimiento.

Esto lo aborda Krishnan (2022), entendiendo que se podría fácilmente caer en un colonialismo de datos, en donde se prioricen los temas con mayor cantidad de datos, reduciendo el enorme potencial de una herramienta como lo es la IA al empoderamiento de un discurso supremacista, acentuando las divisiones epistémicas y culturales presentes en la sociedad.

Teniendo esto en mente, autores como Ricaurte (2022) proponen que se incorporen una serie de capas adicionales al procesamiento de información, en el que se otorgue poder sobre los datos a incorporar y la importancia de estos a las comunidades indígenas y minoritarias a priori, con la intención de que se oriente el significado, en forma y fondo, de los conceptos propios de cada etnia, lenguaje, comunidad y cosmovisión.

Ultimadamente, entender una postura sobre el pluralismo de datos, es entender que existirán diversos conceptos de ética que modelarán las respuestas obtenidas por estos modelos. Sin embargo, se deberá entender que los datos con los que ya se encuentra entrenada la IA tiene una carga de dominación y de visión global por parte de sus creadores, así como la presentación de resultados enmarcados de cierta forma para que se mantenga una visión sociocultural uniforme.

Entender que la IA se desarrolló para mantener un acceso a la realidad de una forma específica y por ende, bajo un estilo de moral puntualmente descrito, será entender que se necesita la creación de una IA desde cero, que sea diseñada desde abajo, moldeada por la diversidad auténtica de valores, culturas y epistemologías humanas, brindando una cantidad robusta de conceptos éticos, que suena problemático al inicio, pero que

acercará esta herramienta a una aplicación democrática, crítica y, ojalá, más cerca de los valores humanos fundamentales (Krishnan, 2022).

### **Implicaciones para seguridad e inteligencia en México**

La introducción de IA en funciones de inteligencia y seguridad exige reforzar controles ex ante y ex post, especialmente cuando existe delegación algorítmica. La evolución jurídica-organizacional del Centro Nacional de Inteligencia (CNI) y sus esquemas de control democráticos ofrecen una base para traducir competencias y límites en requisitos técnicos explícitos (Casillas Zamora, 2024). De forma convergente, el marco de seguridad interior muestra la importancia de la necesidad, proporcionalidad y trazabilidad en cualquier uso de IA (Jiménez Solano, 2024).

A su vez, el debate sobre seguridad interior y el proceso de militarización de la seguridad pública advierten que incorporar tecnologías sin garantías puede desbordar finalidades originales. Implementaciones de IA en tareas policiales o de defensa deben documentar objetivos, umbrales y controles humanos significativos, sujetos a supervisión y evaluación independiente (Jiménez Solano, 2024; Romero, 2024). De esta manera, en seguridad la tutela de derechos opera como restricción y guía: transparencia sobre fuentes de datos, criterios de clasificación y umbrales; explicabilidad proporcional al riesgo; mecanismos de disenso y reparación. La intersección entre inteligencia y derechos exige procedimientos documentados y auditables (Toledo Utrera, 2024).

Por su parte, en ciberseguridad, la orquestación y la automatización inteligente habilitan defensas proactivas, pero deben medirse con métricas que no premien falsos positivos y mantener intervención humana en decisiones críticas (Estrada Nava, 2024). Como ejemplo, el ataque a la Comisión Nacional del Agua (CONAGUA) ilustra la interdependencia entre ciberseguridad, continuidad operativa y bienes públicos esenciales. En tales casos, la alineación no es un lujo, sino un principio para priorizar resiliencia, defensa en profundidad y deber de cuidado cuando se adoptan herramientas automatizadas (Aguilar Obregón, 2024).

El fortalecimiento profesional del analista criminal —productos, estándares metodológicos y validación empírica— es indispensable para evitar dependencias excesivas de sistemas opacos. La IA debe complementar, no sustituir, el análisis estructurado; sus salidas deben tratarse como hipótesis sujetas a verificación humana (Vignettes del Olmo, 2024). En un contexto de policrisis y debilitamiento del multilateralismo, la gobernanza de IA requiere mínimos universales y márgenes locales bien justificados, evitando tanto el relativismo como la imposición (Rosas, 2024).

Casos operativos como la primera captura de Ovidio Guzmán ofrecen lecciones para el diseño de sistemas de apoyo a la decisión: trazabilidad, criterios de validación y separación clara entre indicios y conclusiones (Jaimes Álvarez, 2024). Asimismo, marcos de política exterior y defensa orientados por criterios realistas permiten alinear la innovación con objetivos estratégicos nacionales (Ortiz Arellano, 2024).

## **Conclusiones**

Los esfuerzos actuales de alineación algorítmica, que buscan incorporar valores humanos en la programación central de la inteligencia artificial, están limitados significativamente en cuanto a su capacidad operativa, debido a que, no toman en cuenta la amplia diversidad de valores culturales y morales que existen alrededor del mundo. Se ha registrado que los sistemas de inteligencia artificial suelen reproducir las suposiciones éticas de sus contextos originales, brindando un sesgo inicial, tanto ideológico como ético. Esto puede dar lugar a sesgos y tensiones cuando se emplean en sociedades con marcos culturales y normativos diferentes.

Inicialmente, dejar en claro que los valores humanos no son homogéneos entre diferentes culturas y regiones y que, por esta razón, los sistemas de inteligencia artificial necesitan acoplarse a contextos sociales, jurídicos y culturales concretos para prevenir conflictos éticos. Varios ejemplos analizados demuestran cómo los principios éticos pueden entrar en conflicto en la práctica, por ejemplo, maximizar la precisión o eficiencia de un algoritmo implica sacrificar precisión, equidad, privacidad y hasta la orientación de las respuestas de los modelos de IA. En conjunto,

estos hallazgos subrayan qué, al ir más allá de la alineación algorítmica tradicional, es imprescindible incorporar una visión plural de la ética, reconociendo la multiplicidad de visiones cosmogónicas.

La hipótesis principal se enfoca en la tensión entre el pluralismo moral y la eficacia algorítmica como criterio de base en la construcción de IAs, debido a que los creadores de IA se encuentran con problemas éticos intrínsecos, a pesar de que sus intenciones sean las mejores, priorizando el optimizar un criterio de rendimiento o de velocidad en el algoritmo, dejando abierta la posibilidad de sacrificar otros parámetros de equidad o principios sociales igualmente válidos al analizar los datos existentes.

Esta incompatibilidad no es casualidad, sino que tiene su origen en la ausencia de una definición única y universalmente válida de lo que significa justo o beneficioso. Diversas comunidades tienen prioridades diferentes, como la privacidad individual frente a la seguridad colectiva o la libertad de expresión frente a la protección contra la desinformación y estos valores pueden no ser compatibles en un mismo modelo de IA.

En estas líneas se confirma que la tensión entre eficiencia algorítmica y pluralismo moral no puede eliminarse simplemente afinando parámetros técnicos, evidenciando la diversidad irreductible de los valores humanos. Este reconocimiento concuerda con enfoques filosóficos previos que proponen un pluralismo ético frente al universalismo monocromático, admitiendo la necesidad de incluir múltiples marcos morales y realizar diálogos interculturales en torno cómo, qué y cuáles serán las bases de los valores humanos que estarán dentro del desarrollo de las IA.

Frente a estos desafíos, estas líneas invitan a adoptar estrategias novedosas y más inclusivas para el desarrollo y operatividad de la IA, entre ellas el diseño en conjunto, la descentralización ética y la participación comunitaria. En lugar de imponer valores de forma unidireccional, el diseño conjunto propone involucrar activamente a las múltiples comunidades y actores afectados en la creación de sistemas de IA. Esto se alinea con la herramienta del diagnóstico participativo, así como del diseño participativo, donde los afectados por una tecnología tienen voz y voto en su desarrollo, lo

que abre la oportunidad a diseñar modelos más legítimos y democráticos.

Múltiples autores han demostrado cómo los procesos de creación en conjunto han aportado visiones diferentes a la generación de conocimiento y datos para el entrenamiento de la IA, proveyendo de contextos, necesidades y requerimientos específicos que fácilmente podrían perderse en la homogenización de las bases de datos. Comprender que una descentralización ética aporta una nueva dimensión al entendimiento de la moral dentro de la IA, es conocer los procesos sobre qué prioriza, cómo se manejan los datos y qué particiones se hacen para la simplificación del problema a resolver, esto genera una evolución multinivel de estos conceptos y su aplicación para los principios humanos del futuro y su debida supervisión algorítmica.

Por último, la participación comunitaria a través de los ciudadanos, ONG, auditorías de algoritmos, así como comités locales de ética, asegurarán que la IA mantenga sus principios operativos alineados con los valores humanos y, por ende, entregar respuestas acertadas al contexto social desde el que se emita la petición de información. Promover esta integración humana dentro de una herramienta computacional en desarrollo creará un entendimiento mayor de ambas partes, conocer las entrañas de los valores humanos para conocer las entrañas de la máquina, diseñando en conjunto una realidad que siempre ha estado en mutuo descubrimiento.

## BIBLIOGRAFÍA

- Acosta, C. (2024). La Alineación, el Santo Grial de la IA. El Colombiano. Recuperado de <https://www.elcolombiano.com/opinion/columnistas/carlos-acosta-la-alineacion-el-santo-grial-de-la-ia-FF25648827>
- Aguilar Obregón, E. A. R. (2024). Agua y Seguridad Nacional: El hackeo de la Comisión Nacional del Agua en México. *Revista de Inteligencia y Seguridad*, (2), 99–116. INAP.
- Amnistía Internacional. (2022). Myanmar: Facebook's systems promoted violence against Rohingya. Informe publicado el 29 de septiembre de 2022.
- Benítez, E. J. (2021). La importancia de la diversidad cultural en la ética de la IA. *OdiseIA*. Recuperado de

- <https://www.odiseia.org/post/la-importancia-de-la-diversidad-cultural-en-la-%C3%A9tica-de-la-ia>
- Benítez, E. J. (2024). La importancia de la diversidad cultural en la ética de la IA. Blog OdiseIA. Recuperado de <https://www.odiseia.org/post/la-importancia-de-la-diversidad-cultural-en-la-%C3%A9tica-de-la-ia>
- Bravansky, M., Trhlik, F., & Barez, F. (2024). Rethinking AI cultural alignment. Recuperado de <https://doi.org/10.48550/arXiv.2501.07751>
- Breier, K., Gutiérrez Fernández, G., & Montes de Oca, L. (2025). New Artificial Intelligence Legislation in Mexico. Global Policy Watch. Recuperado de <https://www.globalpolicywatch.com/2025/03/new-artificial-intelligence-legislation-in-mexico/>
- Casillas Zamora, P. W. (2024). Centro Nacional de Inteligencia: Evolución y naturaleza jurídica. *Revista de Inteligencia y Seguridad*, (1), 17–52. INAP.
- Ceceña, A. E., & García Veiga, J. (2021). Los sistemas digitales de vigilancia ampliados por la pandemia. *América Latina en Movimiento* – ALAI. Recuperado de <https://www.alainet.org/es/articulo/212352>
- Coeckelbergh, M. (2025). Three challenges for a global AI ethics: towards a more relational normative vision. *AI and Ethics*. <https://doi.org/10.1007/s43681-025-00791-9>
- Couldry, N., & Mejias, U. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.
- Cumpa Moreno, P. M. (2025). Inteligencia artificial y brecha digital en el Perú: Desafíos para la inclusión de los pueblos indígenas en el marco de un Estado multicultural. LP – Pasión por el Derecho.
- Estrada Nava, C. (2024). Ciberseguridad orquestable: Tendencias de IA para ciberdefensa proactiva y ciberinteligencia automatizable. *Revista de Inteligencia y Seguridad*, (2), 80–98. INAP.
- Gardels, N. (2024, 26 de abril). The Babelian Tower of AI Alignment. *Noema Magazine*. Recuperado de <https://www.noemamag.com/the-babelian-tower-of-ai-alignment/>
- Goffi, E. R., & Momcilovic, A. (2022). Respecting cultural diversity in ethics applied to AI: A new approach for a multicultural governance. *Revista Misión Jurídica*, 15, 111-122. <https://doi.org/10.25058/1794600X.2135>
- High-Level Expert Group on Artificial Intelligence (HLEG). (2019). *Ethics Guidelines for Trustworthy AI*. Comisión Europea.
- Jaimés Álvarez, O. (2024). Labores de inteligencia: Análisis de la primera captura de Ovidio Guzmán. *Revista de Inteligencia y Seguridad*, (1), 89–104. INAP.

- Jiménez Solano, J. (2024). Legislación y regulación sobre seguridad interior. *Revista de Inteligencia y Seguridad*, (1), 53–68. INAP.
- Jonker, A., & Gomstyn, A. (2024). ¿Qué es la alineación de la IA? IBM Topics. Recuperado de <https://www.ibm.com/es-es/think/topics/ai-alignment>
- Knight, W. (2024). La guerra cultural por los valores de la IA acaba de empezar. *Wired* (edición en español).
- Krishnan, A., et al. (2022). Inteligencia artificial: un manifiesto descolonial. En *Inteligencia Artificial Feminista: hacia una agenda de investigación para América Latina y el Caribe*.
- Larsen, B., & Dignum, V. (2024). Cómo alinear la inteligencia artificial con los valores humanos. *Foro Económico Mundial*.
- Law, H. (2024). Against cultural alignment. *Learning from Examples* (blog). Recuperado de <https://www.learningfromexamples.com/p/against-cultural-alignment>
- Liu, Y. (2023). Cross-Cultural Challenges to Artificial Intelligence Ethics. *Computer Sciences & Mathematics Forum*. <https://doi.org/10.3390/cmsf2023008021>
- OECD. (2019). *OECD Principles on Artificial Intelligence*. OECD Legal Instrument 0449.
- Open Government Partnership (OGP). (2021). Algoritmos que rinden cuentas a la ciudadanía. Recuperado de <https://www.opengovpartnership.org/es/stories/making-algorithms-accountable-to-citizens/>
- Ortiz Arellano, E. (2024). Defensa Nacional y Política Exterior del Estado mexicano en la perspectiva de Hans J. Morgenthau: Plan Nacional de Desarrollo 2019–2024. *Revista de Inteligencia y Seguridad*, (1), 105–126. INAP.
- Oxford Insights. (2023). *Government AI Readiness Index 2023*. Oxford: Oxford Insights. Recuperado de <https://oxfordinsights.com/ai-readiness-index-2023>
- Pertuzé, J. (2021). *GuIA.ai: hacia una ética de IA latinoamericana*. Centro de Estudios en Tecnología y Sociedad (CETyS), Universidad de San Andrés, Argentina.
- Pichai, S. (2018). AI at Google: Our Principles. *Google Blog*. Recuperado de <https://blog.google/technology/ai/ai-principles/>
- Rodríguez, Y. J. (2024). La complejidad de codificar valores humanos en sistemas de IA. *Blog personal I+D*.
- Romero, C. (2024). Proceso de militarización de la Seguridad Pública en México. *Revista de Inteligencia y Seguridad*, (1), 127–[fin]. INAP.
- Rosas, M. C. (2024). Policrisis y multilateralismo fallido en el siglo XXI. *Revista de Inteligencia y Seguridad*, (2), 15–30. INAP.
- Samuel, S. (2022). Why it's so damn hard to make AI fair and unbiased. *Vox Media*.

- Taiuru, K. N. (2020). Treaty of Waitangi/Te Tiriti and Māori Ethics Guidelines for AI, Algorithms, Data, and IOT. Publicación independiente, Nueva Zelanda.
- Tao, Y., Viberg, O., Baker, R.S., & Kizilcec, R.F. (2024). Cultural Bias and Cultural Alignment of Large Language Models. *PNAS Nexus*, 3(9), pp 346. <https://doi.org/10.1093/pnasnexus/pgae346>
- Toledo Utrera, A. (2024). La inteligencia para la seguridad nacional como elemento de tutela de los derechos humanos. *Revista de Inteligencia y Seguridad*, (2). INAP.
- UNESCO. (2021). Recomendación sobre la Ética de la Inteligencia Artificial. Conferencia General de la UNESCO, 41ª reunión. Recuperado de <https://unesdoc.unesco.org/ark:/48223/pf0000380455>
- Université de Montréal. (2018). Declaración de Montreal para un Desarrollo Responsable de la IA. Montreal, QC: Université de Montréal.
- Upmann, P. (2023). What Role Does Cultural Context Play in Defining Ethical Standards for AI? Artificial Intelligence Governance Network (AIGN). Recuperado de <https://aign.global/ai-ethics-consulting/patrick-upmann/what-role-does-cultural-context-play-in-defining-ethical-standards-for-ai/>
- Vignettes del Olmo, M. (2024). Claves del análisis criminal en México. *Revista de Inteligencia y Seguridad*, (2), 31–49. INAP.
- World Economic Forum. (2024). AI Value Alignment: Guiding Artificial Intelligence Towards Shared Human Goals. Global Future Council on the Future of AI White Paper. Recuperado de [https://www3.weforum.org/docs/WEF\\_AI\\_Value\\_Alignment\\_2024.pdf](https://www3.weforum.org/docs/WEF_AI_Value_Alignment_2024.pdf)
- World Values Survey (2023). Inglehart–Welzel Cultural Map (WVS Wave 7) [Gráfico]. Recuperado de <https://www.worldvaluessurvey.org/>
- Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Thousand Oaks, CA: SAGE Publications.



## LA INTELIGENCIA CIUDADANA Y EL ANÁLISIS PROSPECTIVO DE LA SEGURIDAD NACIONAL EN LA RELACIÓN MÉXICO – ESTADOS UNIDOS

Rodrigo De León Mondragón

**Resumen:** Este texto forma parte de los resultados del Diplomado “Prospectiva política y planeación estratégica”, del Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacionales (IMEESDN). En síntesis, unir inteligencia ciudadana con prospectiva estratégica permite pasar de la reacción a la anticipación: la participación cívica aporta capilaridad, legitimidad y corrección de sesgos, mientras que la matriz de influencias cruzadas y el MICMAC (Godet) dan estructura para identificar palancas, bisagras y termómetros del sistema. Con salvaguardas de datos, privacidad y explicabilidad algorítmica, la capa cívica se integra a la cooperación México–EE. UU. y a la reforma institucional mediante indicadores accionables (tiempos de triage, judicialización trazable, cierres  $\leq 72$  h, resiliencia anti-desinformación y trazabilidad de armas). Así, una “alianza 2.0” con ciudadanía organizada reduce corrupción y capacidad criminal; sin voluntad política, evaluación y transparencia, la participación deriva en ritual o ruido.

**Palabras clave:** inteligencia ciudadana, participación cívica, prospectiva estratégica.

**Abstrac:** This text is part of the outcomes of the diploma course “Prospectiva política y planeación estratégica” at the Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacionales (IMEESDN). In brief, fusing citizen intelligence with strategic foresight upgrades security from reactive to anticipatory: civic participation provides capillarity, legitimacy, and bias correction, while cross-impact matrices and MICMAC supply structure to surface motors, hinges, and result-thermometers. With data, privacy, and XAI safeguards, the civic layer plugs into Mexico–U.S. cooperation and institutional reform through actionable metrics (triage-to-action times, traceable prosecutions,  $\leq 72$ -hour closures, anti-disinformation resilience, and gun-trace indicators). The result is an “Alliance 2.0” where organized citizens help curb corruption and criminal capacity; absent political will, evaluation, and transparency, participation decays into ritual or noise.

**Key words:** citizen intelligence, civic participation, strategic foresight.

## **Introducción: por qué unir inteligencia ciudadana y prospectiva estratégica**

La conversación contemporánea sobre seguridad ya no puede separar la “inteligencia ciudadana” —la co-producción de información y conocimiento útil para la decisión pública por parte de la sociedad civil— de los enfoques de prospectiva estratégica —los métodos para anticipar trayectorias y puntos de inflexión en sistemas complejos.

La primera aporta capilaridad informativa, legitimidad y corrección de sesgos institucionales; la segunda, estructura, horizonte y disciplina analítica para no improvisar el futuro (Godet, 2001). Integrarlas permite pasar de una seguridad reactiva a una seguridad anticipatoria, empujada por datos y ciudadanía, pero gobernada por reglas claras y con evaluación de impacto (Inter-American Development Bank [IADB], 2018; United Nations Office on Drugs and Crime [UNODC], 2023).

## **Estado del arte: de la denuncia fragmentaria a la co-producción de inteligencia**

La literatura muestra que “inteligencia ciudadana” no es sinónimo de denuncia aislada ni, mucho menos, una etiqueta tecnológica. Operativamente, puede definirse como un proceso de gobernanza colaborativa en el que los ciudadanos —habilitados por marcos institucionales y plataformas digitales— participan en la recolección, verificación, análisis y diseminación de información de seguridad con valor para la decisión pública (IEPADES, 2025; UNDP, 2021).

Este proceso reubica al ciudadano dentro del ciclo de inteligencia: reporta (recolección), valida y contextualiza (procesamiento y análisis), y recibe retroalimentación útil (diseminación), cerrando un lazo de confianza y utilidad pública (ICAI, s. f.; Infoem, s. f.). Tres tradiciones académicas cercanas ayudan a precisar el contorno del concepto:

1. Gobierno abierto. Transparencia, participación y colaboración forman el ecosistema mínimo donde la

inteligencia cívica puede prosperar sin convertirse en “participación simbólica” (ICAI, s. f.; UNAM, s. f.).

2. Policía comunitaria. La inteligencia ciudadana digitaliza y escala el principio de proximidad, pero corre el riesgo de diluir la confianza interpersonal si la interfaz tecnológica sustituye —en vez de reforzar— la relación policía-comunidad (IADB, 2018).
3. Smart cities. La diferencia crítica es quién está al centro: una visión tecno-céntrica convierte al ciudadano en sensor pasivo; una visión cívico-céntrica lo reconoce como analista y co-diseñador de soluciones (CIPPEC, 2017; Alcaldía de Neiva, 2020).

En América Latina, los planes nacionales han abrazado el discurso de “seguridad ciudadana” y prevención, pero las implementaciones suelen regresar a reflejos de “mano dura” y a un sesgo operativo hacia la represión, reproduciendo la brecha entre discurso y realidad (IADB, 2018; UNDP, 2021). La literatura comparada insiste: sin instituciones abiertas y rendición de cuentas diagonal —mecanismos en los que la ciudadanía supervisa y exige resultados—, la participación degenera en ritual, no en inteligencia (Infoem, s. f.).

### **Arquitectura tecnológica: capacidades, límites y ambivalencias**

En el plano operativo, los ecosistemas C2/C4/C5 integran videovigilancia, llamadas de emergencia, botones de pánico y, cada vez más, reportes geolocalizados desde apps cívicas. La IA y el análisis de grandes datos permiten detectar “zonas calientes”, optimizar patrullajes y extraer patrones de incidencia en tiempos que desbordan la capacidad humana (RSD Journal, 2022; SINT, 2024). Sin embargo, la misma arquitectura que potencia la colaboración puede robustecer un panóptico tecnocrático si no hay salvaguardas: reconocimiento facial, drones y biometría, cuando se combinan con repositorios masivos de reportes ciudadanos, crean un potencial de vigilancia ubicua y de decisiones algorítmicas opacas (Lechner, 2016; INCIBE, 2023).

La consecuencia ética y jurídica es doble. Primero, privacidad: la centralización de datos sensibles convierte a las plataformas en objetivos de alto valor y exige una política de minimización,

anonimización y acceso controlado (INCIBE, 2023; UN, s. f.). Segundo, justicia algorítmica: los sistemas no son neutrales; aprenden de datos sesgados (por ejemplo, historiales de detenciones o patrones de denuncia) y pueden amplificar la discriminación mediante bucles de retroalimentación (IADB, 2018). La literatura recomienda explicabilidad (XAI), auditorías periódicas de sesgo y mecanismos de apelación para decisiones automatizadas que afecten derechos (Universidad de Navarra, 2024).

### **Amenazas cognitivas: desinformación y vigilancia horizontal mal encauzada**

El estado del arte identifica a la desinformación como vector crítico: astroturfing, inundación de reportes falsos, manipulación coordinada y uso de medios sintéticos (deepfakes) pueden colapsar la señal de un sistema basado en crowdsourcing o —peor— instrumentalizarlo para persecución política y polarización (Cybersecurity and Infrastructure Security Agency [CISA], 2020; Digital Future Society, 2020; UN, s. f.). Esto configura una “vigilancia social atomizada y algorítmicamente mediada” donde cualquiera puede reportar a cualquiera, pero algoritmos opacos priorizan qué merece atención, con incentivos perversos si la gobernanza y la trazabilidad fallan (Lechner, 2016; Funcas, 2021).

### **¿Por qué importa para la seguridad nacional? Tres razones estratégicas**

1. Capilaridad y legitimidad. La inteligencia ciudadana corrige el “déficit de proximidad” de los aparatos de seguridad: identifica micro-dinámicas territoriales y señales débiles imposibles de captar solo con sensores estatales, reforzando la confianza si hay retroalimentación efectiva (IEPADES, 2025; UNDP, 2021).
2. Anticipación basada en evidencia. Vincular participación con prospectiva permite transformar reportes dispersos en variables, hipótesis y escenarios, priorizando palancas de cambio y desactivando riesgos antes de su escalada (Godet, 2001; IADB, 2018).
3. Gobernanza multinivel. Amenazas transnacionales (delincuencia organizada, armas, ciberataques) requieren orquestación de actores públicos, privados y sociales; la

ciudadanía informada reduce asimetrías de información y presiona por coordinación interinstitucional con métricas transparentes (UNODC, 2023).

### **Cómo conecta con la prospectiva estratégica: de la matriz a la decisión**

Los métodos de impactos cruzados (Godet) y el análisis MICMAC aportan una sintaxis para leer sistemas complejos: al clasificar variables por influencia y dependencia se distinguen palancas motoras, bisagras frágiles y resultados-termómetro. Aplicado a la inteligencia ciudadana, el estado del arte sugiere cuatro grupos de variables recurrentes:

- Motoras: voluntad política sostenida, marcos de gobierno abierto, reforma/fortalecimiento institucional (judicial y policial), estándares de datos y auditoría algorítmica (Godet, 2001; IADB, 2018).
- Bisagra: cooperación interagencial y coordinación multi-actor (pública-privada-social), donde la confianza es el activo escaso (UNDP, 2021).
- Resultado: control territorial percibido, victimización y percepción pública (UNODC, 2023).
- Autónomas (de segundo orden): financiamiento, innovación tecnológica, regulación sectorial, cuyo impacto depende del andamiaje anterior (IADB, 2018).

El valor añadido de la prospectiva es pasar del “qué” (capacidad tecnológica o número de reportes) al “cómo” (relaciones que activan o bloquean cambios). En lugar de perseguir indicadores de resultado, el foco se desplaza a palancas estructurales (p. ej., reglas de transparencia, trazabilidad de reportes, retroalimentación y tiempos de respuesta) que la literatura muestra como determinantes de efectividad y legitimidad (IADB, 2018; UNDP, 2021).

### **Condiciones de éxito y salvaguardas mínimas**

Del conjunto de evidencias comparadas emergen principios prácticos:

- Gobernanza primero, tecnología después. Comités de supervisión con poder real, protocolos de datos (minimización, anonimización, retención), evaluaciones de impacto en derechos humanos y auditorías de sesgo publicadas (ICAI, s. f.; Infoem, s. f.; Universidad de Navarra, 2024).
- Transparencia radical y rendición de cuentas diagonal. Publicación periódica de métricas (tiempos de respuesta, acciones derivadas, aciertos/errores), reglas claras de moderación y trazabilidad de cada reporte para que la ciudadanía evalúe utilidad y riesgos (Infoem, s. f.).
- Evidencia y experimentación controlada. Pilotos con grupos de control, métricas de efecto (reducción real vs. desplazamiento del delito) y cierre de ciclo con retroalimentación a la comunidad (IADB, 2018; IADB, s. f.).
- Resiliencia anti-desinformación. Sistemas de reputación, verificación cruzada, detección de comportamiento no auténtico y canales oficiales de desmentido rápido integrados en la propia plataforma (CISA, 2020; UN, s. f.; Digital Future Society, 2020).
- Justicia algorítmica por diseño. Explicabilidad, evaluación ex ante/ex post de sesgo, derecho de apelación y documentación pública de modelos y datos de entrenamiento en la medida compatible con la seguridad (INCIBE, 2023; Universidad de Navarra, 2024).

### **Aplicación de la inteligencia ciudadana en México: de la seguridad pública a la seguridad nacional**

#### **Panorama y premisas para el caso mexicano**

En México, hablar de “inteligencia ciudadana” requiere distinguir niveles de competencia (seguridad pública, seguridad interior y seguridad nacional) y, a la vez, tender puentes entre ellos. La literatura y la experiencia comparada advierten que la participación cívica sólo produce inteligencia útil cuando se inserta en marcos de gobierno abierto, con reglas de datos claras, mecanismos de supervisión y evaluación basada en evidencia; de lo contrario, degenera en ruido, vigilancia informal o captura política (Godet, 2001; Inter-American Development Bank [IADB], 2018; United

Nations Development Programme [UNDP], 2021; United Nations Office on Drugs and Crime [UNODC], 2023).

En el plano normativo mexicano, la inteligencia —como conocimiento para decidir, producto de recolección, procesamiento y diseminación— tiene asidero legal, y la seguridad ciudadana cuenta con rutas de rendición de cuentas; el reto es operacionalizar esa arquitectura con salvaguardas de derechos y justicia algorítmica (Cámara de Diputados, s. f.; Georgetown University, s. f.; Infoem, s. f.; INCIBE, 2023).

### **Seguridad pública: proximidad digital con reglas de evidencia**

En seguridad pública (ámbito municipal y estatal), la inteligencia ciudadana puede ser el multiplicador de proximidad si se despliega con tres capas integradas:

1. **Arquitectura sociotécnica.** Integrar reportes geolocalizados de la ciudadanía (apps, botones de auxilio, líneas 9-1-1/0-8-9), C2/C4/C5 y fuentes “clásicas” (llamadas, videovigilancia) bajo un estándar mínimo de datos (qué, cuándo, dónde, cómo) y trazabilidad de cada reporte hasta su cierre; publicar métricas periódicas de tiempo de respuesta y acciones derivadas (RSD Journal, 2022; SINT, 2024; Infoem, s. f.).
2. **Evaluación y aprendizaje.** Pilotar intervenciones con grupos de control, medir desplazamiento del delito y efectos reales en victimización y percepción, no sólo output operativo; documentar y abrir resultados (IADB, 2018; IADB, s. f.; UNDP, 2021).
3. **Salvaguardas y confianza.** Minimización/anonimización por defecto, explicabilidad de reglas algorítmicas (XAI), auditorías de sesgo publicadas y derecho de apelación ante decisiones automatizadas (INCIBE, 2023; Universidad de Navarra, 2024).

Casos mexicanos como la “Mesa de Seguridad” en Ciudad Juárez muestran que la formalización de comisiones ciudadanas —incluida la de “inteligencia ciudadana”— puede canalizar información útil si existen canales de retroalimentación y

corresponsabilidad; sin ese ciclo, la participación se frustra o se vuelve simbólica (Casede, s. f.; UNAM, s. f.; ICAI, s. f.).

Además, la literatura sobre cooperación México–Estados Unidos subraya que, incluso a nivel local, la reducción de violencia exige coordinar con palancas federales (control de armas, financiamiento, cooperación operativa) y con políticas de prevención basadas en evidencia (Felbab-Brown, 2022; GAO, 2022; WOLA, 2022).

### **Seguridad interior: alerta temprana, control institucional y antifrágiles cívicos**

En seguridad interior (preservación del orden constitucional y la continuidad institucional), la inteligencia ciudadana no puede sustituir capacidades estatales, pero sí fortalecer tres funciones críticas:

1. Alerta temprana y monitoreo de riesgos. Plataformas cívicas con protocolos de verificación para detectar señales débiles de disrupción (extorsión organizada, bloqueos, sabotaje a infraestructura), integradas a centros estatales con reglas de escalamiento y protección de denunciantes (UNDP, 2021; UNODC, 2023).
2. Control y rendición diagonal. Mecanismos de reporte ciudadano sobre corrupción y abuso (contralorías sociales, comités con facultades de auditoría) con resultados verificables —no sólo buzones— para blindar a policías/ministerios públicos, donde la corrupción es variable “resultado” sensible y palanca de captura institucional (Infoem, s. f.; UNODC, 2023).
3. Resiliencia informativa. Módulos anti-desinformación embebidos (detección de astroturfing, verificación comunitaria, desmentidos oficiales rápidos) para evitar que campañas coordinadas manipulen la agenda de seguridad interior o saturen sistemas con reportes falsos (CISA, 2020; Digital Future Society, 2020; UN, s. f.).

Aplicado con prospectiva (Godet/MICMAC), esto exige tratar como “motoras” la voluntad política y la reforma institucional (procesos penales eficaces, gestión probatoria digital, estándares de datos), y como “bisagra” la coordinación interagencial;

corrupción y control territorial operan como termómetros del sistema, no como objetivos aislados (Godet, 2001; UNDP, 2021; UNODC, 2023).

### **Seguridad nacional: participación cívica con límites, OSINT estratégico y cooperación**

En seguridad nacional (soberanía, integridad territorial y amenazas transnacionales), la participación ciudadana debe moverse en un perímetro estrictamente regulado. Tres campos son viables y valiosos:

1. OSINT estratégico y cartografía social. Comunidades fronterizas, transportistas, cámaras empresariales y academia pueden contribuir con observación estructurada (no intrusiva) sobre cadenas logísticas, corredores de riesgo y fenómenos transfronterizos (fentanilo/precursores, tráfico de armas), bajo gobernanza de datos y canales seguros de diseminación a instancias federales (Rosen, 2021; GAO, 2022; UNODC, 2023).
2. Ciberseguridad y resiliencia crítica. Programas nacionales de “ciber-higiene” y reporte ciudadano de vulnerabilidades en servicios esenciales (agua, energía, salud), con estándares de divulgación responsable, coordinación CERT y rutas de mitigación; la participación aquí reduce asimetrías de información y acelera tiempos de respuesta (Universidad de Navarra, 2024; UNDP, 2021).
3. Ventanas de cooperación internacional. La evidencia muestra que palancas como control de armas en EE. UU., financiamiento condicional y confianza operativa determinan trayectorias; la sociedad civil puede producir insumos técnicos, veeduría y presión pública informada —sin invadir competencias operativas— para sostener la cooperación binacional (Felbab-Brown, 2022; WOLA, 2022; GAO, 2022).

Todo ello debe sujetarse a límites legales: la seguridad nacional no es un campo de “mano alzada” participativa; requiere filtros, clasificación, protección de fuentes, debida diligencia y control parlamentario/judicial ex post, así como lineamientos de derechos

humanos y privacidad (Cámara de Diputados, s. f.; Georgetown University, s. f.; INCIBE, 2023).

### **Gobernanza y prospectiva: hoja de ruta mínima por niveles**

- Seguridad pública (12–18 meses): estándar 3×3 de datos cívicos (qué, dónde, cuándo), tablero público con tiempos de respuesta y cierres, protocolo de verificación comunitaria, auditoría algorítmica semestral, pilotos con grupos de control y publicación de resultados (IADB, 2018; IADB, s. f.; Infoem, s. f.; INCIBE, 2023).
- Seguridad interior (18–24 meses): sistema de alerta temprana con escalamiento y protección de denunciantes; comité ciudadano con facultades de auditoría sobre integridad policial/ministerial; módulo anti-desinformación integrado a C4/C5 con métricas de precisión/recall y reportes trimestrales (CISA, 2020; Digital Future Society, 2020; UN, s. f.; UNDP, 2021).
- Seguridad nacional (24–36 meses): red OSINT civil de bajo riesgo (academia/empresas/comunidades) con protocolos de clasificación y compartición; programa de ciber-higiene y divulgación responsable para infraestructuras críticas; mesa técnica de sociedad civil para insumos de cooperación México–EE. UU. (Felbab-Brown, 2022; GAO, 2022; WOLA, 2022; Rosen, 2021; Universidad de Navarra, 2024).

### **Riesgos para mitigar desde el diseño**

Evitar el vigilantismo y la “vigilancia horizontal” punitiva; blindar privacidad y debidos procesos ante la expansión de biometría y reconocimiento facial; gestionar sesgos en datos de entrenamiento y reportes; y construir confianza con retroalimentación sistemática a la ciudadanía. La desinformación es un vector central: sin estrategias de detección y desmentido, los sistemas participativos se convierten en armas cognitivas contra sí mismos (Lechner, 2016; CISA, 2020; UN, s. f.; UNODC, 2023).

### **Metodología: marco, variables y herramientas**

## **Propósito y alcance**

El objetivo es modelar, con rigor operativo y salvaguardas éticas, la dinámica de seguridad México–Estados Unidos como un sistema complejo y adaptativo. Para ello se emplean dos instrumentos clásicos de prospectiva: la matriz de influencias cruzadas y el análisis MICMAC (Matriz de Impactos Cruzados Multiplicación Aplicada a una Clasificación), a fin de distinguir palancas de cambio (variables motoras), bisagras frágiles, resultados-termómetro y factores relativamente autónomos (Godet, 2001). La innovación metodológica consiste en incorporar de manera explícita la “inteligencia ciudadana organizada” como variable estructural, junto con una variable de “resiliencia informacional/anti-desinformación”, ambas con reglas de datos y de gobernanza (INCIBE, 2023; UN, s. f.).

## **Delimitación del sistema**

La frontera funcional del sistema binacional incluye: decisiones políticas en ambos países; flujos ilícitos (drogas, armas, dinero); capacidades institucionales (policiales, fiscales y judiciales); ecosistema informacional (medios, plataformas, campañas de desinformación); y control territorial/social en zonas de disputa. La literatura muestra que estas capas se acoplan y retroalimentan, de modo que pequeñas variaciones en una palanca —por ejemplo, cooperación bilateral o control de armas— alteran trayectorias de violencia y legitimidad (Felbab-Brown, 2022; GAO, 2022; UNODC, 2023; Rosen, 2021).

## **Fuentes y trazabilidad**

El modelo se alimenta de: a) diagnósticos y evaluaciones oficiales y académicas (GAO, 2022; UNODC, 2023; WOLA, 2022), b) marcos normativos mexicanos que definen inteligencia y niveles de seguridad (Cámara de Diputados, s. f.; Georgetown University, s. f.), c) evidencia de políticas basadas en evaluación contrafactual para seguridad ciudadana (IADB, 2018; IADB, s. f.), y d) lineamientos de gobernanza y riesgos algorítmicos (INCIBE, 2023; Universidad de Navarra, 2024). La definición legal de inteligencia (recolección, procesamiento, diseminación para decidir) sirve de ancla conceptual para integrar participación cívica

con valor de decisión y no meramente “denuncia” (de León M., 2024; Georgetown University, s. f.).

### **Selección de variables estratégicas**

Se emplean criterios de relevancia sistémica, multinivelidad, conexión con actores y potencial prospectivo (Godet, 2001). La base de trabajo retoma diez variables previamente estructuradas y añade dos nuevas para capturar la capa cívico-informacional:

- V1 Voluntad política de México
- V2 Voluntad política de EE. UU.
- V3 Financiamiento internacional para seguridad
- V4 Cooperación bilateral institucional (p. ej., DEA–FGR)
- V5 Corrupción en cuerpos de seguridad
- V6 Capacidad operativa de cárteles
- V7 Presión mediática y percepción pública
- V8 Reforma del sistema judicial mexicano
- V9 Regulación del tráfico de armas en EE. UU.
- V10 Control territorial y social en zonas rurales/urbanas disputadas
- V11 Inteligencia ciudadana organizada (gobierno abierto, trazabilidad, retroalimentación, XAI, auditorías de sesgo)
- V12 Resiliencia informacional y anti-desinformación (detección de astroturfing, verificación cruzada, desmentido rápido)

V11 y V12 materializan, con reglas, la incorporación de participación cívica y la defensa del ecosistema de información frente a manipulación coordinada (Digital Future Society, 2020; CISA, 2020; UN, s. f.; INCIBE, 2023).

### **Explicación ampliada de cada variable y su relevancia estratégica**

#### **V1. Voluntad política de México**

Esta variable captura la disposición sostenida del Poder Ejecutivo y de los gobiernos subnacionales para priorizar la seguridad basada en evidencia, soportar costos políticos de mediano plazo y blindar la política pública frente a ciclos electorales. Su centralidad radica

en que determina la continuidad de reformas, la asignación presupuestaria, la cooperación interagencial y la aceptación de controles externos (auditorías, indicadores, transparencia), todo lo cual afecta la trayectoria del sistema (Godet, 2001). En el caso mexicano, la experiencia acumulada indica que los cambios de administración reconfiguran prioridades, alteran la relación con socios internacionales y redefinen la mezcla entre prevención y contención (Felbab-Brown, 2022). Sin voluntad estable, el resto de las variables —incluidas la cooperación (V4), la reforma judicial (V8) y la capa cívico-informacional (V11, V12)— operan a media máquina. En términos prospectivos, V1 es “motora” porque empuja a otras, pero es sensible a shocks reputacionales (crisis de derechos humanos, escándalos de corrupción) y a coyunturas fiscales.

## **V2. Voluntad política de Estados Unidos**

En el lado estadounidense, la voluntad se traduce en prioridades de cooperación, intensidad del control de precursores químicos y fentanilo, trazabilidad de armas, intercambio de información y apoyo financiero/técnico (GAO, 2022; WOLA, 2022). Es una variable estructural por el peso económico, regulatorio y tecnológico de Estados Unidos y por su capacidad de condicionar agendas bilaterales (Rosen, 2021). Prospectivamente, V2 opera como palanca “motora” que puede habilitar ventanas de oportunidad (p. ej., acuerdos de datos o de marcaje de armas) o, por el contrario, generar fricción si prevalecen marcos punitivos no coordinados. Su interacción con V1 define el tono de la cooperación (V4) y el alineamiento de métricas.

## **V3. Financiamiento internacional para seguridad**

Abarca flujos programáticos (equipamiento, entrenamiento, prevención, desarrollo institucional) y su condicionalidad. No es meramente volumen; importa la calidad del diseño (enlace con reformas y con evaluación), su previsibilidad y la alineación con objetivos verificables (GAO, 2022; IADB, 2018). Es típicamente “autónoma” de segundo orden en el MICMAC: su impacto depende de V1/V2, de la cooperación (V4) y de la reforma (V8). En prospectiva, financiamiento mal anclado a resultados alimenta compras tecnológicas sin gobernanza (riesgo panóptico), mientras

que financiamiento ligado a evidencia y transparencia favorece V11/V12 y efectos sostenibles (UNDP, 2021).

#### **V4. Cooperación bilateral institucional (p. ej., DEA–FGR)**

Es la bisagra operacional del sistema: traduce voluntades (V1, V2) en procesos, protocolos y casos conjuntos. Incluye confianza, interoperabilidad de datos, arreglos de compartición (evidencia digital, balística, precursores), y reglas claras para operaciones (GAO, 2022; WOLA, 2022). Por diseño, “influye y depende”: sin V1/V2 coherentes, se fricciona; sin V8, no cristaliza en sentencias; sin V11/V12, se degrada por ruido informativo. En términos de anticipación, V4 es la palanca para pasar de reacciones tácticas a campañas basadas en inteligencia multifuente y métricas compartidas.

#### **V5. Corrupción en cuerpos de seguridad**

Funciona como un “resultado-termómetro” que, al elevarse, indica fallas en palancas motoras y en la coordinación. Erosiona capacidades, filtra información, genera selectividad ilegal y alimenta desconfianza social, lo que a su vez reduce la colaboración ciudadana (UNODC, 2023). Por su carácter adaptativo, la corrupción reacciona a incentivos: controles internos y externos efectivos, trazabilidad de procesos y protección a denunciantes la deprimen; impunidad y opacidad la amplifican. Prospectivamente, V5 responde con rezago a reformas y a V11 (mecanismos de reporte y verificación).

#### **V6. Capacidad operativa de cárteles**

Condensa logística, finanzas ilícitas, innovación criminal (p. ej., uso de drones), control territorial y capital social coercitivo. Es sensible a V9 (flujo de armas), a V4 (operaciones conjuntas), a V8 (eficacia judicial) y, de forma indirecta, a V11 (alertas tempranas comunitarias que reducen ventanas de impunidad) (Felbab-Brown, 2022; UNODC, 2023). En prospectiva, V6 es “resultado” de alto impacto: si no se reducen sus capacidades adaptativas, los efectos de corto plazo se diluyen por sustitución o desplazamiento.

#### **V7. Presión mediática y percepción pública**

No es sólo “imagen”: afecta legitimidad, ventanas políticas y continuidad de políticas. Narrativas de pánico o polarización pueden empujar soluciones punitivas y desfinanciar la prevención; narrativas informadas y datos abiertos fortalecen la aceptación social de reformas difíciles (UNDP, 2021). V7 interactúa fuertemente con V12 (desinformación) y con V11 (retroalimentación a la ciudadanía). Prospectivamente, cambios en V7 pueden preceder rupturas de trayectoria (apoyo/boicot a reformas, cooperación o militarización).

### **V8. Reforma del sistema judicial mexicano**

Incluye capacidad investigativa, gestión probatoria digital, tiempos procesales, debida diligencia y estándares de calidad de evidencia. Sin V8, capturas operativas no se traducen en sentencias; con V8, se reduce impunidad y se crean efectos disuasorios (SSPC, 2023). V8 es “motora” porque afecta la credibilidad del Estado y realimenta V7; también es habilitadora de V11 (p. ej., uso de evidencia originada en canales cívicos con cadena de custodia) y demanda salvaguardas de XAI cuando median algoritmos (INCIBE, 2023; Universidad de Navarra, 2024).

### **V9. Regulación del tráfico de armas en EE. UU.**

Abarca enforcement de *straw purchasing*, controles a distribuidores, marcaje/trazabilidad y cooperación ATF-México. Su efecto directo sobre letalidad es claro, aunque su traducción operativa depende de V4 y de ventanas políticas (Rosen, 2021; GAO, 2022). En el MICMAC, V9 suele aparecer como “autónoma” con impactos indirectos fuertes vía V6 y V10. Prospectivamente, avances granulares (marcaje, intercambio de balística) pueden generar ganancias no lineales en desarticulación.

### **V10. Control territorial y social en zonas rurales/urbanas disputadas**

Es un indicador compuesto de presencia estatal efectiva (servicios, justicia, policía), aceptación social y capacidad para impedir la gobernanza criminal. Es altamente dependiente: mejora cuando operan V1, V4, V8 y V11, y se degrada con V5 y V6 (UNODC, 2023). En prospectiva, es un “resultado-termómetro” que

confirma si las palancas están alineadas; avances puntuales pueden revertirse si no hay continuidad y servicios públicos.

### **V11. Inteligencia ciudadana organizada (gobierno abierto, trazabilidad, retroalimentación, XAI, auditorías de sesgo)**

Formaliza la participación cívica con reglas: estándares mínimos de datos (qué-dónde-cuándo-cómo), trazabilidad de reportes hasta su cierre, retroalimentación a la comunidad y auditoría de cualquier clasificación algorítmica (INCIBE, 2023; IADB, 2018). Su valor no es el volumen de reportes sino su inserción en procesos de decisión y evaluación. Empuja coordinación (V4), mejora calidad probatoria (V8), eleva legitimidad (V7) y puede deprimir corrupción (V5) al crear circuitos de control social institucionalizado (UNDP, 2021).

### **V12. Resiliencia informacional y anti-desinformación (detección de astroturfing, verificación cruzada, desmentido rápido)**

Actúa como “cortafuegos” del ecosistema informacional. Sin V12, plataformas cívicas son manipulables (bots, inundación de reportes falsos, deepfakes), lo que rompe confianza, satura capacidades y distorsiona prioridades (CISA, 2020; Digital Future Society, 2020; UN, s. f.). Con V12, se preserva la señal de V11 y se blindan V4 y V7. Prospectivamente, V12 estabiliza el sistema y reduce la probabilidad de trayectorias críticas derivadas de choques cognitivos.

### **Construcción de la matriz de influencias directas (MID)**

Cada par ordenado ( $V_i \rightarrow V_j$ ) se valora en escala ordinal 0–3: 0 = sin influencia directa; 1 = débil/condicionada; 2 = moderada/sostenida; 3 = fuerte/estructural. La matriz es direccional (no necesariamente simétrica) y se codifica a partir de revisión de literatura y talleres de juicio experto, documentando la justificación de cada enlace (Godet, 2001; Felbab-Brown, 2022; GAO, 2022; UNODC, 2023). Para evitar sobre-ajuste, se prohíben valores fraccionales y se impone parsimonia: una relación debe sustentarse en evidencia empírica o causalidad plausible.

## **Consistencia, normalización y confiabilidad**

Se aplican tres salvaguardas:

1. Triangulación de codificación: al menos dos analistas asignan puntajes de manera independiente y se resuelven discrepancias registrando razones y fuentes.
2. Normalización por fila (opcional): para comparar perfiles de influencia entre variables con distinta conectividad.
3. Pruebas de sensibilidad  $\pm 1$ : se perturban selectivamente los enlaces más inciertos (p. ej., V9→V6; V11→V4; V12→V7) para verificar la robustez de la clasificación final.

## **Del MID al MICMAC (influencia y dependencia directas/indirectas)**

El análisis MICMAC suma por filas (influencia) y por columnas (dependencia) y, crucialmente, evalúa impactos indirectos a través de multiplicación matricial ( $MID^2$ ,  $MID^3$ , ...) hasta estabilizar el grafo de influencias de orden superior (Godet, 2001). Este paso revela “efectos sombra”: relaciones débiles directas que, por cadenas de transmisión, se vuelven estratégicas (p. ej., V9 puede incidir más en V10 a través de V6 que por un enlace directo).

## **Clasificación en cuadrantes**

Se ubican las variables en cuatro cuadrantes:

- Motoras (alta influencia, baja dependencia): típico de V1, V2, V8 y —según resultados— V11.
- Bisagra (alta influencia y alta dependencia): cooperación V4 suele caer aquí.
- Resultado (baja influencia, alta dependencia): V5, V6, V7, V10 como termómetros del sistema.
- Autónomas (baja influencia y baja dependencia o de segundo orden): V3 y, a veces, V9, cuyo efecto depende de ventanas políticas (Rosen, 2021; GAO, 2022).

## **Integración de inteligencia ciudadana (V11) y resiliencia informacional (V12)**

V11 se operacionaliza con cuatro componentes: estándar de datos (qué-dónde-cuándo-cómo), trazabilidad de reportes hasta su cierre, retroalimentación pública y auditoría algorítmica (XAI) para cualquier clasificación automatizada (INCIBE, 2023; IADB, 2018). El valor sistémico de V11 no es el volumen de reportes, sino su efecto sobre coordinación, legitimidad y reducción de tiempos de respuesta (UNDP, 2021).

V12 incorpora un “cortafuegos” frente a la manipulación: detección de comportamiento no auténtico, verificación comunitaria, *fact-checking* y desmentidos oficiales integrados al mismo flujo, con métricas de precisión/recuperación y tiempos de neutralización (CISA, 2020; Digital Future Society, 2020; UN, s. f.). Sin V12, la capa cívica puede degradarse en ruido o vigilatismo (Lechner, 2016).

## **Diseño de escenarios**

Con la estructura MICMAC se formulan narrativas consistentes a 2025–2030. La práctica es escoger dos ejes de incertidumbre de alto voltaje (p. ej., “voluntad política binacional sostenida” y “calidad del ecosistema informacional”) y proyectar tres-cuatro escenarios plausibles, verificando coherencia interna y trayectorias de transición (Godet, 2001). Cada escenario incluye:

- Supuestos y activación/desactivación de variables clave.
- Implicaciones tácticas y estratégicas.
- Palancas de intervención.
- Señales tempranas (signposts) e indicadores verificables.

## **Indicadores y señales de alerta temprana**

### **Cooperación (V4)**

- *Tiempo medio de triage-a-acción en nodos fronterizos.* Define la latencia entre recepción de información accionable (p. ej., reporte verificado, match balístico, alerta de precursores) y la primera intervención coordinada. Latencias bajas indican interoperabilidad y confianza; alzas sostenidas,

cuellos de botella, fricción política o saturación operativa (GAO, 2022).

- *Porcentaje de casos conjuntos.* Mide la proporción de investigaciones y operativos con participación binacional efectiva respecto del total de casos relevantes. Importa la calidad (resultados judiciales) más que el simple conteo (WOLA, 2022).
- *Acuerdos de datos operables.* No sólo memorandos; indicadores de uso real: número de consultas cruzadas, matched hits balísticos/forenses, y auditorías de cumplimiento de protocolos de protección de datos. Señales tempranas positivas: curvas de aprendizaje estables, reducción de falsos positivos; negativas: brechas de auditoría, caídas en consultas o *timeouts* (GAO, 2022).

### Reforma (V8)

- *Tasa de judicialización con evidencia digital trazable.* Relación entre investigaciones con evidencia digital (videovigilancia, reportes cívicos, análisis forense) que llegan a imputación/sentencia y las iniciadas. Aumentos sugieren mejoras en cadena de custodia y pericia; caídas pueden denotar litigiosidad por mala obtención de evidencia.
- *Cumplimiento de estándares XAI.* Porcentaje de modelos algorítmicos (clasificadores de riesgo, priorización de denuncias) con documentación pública (propósitos, datos de entrenamiento, pruebas de sesgo) y mecanismos de explicación humana comprensible (INCIBE, 2023; Universidad de Navarra, 2024).
- *Número de apelaciones resueltas por decisiones algorítmicas.* Un canal de impugnación saludable debe existir y resolverse con tiempos razonables; picos no explicados pueden indicar sesgo o mala comunicación de criterios.

### Capa cívica (V11)

- *Porcentaje de reportes cerrados con retroalimentación  $\leq 72$  h.* Es la métrica que sostiene la confianza: cuando la ciudadanía recibe una respuesta útil (acción, orientación o cierre con razón), la participación es sostenible; cuando no, cae por fatiga.

- *Densidad de participación por 10 000 habitantes.* Desagregada por territorio y tipología de incidente; permite detectar brechas de acceso/uso (brecha digital, miedo a denunciar).
- *Mejora de tiempos de respuesta.* Diferencia de tiempos de arribo y resolución en zonas con alta participación organizada vs. controles; si no hay mejoras, V11 puede estar siendo simbólica (IADB, 2018; UNDP, 2021).

## Resiliencia (V12)

- *Detección de campañas coordinadas.* Conteo y frecuencia de patrones no auténticos (picos sincronizados, redes de bots, duplicados) en ventanas críticas.
- *Precision/recall de filtros anti-desinformación.* Evaluación periódica con conjuntos de validación: demasiada agresividad (alta *precision*, baja *recall*) invisibiliza señales genuinas; lo contrario inunda de ruido (CISA, 2020).
- *Tiempo de desmentido  $\leq 24$  h.* La latencia de desmentidos oficiales verificables es clave para evitar cristalización de narrativas falsas (UN, s. f.).

## Armas (V9)

- *Trazabilidad y decomisos vinculados a straw purchasing.* Porcentaje de armas decomisadas con ruta reconstruida a compras simuladas; alzas temporales pueden reflejar enforcement efectivo, pero descensos sostenidos junto con caídas en eventos violentos indicarían efecto disuasorio (Rosen, 2021).
- *Cooperación ATF–México con intercambio de balística.* Número de *hits* balísticos compartidos, tiempos de respuesta y casos derivados; es un indicador de la salud técnica de la cooperación.

## Resultados-termómetro (V5, V6, V10)

- *Índices de corrupción percibida/denunciada en seguridad.* Complementar encuestas y canales de denuncia con verificación y seguimiento; la correlación con V11 ayuda a separar “más denuncia” de “más corrupción”.

- *Shocks de letalidad*. Identificar cambios de régimen (picos regionales) y si coinciden con fallas de cooperación (V4) o ataques informacionales (V12).
- *Variación en control territorial*. Indicadores compuestos (servicios públicos, presencia judicial, denuncias, extorsión) para medir avances/retrocesos sostenidos (UNODC, 2023).

### **Validación y evaluación ex post**

Para no confundir actividad con impacto, las intervenciones deben pilotarse con métodos robustos:

- *Diseño experimental o cuasi-experimental*. Asignación aleatoria de sectores a tratamiento (p. ej., despliegue de plataforma cívica con verificación) y control, o bien diferencias-en-diferencias/sintético para estimar efectos netos (IADB, 2018; IADB, s. f.).
- *Medición de desplazamiento y difusión de beneficios*. Cartografiar si la reducción de incidentes en la zona tratada se acompaña de aumentos en colindancias (desplazamiento) o de mejoras circundantes (difusión).
- *Publicación de protocolos y datos*. Transparencia metodológica y bases (anonimizadas) para escrutinio público sostienen legitimidad y aprendizaje (UNDP, 2021).
- *Análisis de costo-efectividad*. Comparar costo por delito evitado o por minuto de respuesta ahorrado frente a alternativas (equipamiento, patrullaje adicional).

### **Ética, derechos y límites legales**

Cualquier capa cívica debe alinearse con marcos de seguridad pública/interior/nacional y con derechos fundamentales:

- *Minimización y anonimización*. Capturar sólo lo necesario, proteger identidades por defecto y definir ventanas de retención estrictas (INCIBE, 2023).
- *Controles de acceso y clasificación proporcional*. Separar dominios (operativo, analítico, rendición de cuentas), registrar accesos y aplicar clasificación ajustada al riesgo.
- *Control parlamentario/judicial ex post en niveles sensibles*. Garantiza que la seguridad nacional y la cooperación

internacional no evadan el escrutinio democrático (Cámara de Diputados, s. f.; Georgetown University, s. f.).

- *Justicia algorítmica*. Documentación de modelos, pruebas y mitigación de sesgo, explicabilidad (XAI) y vías de impugnación accesibles (Universidad de Navarra, 2024).

### **Limitaciones y manejo de incertidumbre**

La matriz y el MICMAC son fotografías estructurales. Pueden omitir shocks exógenos (innovaciones criminales, cambios regulatorios súbitos, eventos geopolíticos) y derivar en falsas certezas si no se actualizan (Godet, 2001). Por ello:

- *Revisión trimestral/semestral de codificación y supuestos*. Ajustar enlaces inciertos (p. ej., V9→V6; V11→V4; V12→V7) con nueva evidencia.
- *Vigilancia de señales débiles*. Indicadores exploratorios (nuevas rutas logísticas, patrones de bots, mutación de MO criminal) que anticipen quiebres.
- *Escenarios adaptativos*. Mantener narrativas alternativas y “puntos de no retorno” para decidir pivotes oportunos (UNDP, 2021).

### **Prospectiva binacional con capa de inteligencia ciudadana**

#### **Relectura estructural con V11–V12**

Dos hallazgos: (i) V11 tiende a comportarse como motora-bisagra: empuja coordinación (V4), eleva calidad probatoria (V8) y legítima políticas (V7), reduciendo dependencia de “operativos ciegos”; (ii) V12 estabiliza el ecosistema: sin resiliencia informacional, la desinformación erosiona confianza, satura capacidades y degrada resultados-termómetro (V5, V6, V10) (Digital Future Society, 2020; CISA, 2020; UN, s. f.).

#### **Escenario 1. Alianza estratégica efectiva 2.0 (deseable y plausible)**

*Supuestos*. V1 y V2 sostenidas; V4 profesionalizada; V8 priorizada; V11 operativo en corredores críticos (OSINT —open-source intelligence— cívico de bajo riesgo, tableros de

retroalimentación, auditorías XAI semestrales); V12 activo.

*Efectos.* Caída de V5 por presión de integridad; V6 pierde adaptabilidad logística; V10 mejora en nodos; V7 se recupera (Felbab-Brown, 2022; GAO, 2022; WOLA, 2022).

*Señales.* Acuerdos ATF-México sobre marcaje y trazabilidad; KPI de cierre de reportes cívicos > 70 % en 72 h; publicación periódica de auditorías de sesgo (Rosen, 2021; IADB, 2018; INCIBE, 2023).

*Riesgos y mitigación.* Captura política de tableros; se mitiga con gobernanza multiactor, auditorías externas y apelación pública de decisiones algorítmicas (Universidad de Navarra, 2024).

## **Escenario 2. Estancamiento controlado con ciudadanía instrumental (tendencial)**

*Supuestos.* V1–V2 intermitentes; V4 por inercia; V8 avanza lento; V11 fragmentaria; V12 reactiva.

*Efectos.* Violencia estable sin mejoras; “islas” de control territorial; legitimidad oscilante (UNDP, 2021; UNODC, 2023).

*Señales.* Tableros de actividad, no de impacto; bajos cierres; pilotos sin evaluación contrafactual (IADB, 2018).

## **Escenario 3. Regresión criminal con ruido cívico (crítico)**

*Supuestos.* V1–V2 colapsan; V4 se rompe; V8 se bloquea; V11 deriva en vigilancia horizontal/doxing; V12 falla.

*Efectos.* V5–V6 dominan; V10 retrocede; el ecosistema informacional se arma contra Estado y sociedad (Lechner, 2016; CISA, 2020; UN, s. f.).

*Señales.* Inundación de reportes falsos, “listas negras” comunitarias, filtraciones masivas, alzas de falsos positivos.

### **Palancas y métricas binacionales verificables**

- *Cooperación (V4) apalancada por V11.* Tiempo triage-acción transfronterizo; % de actuaciones conjuntas originadas en reportes cívicos verificados; acuerdos operativos de datos (GAO, 2022; WOLA, 2022).
- *Reforma (V8) y legitimidad.* Tasa de judicialización con evidencia digital trazable; decisiones explicables (XAI) publicadas y tasa de apelaciones resueltas (INCIBE, 2023; Universidad de Navarra, 2024).
- *Armas (V9).* Decomisos vinculados a *straw purchasing* y trazabilidad balística; cooperación ATF-México (Rosen, 2021).
- *Capa cívica (V11).* Cierre  $\leq 72$  h; densidad de participación y “brecha de sesgo” por territorio; percepción informada (IADB, 2018; UNDP, 2021).
- *Resiliencia (V12).* Precisión/recuperación de filtros y tiempo de desmentido  $\leq 24$  h (CISA, 2020; UN, s. f.).

### **Conclusiones generales**

La inteligencia ciudadana madura cuando se la entiende como política de Estado —no como aplicación móvil— y cuando se la conjuga con prospectiva estratégica para anticipar, priorizar y coordinar. La literatura internacional y regional converge: sin voluntad política sostenida, reglas de gobierno abierto, evaluación rigurosa y salvaguardas de derechos, la promesa de colaboración deviene vigilancia o ruido.

Con esas condiciones, en cambio, la inteligencia ciudadana aporta legitimidad, capilaridad y aprendizaje colectivo, y la prospectiva traduce esa energía cívica en decisiones informadas sobre palancas de cambio y escenarios de largo aliento. En los siguientes pasos aplicaremos este marco a un caso nacional y, finalmente, a una relación bilateral compleja, mostrando cómo las palancas y riesgos aquí identificados se concretan en agendas de acción verificables.

México necesita pasar de la participación simbólica a la co-producción responsable de inteligencia, enlazada con prospectiva para priorizar palancas y anticipar trayectorias. Esto no es una “app”, sino una política de Estado que combina voluntad política, reglas de datos, evaluación rigurosa y cooperación multinivel; la ciudadanía aporta capilaridad, legitimidad y aprendizaje colectivo si —y sólo si— el Estado abre el ciclo con transparencia y rendición de cuentas.

Por su parte, la matriz y el MICMAC permiten pasar de indicadores de resultado a palancas de transformación. Con V11–V12 formalizados, la ciudadanía deja de ser “ruido” y se convierte en fuente legítima de anticipación; la cooperación binacional gana capilaridad y control de sesgos; y la arquitectura informacional se blindada frente a manipulación. El costo: voluntad política sostenida, reforma institucional y transparencia radical. La alternativa — participación simbólica o ruido punitivo— perpetúa trayectorias de estancamiento o regresión.

## REFERENCIAS BIBLIOGRÁFICAS

- Alcaldía de Neiva. (2020). *Modelo de madurez de ciudades y territorios inteligentes*.  
<https://www.alcaldianeiva.gov.co/NuestraAlcaldia/Dependencias/Documents/Informe%20Final%20Modelo%20de%20Madurez%20de%20Ciudadades%20y%20Territorios%20Inteligentes%20-%20Mpio%20de%20Neiva%202020.pdf>
- Cámara de Diputados. (s. f.). *Seguridad y participación ciudadana*.  
<https://portalhcd.diputados.gob.mx/PortalWeb/Micrositios/21ffc78e-f82b-4320-9faa-14580835e0e7.pdf>
- Casede. (s. f.). *Seguridad* [dossier].  
[https://casede.org/BibliotecaCasede/Novedades-PDF/Seguridad\\_GENARO\\_GARCIA\\_LUNA.pdf](https://casede.org/BibliotecaCasede/Novedades-PDF/Seguridad_GENARO_GARCIA_LUNA.pdf)
- CIPPEC. (2017). *Ciudad inteligente*. <https://www.cippec.org/wp-content/uploads/2017/03/985.pdf>
- CISA. (2020). *Tácticas de desinformación*.  
[https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation-spanish\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation-spanish_508.pdf)
- De León Mondragón, Rodrigo. (2024, noviembre 20). Inteligencia, la eficacia de la prevención. *Revista Guinda*.  
<https://revistaguinda.com/opinion/inteligencia-la-eficacia-de-la-prevencion/>
- Digital Future Society. (2020). *Cómo combatir la desinformación: Estrategias de empoderamiento de la ciudadanía digital*.

- <https://digitalfuturesociety.com/app/uploads/2020/10/Como-combatir-la-desinformaci%C3%B3n-Estrategias-empoderamiento-de-la-ciudadania-digital.pdf>
- Felbab-Brown, V. (2022, June 15). Mexico's war on organized crime: Strategic dilemmas and policy failures. *Brookings Institution*. <https://www.brookings.edu/articles/mexicos-security-dilemmas/>
- GAO. (2022). *Drug control: Cooperative efforts to stem flow of illicit drugs* (GAO-22-105961). U.S. Government Accountability Office. <https://www.gao.gov/products/gao-22-105961>
- Georgetown University. (s. f.). *Hacia la Ley de Seguridad Nacional* [Political Database of the Americas]. <https://pdba.georgetown.edu/Security/citizenssecurity/mexico/evaluaciones/LeySeguridadNacional.pdf>
- Godet, M. (2001). *Creating futures: Scenario planning as a strategic management tool* (2nd ed.). Economica.
- IADB. (2018). *La eficacia de las políticas públicas de seguridad ciudadana en América Latina y el Caribe: Cómo medirla y cómo mejorarla*. <https://publications.iadb.org/publications/spanish/document/La-eficacia-de-las-pol%C3%ADticas-p%C3%BAblicas-de-seguridad-ciudadana-en-Am%C3%A9rica-Latina-y-el-Caribe-Como-medirla-y-como-mejorarla.pdf>
- IADB. (s. f.). *Desarrollo y evaluación de programas de seguridad ciudadana en América Latina: Protocolo para la prevención del delito a partir de la evidencia*. <https://publications.iadb.org/publications/spanish/document/Desarrollo-y-evaluaci%C3%B3n-de-programas-de-seguridad-ciudadana-en-Am%C3%A9rica-Latina-Protocolo-para-la-prevenci%C3%B3n-del-delito-a-partir-de-la-evidencia.pdf>
- ICAI. (s. f.). *Modelos de implementación del gobierno abierto en México*. <https://icai.org.mx/images/Gobierno%20Abierto/Biblioteca/EN%20MEXICO/modelos.pdf>
- IIEPADES. (2025, abril). *Inteligencia policial*. <https://iepades.org/wp-content/uploads/2025/04/INTELIGENCIA-POLICIAL-FINAL.pdf>
- INCIBE. (2023). *Inteligencia artificial: Qué es, ventajas y riesgos*. <https://www.incibe.es/ciudadania/blog/inteligencia-artificial-ia-que-es-ventajas-y-riesgos>
- Infoem. (s. f.). *Rendición de cuentas: ABC*. [https://www.infoem.org.mx/doc/publicaciones/ABC\\_rendicionCuentas.pdf](https://www.infoem.org.mx/doc/publicaciones/ABC_rendicionCuentas.pdf)
- Lechner, A. (2016). *Tecnologías aplicadas a la seguridad ciudadana: Desafíos para la justicia transicional ante nuevos mecanismos de control*. Universidad Nacional de Quilmes. [https://ridaa.unq.edu.ar/bitstream/handle/20.500.11807/264/D1\\_A6\\_lechner\\_2016.pdf](https://ridaa.unq.edu.ar/bitstream/handle/20.500.11807/264/D1_A6_lechner_2016.pdf)

- Rosen, J. D. (2021). Arms trafficking to Mexico: A challenge for U.S. domestic gun policy. *Journal of International Affairs*, 74(2), 101–118.
- RSD Journal. (2022). *TIC's como herramientas contra la inseguridad en las ciudades*.  
<https://rsdjournal.org/rsd/article/download/23361/20270>
- SINT. (2024). *Mejorando la seguridad ciudadana con inteligencia artificial*.  
<https://sint.es/mejorando-la-seguridad-ciudadana-con-inteligencia-artificial/>
- UN. (s. f.). *Countering disinformation*. <https://www.un.org/es/countering-disinformation>
- UNAM. (s. f.). *Modelos de implementación del gobierno abierto en México*.  
<https://archivos.juridicas.unam.mx/www/bjv/libros/9/4016/9.pdf>
- UNDP. (2021). *Análisis sobre innovación en seguridad ciudadana y derechos humanos en América Latina y el Caribe*.  
<https://files.acquia.undp.org/public/migration/latinamerica/undp-rblac-es-Analisis-innovacion-seguridad-ciudadana-derechos-humanos-VF.pdf>
- Universidad de Navarra. (2024). *El reto de la inteligencia artificial para la seguridad y defensa*. <https://www.unav.edu/web/global-affairs/el-reto-de-la-inteligencia-artificial-para-la-seguridad-y-defensa>
- UNODC. (2023). *Global report on organized crime 2023*.  
<https://www.unodc.org/unodc/en/organized-crime/index.html>
- Washington Office on Latin America. (2022). *Beyond the war on drugs: U.S.–Mexico cooperation on security*.  
<https://www.wola.org/analysis/us-mexico-security-cooperation/>
- WOLA. (2022). *Beyond the war on drugs: U.S.–Mexico cooperation on security*.  
<https://www.wola.org/analysis/us-mexico-security-cooperation/>



Número 3  
(ENERO-JUNIO 2025)

**“NUEVO GLOSARIO Y PARADIGMAS DE LA DEFENSA Y  
SEGURIDAD: NORLATINISMO, INTELIGENCIA CIUDADANA Y  
NORMATIVIDAD EMERGENTE”**