Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2026,
Volumen 10, Número 2.

https://doi.org/10.37811/cl_rcm.v10i2

LA CIBERSEGURIDAD EN LA PLANEACIÓN NACIONAL DE MÉXICO (2001–2024): JERARQUÍA ESTRATÉGICA Y CONFIGURACIÓN COMO PROBLEMA PÚBLICO

CYBERSECURITY IN MEXICO'S NATIONAL PLANNING (2001–2024): STRATEGIC HIERARCHY AND CONFIGURATION AS A PUBLIC PROBLEM

Norma María Martínez-López
Universidad de la Sierra Sur

Edú Ortega-Ibarra
Universidad de la Sierra Sur

Daniel Robles Torres
Universidad de la Sierra Sur

Christian Cruz Meléndez
Universidad de la Sierra Sur

DOI: https://doi.org/10.37811/cl_rcm.v10i2.23538

La ciberseguridad en la planeación nacional de México (2001–2024): jerarquía estratégica y configuración como problema público

Norma María Martínez-López[1]
normamacademico@gmail.com
https://orcid.org/0000-0002-8945-4759
Universidad de la Sierra Sur
México

Edú Ortega-Ibarra
eoi.unsis.edu.mx@gmail.com
https://orcid.org/0000-0002-6504-7366
Universidad de la Sierra Sur
México

Daniel Robles Torres
danielcanek@gmail.com
https://orcid.org/0000-0002-9641-3971
Universidad de la Sierra Sur
México

Christian Cruz Meléndez
cacruzme@secihti.mx
https://orcid.org/0000-0002-6105-9167
Universidad de la Sierra Sur
México

RESUMEN

El artículo tiene como objetivo analizar la incorporación de la ciberseguridad en la planeación nacional mexicana a partir de los Planes Nacionales de Desarrollo 2001–2024, con el fin de examinar su jerarquía como problema público. Para ello, se emplea un enfoque cualitativo de tipo documental basado en la técnica de análisis de contenido de los objetivos, estrategias y enfoques vinculados con la ciberseguridad en los distintos sexenios. Los resultados muestran la ausencia de objetivos autónomos de ciberseguridad y el predominio de referencias indirectas subordinadas a marcos de modernización administrativa, seguridad pública, seguridad nacional y seguridad interior. Asimismo, se observa una incorporación discontinua y funcional del tema, sin consolidarse como un campo estratégico de política pública. En general, estos hallazgos indican que la planeación nacional mexicana ha reconocido parcialmente la ciberseguridad, pero no la ha jerarquizado de manera suficiente, lo que evidencia limitaciones estructurales para su integración como prioridad en la acción del Estado.

Palabras clave: ciberseguridad; planeación nacional; políticas públicas; agenda gubernamental, jerarquía de problemas públicos

[1] Autor principal.
Correspondencia: normamacademico@gmail.com

Cybersecurity in Mexico's National Planning (2001–2024): Strategic Hierarchy and Configuration as a Public Problem

ABSTRACT

This article aims to analyze the incorporation of cybersecurity into Mexico's national planning through the National Development Plans from 2001 to 2024, in order to examine its hierarchy as a public problem. A qualitative documentary approach is employed, based on content analysis of the objectives, strategies, and thematic orientations related to cybersecurity across different presidential administrations. The findings reveal the absence of autonomous cybersecurity objectives and the predominance of indirect references subordinated to traditional frameworks such as administrative modernization, public security, national security, and internal security. Furthermore, the results indicate a discontinuous and functional incorporation of cybersecurity, without consolidation as a strategic field of public policy. Overall, the study shows that while cybersecurity has been partially recognized within national planning, it has not been sufficiently prioritized, highlighting structural limitations for its integration as a core component of state action.

***Keywords*:** cybersecurity; national planning; public policy; Government agenda; Public problem hierarchy

Artículo recibido 02 febrero 2026
Aceptado para publicación: 27 febrero 2026

INTRODUCCIÓN

Desde la expansión de Internet en la década de 1990, el entorno digital ha transformado de manera profunda la organización social, económica y política de los Estados, al tiempo que ha generado nuevas vulnerabilidades asociadas a la interconectividad global. En este contexto, la ciberseguridad ha emergido progresivamente como un campo de atención gubernamental, especialmente tras eventos que evidenciaron el carácter disruptivo de las amenazas cibernéticas, como las operaciones en el ciberespacio vinculadas al conflicto de Kosovo en 1999 y los ataques contra Estonia en 2007 (Wiedemar, 2023; Abad, 2020; McGuinness, 2007). A partir de entonces, diversos países comenzaron a desarrollar estrategias orientadas a proteger infraestructuras críticas, sistemas de información y capacidades estatales frente a riesgos digitales crecientes.

Sin embargo, el reconocimiento de la ciberseguridad como un problema relevante no implica necesariamente su consolidación como prioridad estratégica dentro de la acción estatal. En América Latina y el Caribe, aunque organismos como la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo han impulsado el fortalecimiento de capacidades en esta materia, persisten rezagos en su incorporación integral a las políticas públicas, particularmente en los instrumentos de planeación nacional, donde suelen privilegiarse los beneficios de la digitalización por encima de sus riesgos asociados (BID & OEA, 2016). Esto adquiere especial relevancia en un contexto en el que la creciente dependencia de infraestructuras y servicios digitales incrementa la exposición a riesgos con implicaciones para la seguridad, la economía y la gobernabilidad.

En México, los Planes Nacionales de Desarrollo (PND) constituyen el principal instrumento rector de la acción gubernamental, al establecer objetivos, estrategias y prioridades del desarrollo (Cámara de Diputados del H. Congreso de la Unión, 2024). Por ello, su análisis permite examinar no solo la inclusión de determinados temas, sino también el lugar que ocupan dentro del sistema de prioridades del Estado. No obstante, los estudios sobre ciberseguridad en México se han concentrado sobre todo en aspectos normativos o técnicos, dejando relativamente inexplorada su posición dentro de la planeación nacional. En particular, persiste un vacío respecto a cómo ha sido incorporada en los PND y qué revela esta incorporación sobre su jerarquía como problema público. En esta línea, diversos estudios han abordado la ciberseguridad en México desde enfoques normativos o técnicos, señalando problemas en la

consolidación de una política de ciberseguridad con visión estratégica y articulación suficiente frente a sus socios regionales (Aguilar Antonio, 2024; Piña Libién, 2019; Aguilar Antonio, 2020). No obstante, estos análisis han prestado menor atención a su posición dentro de la planeación nacional, lo que refuerza la pertinencia de examinar su ubicación dentro de los Planes Nacionales de Desarrollo.

A partir de este vacío, el artículo busca responder qué revela la incorporación de la ciberseguridad en los Planes Nacionales de Desarrollo de México entre 2001 y 2024 sobre su jerarquía como problema público dentro de la planeación nacional. Para abordar este problema, el estudio propone un modelo analítico de jerarquización de problemas públicos, articulado en tres dimensiones de la acción estatal: agenda gubernamental, planeación nacional y política pública. Este enfoque se sustenta en la literatura sobre agenda gubernamental, planeación y políticas públicas, particularmente en los aportes de Aguilar Villanueva (1993), Matus (1987), Parsons (2007), Isuani (2012) y, Mballa y González López (2017), que permiten analizar el proceso mediante el cual los problemas públicos son reconocidos, jerarquizados e instrumentados por el Estado. Por otra parte, este modelo se operacionaliza mediante el análisis de tres dimensiones empíricas: la proporción de referencias vinculadas con la ciberseguridad, su ubicación temática dentro de la planeación nacional y el enfoque con el que fueron formuladas.

Con base en ello, se emplea un enfoque cualitativo mediante análisis de contenido deductivo de los objetivos y estrategias contenidos en los PND correspondientes a los sexenios de Vicente Fox, Felipe Calderón, Enrique Peña Nieto y Andrés Manuel López Obrador. En este sentido, el artículo contribuye al campo de estudio al introducir una perspectiva analítica centrada en la jerarquía estratégica de los problemas públicos, aplicable no solo al caso de la ciberseguridad, sino también al análisis de otros temas emergentes en la agenda gubernamental.

MARCO TEÓRICO

Problemas públicos y construcción de agenda gubernamental

Las necesidades sociales surgen cuando un conjunto de carencias y demandas deja de ser una experiencia aislada y comienza a afectar de manera compartida a una población; en ese momento, puede transformarse en un problema público si actores con capacidad de influencia, dentro o fuera del Estado, lo reconocen como asunto que requiere intervención gubernamental (Mballa & González López, 2017; Olavarría Gambi, 2007: Sandoval Escalante, 2023). En este proceso, no basta con que exista una

afectación al bienestar social, a la armonía colectiva o al entorno, sino que también intervienen juicios éticos, conocimiento especializado y relaciones de poder que contribuyen a visibilizar el problema. Por ello, la conversión de una necesidad en problema público implica su institucionalización mediante marcos normativos y legales, lo que permite su incorporación a las agendas del Estado. Sin embargo, esta transformación no es automática ni lineal, ya que supone disputas constantes entre autoridades y diversos actores sociales por definir qué demandas serán reconocidas y cuáles quedarán fuera de la acción gubernamental (Mballa & González López, 2017).

En este marco, la agenda gubernamental puede entenderse como el conjunto de problemas que logran captar la atención de las autoridades y que son considerados susceptibles de intervención (Cobb et al., 1976; Aguilar Villanueva, 1993; Ramírez, 2007; Aguilar Villanueva, 2017). Como señalan estos autores, la agenda no incorpora todos los problemas existentes, sino únicamente aquellos que logran posicionarse dentro del espacio de decisión política. Sin embargo, la inclusión de un tema en la agenda no garantiza su atención prioritaria, ya que los gobiernos enfrentan múltiples demandas que compiten por recursos, tiempo y capacidad institucional (Aguilar Villanueva, 1993; González Ibarra & Hernández Bazán, 2021).

Por ende, el reconocimiento de un problema en la agenda constituye una condición necesaria, pero no suficiente, para que éste adquiera una posición central dentro de la acción estatal. Aunque la incorporación de un tema a la agenda supone un primer nivel de visibilizarían, ello no permite determinar todavía el lugar que ocupa dentro de las prioridades gubernamentales. Para ello resulta necesario examinar la planeación nacional.

Planeación nacional y jerarquización de prioridades públicas

Desde la perspectiva de la administración pública, la planeación se refiere al proceso de fijar los objetivos generales de una o varias instituciones en distintos horizontes temporales en base a un apropiado diagnóstico de las necesidades sociales, así como de delimitar el marco normativo que orienta su actuación. De igual manera, implica diseñar planes, programas y proyectos, e identificar las estrategias, medidas y recursos indispensables para su cumplimiento (Chapoy Bonifaz, 2003; Núñez Medina, et al., 2020).

La planeación en la administración pública parte de un criterio de racionalidad, ya que supone elegir, entre diversas alternativas de acción, aquellas más adecuadas para alcanzar los objetivos del desarrollo. En ese sentido, no se reduce a la formulación de metas, planes o programas, sino que implica articular prioridades de corto, mediano y largo plazo con mecanismos de gestión, asignación de recursos e inversiones públicas capaces de materializar las transformaciones previstas. Así, su relevancia radica en su capacidad para ordenar la acción estatal y orientar de manera coherente la intervención gubernamental (Chapoy Bonifaz, 2003).

Desde una perspectiva crítica, Matus (1987) advierte que la planeación solo adquiere sentido cuando deja de ser un ejercicio formal y se convierte en una guía efectiva para la acción gubernamental. Bajo esta lógica, los planes sectoriales o temáticos únicamente resultan eficaces si se insertan en una planeación general que realmente oriente la toma de decisiones del gobierno. De ahí que el autor señale la frecuente brecha entre los planes formulados como compromisos oficiales y las decisiones que, en la práctica, conducen la acción cotidiana de los gobernantes. Por lo tanto, la utilidad de la planeación no reside en su sola existencia documental, sino en su capacidad para anticipar problemas, jerarquizar prioridades y conducir efectivamente la acción del Estado.

En México, la Ley de Planeación constituye el fundamento jurídico de la planeación nacional en materia de acción gubernamental, al establecer que, la planeación debe desarrollarse como un medio para garantizar el desempeño eficaz de las responsabilidades del Estado. Desde esta óptica, la planeación nacional del desarrollo puede entenderse como un proceso de organización racional y sistemática de acciones que, a partir del ejercicio de las atribuciones del Ejecutivo Federal, busca transformar la realidad del país conforme a las normas, principios y objetivos previstos en la Constitución y en la propia ley (Cámara de Diputados del H. Congreso de la Unión, 2024). Por ende, el Plan Nacional de Desarrollo, establece los propósitos y prioridades de los gobiernos (Chapoy Bonifaz, 2003). Por otra parte, la Ley Orgánica de la Administración Pública Federal, establece que la actuación de las dependencias y entidades públicas debe orientarse conforme a las prioridades definidas en la planeación nacional del desarrollo, de modo que sus acciones contribuyan al cumplimiento de los objetivos estratégicos fijados por el Estado (Cámara de Diputados del H. Congreso de la Unión, 2025) y de la misma manera lo confirma la Ley de Planeación.

En la administración pública, la planeación orienta de manera obligatoria la actuación de las instituciones mediante programas sectoriales de mediano plazo y programas operativos anuales, en los que se definen objetivos, políticas, acciones, responsables, recursos y metas concretas (Chapoy Bonifaz, 2003). En esa misma lógica, Martín (2005) señala que la definición de una estrategia de gobierno implica, además, jerarquizar las prioridades del desarrollo nacional, de modo que el plan no solo organice la acción estatal, sino que también funcione como principio ordenador de las políticas públicas. En este sentido, si la agenda gubernamental permite identificar qué problemas son reconocidos por el Estado, la planeación nacional permite observar cuáles de ellos son efectivamente jerarquizados como prioridades estratégicas. Sin embargo, para comprender cómo estas prioridades se traducen en acciones concretas, resulta necesario analizar el ámbito de las políticas públicas, en donde dichas definiciones adquieren forma operativa.

Ciberseguridad como objeto de política pública

Las políticas públicas pueden entenderse como el conjunto de decisiones y acciones mediante las cuales el Estado interviene para atender problemas públicos, es decir, situaciones que trascienden el ámbito individual y adquieren relevancia colectiva al afectar el bienestar social, la seguridad o la estabilidad institucional (Mballa & González López, 2017; Olavarría Gambi, 2007; Olaya & gallego, 2022). En este proceso, la agenda, la planeación nacional y las políticas públicas constituyen dimensiones articuladas de la acción estatal: mientras la agenda permite visibilizar determinados problemas, la planeación nacional los jerarquiza como prioridades estratégicas, y las políticas públicas traducen esas prioridades en objetivos, estrategias e instrumentos concretos de intervención.

Desde esta perspectiva, una política pública no surge de una decisión aislada, sino de un proceso de reconocimiento, incorporación y proyección institucional del problema en la acción gubernamental (Parsons, 2007). Además, su eficacia depende no solo de su formulación, sino también de la coherencia entre el problema identificado, los medios empleados y los resultados esperados (Cejudo & Michel, 2016; Salazar Vargas, 2019). Bajo esta lógica, la ciberseguridad puede asumirse como un problema público en la medida en que las amenazas digitales comprometen servicios, instituciones, información estratégica e incluso la confianza ciudadana en la capacidad del Estado para proteger el entorno digital.

Por lo tanto, abordar la ciberseguridad como política pública implica reconocer que su atención no puede limitarse a respuestas técnicas aisladas, sino que requiere marcos normativos, capacidades institucionales, coordinación intergubernamental e instrumentos específicos de intervención. Como señalan Howlett (2023), Tiburcio Zamudio (2024), Isuani (2012) y Cejudo y Michel (2016), los instrumentos de política pública son los medios que permiten convertir objetivos en acciones, por lo que su coherencia y complementariedad resultan esenciales frente a problemas complejos. Esta exigencia ha sido confirmada por análisis recientes sobre el caso mexicano, los cuales advierten que una ley o marco de ciberseguridad resulta insuficiente si no se sustenta en principios integrales, capacidades técnicas y comprensión especializada del problema, evitando así respuestas parciales o meramente reactivas (Aguilar Antonio & Quechol Maciel, 2025).

Asimismo, para que una política pública sea viable y efectiva, debe contar con condiciones mínimas de implementación, entre ellas un dispositivo normativo que le otorgue dirección, un dispositivo de gestión que haga posible su ejecución y un conjunto de recursos básicos que garantice su operación (Isuani, 2012). Esta exigencia adquiere especial relevancia en ciberseguridad, dado que se trata de un ámbito transfronterizo, fragmentado y altamente interconectado, cuya gobernanza involucra a múltiples actores estatales y no estatales (Parto & Els, 2024; Van den Berg & Keymolen, 2017). Por ello, una política pública de ciberseguridad requiere no solo leyes y estrategias, sino también mecanismos de gestión, recursos, cooperación y capacidades técnicas que permitan prevenir, mitigar y responder de manera efectiva a los riesgos del ciberespacio.

En suma, las perspectivas sobre problemas públicos, agenda gubernamental, planeación nacional y políticas públicas permiten comprender que la acción estatal no responde de manera automática a la existencia de riesgos o necesidades, sino a procesos de reconocimiento, jerarquización e instrumentación. Mientras la agenda define qué problemas logran visibilizarse en el espacio de decisión política (Aguilar Villanueva, 1993; Cobb et al., 1976), la planeación nacional establece su posición dentro del sistema de prioridades del Estado (Matus, 1987; Chapoy Bonifaz, 2003), y las políticas públicas traducen dichas prioridades en acciones concretas mediante objetivos, estrategias e instrumentos (Parsons, 2007; Cejudo & Michel, 2016). Desde esta perspectiva, la ciberseguridad puede analizarse no solo como un riesgo asociado al entorno digital, sino como un problema público cuya

relevancia depende de la forma en que es incorporado, jerarquizado e instrumentado por el Estado. En este sentido, el estudio de los Planes Nacionales de Desarrollo permite examinar empíricamente su posición dentro de la estructura de prioridades gubernamentales, a partir de tres dimensiones analíticas: la proporción de referencias vinculadas con la ciberseguridad, su ubicación temática dentro de la planeación nacional y el enfoque con el que es formulada, lo que permite evaluar su jerarquía como problema público en el ámbito programático. Desde una perspectiva comparada, la literatura reciente también recalca que las políticas de ciberseguridad más robustas se construyen a partir de esquemas de gobernanza que articulan gestión del riesgo, intercambio seguro de información y dirección estratégica, lo que resulta especialmente relevante para evaluar si un tema ha sido realmente institucionalizado como prioridad pública (Figueroa et al., 2025).

METODOLOGÍA

El presente estudio se desarrolla desde un enfoque cualitativo de carácter analítico-comparativo, con el propósito de examinar la incorporación de la ciberseguridad en la planeación nacional de México y analizar su jerarquía como problema público. Se empleó un diseño longitudinal y comparativo, tomando como corpus cuatro documentos correspondientes a los Planes Nacionales de Desarrollo de los sexenios de Vicente Fox (2001–2006), Felipe Calderón (2007–2012), Enrique Peña Nieto (2013–2018) y Andrés Manuel López Obrador (2019–2024), específicamente en sus apartados de seguridad. La técnica de recolección de datos fue la revisión documental, mientras que para el análisis se utilizó la técnica de análisis de contenido cualitativo deductivo. La unidad de análisis estuvo integrada por los objetivos y estrategias con relación directa o indirecta con la ciberseguridad; la primera se definió como mención explícita al tema, y la segunda como referencias a tecnologías de la información, delitos informáticos, sistemas digitales o procesos de modernización con implicaciones en seguridad. El procedimiento consistió, en primer lugar, en revisar los apartados de seguridad de cada plan para identificar fragmentos de texto asociados con la ciberseguridad y, en segundo lugar, en codificarlos y clasificarlos a partir de categorías analíticas previamente definidas: proporción, ubicación temática y enfoque. La información se organizó en matrices comparativas por sexenio, lo que permitió examinar tanto la densidad como la forma de incorporación del tema en la planeación nacional.

RESULTADOS

Lugar jerárquico de la ciberseguridad en la planeación nacional

La Tabla 1 muestra que, en los cuatro sexenios analizados, persiste un patrón en el que, los objetivos vinculados indirectamente con la ciberseguridad son menores que los objetivos tradicionales de seguridad. En términos proporcionales, su presencia es reducida en todos los periodos. De manera comparativa, el sexenio de Vicente Fox presenta la mayor proporción relativa, con 4 de 8 objetivos, mientras que el de Andrés Manuel López Obrador registra 2 objetivos indirectos pese al mayor número total de objetivos. Asimismo, en ningún sexenio se identifican objetivos autónomos de ciberseguridad. En general, los datos muestran una presencia reducida de objetivos relacionados con este tema a lo largo del periodo analizado y una continuidad en la ausencia de objetivos específicos.

Tabla 1. Distribución de objetivos vinculados con la ciberseguridad en los Planes Nacionales de Desarrollo, 2001–2024

Sexenio	Objetivos tradicionales vinculados con la seguridad	Objetivos con relación indirecta a la ciberseguridad	Objetivos autónomos de ciberseguridad
Vicente Fox (2001–2006)	8	4	0
Felipe Calderón (2007–2012)	35	5	0
Enrique Peña Nieto (2013–2018)	6	2	0
Andrés Manuel López Obrador (2019–2024)	35	2	0
Total	84	13	0

Fuente: Elaboración propia con base en los Planes Nacionales de Desarrollo 2001–2024.

La Tabla 2 muestra que, a lo largo de los cuatro sexenios, las estrategias con relación indirecta a la ciberseguridad mantienen una presencia reducida frente a las estrategias tradicionales de seguridad, mientras que las estrategias autónomas están ausentes en todo el periodo analizado. Esta regularidad permite identificar una tendencia de baja proporción de estrategias vinculadas con la ciberseguridad entre 2001 y 2024. En términos comparativos, el mayor número de estrategias indirectas se registra en el sexenio de Vicente Fox, con 8, y el menor en el de Enrique Peña Nieto, con 3. Aunque existen variaciones en los valores absolutos entre sexenios, la tendencia general se mantiene constante, ya que las estrategias relacionadas con la ciberseguridad son numéricamente menores en todos los periodos.

Tabla 2. Distribución de estrategias vinculadas con la ciberseguridad en los Planes Nacionales de Desarrollo, 2001–2024

Sexenio	Estrategias tradicionales vinculadas con la seguridad	Estrategias con relación indirecta con la ciberseguridad	Estrategias autónomas de ciberseguridad
Vicente Fox (2001–2006)	47	8	0
Felipe Calderón (2007–2012)	168	7	0
Enrique Peña Nieto (2013–2018)	21	3	0
Andrés Manuel López Obrador (2019–2024)	7	4	0
Total	243	22	0

Fuente: Elaboración propia con base en los Planes Nacionales de Desarrollo 2001–2024.

La Tabla 3 muestra que los objetivos vinculados indirectamente con la ciberseguridad se concentran en tres ámbitos principales: modernización institucional, seguridad pública y seguridad nacional. Esta distribución permite identificar un patrón de concentración temática en esas tres categorías. En el

conjunto analizado no se observan objetivos agrupados en una categoría específica de ciberseguridad. En cambio, las referencias se mantienen ubicadas de forma recurrente en esos tres ámbitos a lo largo del periodo considerado.

Tabla 3. Enfoques identificados en los objetivos vinculados con la ciberseguridad en los Planes Nacionales de Desarrollo, 2001–2024

Enfoque	Descripción general
Modernización	Objetivos orientados al fortalecimiento tecnológico, la digitalización gubernamental y la modernización administrativa del Estado.
Seguridad pública	Objetivos relacionados con la prevención del delito, la protección de la ciudadanía y el fortalecimiento de capacidades institucionales en materia de seguridad.
Seguridad nacional	Objetivos enfocados en la defensa del Estado, la protección de infraestructuras estratégicas y la preservación de la soberanía frente a amenazas.
Seguridad interior	Objetivos vinculados con la estabilidad interna, la gobernabilidad y la contención de riesgos que pueden afectar el orden institucional.

Fuente: Elaboración propia con base en los Planes Nacionales de Desarrollo 2001–2024.

Ubicación temática y enfoque de la ciberseguridad en las estrategias

La Tabla 4 muestra que, en los cuatro sexenios analizados, las estrategias vinculadas indirectamente con la ciberseguridad se concentran en categorías recurrentes como seguridad y tecnología aplicada, inteligencia estratégica, análisis de riesgos, investigación criminal digital, capacitación y planificación. Esta distribución permite identificar un patrón de concentración en ámbitos operativos relacionados con funciones de seguridad. Asimismo, no se registran categorías específicas o exclusivas de ciberseguridad como campo independiente.

En términos comparativos, se observan variaciones en el énfasis temático entre sexenios: en Vicente Fox predominan estrategias asociadas a modernización administrativa; en Felipe Calderón, a seguridad pública; en Enrique Peña Nieto, a seguridad nacional y gestión de riesgos; y en López Obrador, a seguridad interior. No obstante, la tendencia general se mantiene constante a lo largo del periodo, con una distribución temática recurrente de las estrategias en los mismos ámbitos.

Tabla 4. Enfoques de las estrategias vinculadas con la ciberseguridad en los Planes Nacionales de Desarrollo, 2001–2024

Sexenio	Categorías estratégicas identificadas	Enfoque predominante
Vicente Fox Quesada (2001–2006)	Seguridad y tecnología aplicada; cooperación internacional; planificación y prevención de riesgos; inteligencia estratégica y análisis de riesgos; capacitación y profesionalización; investigación criminal digital e inteligencia estratégica	Modernización del Estado y fortalecimiento administrativo
Felipe Calderón (2007–2012)	Investigación criminal digital e inteligencia estratégica; seguridad y tecnología aplicada; capacitación y profesionalización; cooperación internacional; planificación y prevención de riesgos; regulación y seguridad digital	Combate al crimen organizado y seguridad pública
Enrique Peña Nieto (2013–2018)	Inteligencia estratégica y análisis de riesgos; presencia explícita del concepto; capacitación y profesionalización; gestión de la información digital	Seguridad nacional y gestión estratégica de riesgos
Andrés Manuel López Obrador (2019–2024)	Investigación criminal digital e inteligencia estratégica	Seguridad interior, pacificación y soberanía
Síntesis general	Predominan categorías asociadas con modernización tecnológica, gestión de riesgos, inteligencia estratégica y seguridad digital, aunque con distinta jerarquización según el sexenio	La ciberseguridad se incorpora de forma subordinada a marcos de modernización, seguridad pública, seguridad nacional o seguridad interior, más que como un campo autónomo de política pública

Fuente: Elaboración propia con base en los Planes Nacionales de Desarrollo 2001–2024.

Implicaciones para la política pública

A partir de los hallazgos del análisis de los Planes Nacionales de Desarrollo 2001–2024, puede advertirse que la incorporación de la ciberseguridad en la planeación nacional mexicana ha sido limitada, discontinua y, en buena medida, subordinada a marcos más amplios de modernización administrativa, seguridad pública, seguridad nacional y seguridad interior. Esta configuración no solo muestra la ausencia de un reconocimiento autónomo del tema como problema público estratégico, sino que también plantea la necesidad de traducir los resultados del estudio en orientaciones que contribuyan a fortalecer su tratamiento institucional.

Desde esta perspectiva, las implicaciones del análisis apuntan a la conveniencia de avanzar hacia instrumentos de planeación que otorguen mayor claridad conceptual, continuidad programática y articulación interinstitucional a la ciberseguridad. En este sentido, la Tabla 5 sintetiza los principales hallazgos del estudio, sus implicaciones analíticas y algunas orientaciones generales para la política pública, encaminadas a fortalecer su jerarquización dentro de la acción del Estado mexicano.

Tabla 5. Implicaciones analíticas para la política pública derivadas del análisis de la ciberseguridad en los Planes Nacionales de Desarrollo, 2001–2024

Hallazgo principal	Implicación analítica	Orientación general
Ausencia de objetivos autónomos de ciberseguridad	La ciberseguridad no ha sido reconocida como problema público independiente	Incorporar objetivos explícitos de ciberseguridad en los instrumentos de planeación nacional
Predominio de estrategias subordinadas a marcos tradicionales	El tema se articula desde seguridad, modernización o control, pero no desde una política propia	Diseñar una política nacional integral con enfoque transversal e interinstitucional
Variabilidad sexenal en los enfoques estratégicos	No existe continuidad programática suficiente	Establecer lineamientos de largo plazo que trasciendan los ciclos gubernamentales
Débil presencia conceptual explícita	Hay ambigüedad en la definición estatal del problema	Fortalecer el desarrollo conceptual, normativo y programático de la ciberseguridad
Orientación operativa más que estratégica	Se privilegia la respuesta funcional sobre la institucionalización	Articular capacidades técnicas, jurídicas, organizacionales y de gobernanza

Fuente: Elaboración propia.

DISCUSIÓN

Los hallazgos del estudio permiten sostener que la ciberseguridad ha sido incorporada en la planeación nacional mexicana de manera limitada y sin consolidarse como un problema público plenamente institucionalizado. Desde el enfoque de políticas públicas, la presencia de un tema en documentos oficiales no implica por sí misma su reconocimiento sustantivo como prioridad, sino que este depende de su jerarquización, su definición conceptual y su traducción en instrumentos de acción (Aguilar Villanueva, 1993, 2017; Parsons, 2007; Cejudo & Michel, 2016). En este sentido, el análisis de los Planes Nacionales de Desarrollo evidencia que la ciberseguridad ha alcanzado una visibilidad parcial, pero sin configurarse como un eje autónomo dentro de la acción estatal.

En el nivel de los objetivos, que expresa la forma en que el Estado delimita y jerarquiza los problemas dentro de la agenda gubernamental, los resultados muestran una baja proporción de referencias y la ausencia de objetivos específicos de ciberseguridad. Este comportamiento indica que el tema no ha logrado posicionarse como un problema claramente diferenciado dentro del sistema de prioridades del Estado. Como señalan Cobb et al. (1976), Aguilar Villanueva (1993) y Ramírez Brouchoud (2007), la agenda pública es selectiva y solo incorpora aquellos problemas que alcanzan reconocimiento político suficiente; en este caso, la ciberseguridad permanece integrada a problemáticas más amplias como la seguridad, la modernización administrativa o la gestión institucional.

Desde la perspectiva de la planeación nacional, esta configuración adquiere mayor relevancia. De acuerdo con Matus (1987), la planeación implica no solo organizar la acción estatal, sino jerarquizar los problemas que orientan la toma de decisiones. Sin embargo, la ausencia de objetivos autónomos y la concentración temática en ámbitos tradicionales indican que el entorno digital no ha sido conceptualizado como un dominio estratégico con implicaciones propias. En este sentido, la planeación nacional ha incorporado la ciberseguridad como un componente funcional de agendas preexistentes, en línea con lo planteado por Chapoy Bonifaz (2003) y Martín (2005), quienes señalan que la planeación define tanto prioridades como formas de intervención.

El enfoque de los objetivos refuerza esta observación. La concentración de referencias en categorías como modernización institucional, seguridad pública y seguridad nacional muestra que la dimensión digital es encuadrada principalmente en función de su utilidad para fortalecer capacidades

administrativas y de seguridad existentes. Desde la literatura sobre problemas públicos, esto sugiere que la ciberseguridad no ha sido plenamente delimitada como un problema con lógica propia, ya que su definición depende de marcos interpretativos previamente institucionalizados (Mballa & González López, 2017; Olavarría Gambi, 2007; Sandoval Escalante, 2023).

A diferencia del nivel de los objetivos, el análisis de las estrategias permite observar cómo el problema es operado en la práctica gubernamental. En este plano, los resultados muestran que, aunque el componente digital está presente en diversas líneas de acción, su incorporación no da lugar a un conjunto de instrumentos diseñados específicamente para la gestión del riesgo cibernético. En cambio, las estrategias se integran a mecanismos ya existentes dentro de la estructura estatal, particularmente en ámbitos como la vigilancia, la inteligencia, la investigación criminal y la coordinación institucional.

En términos de políticas públicas, esta configuración evidencia una disociación entre la naturaleza del problema y los instrumentos utilizados para su atención. Como señalan Parsons (2007), Cejudo y Michel (2016) e Isuani (2012), la efectividad de una política pública depende de la correspondencia entre la definición del problema, los medios empleados y los resultados esperados. Además, para que una política pública sea viable y efectiva, debe contar con condiciones mínimas de implementación, entre ellas un dispositivo normativo que le otorgue dirección, un dispositivo de gestión que haga posible su ejecución y un conjunto de recursos básicos que garantice su operación (Isuani, 2012). No obstante, en el caso analizado, las estrategias no se estructuran a partir de la especificidad del riesgo digital, sino que se insertan en marcos de acción previamente definidos, lo que limita su capacidad para responder de manera integral a las características del ciberespacio.

Las variaciones observadas entre sexenios refuerzan esta tendencia. Si bien cada administración incorpora el componente digital de acuerdo con sus propias prioridades; modernización administrativa, combate al crimen organizado, seguridad nacional o seguridad interior, en todos los casos las estrategias mantienen una orientación dependiente de agendas más amplias. Este comportamiento indica que la ciberseguridad no solo carece de autonomía en su definición, sino también en su ejecución, al no traducirse en un campo de intervención diferenciado dentro de la acción pública.

Este patrón coincide con diagnósticos recientes sobre la evolución de la ciberseguridad en México. Aguilar Antonio (2024) señala que el país presenta un desarrollo desigual y fragmentado en comparación

con sus socios regionales, mientras que Aguilar Antonio y Quechol Maciel (2025) advierten que los avances normativos no son suficientes sin una comprensión integral del problema. De manera complementaria, estudios como los de Parto y Els (2024) y Van den Berg y Keymolen (2017) han destacado que la gobernanza de la ciberseguridad requiere coordinación institucional, claridad organizacional y mecanismos integrales de gestión del riesgo, elementos que no se observan de forma consistente en la planeación nacional mexicana.

A nivel regional, estos resultados también dialogan con diagnósticos previos del Banco Interamericano de Desarrollo y la Organización de los Estados Americanos (2016), que identifican rezagos en América Latina en la consolidación de capacidades institucionales de ciberseguridad. En el caso mexicano, el análisis longitudinal muestra que, aunque el tema ha estado presente de manera tangencial, ello no se ha traducido en continuidad programática ni en una configuración estratégica claramente definida.

En general, la evidencia permite observar una relación consistente entre la forma en que el problema es definido en la agenda (objetivos) y la manera en que es operado en la práctica (estrategias). Mientras que los objetivos reflejan una delimitación indirecta y subordinada del problema, las estrategias muestran una operacionalización integrada a funciones estatales preexistentes. Esta correspondencia sugiere que la ciberseguridad ha sido tratada como un componente funcional dentro de la acción estatal, más que como un campo de política pública con lógica propia.

A modo de cierre, estos hallazgos abren una reflexión sobre la capacidad adaptativa de la planeación nacional frente a problemas emergentes. Si el entorno digital ha transformado de manera sustantiva la seguridad, la economía y la acción gubernamental, la persistencia de patrones de incorporación indirecta y dependiente sugiere que el Estado mexicano enfrenta dificultades para reconfigurar sus esquemas de intervención frente a nuevas formas de riesgo. En este sentido, el análisis de la ciberseguridad no solo aporta al campo específico, sino que permite examinar de manera más amplia los límites de la planeación estatal para jerarquizar problemas públicos en contextos de transformación digital acelerada.

CONCLUSIONES

El análisis realizado permite sostener que la incorporación de la ciberseguridad en la planeación nacional mexicana no ha derivado en una reconfiguración sustantiva de los criterios mediante los cuales el Estado define y organiza sus prioridades. Más allá de su presencia en objetivos y estrategias, los resultados

muestran que su integración no ha modificado la estructura general de la acción pública, sino que se ha mantenido dentro de marcos previamente establecidos.

En este sentido, la evidencia pone de relieve una brecha entre la creciente centralidad del entorno digital y la capacidad del Estado para ajustar sus esquemas de intervención. La expansión del ciberespacio como ámbito de interacción social, económica y gubernamental no se ha traducido en una transformación equivalente en la forma en que los problemas públicos son reconocidos, delimitados y jerarquizados dentro de la planeación nacional.

Desde una perspectiva más amplia, estos hallazgos sugieren que la planeación estatal tiende a responder a los cambios tecnológicos mediante procesos de incorporación incremental, en los que los nuevos elementos se integran a estructuras existentes sin alterar su lógica de funcionamiento. Esto limita la posibilidad de construir marcos de acción acordes con la complejidad, interdependencia y dinamismo propios del entorno digital.

En este contexto, el desafío no radica únicamente en ampliar la presencia de la ciberseguridad en los instrumentos de planeación, sino en revisar los principios bajo los cuales el Estado identifica y organiza sus prioridades estratégicas. Ello implica avanzar hacia esquemas de planeación capaces de reconocer el ciberespacio como un ámbito que redefine las condiciones de la acción pública, incorporando no solo dimensiones operativas, sino también elementos de gobernanza, articulación institucional y atención integral de riesgos.

REFERENCIAS BIBLIOGRÁFICAS

Abad, W. A. (2020). Ciberataques: desafíos en el ciberespacio. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, *13*(1), 13. https://doi.org/10.24133/age.n13.2020.11

Aguilar Antonio, J. M. (2020). Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional. *Revista Legislativa de Estudios Sociales y de Opinión Pública, 13* (29),83-120. Recuperado de https://biblat.unam.mx/hevila/Revistalegislativadeestudiossocialesydeopinionpublica/2020/vol13/no29/3.pdf

Aguilar Antonio, J. M. (2024). Rezago y asimetrías de las políticas nacional e internacional de ciberseguridad de México frente a Estados Unidos y Canadá: Retos de cooperación para

Norteamérica. *Norteamérica, 19*(1), 35–68. https://doi.org/10.22201/cisan.24487228e.2024.1.663

Aguilar Antonio, J. M., & Quechol, M. K. (2025). ¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019–2023). *Paakat: Revista de Tecnología y Sociedad, 15*(28), e892. https://doi.org/10.32870/pk.a15n28.892

Aguilar Villanueva, L. F. (Ed.). (2017). *Problemas públicos y agenda de gobierno* (3a. ed.). Miguel Ángel Porrúa.

Aguilar Villanueva, L.F. (1993). *Problemas públicos y agenda de gobierno.* Porrúa.

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*

Cámara de Diputados del H. Congreso de la Unión. (2024). *Ley de Planeación*. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LPlan.pdf

Cámara de Diputados del H. Congreso de la Unión. (2025). *Ley Orgánica de la Administración Pública Federal*. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LPlan.pdf

Cejudo, G., & Michel, C. (2016). Coherencia y políticas públicas: Metas, instrumentos y poblaciones objetivo. *Gestión y política pública, 25* (1), 3-31. Recuperado de https://www.scielo.org.mx/scielo.php?pid=S1405-10792016000100001&script=sci_arttext

Chapoy Bonifaz, D. B. (2003). *Planeación, programación y presupuestación*. Instituto de Investigaciones Jurídicas, UNAM.

Cobb, R., Ross, J.-K., & Ross, M. H. (1976). Agenda Building as a Comparative Political Process. *The American Political Science Review*, *70*(1), 126–138. https://doi.org/10.2307/1960328

Figueroa, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals. *International Journal of Information Security, 24*, 121. https://doi.org/10.1007/s10207-025-01024-0

González Ibarra, M.R., & Hernández Bazán, F. (2021). Agenda política hacia el bienestar y la cohesión social en el gobierno de la cuarta transformación en México. *Polis, 17* (1). Recuperado de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-23332021000100043

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding local government cybersecurity policy: A concept map and framework. *Information, 15*(6), 342. https://doi.org/10.3390/info15060342

Howlett, M. (2023). *What is a policy tool? An overview of the tools approach to public policy*. En M. Howlett (Ed.), *The Routledge handbook of policy tools* (pp. 3–18). Routledge. Recuperado de https://www.taylorfrancis.com/chapters/edit/10.4324/9781003163954-2/policy-tool-michael-howlett

Isuani, J. F. (2012). Instrumentos de políticas públicas. Factores claves de las capacidades estatales. *Documentos y Aportes en Administración Pública y Gestión Estatal: DAAPGE,* (19), 51-74. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4119279

Matus, C. (1987). Planificación y gobierno. *Revista de la CEPAL, 31.* . Recuperado de https://repositorio.esocite.la/982/1/Matus1987-PlanificacionGobierno.pdf

Mballa, L.V., & González López, C. (2017). La complejidad de los problemas públicos: institucionalización de las situaciones problemáticas y anterioridad de la solución a la acción pública. *Revista Enfoques: Ciencia Política y Administración Pública*, *XV*(27), 97-121. . Recuperado de https://www.redalyc.org/pdf/960/96055458005.pdf

McGuinness, D. (2007, julio 30). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. BBC. Recuperado de https://www.bbc.com/mundo/noticias-39800133

Núñez Medina, J.M., De León Dávila, F.J., & Martínez Aguilar, L.R. (2020). Desafíos de la Planeación Gubernamental en México. *De iure revista jurídica.*

Olavarría Gambi, M. (2007). *Conceptos básicos en el análisis de políticas públicas. Documento de trabajo.* Universidad de Chile. Recuperado de https://repositorio.uchile.cl/bitstream/handle/2250/123548/Conceptos_%20Basicos_Politicas_Publicas.pdf

Olaya, A., & Gallego, L. (2022). La definición y estructuración del problema público. En S. Leyva et al. (Eds.), *Modelo para el análisis y diseño de políticas públicas (MADPP)* (pp. 41-67). Editorial EAFIT. Recuperado de https://editorial.eafit.edu.co/index.php/editorial/catalog/book/163

Parsons, W. (2007). *Políticas públicas: una introducción o lo teoría y lo práctica del análisis de políticas públicas.* FLACSO. Recuperado de https://www.fhyce.edu.py/wp-content/uploads/2020/08/Politicas-Publicas.pdf

Parto, M., & Els, D.B. (2024). The New F-word: The case of fragmentation in Dutch cybersecurity governance. *Computer Law & Security Review*, (55). Recuperado de https://www.sciencedirect.com/science/article/pii/S0267364924000980

Piña Libién, H. R. (2019). Cibercriminalidad y ciberseguridad en México. *Ius Comitiãlis*, *2*(4), 47-69. Recuperado de https://iuscomitialis.uaemex.mx/article/view/13203/10538.

Ramírez Brouchoud, M.F. (2007). El diseño de la agenda política y la construcción de alternativas de solución en la política de inmigración española. *Civilizar. Ciencias Sociales y Humanas*, 7 (13), 249-264. Recuperado de https://www.redalyc.org/pdf/1002/100221524014.pdf

Salazar Vargas, C. (2019). Políticas públicas. Konrad Adenauer Stiftung. Recuperado de https://dialogopolitico.org/wp-content/uploads/2020/04/politicas_publicas_kas_honduras.pdf

Sandoval Escalante, B. (2023). Método para analizar la definición de un problema público. *Journal of Public Governance and Policy: Latin American Review*, *2*(9), 123-141. Recuperado de https://journalofpublicgovernance.cucea.udg.mx/index.php/jpgp/article/view/7913

Tiburcio Zamudio, K. S. (2024). ¿Alerta de violencia de género contra las mujeres como un instrumento de política pública? *La ventana. Revista de estudios de género, 7*(60). Recuperado de https://www.scielo.org.mx/scielo.php?pid=S1405-94362024000200038&script=sci_arttext#B10

Van den Berg, B., & Keymolen, E. (2017). Regulating security on the Internet: control versus trust. *International Review of Law, Computers & Technology, 31*(2), 188-205. Recuperado de https://www.tandfonline.com/doi/epdf/10.1080/13600869.2017.1298504?src=getftr&utm_source=sciencedirect_contenthosting&getft_integrator=sciencedirect_contenthosting

Wiedemar, S. (2023, mayo). *NATO and Article 5 in cyberspace* (CSS Analyses in Security Policy No. 323). Center for Security Studies (CSS), ETH Zürich. Recuperado de

https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf