Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA
UNIDAD XOCHIMILCO

División de Ciencias Sociales y Humanidades

RECONSTRUCCIÓN DE LA POLÍTICA DE CIBERSEGURIDAD EN MÉXICO DURANTE EL SEXENIO DE ANDRÉS MANUEL LÓPEZ OBRADOR

T R A B A J O T E R M I N A L
QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN POLÍTICA Y GESTIÓN SOCIAL

P R E S E N T A:

MENDOZA LARA ERICK

Asesora:

Dra. Angélica Rosas Huerta

Ciudad de México

Abril 2025

Índice

Introducción *3*

Capítulo 1. Las políticas públicas y la ciberseguridad *10*

1.1 La política pública y sus instrumentos de acción pública **10**

1.2 Una política pública de ciberseguridad **13**

1.3 Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos **15**

Capítulo 2. Evolución histórica de la política de ciberseguridad en México (2012-2018) *30*

2.1 El surgimiento de la ciberseguridad en la agenda gubernamental mexicana **30**

2.2 La limitada Estrategia Digital Nacional 2013-2018 ..... **31**

2.3 La institucionalización de las dimensiones de ciberseguridad en México **33**

2.3.1 El Modelo Homologado de Policía Cibernética **35**

2.3.2 La Estrategia Nacional de Ciberseguridad **39**

Capítulo 3. Reconstrucción de la política de ciberseguridad en materia de seguridad pública (2018-2024) *44*

3.1 El contexto político, las demandas sociales y la (des)priorización de la ciberseguridad en México **44**

3.2 La política de ciberseguridad en la seguridad pública de AMLO **48**

3.2.1 Instrumentos normativos **48**

3.2.2 Instrumentos organizativos **57**

3.2.3 Instrumentos programáticos **65**

3.2.4 Instrumentos financieros **73**

Capítulo 4. Identificación y evaluación de las preferencias y capacidades institucionales del Estado mexicano en ciberseguridad en el periodo obradorista (2018-2024) *84*

4.1 Estructura organizacional en ciberseguridad **84**

4.2 Enfoque de la normativa sobre ciberseguridad **87**

4.3 Enfoque de las políticas asociadas a las respuestas ante incidentes informáticos, a la protección de la infraestructura crítica y a la persecución del ciberdelito **91**

4.4 Cooperación internacional **92**

4.5 Valoración cuantitativa **93**

Conclusiones *97*

Bibliografía *99*

Introducción

Hace una década atrás, en 2013, la Oficina de Naciones Unidas contra la Droga y el Delito (ONUDC, 2013) advirtió por primera vez el surgimiento de una tendencia en la utilización de tecnologías de información y comunicación globalizadas para perpetrar actos delictivos de alcance transnacional: el ciberdelito. Este tipo de delito también conocido como "delito cibernético", "crimen digital" o "cibercrimen", no tiene un consenso internacional para definirlo, pero la Oficina abordó este debate: ¿debe adoptarse una definición específica y detallada de los delitos puramente cibernéticos, o es preferible optar por una definición más amplia que permita aplicar herramientas de investigación cibernética a cualquier delito que deje evidencia electrónica? (ONUDC, 2013).

La Oficina de Naciones Unidas contra la Droga y el Delito recomendó no establecerlo como un término técnico, sino como un conjunto de actos que podrían considerarse como delitos cibernéticos, en los que los clasificó en tres clases de actos:

1) Actos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos:
    a. Acceso ilegal a un sistema informático;
    b. Acceso ilegal, interceptación o adquisición de datos informáticos;
    c. Interferencia ilegal de datos o daños a un sistema;
    d. Producción, distribución o posesión informática de herramientas para el mal uso.
2) Actos informáticos por beneficio financiero o daños personales:
    a. Fraude o falsificación informática;
    b. Delitos informáticos relacionados con la identidad;
    c. Delitos informáticos contra derechos de autor o marcas comerciales;
    d. Envío o control de spam;
    e. Actos informáticos que causen daño personal;
3) Actos informáticos relacionados con el contenido:
    a. Actos informáticos que involucran discurso de odio;
    b. Producción, distribución o posesión informática de pornografía infantil;
    c. Actos informáticos en respaldo de delitos de terrorismo. (pág.18)

Pero también la ONUDC reconoció que, ante el avance hacia un acceso universal a Internet, posiblemente sea necesario adoptar un enfoque híbrido. Este enfoque debería operar en

múltiples niveles, siendo específico y detallado para definir ciertos actos individuales de delito cibernético, pero lo suficientemente amplio para garantizar que los poderes investigativos y los mecanismos de cooperación internacional puedan aplicarse a la creciente migración de los delitos tradicionales hacia el entorno digital (pág. 25).

La ONUDC también subrayó la importancia de medir el delito cibernético, como la de cualquier otro delito, para la prevención y reducción de los mismos; en un ámbito global "al desglosar los datos por tipo de acto de delito cibernético logran ofrecer un alto grado de consistencia y capacidad de comparación" (pág. 26).

Es por ello si no se hubieran medido o registrado eventos de ciberdelitos, no hubiera sido posible identificar el crecimiento que los ciberdelitos han tenido a nivel internacional. En este sentido, internacionalmente en el sector financiero entre 2013 y 2023 se registró incremento de 291% en incidentes cibernéticos (actos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos), pasando de 856 a 3,348 incidentes registrados (Verizon, 2024); además de las pérdidas en miles de millones de dólares por fraudes con tarjetas de crédito y débito (actos informáticos por beneficio financiero) que a nivel mundial creció 84% de 2014 a 2022, pasando de 8.11 a 33.45 miles de millones de dólares (Nilson Report, 2023); también, de 2016 a 2022, la cantidad de páginas web reportadas con contenido de pornografía infantil (actos informáticos relacionados con el contenido) creció de 38,424 a 418.85, que corresponde a 418% de incremento (Internet Watch Foundation, 2023).

En México las estadísticas federales de los delitos cibernéticos desglosados por su clase comenzaron a ser publicados anualmente por primera vez en el Censo Nacional de Gobierno Federal de 2017. En este censo, la Guardia Nacional registra los delitos cibernéticos desglosados en agravios contra personas, fraudes y extorsiones, eventos de seguridad informática, y delitos contra menores.

En 2017 fueron reportados un total de 9,913 eventos definidos como incidentes cibernéticos, llegando a 2023 con un incremento de un 372%, en los que fueron reportados 46,859 incidentes cibernéticos (INEGI, 2024). Como se observa en la Tabla 1, el panorama de los

prinicpales incidentes cibernéticos en México muestra una tendencia de crecimiento entre 2017 y 2023.

Tabla 1. Historial de los principales incidentes cibernéticos reportados.

Tipo de incidente cibernético	2017	2018	2019	2020	2021	2022	2023
Amenazas	991	1,321	1,239	1,657	2,834	5,533	7,069
Suplantación de identidad	483	640	427	731	916	899	1,789
Extorsión	429	975	1,207	1,442	980	1,641	4,114
Fraude al comercio electrónico	3,623	4,491	3,695	6,250	5,771	4,486	6,303
Phisihing	213	432	354	293	181	109	202
Robo de contraseñas en redes sociales	446	520	0	0	732	1,490	10,300
Acoso contra menor de edad	45	164	215	232	256	145	277
Ciberbullying	20	27	28	26	3	16	114
Pornografía infantil	137	218	121	451	41	35	72
Robo de contraseñas en redes sociales a menores de edad	-	-	551	781	42	20	532
Reporte ciudadano de páginas web	-	-	1,357	4,192	1,381	701	315

Fuente: Elaboración propia con datos de INEGI (2024)

Los datos documentan el crecimiento de los incidentes cibernéticos. Sobresalen los incrementos exponenciales durante estos años en las categorías de robo de contraseñas en redes sociales (de 446 a 10,300 incidentes; un aumento de 2,209%), amenazas cibernéticas (de 991 a 7,069; un amento de 613%) o la extorsión digital (de 429 a 4,114 incidentes; un aumento de 858%), lo que sugiere una evolución significativa en el ataque digital.

La creciente de los ciberdelitos, no sólo a nivel nacional, lleva a los paises a tomar medidas para reducirlo. La ONUDC define esta acción como prevención del delito, involucrando estrategias y medidas para reducir el riesgo de que ocurran ciberdelitos, y mitigar sus posibles efectos nocivos para las personas y la sociedad. Entre las acciones de prevención se encuentran la promulgación de leyes, un liderazgo efectivo, el desarrollo de capacidad de justicia penal y de aplicación de la ley, la educación y concientización, el desarrollo de una

base firme de conocimientos, y cooperación entre gobiernos, comunidades, el sector privado y a nivel internacional (ONUDC, 2013, pág. 26).

Un ejemplo reciente de ello es el acuerdo alcanzado en 2016 por el Consejo de la Unión Europea, que establece nuevos pasos decisivos para combatir las actividades delictivas en el ciberespacio, buscando mejorar los procedimientos de asistencia judicial y facilitar el reconocimiento mutuo en el ámbito digital, utilizando instrumentos electrónicos y formularios estandarizados, asimismo mejorando la cooperación con los proveedores de servicios mediante el desarrollo consensuado de un marco común para solicitar información. Logrando iniciar un año después las negociaciones para un reglamento sobre la ciberseguridad que fue aprobado en 2018.

Aunque los países líderes en el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones de la Organización de las Naciones Unidas, que califica las estrategías nacionales de ciberseguridad, tuvieron una temprana adopción de una estrategia nacional, con Estados Unidos a la vanguardia desde 2003, seguido por Australia (2009), Canadá (2010) y Austria (2013) (Shafqat y Masood, 2016); fue en México hasta el sexenio de Enrique Peña Nieto (2012-2017) cuando la respuesta del estado mexicano a este nuevo enfoque de crimen fue establecido y guiado a partir de su programa de seguridad pública con el propósito de fortalecer la ciberseguridad y la ciberdefensa.

En 2017, su gobierno desarrolló la Estrategia Nacional de Ciberseguridad, con ayuda y recomendaciones de la Organización de los Estados Americanos (OEA) (Rodríguez, 2018). También el Modelo Homologado de Unidades de Policía Cibernética para ser implementado estatalmente y evaluado anualmente con aportaciones del Fondo de Aportaciones para la Seguridad Pública para los estados y el Distrito Federal.

Con la llegada de Andrés Manuel López Obrador (AMLO) a la presidencia en 2018, surgieron expectativas sobre la continuidad y evolución de las políticas para proteger a los ciudadanos en el entorno digital. (Rodríguez, 2018). Ya que el Modelo Homologado de Unidades de Policía Cibernética se encontraba en fase de implementación en las entidades federativas cuando entró a la presidencia, la nueva administración siguió con su implementación y con la aportación federal durante todo su sexenio.

Pero en su gobierno fue hasta 2023, cuando creó por decreto la Comisión Intersecretarial de Tecnologías de la Información y Comunicación y de la Seguridad de la Información, con la tarea de la implementación de las políticas federales en materia de tecnologías de la información y comunicación, y de la seguridad de la información (ciberseguridad) (Diario Oficial de la Federación, 2023a); un meses después de revelarse que la SEDENA sufrió un ataque cibernético resultando en la filtración de miles de documentos clasificados y de información de seguridad nacional (Latinus_us, 2022).

Para comprender mejor esta problemática, es necesario revisar los estudios previos sobre políticas públicas de ciberseguridad. La literatura existente puede analizarse en distintos niveles, identificándose en diferentes aproximaciones metodológicas y alcances en el análisis de políticas públicas en esta materia.

A nivel internacional, desde la academia, se han desarrollado estudios sobre políticas nacionales de ciberseguridad. Por ejemplo, Santos Vidal (2022) analiza el marco regulatorio y los instrumentos estratégicos de ciberseguridad en Ecuador durante 2013-2022, examinando políticas, legislación e instituciones generadas para enfrentar amenazas cibernéticas. Por su parte, Ochoa y Fernanda (2019) estudia la evolución de la política de ciberseguridad de Canadá entre 2010 y 2018, analizando la estructura, objetivos y actores relevantes en su implementación.

En el contexto mexicano, Arteaga (2021) examinó los ciberdelitos y las políticas locales de información en ciberseguridad en Tamaulipas, concluyendo una necesidad de fortalecer el marco jurídico específico para ciberdelitos y mejorar las capacidades institucionales.

Sin embargo, se identificaron importantes vacíos en la literatura existente. En primer lugar, no existen estudios que evalúen específicamente períodos presidenciales en México en materia de ciberseguridad. Además, los análisis previos, aunque valiosos, carecen de marcos analíticos especializados que permitan evaluar tanto preferencias como capacidades institucionales de manera sistemática.

En este contexto, la presente investigación buscó contribuir a llenar estos vacíos mediante la aplicación parcial del marco analítico desarrollado por Bustos y Aguerre (2022) en su trabajo *Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países*

latinoamericanos del Centro Latam Digital. Este marco proporciona referentes analíticos que permiten analizar las capacidades institucionales de los gobiernos han construido para atender la problemática del ciberdelito.

Esto nos lleva a plantear las siguientes preguntas de investigación: ¿en la administración de Andrés Manuel López Obrador se desarrolló una política de seguridad cibernética en materia de seguridad pública? y ¿qué fortalezas y debilidades institucionales tiene?

Este trabajo tiene el objetivo de reconstruir y analizar la política de seguridad cibernética en la seguridad pública de México durante el sexenio de Andrés Manuel López Obrador (2018-2024). Para lograrlo, el trabajo se guía por dos objetivos específicos: en primer lugar, identificar las acciones de política desarrolladas por el gobierno de Andrés Manuel López Obrador para atender la problemática de la seguridad cibernética en materia de seguridad pública en México. En segundo lugar, se busca evaluar las capacidades institucionales desarrolladas sobre la política de ciberseguridad en la seguridad pública en México.

La presente investigación se estructura en cuatro capítulos, además de la introducción y las conclusiones, diseñados para responder a las preguntas sobre el desarrollo de una política de seguridad cibernética en la administración de AMLO y sus fortalezas y debilidades institucionales.

El primer capítulo presenta el marco teórico-conceptual y metodológico que guía el análisis. Se inicia con una conceptualización de política pública y se desarrolla el enfoque de los instrumentos de acción pública, que permite reconstruir la política de ciberseguridad a través de sus elementos normativos, organizativos, programáticos y financieros. Posteriormente, se recuperan aportes para entender los elementos de la ciberseguridad y sus dimensiones, así como el *Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos* de Bustos y Aguerre (2022) y la propuesta para su implementación en esta investigación en materia de seguridad pública.

El segundo capítulo establece el contexto histórico de la política de ciberseguridad en México iniciando desde su primera adopción en el sexenio de Enrique Peña Nieto de 2012 hasta el término de mandato en 2018, en el que se desarrollaron ciertos instumentos de acción pública que permiten comprender el punto de partida institucional de la administración de AMLO.

El tercer capítulo constituye el inicio del núcleo del análisis, enfocándose directamente en los objetivos de investigación al examinar el actuar federal en temas de ciberseguridad y seguridad pública durante el gobierno de AMLO (2018-2024). Este análisis identifica los instrumentos de acción pública su gobierno, cumpliendo con el primer objetivo específico.

El cuarto y último capítulo, aborda el análisis y evaluación de las preferencias institucionales y de las capacidades institucionales del gobierno mexicano sobre el problema de los ciberdelitos, respondiendo así a la segunda pregunta de investigación. Finalmente, las conclusiones sintetizan los hallazgos para responder de manera comprehensiva a las preguntas de investigación.

Capítulo 1. Las políticas públicas y la ciberseguridad

En este capítulo se presenta el marco conceptual y metodológico que se utiliza para analizar la política de ciberseguridad en México durante el periodo 2018-2024. El objetivo es establecer las bases teóricas y herramientas analíticas que permiten examinar esta política pública.

Para ello, primero se aborda la conceptualización de política pública y sus instrumentos de acción, lo que nos permite identificar las diferentes formas en que el gobierno interviene para atender problemas que enfrenta la sociedad. Posteriormente, se plantea el papel del Estado en materia de ciberseguridad y seguridad pública.

Finalmente, se recupera la metodología de análisis de capacidades propuesta por Bustos y Aguerre (2022) en su *Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos*.

1.1 La política pública y sus instrumentos de acción pública

El concepto de *política* es complejo y diversos autores le han dado una defínción, pero podemos empezar a entenderla a través desde tres dimensiones que se interrelacionan entre sí: como estructura (polity), como proceso (politics) y como resultado (policy) (Valles, 2006).

La primera dimensión es vista como una estructura, traducido al español como *lo* político, se refiere al marco institucional y normativo donde la actividad política se desarrolla. Esta es la dimensión que establece las reglas del juego y las estructuras formales dentro de las cuales se desarrollan las otras dimensiones. Comprende tanto las instituciones formales como las normas y procedimientos que regulan la vida política.

La segunda dimensión, *la* política, se centra en la dinámica del conflicto y consenso entre actores. Es aquí donde ocurre el proceso de politización, mediante el cual un tema trasciende de ser un conflicto particular para convertirse en un asunto de interés público. Esta dimensión involucra las negociaciones, alianzas y confrontaciones entre diversos actores políticos y sociales que buscan influir en la toma de decisiones.

En la tercera dimensión se traducen las decisiones de *la* politica en programas, proyectos y acciones específicas orientadas a atender las demandas y necesidades sociales. Al considerar la *política* como un resultado, se considera que ese resultado tiene como destino la regulación de desacuerdos y tensiones existentes en diferentes ámbitos de la vida colectiva (Valles, 2006). Este resultado se materializa en lo que conocemos como *política pública*, cuya definición tampoco tiene una definición única pero que ha sido abordada desde múltiples autores.

En este sentido, el Dr. Luis F. Aguilar Villanueva ha ofrecido diversas conceptualizaciones que enfatizan diferentes aspectos de las políticas públicas. Para los propósitos de este trabajo, adoptaremos su definición de políticas públicas como:

> Un conjunto (secuencia, sistema, ciclo, espiral) de acciones intencionales y causales. […] acciones intencionales porque se orientan a realizar objetivos considerados de valor para la sociedad o a resolver problemas cuya solución se considera de interés o beneficio público, y son acciones causales porque son consideradas idóneas y eficaces para realizar el objetivo o resolver el problema. (Aguilar, 2012, pág. 29)

Es importante señalar que una política pública es, en esencia, una abstracción que se materializa a través de diversos instrumentos y acciones concretas. No podemos ver o tocar una política pública directamente, como señala Meny y Thoenig (1992), quienes explican que una política pública se presenta como un programa de acción gubernamental en un sector de la sociedad o en un espacio geográfico, pero que en la práctica, identificar sus límites y especificidades es complejo.

Sin embargo, podemos identificarlas a través de características que señalan los mismos autores: el contenido que moviliza recursos para generar resultados; un programa que integra actividades en un marco general; una orientación normativa que refleja finalidades y preferencias específicas; un factor de coerción que deriva de la naturaleza autoritaria del actor gubernamental; y una competencia social al afectar situaciones, intereses y comportamientos de la sociedad (Meny y Thoenig, 1992).

Estas características permiten comprender cómo se materializa una política pública. No obstante, es importante considerar que para su implementación, el gobierno debe primero

reconocer aquellas problemáticas que requieren intervención estatal. Pero cabe destacar que no todos los problemas sociales se convierten en problemas públicos merecedores de atención gubernamental

Este reconocimiento ocurre cuando un problema ingresa a la agenda institucional, también llamada agenda gubernamental, que está constituida por aquellos asuntos formalmente aceptados por los tomadores de decisiones para su atención, después de que diversos actores y sectores de la sociedad han movilizado recursos e intereses para posicionarlo como prioritario (Aguilar, 1993; Meny y Thoenig, 1992).

Una vez que un problema ingresa en la agenda gubernamental, el Estado despliega diversas acciones de política pública para atenderlo. Rosas (2021) identifica cuatro tipos fundamentales de instrumentos de acción pública que permiten analizar cómo el gobierno interviene para atender un problema público:

El primer tipo corresponde a los instrumentos normativos. Estos comprenden todas aquellas normas legales, desde constituciones hasta reglamentos, que regulan la intervención de la autoridad pública en los asuntos públicos. Estos establecen el marco legal bajo el cual se desarrollará la acción gubernamental.

El segundo tipo son los instrumentos organizativos, que se refieren a las estructuras públicas o mixtas creadas o modificadas para la acción pública en un ámbito específico. Estas pueden ser desde secretarías de Estado hasta órganos autónomos, donde diversos actores (públicos y privados) colaboran en la atención de los problemas públicos.

En tercer lugar encontramos los instrumentos programáticos, que son los documentos gubernamentales que orientan y delimitan la acción pública en un periodo determinado. Incluyen tanto planes, que proporcionan un marco general de acción y justifican la intervención gubernamental, como programas específicos que establecen objetivos, acciones y recursos necesarios para atender aspectos particulares del problema.

El cuarto tipo corresponde a los instrumentos financieros, que son aquellos mecanismos que movilizan recursos económicos, tanto públicos como privados, nacionales o internacionales, para implementar las acciones gubernamentales y alcanzar los objetivos planteados.

En esta investigación, estos instrumentos serán utilizados para resolver el objetivo central y resolver parcialmente el primer objetivo específico.

1.2 Una política pública de ciberseguridad

La política de ciberseguridad carece de una definición fija entre la literatura especializada. Esta ausencia de consenso se deriva tanto de la naturaleza abstracta inherente a toda política pública como de la complejidad que añade la dimensión de ciberseguridad. No obstante, es posible construir una comprensión de esta política mediante la evolución del papel del Estado frente a las amenazas cibernéticas.

Fonfría (2020) identifica una evolución que se manifiesta en dos funciones del Estado en ello: primero, el Estado como propietario de redes e infraestructura de información que requieren protección; y segundo, como actor responsable de resolver los problemas de seguridad digital desde una perspectiva de política de seguridad.

Esta evolución implicó que las nuevas funciones no sustituyeron a las anteriores sino que se agregaron, incrementando la complejidad del ámbito. Por lo que la ciberseguridad puede ser entendida como:

> Colección de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, garantía y tecnologías que se pueden utilizar para proteger la disponibilidad, integridad y confidencialidad de los activos en las infraestructuras conectadas pertenecientes al gobierno, las organizaciones privadas y los ciudadanos; estos activos incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios digitales, sistemas de telecomunicaciones y datos en el entorno digital. (International Telecommunication Union, 2021)

En el contexto mexicano, esta conceptualización se adaptó al marco institucional del país. El gobierno mexicano, en su Estrategia Nacional de Ciberseguridad de 2017, la definió como el "conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación" (Gobierno de México, 2017a).

Es así como es reflejada la doble dimensión que debe atender una política pública de ciberseguridad. Por un lado, desde la perspectiva de seguridad nacional, el Estado debe garantizar la protección de infraestructuras críticas, aquellas "infraestructuras de información esenciales consideradas estratégicas por estar relacionadas con la provisión de bienes y de prestación de servicios públicos esenciales y cuya afectación pudiera comprometer la Seguridad Nacional" (Gobierno de México, 2017a). Esta protección incluye garantizar la integridad de las redes gubernamentales y los servicios públicos esenciales.

Por otro lado, existe una dimensión de seguridad pública que se desarrolla en el ciberespacio, definido como el "entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico" (Gobierno de México, 2017a).

Este ciberespacio es principalmente Internet, el espacio virtual donde las personas interactúan, realizan transacciones y desarrollan actividades cotidianas. En esta dimensión, el Estado debe establecer mecanismos para proteger a los usuarios, prevenir los ciberdelitos, entendidos por el gobierno mexicano como aquellas "acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional" (Gobierno de México, 2017a), y garantizar el ejercicio seguro de los derechos digitales.

Retomando la clasificación de ciberdelitos de la ONUDC (2013) que clasifica estos actos en tres categorías, podemos ilustrar cómo las diferentes amenazas cibernéticas se relacionan con las dimensiones de seguridad nacional y seguridad pública.

El primer tipo de actos, contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos, se vincula principalmente con la dimensión de seguridad nacional cuando afecta infraestructuras gubernamentales críticas. Un ejemplo de esto fue el hackeo conocido como los *Guacamaya Leaks*, donde un grupo de hacktivistas se infiltró en los sistemas informáticos de la Secretaría de la Defensa Nacional, logrando sustraer 6 terabytes de información confidencial, entre ellos documentos de inteligencia sobre el crimen organizado y registros de salud del Presidente de la República (Latinus_us, 2022).

El segundo tipo, actos informáticos por beneficio financiero o daños personales, corresponde a la dimensión de seguridad pública, pues afecta directamente la integridad patrimonial de los ciudadanos. Por ejemplo, como se mencionó, en México el phishing bancario y el fraude en comercio electrónico han incrementado significativamente: durante 2023 se registraron 6,303 casos de fraude al comercio electrónico y 202 casos de phishing, donde los ciudadanos son engañados mediante correos o sitios web falsos que suplantan la identidad de instituciones bancarias para obtener sus datos personales y financieros (INEGI, 2024).

El tercer tipo, actos informáticos relacionados con el contenido, como la producción y distribución de pornografía infantil o actos que respaldan delitos de terrorismo, también se inscribe en la dimensión de seguridad pública al atentar contra la integridad y dignidad de las personas. En México, durante 2023 se registraron 72 casos de pornografía infantil, fenómeno que ha mostrado una escalada presencia en el entorno digital, así como 277 casos de acoso contra menores de edad y 114 casos de ciberbullying (INEGI, 2024). Esta diversidad de amenazas cibernéticas requiere que el Estado desarrolle respuestas igualmente complejas.

1.3 Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos

El marco analítico desarrollado por Bustos y Aguerre (2022) es una herramienta metodológica diseñada específicamente para el análisis de políticas públicas de ciberseguridad en estados latinoamercanos, tomando una perspectiva de los ciberdelitos y la ciberdefensa considerando su relación con la gobernanza amplia de la ciberseguridad a nivel nacional. El principal objetivo de este marco es:

> Ofrecer un marco analítico integrado para un análisis comprensivo de las políticas públicas sobre ciberseguridad en los países bajo estudio, entendiendo a estas en un sentido amplio (es decir, considerando a las problemáticas asociadas de los ciberdelitos y la ciberdefensa como ámbitos de incumbencia estatal diferenciados pero involucrados en una noción amplia de la gobernanza de la ciberseguridad). (Bustos y Aguerre, 2022, pág. 4)

Si bien no menciona explícitamente las dimensiones de seguridad pública y defensa nacional, estas se reflejan en su definición de la gobernanza de la ciberseguridad, como los ciberdelitos vinculados a las políticas de seguridad pública, ya que abordan la prevención, investigación

y sanción de actividades ilegales en el ciberespacio; mientras que la ciberdefensa con las de defensa nacional, enfocándose en la protección del Estado frente a ciberataques que amenazan su seguridad y estabilidad (Bustos y Aguerre, 2022, pág. 4).

La propuesta de Bustos y Aguerre (2022) es "considerar a la ciberseguridad, el ciberdelito y la ciberdefensa como ámbitos de incumbencia estatal diferenciados, pero involucrados en una noción amplia de la gobernanza de la ciberseguridad (pág. 4)". Esta diferenciación hace que no se limite solo a solo a dos dimensiones de seguiridad, sino a "considerar que el problema de la ciberseguridad como objeto de la política pública se encuentra atravesado por diversas dimensiones que atraviesan el aparato estatal tanto en sus múltiples funciones como en sus diversas jurisdicciones. Tanto técnica como prácticamente, el asunto presenta cruces con aspectos de defensa nacional, infraestructura crítica, desarrollo de capacidades (organizativas e individuales), prevención e investigación de ciberdelitos, y relaciones diplomáticas, entre otros asuntos (pág. 4)".

La gobernanza de la ciberseguridad se presenta, por lo tanto, como un ente multidimensional que abarca la seguridad pública como la defensa nacional, pero también reconoce la importancia de otros factores como la cooperación internacional y la ciberdiplomacia, la cual Bustos y Aguerre (2022) la entienden como un mecanismo diplomático orientado a establecer normas y fomentar la cooperación en el ciberespacio; así como el desarrollo de capacidades para enfrentar las amenazas cibernéticas de manera efectiva.

En segundo lugar, Bustos y Aguerre (2022, pág. 4) propone el concepto de "senderos de desarrollo institucional", definido como las trayectorias que siguen los países en su evolución hacia la mejora de sus capacidades en ciberseguridad. En lugar de simplemente medir el progreso a través de índices de madurez, su enfoque se concentra en entender las dinámicas que explican la formación de las preferencias institucionales para la construcción de capacidades.

Estas preferencias institucionales son concebidas por Bustos y Aguerre (2022, pág. 5) dentro dentro del ámbito de la gobernanza del ciberespacio y las políticas de ciberseguridad en dos niveles: en las posiciones que los estados adoptan en materia de ciberdiplomacia internacional y en los diseños institucionales de sus políticas nacionales de ciberseguridad.

En este sentido, el marco analítico también tiene como objetivo:

> Brindar herramientas para un análisis situado de los senderos de desarrollo institucional adoptados en materia de ciberseguridad en el nivel nacional, indagando tanto en las dinámicas que explican los procesos de formación de preferencias como en aquellas que explican los procesos de construcción de capacidades. (Bustos y Aguerre, 2022, pág. 4)

Para operacionalizar los objetivos planteados, Bustos y Aguerre (2022) proponen iniciar con un análisis descriptivo inicial que permita identificar y comprender las dinámicas institucionales y normativas relacionadas con la ciberseguridad, considerando los ciberdelitos y la ciberdefensa. Este análisis se estructura en torno a seis componentes como se detalla en la Tabla 2, y de los cuales cada uno cuenta con un método de representación gráfica que facilita su comprensión.

En primer lugar, el mapeo de actores busca identificar los organismos federales, nacionales o reginonales involucradas los ámbitos de la ciberseguridad, los ciberdelitos y la ciberdefensa; y aquellas que actúan como puentes entre más de un área. Este componente responde preguntas relacionadas con su participación, coordinación y roles específicos.

En segundo lugar, las trayectorias institucionales se abordan mediante la descripción histórica de la creación y evolución de organismos públicos, normativas y programas enfocados en el desarrollo de capacidades, incluyendo instrumentos de cooperación internacional y público-privada, permitiendo documentar cambios estructurales a lo largo del tiempo mediante líneas de tiempo específicas para los ámbitos de ciberseguridad, ciberdelitos y ciberdefensa.

El tercer componente se centra específicamente en materia de la normativa nacional, que incluye el mapeo de leyes específicas e indirectamente relacionadas con ciberseguridad, ciberdelitos y ciberdefensa. El cuarto componente se centra en la recopilación de las definiciones conceptuales usadas por los organismos estatales, como “ciberseguridad”, “ciberdelito” o “infraestructuras críticas”.

En quinto lugar, se recopilan las estrategias nacionales existentes, considerando su enfoque, procesos de consulta, diseño institucional, objetivos y prioridades, su aplicación y asignación de recursos. Finalmente, se examina la cooperación internacional y los alineamientos

geopolíticos en materia de ciberseguridad, identificando las influencias normativas provenientes de organismos internacionales, estándares de cooperación, y el grado de alineamiento entre preferencias nacionales y directrices internacionales.

Tabla 2. Análisis descriptivo inicial del Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos

Componente	Descripción
a. Mapeo de actores	• Identificación de actores estatales en políticas de ciberseguridad, ciberdelitos y ciberdefensa. • Todos los actores formales y un diagnóstico realista de los actores efectivamente involucrados. • Enfoque en niveles nacional, federal y regional. • Análisis de participación en gobernanza, formación de preferencias y la construcción de capacidades. • Consideración de los mecanismos de coordinación interinstitucional y la identificación de actores que funcionan como puente entre ámbitos. • Estudio de senderos de desarrollo institucional. • Realización de un diagrama de Venn de tres conjuntos.
b. Trayectorias institucionales	• Evolución histórica de trayectorias institucionales en ámbitos de ciberseguridad, ciberdelitos y ciberdefensa. • Documentación de creación y modificación de organismos públicos. • Registro de desarrollo normativo general y específico. • Seguimiento de instrumentos de cooperación internacional y público-privados. • Identificación de programas de desarrollo de capacidades. • Realización de tres líneas de tiempo paralelas (una por ámbito).
c. Normativa nacional	• Mapeo completo del marco normativo en los tres ámbitos. • Diferenciación entre normativas específicas y vinculadas. • Identificación de impactos directos e indirectos en la gobernanza de la ciberseguridad. • Alcance y profundidad del marco regulatorio. • Creación de un cuadro de múltiple entrada.
d. Definiciones conceptuales	• Análisis de definiciones oficiales: ciberespacio, ciberseguridad, ciberdefensa, ciberdelitos y ciberdiplomacia.

	• Examen específico de conceptos de infraestructura crítica y sus variantes. • Identificación de fuentes oficiales e influencias internacionales. • Documentación de variaciones conceptuales entre organismos. • Identificación de riesgos y contramedidas establecidas.
e. Estrategias nacionales	• Identificación de estrategias existentes. • Revisión de procesos de consulta para su creación. • Revisión del diseño institucional propuesto. • Revisión de prioridades y objetivos establecidos. • Revisión de la efectividad en implementación. • Revisión de los recursos asignados y una determinación de la acordancia a los objetivos establecidos.
f. Ciberdiplomacia	• Identificación de la diplomacia normativa y el alineamiento con instrumentos internacionales. • Análisis de influencia de organismos internacionales (ONU, OEA). • Creación de una tabla de múltiple entrada por ámbito de aplicación (ciberseguridad, ciberdelitos y ciberdefensa).

Fuente: Elaboración propia con información de Bustos y Aguerre (2022).

Después de realizar el análisis inicial, Bustos y Aguerre (2022) proponen continuar con el análisis de preferencias institucionales, basado en cinco categorías binomiales que permiten observar cómo las decisiones institucionales pueden clasificarse según diferentes enfoques descritas en la Tabla 3.

La primera variable considerada es el protagonismo institucional. Aquí se distingue entre el liderazgo ejercido por agencias con un mayor rol político como ministerios (secretarías de Estado para el caso mexicano) o jefaturas de gabinete, y aquellas con un rol más técnico como agencias especializadas o ministerios de modernización.

La segunda variable corresponde al enfoque de la ciberseguridad, que puede ser limitado o extensivo. Un enfoque limitado se centra exclusivamente en la tipificación penal de los delitos cometidos en el ciberespacio, mientras que un enfoque extensivo abarca también la prevención y la resiliencia, incluyendo la protección de infraestructuras críticas.

Las políticas asociadas a la respuesta ante incidentes informáticos constituyen la tercera variable. Estas políticas pueden adoptar un enfoque multisectorial, que promueva la cooperación público-privada, o un enfoque gubernamental, en el que la gestión de incidentes queda exclusivamente en manos del Estado, con nula participación del sector privado.

La cuarta variable es el enfoque de las políticas de protección de infraestructuras críticas, que sigue una lógica similar. Se distinguen aquellas políticas con un enfoque multisectorial, donde el sector privado participa activamente en la formulación de normativas, frente a un enfoque gubernamental, en el que la normativa y la implementación dependen únicamente de organismos estatales.

Finalmente, el alineamiento internacional en materia de ciberdelitos constituye la quinta variable. Se considera el alineamiento con los estándares promovidos por Occidente (Estados Unidos y la Unión Europea), como el Convenio de Budapest, y aquellos impulsados por China y Rusia en los acuerdos de la Organización para la Cooperación de Shanghái.

Tabla 3. Análisis de preferencias según categorías binominales del marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos

Variable	Categoría 1	Indicador	Categoría 2	Indicador
Organismo coordinador de las políticas de ciberseguridad	Agencia estatal con rol político	Ministerio de Seguridad, Defensa, Jefatura de Gabinete o cualquier agencia con peso político en decisiones de ciberseguridad.	Agencia estatal con rol técnico	Ministerio de Modernización o agencia técnica especializada con autonomía administrativa y experiencia técnica específica en ciberseguridad.
Enfoque de la ciberseguridad	Tipificación penal de delitos en el ciberespacio	Políticas centradas únicamente en la sanción de delitos cibernéticos.	Prevención y resiliencia	Políticas que, además de tipificar delitos, se orientan a la prevención, fortalecimiento institucional y protección de infraestructuras críticas.
Enfoque de las políticas asociadas a las respuestas ante	Enfoque multisectorial	Participación del sector privado y otras partes interesadas en la definición de	Enfoque gubernamental	Estrategias exclusivamente gubernamentales; coordinación de incidentes bajo

incidentes informáticos:		estrategias de respuesta a incidentes; fomento del intercambio de información.		organismos estatales sin participación de actores privados o internacionales.
Enfoque de las políticas asociadas a la protección de la infraestructura crítica	Enfoque multisectorial	Presencia de mecanismos formales de consulta pública y participación privada en la formulación de normativa sobre infraestructuras críticas.	Enfoque gubernamental	Normativas elaboradas exclusivamente por el sector estatal; exigencia de localización de datos dentro del país para prestadores de servicios de infraestructura.
Alineamiento internacional en materia de ciberdelitos	Alineamiento con el Consejo de Europa	Ratificación del Convenio de Budapest; alineamiento con estándares regulatorios de la Unión Europea o Estados Unidos.	Alineamiento con la Organización para la Cooperación de Shangai	Ratificación de acuerdos de la Organización para la Cooperación de Shanghái; alineamiento con estándares regulatorios promovidos por China y Rusia.

Fuente: Elaboración propia con información de Bustos y Aguerre (2022).

Después, Bustos y Aguerre (2022) proponen realizar el análisis de capacidades, "usando una serie de indicadores empíricos para evaluar el grado de desarrollo de capacidades en cada ámbito de aplicación" (pág. 13), divididos en los ámbitos de ciberdelitos y la ciberseguridad enfocado a las respuestas a incidentes informáticos y a la protección de infraestructuras criticas (Tabla 4).

La propuesta metodológica no parte de una secuencia lineal o de etapas de maduración predeterminadas, ya que, según los autores, este tipo de enfoques suele asumir un desarrollo tecnológico de las capacidades, lo que limita la comprensión de la complejidad de estos procesos.

En cambio, el modelo se apoya en variables de intervalo que permiten medir el grado de maduración, cuyos extremos corresponden a capacidades iniciales y capacidades avanzadas. Es importante señalar que este análisis no mide la eficacia con la que dichas capacidades son implementadas, sino únicamente su nivel de desarrollo en términos de su existencia y características formales.

A través de estos indicadores definidos, se busca determinar cuán cerca se encuentra cada caso de uno u otro extremo. Por ejemplo, si en el ámbito de ciberdelitos se identifican tres de los diez indicadores propuestos, se concluirá que el caso se encuentra en un estado más cercano al desarrollo inicial que al avanzado, al cumplir únicamente una fracción del total esperado.

Tabla 4. Análisis de capacidades del marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos

Variable	**Indicadores**
A. Ciberdelitos	1. Existencia de normativa específica relativa a ciber-delitos. 2. Existencia de normativa específica relativa a actividades ciber-terroristas. 3. Existencia de un organismo de coordinación con la misión y la autoridad principal de velar por el cumplimiento de la normativa relativa a ciber-delitos. 4. Existencia de mecanismos de cooperación y coordinación entre los ministerios y las agencias nacionales afectados al combate al ciber-delito. 5. Ratificación de acuerdos internacionales vinculados a la delincuencia cibernética. 6. Existencia de mecanismos de cooperación implementados entre agencias estatales y organismos internacionales en materia de ciber-delito. 7. Existencia de los mecanismos de cooperación implementados entre agencias estatales y organismos internacionales en materia de ciber-terrorismo. 8. Participación en negociaciones de acuerdos internacionales vinculados a la delincuencia cibernética. 9. Existencia de programas de fortalecimiento institucional de los organismos encargados de velar por la aplicación de la normativa relativa a ciber-delitos. 10. Existencia de mecanismos de capacitación de personal especializado en la administración de justicia, así como de incentivos para la profesionalización de dicho personal.
B. Ciberseguridad: respuestas a	1. Existencia de normativa nacional relativa a incidentes informáticos y emergencias de seguridad cibernética. 2. Existencia de un registro central de incidentes cibernéticos a nivel nacional.

incidentes informáticos	3. Si existe un registro central de incidentes cibernéticos a nivel nacional, sus prioridades reciben actualizaciones regulares y sistemáticas de acuerdo con la evolución del entorno de amenazas. 4. Existencia de un CSIRT nacional para la gestión de respuesta a incidentes. 5. Existencia de un registro claro y transparente de los directores de incidentes en cada agencia y ministerio a nivel nacional. 6. Existencia de un CSIRT para la gestión de respuesta a incidentes en el sector público. 7. Existencia de un mecanismo para identificar las dependencias intersectoriales con el objeto de garantizar tanto la continuidad de las operaciones como los mecanismos de recuperación de desastres. 8. Existencia de un sistema de alerta temprana disponible para su utilización por los CSIRT sectoriales. 9. Existencia de un plan nacional de respuesta a incidentes informáticos orientado a garantizar una respuesta coordinada, con líneas de comunicación, procesos, funciones y responsabilidades claras y definidas. 10. Existencia de una Estrategia Nacional de Ciberseguridad de aplicación efectiva donde se articula un plan nacional de respuesta a incidentes informáticos con el resto de las prioridades emanadas de dicha estrategia. 11. Si existe una Estrategia Nacional de Ciberseguridad, se encuentra evidencia de que sus objetivos relativos a las respuestas a incidentes informáticos se ponen en aplicación, y se actualizan de forma regular. 12. Existencia de un canal de contacto entre el sector público y las organizaciones del sector privado que han sido oportunamente identificadas como actores clave para la ciberseguridad nacional, existan o no mecanismos formales de coordinación o de intercambio de información. 13. Existencia de una estructura institucional, con la autoridad competente y un mandato específico, que vele por la transferencia de información fidedigna entre las diversas agencias estatales y las industrias críticas, así como la cooperación en materia de análisis de incidentes y apoyo. 14. Existencia de un mecanismo para poner a prueba la resiliencia de la nación ante los incidentes informáticos y las crisis de ciberseguridad, el cual supone al menos un escenario de ejercicio simple, con un ámbito geográfico específico, así como recursos y coordinación limitados, y en cuyo planeamiento participa una cantidad limitada de actores clave. 15. Si existe el mecanismo aludido en el punto anterior, el programa de ejercicio que dispone: plantea un escenario complejo tanto términos técnicos como políticos, un alcance geográfico amplio, la participación de múltiples partes interesadas (incluyendo observadores internacionales), el

	abordaje de desafíos internacionales, la participación y la producción de objetivos mensurables y resultados escalables para el desarrollo de políticas y la toma de decisiones de carácter estratégicas. 16. Existencia de mecanismos de investigación orientados a identificar y analizar las tendencias de incidentes de ciberseguridad de preocupación nacional. 17. Existencia de mecanismos de cooperación internacional (ya intergubernamental, ya multisectorial) para el intercambio de información de vulnerabilidades, incidentes o soluciones. 18. Existencia de un mecanismo de cooperación con la comunidad internacional que facilita la participación del país en ejercicios internacionales de gestión de crisis.
C. Ciberseguridad: protección a infraestructuras críticas	1. Existencia de normativa nacional específicamente relativa a la protección de la Infraestructura Crítica Nacional (ICN). 2. Si se fomenta la auto-regulación, se han establecido directrices sobre mejores prácticas cibernéticas de ICN y medidas de seguridad mínimas. 3. Existencia de un registro de activos de la ICN, háyanse identificado o no las prioridades y dependencias de estos. 4. Si existe un registro de activos de la ICN, este cuenta con la identificación y el mapeo de dependencias intersectoriales que aborden la continuidad de las operaciones y los mecanismos de recuperación de desastres. 5. Evidencia de que se realiza de forma regular una auditoría de los activos de la ICN y de que la lista de prioridades de los activos se reevalúa regularmente para adaptarse a los cambios en el entorno de amenazas. 6. Existencia de un mapa de riesgos que podrían afectar a la ICN donde se identifiquen claramente las amenazas, las probabilidades de ocurrencia de los incidentes y sus impactos potenciales, y el cual guía las inversiones estratégicas adoptadas por el Estado. 7. Existencia de un organismo estatal de coordinación con la misión y la autoridad principal de velar por la protección de la ICN, el cumplimiento de la normativa relativa a la misma y la transmisión de información fidedigna a las demás agencias gubernamentales y actores clave de la ICN. 8. Existencia de una red de puntos de contacto nacionales autorizadas para industrias críticas que son esenciales para el funcionamiento y la recuperación de los servicios e infraestructuras críticas. 9. Existencia de mecanismos de cooperación y coordinación entre los ministerios y las agencias nacionales afectados a la protección de la ICN. 10. Evidencia de un diálogo regular entre los niveles ejecutivos estratégicos y tácticos respecto de las prácticas de ciberseguridad para la protección de la ICN.

	11. Existencia de mecanismos de coordinación intersectorial y transversal de partes interesadas para abordar interdependencias críticas, y/o la elaboración de normas relativas a la protección de ICN, y/o para determinar qué industrias y organismos son críticos para el ecosistema cibernético nacional. 12. Existencia de un mecanismo entre el sector público y privado para la divulgación periódica de vulnerabilidades de la ICN. 13. Evidencia de que existe una clara asignación de responsabilidades y obligaciones por parte del Estado entre los propietarios y operadores de los activos de la ICN. 14. Existencia de un mecanismo para la desclasificación oportuna de información de inteligencia relacionada con la ICN para su intercambio con diversas áreas de gobierno e industrias críticas. 15. Evidencia de que realizan ejercicios para prepararse para un evento que ponga en riesgo la ICN y para evaluar regularmente su resiliencia. 16. Evidencia de que se realizan evaluaciones de la gravedad de incidentes relacionados con activos de la ICN y de que la planeación de la respuesta futura se basa en dicha evaluación. 17. Existencia de un mercado de seguros para la ciberseguridad de los activos afectados a la ICN. 18. Evidencia de que se han explorado opciones para el reaseguro para apoyar la continuidad del negocio de la ICN. 19. Evidencia de avances en materia de capacitación de cuadros técnicos para la gestión de la seguridad de la ICN. 20. Evidencia de un alineamiento de los estándares nacionales con los estándares más difundidos en la comunidad internacional.

Fuente: Elaboración propia con información de Bustos y Aguerre (2022).

Para esta investigación, considerando las restricciones de tiempo y su alcance, se recupera parcialmente el marco analitico de Bustos y Aguerre (2022) con aquello relacionado a la materia de ciberdelitos y segurridad pública, para resolver el segundo objetivo específico (identificar las capacidades institucionales desarrolladas para implementar la política de ciberseguridad en México) y complementar a resolver el primero (identificar las acciones de política desarrolladas por el gobierno de Andrés Manuel López Obrador para atender la problemática de la seguridad cibernética en materia de seguridad pública en México).

La presente investigación adopta y adapta el marco analítico propuesto por Bustos y Aguerre (2022) para evaluar las capacidades institucionales en ciberseguridad, con el fin de ajustarlo

a las particularidades del contexto mexicano y a los objetivos específicos del estudio. Esta adaptación se fundamenta en tres ejes metodológicos: la integración de indicadores originales bajo preferencias institucionales redefinidas, la creación de nuevas preferencias institucionales para abordar vacíos identificados y la operacionalización de los indicadores cuantificables que permitan una evaluación estructurada. De igual forma se recuperó la valoración de los indicadores que proponen Bustos y Aguerre (2022).

La Tabla 5 detalla la articulación entre estos elementos, vinculando indicadores, preferencias y valores asignados, mientras que la Tabla 6 despliega la matriz final de evaluación, donde se contrastan las capacidades gubernamentales identificadas con las preferencias institucionales propuestas.

El primer eje de adaptación consistió en agregar nuevas preferencias para superar las limitaciones del marco original. Inicialmente, las variables y preferencias institucionales no consideraban la posibilidad de su ausencia, por lo que se incorporó esta opción en cada una de ellas. Además, las preferencias institucionales originales *"Enfoque de las políticas asociadas a las respuestas ante incidentes informáticos"* y *"Enfoque de las políticas asociadas a la protección de la infraestructura crítica"*, fueron conjuntadas para describir integralmente el *"Enfoque de las políticas asociadas a las respuestas ante incidentes informáticos, a la protección de la infraestructura crítica y a la persecución del ciberdelito"*. Por último, se modificó el indicador que evaluaba la existencia de un organismo técnico o autónomo, reemplazándolo por indicadores que reflejan cómo están estructurados estos organismos dentro del Estado.

El segundo eje implicó vincular los indicadores originales del marco de referencia con las preferencias institucionales redefinidas. Por ejemplo, la variable *"Estructura organizacional en ciberseguridad"* se evaluó mediante el indicador #3 (*"Existencia de un organismo de coordinación..."*), el cual permite determinar si las responsabilidades recaen en una entidad única o en múltiples instituciones. Esto derivó en la creación de la preferencia como *"andamiaje organizacional fragmentado"* (para casos con múltiples organismos sin liderazgo centralizado) y *"andamiaje organizacional centrado en un organismo rector"* (para estructuras jerárquicas unificadas).

Tabla 5. Articulación de la propuesta para la investigación

Variable	Preferencia institucional	Indicador original de la capacidad institucional	Valor asignado
Estructura organizacional en ciberseguridad	Andamiaje organizacional centrado en un organismo rector	#3	1
	Andamiaje organizacional fragmentado	#3	1
	Ausencia de organismos	-	0
Enfoque de la normativa sobre ciberseguridad	Políticas y marcos jurídicos con enfoque integral	#1 + #2 + #9+ #10	4
	Marco jurídico con enfoque punitivo	#1	1
	Vacío normativo y reactividad	-	0
Enfoque de las políticas asociadas a las respuestas ante incidentes informáticos, a la protección de la infraestructura crítica y a la persecución del ciberdelito	Enfoque multisectorial	#4 + #6 + #7	3
	Enfoque gubernamental	#4	1
	Ausencia de enfoque definido	-	0
Cooperación Internacional	Alineamiento con el Consejo de Europa	#5 + #8	2
	Alineamiento con la Organización para la Cooperación de Shangai	#5 + #8	2
	Alineamiento nacional con otros acuerdos internacional en materia de ciberseguridad y ciberdelitos	#5 + #8	2
	Sin alineamiento internacional	-	0

Fuente: Elaboración propia

El tercer eje metodológico implicó la traducción de los hallazgos cualitativos en una matriz de evaluación cuantitativa. Cada preferencia institucional se asoció a valores numéricos específicos, determinados por el cumplimiento de los indicadores vinculados. Por ejemplo, la preferencia "*políticas y marcos jurídicos con enfoque integra*l" asigna 4 puntos si se verifica la existencia de normativa contra ciberdelitos (#1), medidas ante ciberterrorismo (#2), programas de fortalecimiento institucional (#9) y capacitación especializada (#10).

Teniendo una matriz final de evaluación con una puntuación máxima de 10, donde esta es capacidades avanzadas y el 0 capacidades iniciales en materia de ciberseguridad y ciberdelitos.

Tabla 6. Matriz de evaluación preferencias institucionales y de capacidades

Variable	Preferencia institucional	Indicadores de las capacidades institucionales mexicanas	Valor
Estructura organizacional en ciberseguridad	Andamiaje organizacional centrado en un organismo rector	Existe una única secretaría de Estado u organismo (con o sin autonomía administrativa y presupuestal, de enfoque técnico o político) encargado de implementar y ejecutar políticas de ciberseguridad y tareas operativas.	1
	Andamiaje organizacional fragmentado	Existen múltiples secretarías de Estado u organismos (con o sin autonomía, técnicos o políticos) que implementan políticas de ciberseguridad, sin que exista un ente único designado como responsable principal.	1
	Ausencia de organismos estatales	No existe una secretaría de Estado u organismo designado responsable de las políticas de ciberseguridad nacionales.	0
Enfoque de la normativa sobre ciberseguridad	Políticas y marcos jurídicos con enfoque integral	Existencia de normativas que, además de castigar ciberdelitos, establecen medidas preventivas, requisitos de seguridad para organizaciones, programas de fortalecimiento institucional y protección de infraestructuras críticas.	4
	Marco jurídico con enfoque punitivo	Existencia de normativas centradas exclusivamente en el castigo de ciberdelitos, sin considerar medidas preventivas o de fortalecimiento institucional.	1
	Vacío normativo y reactividad	No existe legislación específica ni políticas públicas en materia de ciberseguridad; las acciones estatales se limitan a respuestas reactivas ante incidentes graves sin estrategias estructuradas	0
Enfoque de las políticas asociadas a las respuestas ante incidentes informáticos, a la protección de la infraestructura crítica y a la persecución del ciberdelito	Enfoque multisectorial	Existencia de políticas públicas contemplando la participación del sector público y privado y otras partes interesadas en para la respuesta a ciberincidentes, intercambio de información, protección de infraestructuras críticas y el combate al ciberdelito.	3
	Enfoque gubernamental	Existencia de políticas públicas exclusivamente gubernamentales para la respuesta a ciberincidentes, intercambio de información, protección de infraestructuras críticas y el combate al ciberdelito sin participación de actores privados.	1
	Ausencia de enfoque definido	No existen políticas definidas para la respuesta ante incidentes informáticos y el combate al ciberdelito.	0

Cooperación Internacional	Alineamiento con el Consejo de Europa	Ratificación del Convenio de Budapest; alineamiento con estándares regulatorios de la Unión Europea o Estados Unidos.	2
	Alineamiento nacional con otros acuerdos internacional en materia de ciberseguridad y ciberdelitos	Adhesión nacional a otros acuerdos internacionales con estándares específicos en materia de ciberdelitos y ciberseguridad.	2
	Sin alineamiento internacional	El Estado no suscribe acuerdos internacionales específicos en materia de ciberdelitos y ciberseguridad	0

Fuente: Elaboración propia

Capítulo 2. Evolución histórica de la política de ciberseguridad en México (2012-2018)

Este capítulo recupera y se describe la evolución de la política de ciberseguridad en México durante la administración de Enrique Peña Nieto (2012-2018), estableciendo el marco institucional que heredaría posteriormente el gobierno de Andrés Manuel López Obrador.

El contexto histórico de la política nacional ciberseguridad en México comienza en este sexenio, ya que fue durante el gobierno de Peña Nieto cuando se incorporó por primera vez el problema de la ciberseguridad en la agenda gubernamental, implementando las primeras acciones para su atención. Este periodo marcó el reconocimiento formal de la ciberseguridad como una prioridad nacional y sentó las bases para las políticas y estrategias que se implementarían posterirmente.

Esta revisión histórica identifica los actores gubernamentales involucrados y la evolución normativa e institucional durante este periodo, sentando las bases para comprender el punto de partida de la administración siguiente.

2.1 El surgimiento de la ciberseguridad en la agenda gubernamental mexicana

El primero de diciembre de 2012, Enrique Peña Nieto asumió la presidencia de México marcando el regreso del Partido Revolucionario Institucional (PRI) a la presidencia después de 12 años. Su transición presidencial estuvo enmarcada por una compleja situación de inseguridad pública, heredada de una estrategia de combate frontal al narcotráfico, pero durante los primeros días de su gobierno, Peña Nieto logró concretar el *Pacto por México*, un acuerdo político firmado el 2 de diciembre de 2012 en el Castillo de Chapultepec con las principales fuerzas políticas del país (PRI, PAN y PRD) para impulsar reformas estructurales en diversos sectores, incluyendo telecomunicaciones y seguridad (Herrera y Urrutia, 2012).

En este contexto, el Plan Nacional de Desarrollo 2014-2018 (PND a partir de ahora) desarrollado por el gobierno del presidente Peña Nieto, planteó una visión integral sobre la

transformación digital del gobierno, reconociendo tanto las oportunidades como los riesgos que presentaban las nuevas tecnologías.

En este Plan de Desarrollo, la ciberseguridad emergió dentro del objetivo 1.2 "Garantizar la Seguridad Nacional", una de sus estrategias estableció la necesidad de "fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la Seguridad Nacional" (Diario Oficial de la Federación, 2013).

Esta estrategia estableció diez líneas de acción, siendo cuatro asociadas a la ciberseguridad. La primera de ellas mandató integrar una agenda de Seguridad Nacional que identificara amenazas y riesgos nacionales e internacionales contra los objetivos e intereses nacionales estratégicos. La segunda, instruyó impulsar iniciativas de ley para fortalecer lo que se denominó "la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad" (Diario Oficial de la Federación, 2013). Tercero, ordenó diseñar y operar un Sistema Nacional de inteligencia civil que permitiera la interconexión de bases de datos nacionales. Y el cuarto, mandató diseñar e impulsar una estrategia de seguridad de la información para garantizar la integridad, confidencialidad y disponibilidad de la información de personas e instituciones públicas y privadas en México.

Es decir, por primera vez en la historia gubernamental de México, el gobierno federal reconoció en su agenda institucional las dimensiones de la ciberseguridad en la defensa nacional y en la seguridad pública.

2.2 La limitada Estrategia Digital Nacional 2013-2018

Seis meses después de la publicación del PND, en noviembre de 2013, el presidente presentó la Estrategia Digital Nacional 2013-2018 (EDN a partir de ahora), un plan de acción federal para “fomentar la adopción y el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) e insertar a México en la Sociedad de la Información y el Conocimiento” durante esos últimos cinco años de la administración peñista y coordinada por la Coordinación de Estrategia Digital Nacional, un órgano adscrito a la Oficina de la Presidencia (Secretaría de Gobernación, 2013, p. 9).

Esta estrategia surgió como resultado de esfuerzos previos tanto públicos como privados, incluyendo la Secretaría de Comunicaciones y Transportes y diferentes cámaras de comercio de telecomunicaciones (la Asociación Mexicana de la Industria de Tecnologías de Información, A.C.; la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información, Sector Electrónico y de Telecomunicaciones; y la Fundación México Digital), para generar ese acercamiento de la sociedad a la tecnología (Cruz, 2015).

La EDN se concibió y diseñó abarcando diversas áreas estratégicas como la educación, la salud y la economía, con el propósito de impulsar su desarrollo en materia tecnológica y digital. Para cumplir con sus objetivos, se identificaron una serie de condiciones fundamentales conocidas como "habilitadores transversales". Estos habilitadores representarían herramientas esenciales para orientar las acciones de la estrategia y garantizar la viabilidad de sus metas.

Entre estos elementos se encontraba la conectividad, orientada a garantizar el acceso a internet mediante el desarrollo de infraestructura y la competencia en el sector de las TIC; la inclusión y las habilidades digitales, dirigidas a reducir la brecha tecnológica a través de la capacitación; la interoperabilidad e identidad digital, que facilitarían la integración de sistemas y el acceso seguro a servicios públicos; un marco jurídico actualizado, necesario para regular y proteger derechos en el entorno digital; y los datos abiertos, concebidos como una herramienta clave para fomentar la transparencia, el acceso a la información y la participación ciudadana .

Sin embargo, uno de los aspectos más criticados de la Estrategia Digital Nacional fue la ausencia de un habilitador dedicado específicamente a la ciberseguridad en materia de seguridad pública (Islas, 2018). A pesar de que la estrategia buscaba impulsar la adopción tecnológica en múltiples sectores, desde servicios gubernamentales hasta transacciones comerciales, no contempló las medidas necesarias para proteger a los usuarios en el entorno digital.

Aquel componente de ciberseguridad en el gobierno federal llegaría hasta la publicación de los dos programas nacionales de seguridad publicados un año después en 2014. Por un lado, el Programa Nacional de Seguridad Pública 2014-2018 incorporó elementos para atender los

ciberdelitos que afectaban directamente a la ciudadanía. Por otro lado, el Programa para la Seguridad Nacional 2014-2018 abordó los aspectos relacionados con la protección de infraestructuras críticas y seguridad nacional.

Cabe resaltar que durante esta administración de Enrique Peña Nieto, no existió un registro público o gubernamental sobre los ciberdelitos perpetrados en territorio mexicano. Sin embargo, se documentó que, al inicio de su sexenio en 2012, los ciberdelitos causaron daños a México por un valor de 2 mil millones de dólares, según el estudio de la empresa de ciberseguridad Norton (2012). Para 2016, el mismo estudio reportó que los costos por daños se elevaron a 5.5 mil millones de dólares (Norton, 2016).

2.3 La institucionalización de las dimensiones de ciberseguridad en México

El gobierno federal en sus dos programas nacionales de seguridad, el Programa para la Seguridad Nacional y el Programa Nacional de Seguridad Pública, definieron las dos dimensiones bajo las cuales se abordaría la ciberseguridad en México, estableciendo las bases para una respuesta institucional ante las amenazas digitales.

El primero, el Programa para la Seguridad Nacional 2014-2018, fue el documento guía en la materia de defensa nacional que estableció un enfoque que reconocía, como parte del PND, los riesgos derivados de la transformación del panorama tecnológico como parte de la agenda de seguridad nacional. Su primer objetivo estratégico de "Consolidar el Sistema de Seguridad Nacional", el programa enfatizó la necesidad de atender de manera integral las vulnerabilidades, riesgos y amenazas que surgían del entorno digital (Diario Oficial de la Federación, 2014a).

Reconoció la continuidad operativa del Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), creado en 2012 durante el sexenio de Felipe Calderón bajo la entonces Policía Federal (Noticias 24 Horas, 2012) como parte de los esfuerzos existentes en materia de ciberseguridad. El programa también estableció la necesidad de desarrollar el Sistema Nacional de Inteligencia con productos de inteligencia estratégica, incluyendo aquellos relacionados con las amenazas cibernéticas. Esta visión buscaba que las

instituciones de seguridad y defensa pudieran evaluar oportunamente los desafíos presentes y futuros en el entorno digital (Diario Oficial de la Federación, 2014a).

Por su parte, el Programa Nacional de Seguridad Pública 2014-2018 abordó la dimensión de seguridad pública al incorporar por primera vez la atención a los ciberdelitos en territorio nacional, alineado con los objetivos del PND relacionados con mejorar las condiciones de seguridad pública y garantizar un sistema de justicia eficaz.

Bajo su objetivo de "consolidar una coordinación efectiva para el diseño, implementación y evaluación de la política de seguridad pública", el programa estableció una estrategia de "detectar y atender oportunamente los delitos cibernéticos" (Diario Oficial de la Federación, 2014b). Esta estrategia planteó un abordaje que debería tratarse a través de nueve líneas de acción que cubrían desde el fortalecimiento de capacidades institucionales hasta la protección de infraestructura tecnológica estratégica:

> 2.7.1 Fortalecer las capacidades y la infraestructura tecnológica de las instituciones de seguridad pública para prevenir e investigar delitos cibernéticos.
>
> 2.7.2 Desarrollar investigación científica para la prevención e investigación de los delitos cibernéticos.
>
> 2.7.3 Implementar acciones contra delitos cibernéticos de mayor impacto: pornografía infantil, fraude, extorsión, usurpación de identidad y contra derechos de autor.
>
> 2.7.4 Diseñar protocolos de operación para la prevención de delitos cibernéticos en las instancias que administran información considerada reservada o confidencial.
>
> 2.7.5 Promover la creación y fortalecimiento de unidades especializadas en la prevención e investigación de delitos que se cometen por internet.
>
> 2.7.6 Desarrollar un modelo de policía cibernética para las Entidades Federativas.
>
> 2.7.7 Generar indicadores y estadísticas de delitos informáticos para el diseño de estrategias de prevención.
>
> 2.7.8 Impulsar acciones para consolidar los esquemas de seguridad cibernética que coadyuven al desarrollo de la economía digital.
>
> 2.7.9 Fortalecer la seguridad de la infraestructura tecnológica estratégica del país. (Diario Oficial de la Federación, 2014b)

2.3.1 El Modelo Homologado de Policía Cibernética

En abril de 2016, la Policía Federal en conjunto con el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP a partir de ahora), órgano operativo del Consejo Nacional de Seguridad Pública (máxima instancia de coordinación y definición de políticas públicas en materia de seguridad pública, que es parte del Sistema Nacional de Seguridad Pública e integrada por el Presidente de la República quien lo preside, los Secretarios de Gobernación, Defensa Nacional, Marina, el Procurador General de la República, los Gobernadores de los Estados, el Jefe del Gobierno de la Ciudad de México, el Comisionado Nacional de Seguridad y el Secretario Ejecutivo) realizaron un diagnóstico para medir el nivel de madurez de las Policías Estatales en materia de seguridad cibernética, evaluando sus legislaciones, sus recursos humanos, el equipamiento e infraestructura, la operación y los mecanismos control (Gobierno de México, s.f.).

Los resultados arrojaron un panorama desigual en cuanto al desarrollo de capacidades estatales. En el vector de legislación, se identificó que solo 17 de las 32 entidades federativas contaban con una unidad cibernética y un marco normativo adecuado. Ante esta situación, se recomendó fomentar en las 15 entidades restantes las gestiones legislativas necesarias para la creación de dichas unidades cibernéticas.

En cuanto a recursos humanos, se observó un nivel de cumplimiento promedio del 44%, evidenciando una carencia significativa de personal capacitado. Se propuso programar capacitaciones básicas y especializadas en delitos cibernéticos para las unidades estatales, con el fin de homologar los conocimientos técnicos del personal encargado.

Respecto al equipamiento e infraestructura, el diagnóstico reportó un cumplimiento del 38%, destacando que únicamente cuatro entidades federativas disponían del equipamiento necesario para la resolución de delitos cibernéticos. Por tanto, se sugirió implementar acciones orientadas al fortalecimiento de la infraestructura y equipamiento, con el apoyo del SESNSP.

En el vector de operación, se encontró que solo diez entidades contaban con manuales y procedimientos operativos, de los cuales únicamente siete estaban enfocados en la operación cibernética. Ante esta situación, se recomendó realizar reuniones regionales de trabajo e

iniciar la habilitación operativa de las policías cibernéticas estatales, con el objetivo de incrementar el nivel de madurez operativa y avanzar hacia una estandarización en su funcionamiento.

Finalmente, en lo referente a los mecanismos de difusión y control, se identificó la necesidad de generar e implementar indicadores básicos sobre ciberdelitos, lo que permitiría homologar un lenguaje común entre las distintas entidades federativas (SSPC y GN, 2023, pág. 6).

Este diagnóstico permitió establecer una línea base sobre las capacidades institucionales de las unidades cibernéticas estatales, clasificándolas en tres niveles de madurez según su grado de desarrollo operativo en materia de delitos cibernéticos. Además, se incluyeron aquellas entidades que no proporcionaron información y las que declararon no tener competencia en el tema (Mapa 1).

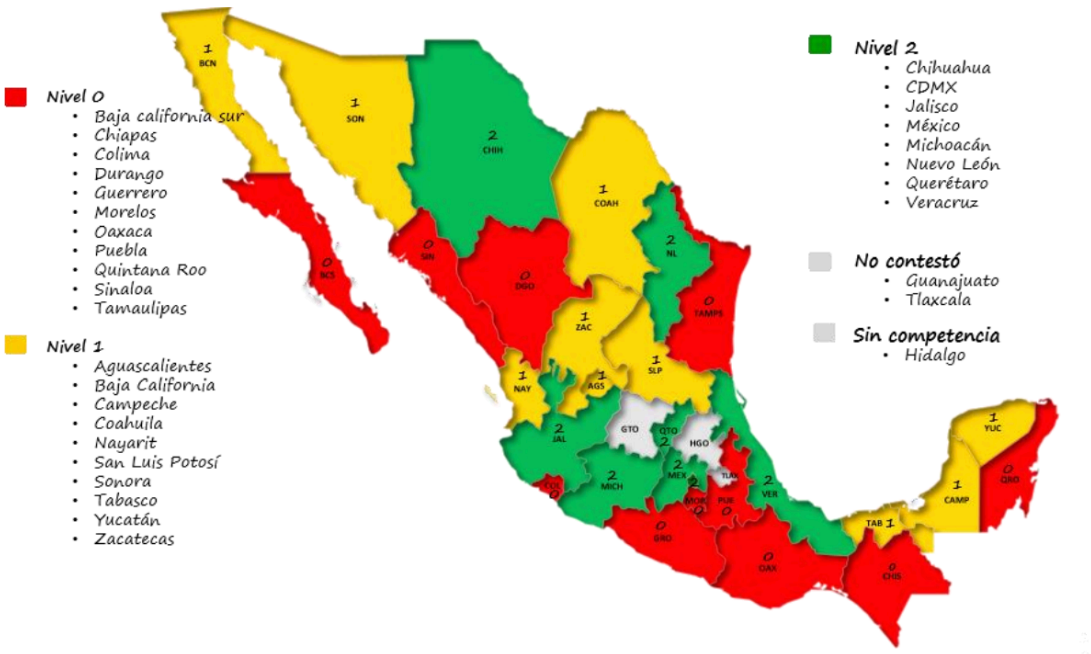
El Nivel 0, correspondiente al 35% de las entidades federativas, agrupó a aquellas que no contaban con una unidad cibernética en funcionamiento. En este nivel se ubicaron Baja California Sur, Chiapas, Colima, Durango, Guerrero, Morelos, Oaxaca, Puebla, Quintana Roo, Sinaloa y Tamaulipas.

El Nivel 1, que representó al 32% de las entidades, incluyeron a aquellas con unidades cibernéticas de operación básica, pero sin procesos documentados ni estructura formal para el tratamiento de delitos cibernéticos. Este grupo lo integraron Aguascalientes, Baja California, Campeche, Coahuila, Nayarit, San Luis Potosí, Sonora, Tabasco, Yucatán y Zacatecas.

El Nivel 2, que abarcó al 25 % de las entidades, incluyeron a las unidades con una operación básica-intermedia y procesos parcialmente repetitivos. Las entidades clasificadas en este nivel fueron Chihuahua, Ciudad de México, Jalisco, Estado de México, Michoacán, Nuevo León, Querétaro y Veracruz.

Adicionalmente, Guanajuato y Tlaxcala no proporcionaron información sobre sus capacidades cibernéticas, e Hidalgo, que se declaró sin competencia en el tema, siendo el restante 8%.

Mapa 1. Madurez por unidades de policía cibernética estatales.



Fuente: Recuperado de SSPC y GN, 2023, pág. 7.

El diseño de un modelo homologado comenzó formalmente en agosto de 2016 con el Acuerdo 12/XL/16 del Consejo Nacional de Seguridad Pública tomó el papel protagónico en el proceso de implementación. Este acuerdo instruyó al Comisionado Nacional de Seguridad, por conducto de la Policía Federal y SESNSP, elaborar el *Modelo Homologado de Unidades de Policía Cibernética* y desarrollar el proceso gradual para su implementación (Gobierno de México, s.f.).

En seguimiento a este acuerdo, el Consejo Nacional de Seguridad Pública aprobó el modelo en su cuadragésima primera sesión ordinaria de diciembre de 2016, en el Acuerdo 06/XLI/16, que formalizó y estableció su implementación obligatoria a partir de 2017, cronológicamente siendo en la última parte de la administración de Peña Nieto, comprometiendo a las entidades federativas a asignar recursos del Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal (FASP) (Gobierno de México, s.f.). Para ello, en el ejercicio de 2017, el FASP contenía recursos para el *Subprograma de Modelo Homologado de las Unidades de Policía.*

En su estructura, el Modelo estableció un esquema para el tratamiento de delitos cibernéticos basado en los procesos de prevención, atención, reacción e investigación, complementados por un proceso transversal de gestión. La prevención se realizaría mediante campañas y capacitación ciudadana, mientras que la atención se centraría en la recepción y canalización de denuncias. El componente de reacción incluiría la identificación y análisis de incidentes de ciberdelitos, complementado por un proceso de investigación que contempla el análisis forense de dispositivos electrónicos y el patrullaje en la red pública. El proceso de gestión, por su parte, garantizaría el registro, clasificación y alertamiento adecuado de todos los casos.

En la parte de su implementación, el Modelo estableció que cada gobierno estatal dependería de su estrategia y estructura de la seguridad pública y procuración de justicia. Para un estado que contara con una Secretaría de Seguridad Pública y una Procuraduría General de Justicia Estatal, se recomendó la implementación de la Policía Cibernética dentro de la Secretaría de Seguridad Pública. En las entidades federativas que ya contaban con una Unidad de Policía Cibernética, el Modelo serviría como base para su reestructuración.

Asimismo, estableció tres niveles progresivos de madurez para las unidades policiales. Estos iniciando con las unidades con capacidades básicas de prevención en el nivel 0, avanzando hacia funciones de atención ciudadana y ciberpatrullaje en el nivel 1, y culminando con el desarrollo de capacidades especializadas de investigación y análisis forense en el nivel 2 (Gobierno de México, s.f). Este esquema gradual permitiría a las entidades federativas desarrollar sus capacidades de manera sistemática según sus recursos y necesidades.

En el caso de que la entidad no contara con una Unidad de Policía Cibernética, era necesario que de manera paralela a su creación e implementación del Modelo, el estado propusiera las medidas legislativas que le permitieran un marco legal apropiado para su funcionamiento.

Como parte del Modelo, se incluyó el diseño un programa de formación para los integrantes de las unidades que contemplaba tres etapas de capacitación: básica, para policías con menos de un año en la Unidad; intermedia, dirigida a personal en activo que requería especialización; y avanzada, para el desarrollo de capacidades técnicas especializadas. Este programa incluía materias desde estrategias de prevención y análisis de amenazas, hasta

temas avanzados como análisis forense, ethical hacking y gestión de seguridad de la información bajo estándares internacionales (Gobierno de México, s.f.).

En materia de infraestructura, el Modelo incluyó una guía de criterios básicos que definía los espacios físicos mínimos requeridos según el nivel de madurez de cada Unidad. La guía recomendaba que las Unidades se ubicaran preferentemente dentro de las instalaciones del Centro de Comando, Control, Comunicación y Cómputo (C4) o su similar en cada entidad federativa. Esta guía consideraba desde espacios básicos como áreas de atención ciudadana, hasta laboratorios especializados de análisis forense para las unidades más avanzadas (Gobierno de México, s.f.).

Sin embargo, después de la publicación del Modelo, no hubo más comunicados ni información oficial por parte de la Presidencia o el gobierno federal dentro del periodo de la administración peñista respecto a su implementación. No obstante, los informes anuales del FASP reflejarón cómo los gobiernos estatales asignanron recursos a sus unidades policiales, asegurando su operación y desarrollo gradual en los años posteriores ya en el periodo de AMLO.

2.3.2 La Estrategia Nacional de Ciberseguridad

Para el año 2017, el gobierno federal inició un proceso para desarrollar la Estrategia Nacional de Ciberseguridad (ENCS a partir de ahora). Este se caracterizó por una serie de consultas y diálogos que involucraron a diversos sectores de la sociedad mexicana, incluyendo organizaciones civiles, empresas privadas, expertos técnicos, académicos y representantes gubernamentales de los tres poderes y niveles de gobierno.

El proceso se inauguró en marzo de 2017 con el lanzamiento de la Campaña Ciberseguridad México 2017 en el C5 de Ecatepec, y continuó con una serie de talleres técnicos organizados en conjunto con la Organización de Estados Americanos (OEA), ente que resultaría relevante en la creación de la estrategia al entregar en junio de ese año, una serie de recomendaciones al gobierno mexicano para su creación durante la Asamblea General de la OEA en Cancún (Gobierno de México, 2017a).

Las sesiones de trabajo ocurrieron en diversas sedes. El Tecnológico de Monterrey Campus Ciudad de México realizó un taller con las partes interesadas en junio, mientras que el Senado de la República y el Museo Memoria y Tolerancia albergaron foros de discusión en julio y agosto. Las sesiones especializadas se llevaron a cabo en el Instituto Federal de Telecomunicaciones y la Comisión Nacional Bancaria y de Valores, esta última centrada en la estabilidad del sistema financiero (Gobierno de México, 2017a).

Un momento clave fue la creación en octubre de la Subcomisión de Ciberseguridad de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE a partir de ahora), para dar seguimiento y coordinar la implementación de la Estrategia Nacional de Ciberseguridad, con la responsabilidad de coordinar las acciones gubernamentales y articular la participación de los diversos actores interesados (sociedad civil, sector privado, comunidades técnicas y académicas).

El CIDGE (2005-2023) fue la comisión federal establecida para promover y consolidar el uso de las TIC en la Administración Pública Federal, mediante la coordinación de acciones propuestas por la Secretaría de la Función Pública (Gobierno de México, 2017b).

Como parte inicial de las actividades Subcomisión de Ciberseguridad dentro de la Campaña Ciberseguridad México, se realizaron sus dos primeras sesiones durante ese mismo mes de octubre, marcando el comienzo formal de su operación.

El desarrollo de la ENCS incluyó la presentación de estudios técnicos de evaluación de la ciberseguridad en México y de aspectos de protección de datos personales mediante un conversatorio realizado en el INAI. El proceso culminó en noviembre con el 5to Encuentro Latinoamericano de Ciberseguridad, Ciberdelitos e Informática Forense, organizado por la UNAM e INFOTEC (Gobierno de México, 2017a). Este proceso de nueve meses estableció las bases para la formulación de la estrategia nacional.

La Estrategia estableció una visión en la que “en 2030, México será una nación resiliente ante los riesgos y amenazas en el ciberespacio que aprovecha con responsabilidad el potencial de las TIC para el desarrollo sostenible en un entorno confiable para todos” (Gobierno de México, 2017a, p. 16).

Para ello, se establecieron cinco objetivos que abarcaron diferentes ámbitos. En el ámbito social, buscó garantizar los derechos y libertades de los ciudadanos en el ciberespacio y su entorno digital. En la esfera económica, promover la innovación y el desarrollo tecnológico para la ciberseguridad de la economía de los sectores productivos. Para las instituciones públicas, la protección de información y los sistemas informáticos para su funcionamiento y continuidad. En materia de seguridad pública, incrementar las capacidades de prevención e investigación de delitos cibernéticos, mientras que en seguridad nacional desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que pudieran alterar el desarrollo y la soberanía nacional (Gobierno de México, 2017a).

Para implementar estos objetivos, la estrategia desarrolló ejes transversales interconectados. Estos abarcaron desde el fomento de una cultura de ciberseguridad y el desarrollo de capacidades técnicas, hasta la creación de marcos regulatorios y sistemas de medición. La coordinación entre actores y el impulso a la investigación serían elementos centrales que permitirían una aproximación integral al desafío de la ciberseguridad.

Esta estructura se fundamentó en principios que priorizan los derechos humanos, incorporaron la gestión de riesgos y la colaboración multisectorial (Gobierno de México, 2017a). Para su implementación fueron creados grupos de trabajo por cada uno de los cinco objetivos estratégicos y los ocho ejes transversales, emepzando a reunirse en febrero de 2018, a diez meses del cambio de administración federal.

Para noviembre, a solo una semana de que Andrés Manuel López Obrador tomara posesión el 1 de diciembre, fue publicado por el Gobierno de México (2018) el documento titulado “Memoria y Recomendaciones ENCS” en el que se detallan las acciones y reuniones que las mesas tuvieron en anteriores meses.

Como el caso de la protección de la sociedad y derechos, liderado por el SIPINNA y el IFT. Este grupo tuvo como misión diseñar e implementar acciones orientadas a garantizar el respeto de los derechos de la sociedad en el entorno digital. En mayo de 2018, se realizaron mesas de trabajo en el Instituto Federal de Telecomunicaciones, donde se definieron áreas clave de acción y se trazaron rutas críticas para su implementación (Gobierno de México, 2018, pág. 5). Entre los temas abordados, destacó la necesidad de fortalecer las políticas

públicas relacionadas con el uso y aprovechamiento de las TIC. Asimismo, se propuso promover mejores prácticas con enfoque de derechos humanos y no discriminación, asegurando que estas políticas se mantuvieran alineadas con los estándares internacionales (Gobierno de México, 2018, pág. 6).

Otro asunto fue la gestión de riesgos en el ciberespacio. Liderada por la Asociación de Internet MX, esta mesa de trabajo se enfocó en delinear una estrategia para concientizar a la población sobre el uso responsable de las TIC y establecer mecanismos efectivos para la prevención de riesgos digitales. Se destacó la importancia de crear campañas de sensibilización dirigidas a distintos sectores de la sociedad, fomentando una cultura de seguridad digital que permitiera mitigar posibles amenazas cibernéticas (Gobierno de México, 2018, pág. 6).

En cuanto a la actualización del marco jurídico, la UNAM lideró una serie de discusiones orientadas a revisar y armonizar las leyes existentes en materia de ciberseguridad. Los participantes de esta mesa concluyeron que era fundamental adaptar la legislación nacional a los cambios tecnológicos acelerados, considerando siempre un enfoque de respeto a los derechos humanos. También se recomendó actualizar el marco para delitos cibernéticos y garantizar la protección de datos personales (Gobierno de México, 2018, pág. 6).

De manera paralela, el grupo encargado de la protección de la economía e innovación, liderado por la Secretaría de Economía y la CANIETI, desarrolló una serie de acciones encaminadas a fomentar la confianza en el comercio electrónico y los servicios digitales. Una de las principales iniciativas fue la publicación de un artículo en la revista de negocios de ProMéxico, cuyo objetivo era difundir la ENCS entre los sectores productivos y académicos, sensibilizándolos sobre la importancia de implementar medidas de ciberseguridad robustas (Gobierno de México, 2018, pág. 42). Además, se planteó la creación de programas de formación en ciberseguridad, dirigidos a los sectores productivos, con el fin de promover el desarrollo de capacidades tecnológicas y la innovación en esta área (Gobierno de México, 2018, pág. 43).

Por otro lado, el grupo enfocado en la protección de las instituciones públicas, encabezado por la Secretaría de la Función Pública (SFP), llevó a cabo diversas actividades orientadas a

fortalecer la seguridad digital en el sector público. Entre las acciones realizadas, destacó la organización de cinco talleres presenciales, con una participación total de 663 servidores públicos federales, en los que se abordaron temas de ciberseguridad financiera, ciberseguridad infantil y medidas básicas de protección digital.

Asimismo, se impartieron ocho talleres virtuales dirigidos a servidores públicos estatales y municipales, mediante la plataforma Zoom, enfocados en la prevención de delitos cibernéticos y el uso responsable de las TIC (Gobierno de México, 2018, pág. 13), encabezado por la Secretaría de la Función Pública (SFP), trabajó en el fortalecimiento de los mecanismos de protección en materia de ciberseguridad dentro del sector gubernamental.

Adicionalmente, el grupo liderado por la Secretaría de Relaciones Exteriores sobre la medición y el seguimiento de la política, junto con el apoyo y el esfuerzo conjunto del INEGI, la Presidencia de la República, la Policía Federal, la SEP, la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), el INFOTEC (Conahcyt) y el IPN, desarrollaron el llamado Índice de Ciberseguridad-Mx, diseñado para medir la implementación y efectividad de la ENCS.

Su principal objetivo fue y sería evaluar la preparación de México en materia de ciberseguridad para enfrentar riesgos, amenazas y ataques informáticos sofisticados, además de medir el grado de aprovechamiento de las Tecnologías de la Información y Comunicación, solo que al ser propuesto a poco tiempo del término de la administración de Peña Nieto, dependería de su sucesor usarlo por primera vez.

Esta estrategia, junto con el conocimiento generado por las mesas de trabajo, no solo quedaría disponible para que el nuevo gobierno retomara y continuara con su implementación, sino que también representaba una base para seguir construyendo políticas públicas sólidas en materia de ciberseguridad. Su adopción y seguimiento permitirían fortalecer la capacidad del país para enfrentar amenazas digitales y aprovechar las oportunidades que brindan las tecnologías emergentes. Además, sería una herramienta que permitiría establecer un marco de colaboración interinstitucional y multisectorial para garantizar el cumplimiento de los objetivos.

Capítulo 3. Reconstrucción de la política de ciberseguridad en materia de seguridad pública (2018-2024)

El presente capítulo constituye la primera parte del núcleo analítico de esta investigación, cuyo objetivo central es reconstruir la política de ciberseguridad en materia de seguridad pública desarrollada durante la administración del presidente Andrés Manuel López Obrador, en el periodo comprendido entre 2018 y 2024. En este sentido, el capítulo se encuentra estructurado en dos secciones. En el que la primera de ellas aborda el contexto político y social de la llegada de AMLO a la presdencia y cómo fue su discruso ante la cibersegruidad y los delitos cibenéticos. El segundo identifica y analiza los instrumentos de acción pública que han sido diseñados, adoptados o modificados en dicho periodo en torno a la ciberseguridad vinculada a la seguridad pública.

3.1 El contexto político, las demandas sociales y la (des)priorización de la ciberseguridad en México

En el sexenio de Enrique Peña Nieto (2012-2018), la respuesta del Estado mexicano ante el creciente fenómeno del ciberdelito se articuló a través de instrumentos de acción pública identificados en el capítulo 1, de los cuales algunos serían los que la siguiente administración recibiría.

En primer lugar, la Estrategia Nacional de Ciberseguridad (ENCS) desarrollada en el último año de la gestión peñista, buscaba coordinar acciones entre diversos sectores para proteger infraestructuras críticas, garantizar la privacidad de datos y fomentar una cultura digital segura. Si bien su diseño y lanzamiento tuvieron lugar bajo la administración de Peña Nieto, su implementación y seguimiento a nivel nacional estarían a disposición de la voluntad de la siguiente administración.

Además, como parte de los instrumentos organizativos, en el ámbito de la Policía Federal, el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) fue objeto de continuidad operativa. Esta continuidad fue reconocida en el Programa para la Seguridad Nacional 2014-2018, el cual incluyó al CERT-MX como parte de los mecanismos existentes para atender riesgos y amenazas en el ciberespacio.

En marzo de 2018 cuando Andrés Manuel López Obrador era candidato presidencial por la alianza "Juntos Haremos Historia" de los partidos Movimiento de Regeneración Nacional (Morena), Partido del Trabajo (PT) y Partido Encuentro Social (PES), su figura emergió como símbolo de ruptura y esperanza del cambio, impulsado por un discurso de transformación y combate a la corrupción, generó grandes expectativas en diversos ámbitos de la administración pública, incluyendo la seguridad (Illades, 2018; Edeza, 2018). Sin embargo resulta destacable que pese a la amplitud de sus propuestas, el tema de ciberseguridad y delitos informáticos estuvo ausente en su plataforma electoral, a pesar del creciente aumento en ataques informáticos contra la ciudadanía

Durante el arranque de su campaña, el primero de abril de 2018, el líder político ofreció un discurso que enfatizaba la necesidad de modernizar el país "desde abajo" (Beauregard, 2018) pero no considerando una visión de fortalecimiento tecnoógico o de ciberseguridad en su discurso.

En el contexto electoral se destacó la aprobación masiva hacia su candidatura, reflejada en una intención de voto que superaba el 40% y que superaba al de sus competidores, evidenció el sólido respaldo popular a sus propuestas de transformación y el creciente desencanto del electorado con el modelo político tradicional (Forbes México, 2018). Sin embargo, en ningún momento de su campaña se incluyeron propuestas o menciones sobre políticas de ciberseguridad o combate a delitos cibernéticos, a pesar de la creciente relevancia de estos temas en la agenda digital global.

En su discurso de cierre de campaña en el Estadio Azteca, López Obrador culminó su propuesta política sin incluir ningún elemento relacionado con ciberseguridad o combate a delitos digitales (Ureste, 2018). Este hecho marcó el tono de una campaña que, en su conjunto, había omitido sistemáticamente abordar los desafíos tecnológicos del país, a pesar del creciente problema en el país.

El acto final, que reunió a miles de simpatizantes y cerró la gira nacional, se concentró exclusivamente en temas de política tradicional, sin proponer medidas para proteger infraestructuras críticas, ciudadanos frente a ciberdelitos o políticas de seguridad digital. Así

concluyó su campaña: con un llamado al cambio estructural tradicional, pero sin reconocer el marco de seguridad digital mexicano.

El 1 de julio de 2018 se llevaron a cabo las elecciones federales en México. Con una lista nominal de electores de 89,123,355 ciudadanos registrados, se realizaron votaciones para renovar la Presidencia de la República, 128 escaños en el Senado, 500 en la Cámara de Diputados, ocho gubernaturas y la Jefatura de Gobierno de la Ciudad de México y de cargos locales (INE, 2018a).

Con un 53.19% de los votos, López Obrador alcanzó un total de 30 millones 113 mil 483 sufragios, su más cercano competidor, Ricardo Anaya, de la coalición Por México al Frente, obtuvo 12 millones 610 mil 120 votos, representando el 22.27% de la votación(INE, 2018b).

El 1 de diciembre de 2018, Andrés Manuel López Obrador asumió la Presidencia de México en una ceremonia realizada en el Palacio Legislativo de San Lázaro. Durante el acto, recibió la banda presidencial de manos de su antecesor, Enrique Peña Nieto, y rindió protesta ante el Congreso de la Unión. En su primer discurso como presidente, López Obrador reiteró compromisos expuestos en campaña, como el combate a la corrupción, la austeridad en el gobierno pero el nuevo presidente no mencionó estrategias para enfrentar desafíos tecnológicos (BBC,2018).

Desde el inicio de su mandato, López Obrador estableció las prioridades de su administración con un enfoque centrado en la austeridad, el combate a la corrupción y la reconfiguración de las instituciones de seguridad reflejadas en el Plan Nacional de Desarrollo (PND) 2019-2024, donde se marcaron cambios significativos respecto a su antecesor.

Uno de los contrastes se dio en la agenda digital y la ciberseguridad. Mientras que el PND 2013-2018 de Enrique Peña Nieto había integrado la agenda digital como un eje transversal, abordando temas como la protección de datos y la modernización tecnológica, el documento presentado por la administración de López Obrador omitió por completo referencias a lo digital y a la ciberseguridad. En su diagnóstico y propuesta de acción, el documento se enfocó en atender la violencia delictiva, la descomposición institucional y el deterioro del tejido social, problemáticas agrupadas bajo el concepto general de "inseguridad", sin que se consideraran sus nuevas expresiones en el ámbito digital. Su enfoque se enfocó en la creación

de la Guardia Nacional, la organización que sustituiría a la Policía Federal, presentada como solución a la crisis de violencia (DOF, 2019c).

Así mismo, la Estrategia Nacional de Ciberseguridad desarrollada por el sexenio de Enrique Peña Nieto no encontró continuidad en el gobierno de Andrés Manuel López Obrador, pues durante esta nueva administración, no se formuló ni adaptó una nueva estrategia nacional de ciberseguridad, y los objetivos previamente establecidos en torno a la materia se diluyeron ante la falta de prioridad política. En contraste, el Modelo Homologado de Policía Cibernética sí fue retomado y siguió implementándose con recursos federales del Fondo de Aportaciones para la Seguridad Pública (FASP) en las entidades federativas, aunque sin articularse dentro de una política nacional integral de ciberseguridad.

El giro en la institucionalización de la ciberseguridad durante el periodo de AMLO llegó con la publicación del Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024, que reconoció oficialmente el problema de la deficiencia tecnológica del Estado frente a los delitos cibernéticos. Este programa abordó la situación mediante estrategias prioritarias enfocadas en mejorar la infraestructura tecnológica de las instituciones de seguridad pública, establecer medidas para la protección contra ciberataques, lograr la homologación de sistemas y optimizar la interconexión tecnológica entre las instituciones de seguridad de los tres órdenes de gobierno, con el objetivo de fortalecer la capacidad del Estado para prevenir y combatir los ciberdelitos.

Posterirmente un año despúes, en 2021, fue publicada la Estrategia Digital Nacional (EDN) 2021-2024 en la que mandató el diseño e implementación del Protocolo Homologado para la Gestión de Incidentes Cibernéticos, siendo el instrumento que serviría para estandarizar respuestas ante ataques digitales en todos los niveles de gobierno al contar con un procedimiento de actuación dividido en fases que incluyen la prevención, la protección y la respuesta ante incidentes cibernéticos para lograr su objetivo de fortalecer la ciberseguridad en las dependencias federales, entidades federativas, organismos constitucionales autónomos, academia e instancias del sector privado.

También, el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos asignó nuevas tareas al Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX),

creado en 2012 durante la administración de Felipe Calderón. Bajo el gobierno de López Obrador, este centro fue instruido para desempeñar funciones específicas dentro de las fases de detección, respuesta y recuperación ante incidentes cibernéticos, así como en su actualización y mejora continua de las capacidades institucionales (Guardia Nacional, 2021).

La forma en que el gobierno de López Obrador recunfiguró la herencia institucional y organizacional de política de ciberseguridad nacional es analizada en las siguientes secciones del capítulo.

3.2 La política de ciberseguridad en la seguridad pública de AMLO

Para reconstruir la política de ciberseguridad en materia de seguridad pública en el periodo de Andrés Manuel López Obrador, es necesario recordar que, según Rosas (2021), la intervención del gobierno en el problema se articula mediante instrumentos de acción pública, que se dividen en normativos, organizativos, programáticos y financieros.

Al enfocar estos instrumentos en la intervención gubernamental frente al ciberdelito en la seguridad pública, resulta posible reconstruir la política implementada durante dicho periodo presidencial.

3.2.1 Instrumentos normativos

Los instrumentos normativos vigentes durante el sexenio de Andrés Manuel López Obrador, enlistados en la Tabla 7, constituyen el marco jurídico que regula la intervención del Estado mexicano en materia de ciberseguridad como parte de la seguridad pública. De acuerdo con Rosas (2021), estos instrumentos definen las bases legales para la política pública del problema de los ciberdelitos, articulando la acción gubernamental mediante normas que delimitan las competencias y obligaciones de las autoridades.

La Constitución Política de los Estados Unidos Mexicanos (CPEUM, a partir de ahora) establece en su artículo 1º, párrafo 3, adicionado mediante la reforma constitucional en materia de derechos humanos de 2011, que las autoridades deben garantizar los derechos humanos, esto incluyendo su protección en entornos digitales.

Tabla 7. Instrumentos normativos de la acción pública del Estado en ciberseguridad en materia de seguridad pública

Normativa	Artículos	Descripción	Año
Constitución Política de los Estados Unidos Mexicanos	Art 1, párrafo 3	El Estado es garante de los derechos humanos.	2011
	Art. 16, párrafo 2 y 3	Protección a la inviolabilidad de la persona y su domicilio, y a la protección de sus datos personales.	2017 y 2009
	Art. 21	La investigación de los delitos corresponde al Ministerio Público (FGR) y a las policías, siendo Ministerio Público el único que pueda ejercer la acción penal ante los tribunales correspondientes. Además que la seguridad pública es función del Estado.	2019
	Art. 73, fracción XXI, inciso b	Facultad del Congreso de la Unión de legislar sobre delitos federales.	1917
	Art. 133	Facultad del Estado para suscribir tratados internacionales.	1917
Código Penal Federal	Art. 210	Castigo de la revelación de secretos por parte de cualquier persona que los conozca debido a su empleo, cargo o puesto	1999
	Art. 211	Aumento de las penas, cuando el responsable sea servidor público, profesional o cuando el secreto tenga carácter industrial	
	Art. 211 Bis	Castigo del uso indebido de información e imágenes obtenidas mediante intervención de comunicaciones privadas	
	Arts. 211 Bis 1 al 7	Castigos al acceso ilícito a sistemas y equipos de informática	
	199 Octies, Nonies y Decies	Castigo a la violación a la intimidad sexual (divulgación, distribución o publicación de contenido íntimo sexual de una persona sin su consentimiento, con casos en los que se agravan las penas.	2021
Ley General de Acceso de las Mujeres a Una Vida Libre de Violencia	Art. 20 Quáter	Definió el concepto de violencia digital como la publicación de contenido íntimo sexual de una persona sin su consentimiento, y de la cúal los artículos 199 Octies, Nonies y Decies del CPF sanciona.	2021
Ley General de Protección de Datos Personales	Art. 19	Obligación de los responsables del tratamiento de datos personales en el sector privado a implementar medidas de seguridad	2017

en Posesión de Sujetos Obligados		administrativas, técnicas y físicas para proteger los datos personales.	
	Art. 63, fracción VIII	Faculta al INAI para iniciar procedimientos sancionadores contra entidades privadas que incumplan con la confidencialidad de los datos personales.	
	Art. 64, fracción III	Establece multas económicas por infracciones relacionadas con la confidencialidad de datos, que van desde 200 hasta 320,000 días de salario mínimo.	
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Art. 31	Obliga a las instituciones públicas establecer medidas de seguridad administrativas, físicas y técnicas para proteger datos personales.	2017
	Art. 163	Señala como causa de sanción el incumplimiento del deber de confidencialidad por parte de responsables públicos.	
	Art. 164 y 165	Establece que las infracciones en el sector público serán remitidas a la autoridad competente para aplicar sanciones administrativas, civiles o penales, determinaas por separado, siguiendo los procedimientos legales correspondientes.	

Fuente: Elaboración propia

Este mandato obliga al Estado a diseñar políticas de ciberseguridad que prevengan violaciones a estos derechos derivadas del uso de tecnologías, tales como el acceso no autorizado a información privada por beneficio financiero o daños personales. El texto constitucional señala que:

> Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley. (CPEUM, 2025, pág. 1)

El artículo 16 de la CPEUM, en sus párrafos 2 y 3, el primero reformado en 2017 del texto original de 1917, y el segundo adicionado en 2009, se protege la inviolabilidad de la persona y su domicilio, así como la protección de sus datos personales, extendiéndose esta protección a la esfera digital y resguardando los datos personales frente a accesos indebidos. El párrafo

2 fue reformado en 2017, modificando el texto original de 1917, mientras que el párrafo 3 fue adicionado en 2009:

> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.
>
> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (CPEUM, 2025, pág. 19)

El artículo 21 constitucional, reformado en 2019, estableció que "la investigación de los delitos corresponde al Ministerio Público [Fiscalía General de la República] y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función" (SCJN, 2025), y que el Ministerio Público (FGR) es el único que pueda ejercer la acción penal ante los tribunales correspondientes. También consagró que la seguridad pública es una función del Estado, y al establecer que las autoridades deben salvaguardar el patrimonio y la integridad de los ciudadanos, este artículo amplía el alcance de la seguridad pública a delitos cometidos digitalmente.

> La seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta Constitución y las leyes en la materia. (Diario Oficial de la Federación, 2019)

El constitucional 73, fracción XXI, inciso b, presente desde el texto original de 1917, otorga al Congreso de la Unión la facultad de legislar sobre delitos federales, esta competencia habilita la creación de figuras penales específicas para sancionar ciberdelitos:

> El Congreso tiene facultad: […] XXI. Para expedir: […]

> b) La legislación que establezca los delitos y las faltas contra la Federación y las penas y sanciones que por ellos deban imponerse; así como legislar en materia de delincuencia organizada. (CPEUM, 2025, pág. 72)

Finalmente, el artículo 133 constitucional habilita al Estado para alinearse con políticas de ciberseguridad globales, presente desde el texto original de 1917, al establecer que los tratados internacionales que sean aprobados conforme a la ley son supremos y prevalecerán sobre las leyes locales:

> Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada entidad federativa se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de las entidades federativas. (CPEUM, 2025, pág. 155)

Mientras que en el Código Penal Federal, documento que define los delitos federales y sus penas, en su Título Noveno denominado "*Revelación de secretos y acceso ilícito a sistemas y equipos de informática*" adicionado en 1999, establece el marco jurídico que habilita al Estado mexicano para intervenir y sancionar ciberdelitos o conductas que vulneran la privacidad, la integridad de la información y la seguridad en entornos digitales. El título de esta normativa se divide en dos capítulos que regulan delitos específicos asociados al manejo no autorizado de datos y a la intrusión en sistemas informáticos.

En su Capítulo I, sobre la "*Revelación de secretos*", se sanciona la divulgación ilegítima de información confidencial obtenida en contextos profesionales, técnicos o públicos. El artículo 210 castiga la revelación de secretos por parte de cualquier persona que los conozca debido a su empleo, cargo o puesto, imponiendo sanciones de treinta a doscientas jornadas de trabajo comunitario (CPF, 2024, pág.70).

El artículo 211 aumenta las penas, incluyendo prisión y suspensión profesional, cuando el responsable sea un servidor público, un profesional o cuando el secreto tenga carácter industrial, como en casos de propiedad intelectual (CPF, 2024, pág.70).

Adicionalmente, el artículo 211 Bis penaliza el uso indebido de información e imágenes obtenidas mediante intervención de comunicaciones privadas, con penas de hasta doce años de prisión (CPF, 2024, pág.70).

De su Capítulo II, sobre el "*Acceso ilícito a sistemas y equipos de informática*", en su artículo 211 Bis 1 sanciona al que "sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad" (CPF, 2024, pág.70) con multa de cien a trescientos días y de seis meses a dos años en prisión.

Mientras que el artículo 211 Bis 2 sanciona al que "sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad" (CPF, 2024, pág.70) con prisión de uno a cuatro años y de doscientos a seiscientos días multa.

El artículo 211 Bis 3, sanciona a aquel que "estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan" (CPF, 2024, pág.71) con prisión dos a ocho años y de trescientos a novecientos días multa.

El Artículo 211 bis 4, se sanciona al que "modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad" (CPF, 2024, pág.71) con prisión de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Mientras que el artículo 211 bis 5, sanciona al que tenga autorización pero cometa la misma falta con la misma pena (CPF, 2024).

Así mismo, este capítulo finaliza estableciendo que las penas de estos artículos podrán aumentar hasta en una mitad cuando la información recabada sea usada para provecho propio o ajeno, según el a Artículo 211 bis 7 (CPF, 2024).

Estas disposiciones del Código Penal Federal facultan al Estado para sancionar una ruptura de la confidencialidad de la información al tipificar conductas ciertas actividades ilícitas en entornos digitales. Pero esta normativa mexicana fue modificada en 2021, cuando fue

publicado el "*Decreto por el que se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal*", decreto que se le conoce mediáticamente como *Ley Olimpia*, de la cual en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia quedó establecida el concepto de violencia digital en su árticulo 20 Quáter, en el cual establece que será sancionada dentro del Código Penal Federal:

> ARTÍCULO 20 Quáter.- Violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.
>
> Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación.
>
> Para efectos del presente Capítulo se entenderá por Tecnologías de la Información y la Comunicación aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos.
>
> La violencia digital será sancionada en la forma y términos que establezca el Código Penal Federal. (DOF, 2021a)

Mientras que el decreto agregó aquellas sanciones dentro del CPF, adicionando dentro de su Título Séptimo Bis "*Delitos contra la Indemnidad de la Privacidad de la Información Sexual*" un Capítulo II, denominado "*Violación a la Intimidad Sexual*", compuesto por los artículos 199 Octies, 199 Nonies y 199 Decies.

El primero de ellos, el art. 199 Octies, establece que:

> Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.

> Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.
>
> Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización. (DOF, 2021a)

El segundo artículo, el 199 Nonies, establece las mismas sanciones cuando el contenido íntimo sexual no corresponde a la persona señalada. Es decir, cuando se difunden, comparten, distribuyen o publican imágenes, videos o audios atribuyéndolos a alguien, aunque en realidad no sean de esa persona (DOF, 2021a).

En ambos casos, aquellas sanciones pueden aumenrar hasta la mitad en el mínimo y el máximo de la pena cuando el delito de violación a la intimidad sexual se cometa bajo ciertas circunstancias agravantes definidos en el artículo 199 Decies:

I. Si el responsable es el cónyuge, concubinario(a) o cualquier persona con la que la víctima tenga o haya tenido una relación sentimental, afectiva o de confianza.
II. Si el delito es cometido por un servidor público en el ejercicio de sus funciones.
III. Si la víctima no puede comprender el significado del hecho o no tiene la capacidad para resistirlo.
IV. Si el delito se comete con el fin de obtener algún tipo de beneficio no lucrativo.
V. Si se realiza con fines lucrativos.
VI. Si, como consecuencia del delito, la víctima atenta contra su integridad o su propia vida. (DOF, 2021a)

Por otro lado, existen dos ordenamientos que obligan desde su publicacón en 2017 a la protección de información datos personales en el ámbito privado y público: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, a partir de ahora), que regula el tratamiento de datos por parte de entidades privadas, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, a partir de ahora), aplicable a entidades públicas.

En este sentido, si se produce un hackeo o una filtración de información personal, la responsabilidad recae en el sujeto obligado o en el responsable del tratamiento de dichos

datos, quien deberá responder legalmente por no haber implementado las medidas de seguridad necesarias para la protección de aquellos datos.

Dentro de la LFPDPPP, se establece la obligación de los entes privados a la protección de la información y de datos personales que manejan y tratan, configurándose como el instrumento normativo que garantiza la seguridad de la información en el ámbito no gubernamental:

> Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. (LFPDPPP, 2017, pág. 6)

Para asegurar el cumplimiento de esta disposición, la ley otorga facultades específicas al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Según el artículo 63, fracción VIII, el instituto puede iniciar procedimientos sancionadores contra entidades privadas que no mantengan la confidencialidad de la información personal (LFPDPPP, 2017).

La ley contempla las sanciones en su artículo 64, fracción III. Las infracciones relacionadas con la confidencialidad pueden ser castigadas con multas que van desde 200 hasta 320,000 días de salario mínimo (LFPDPPP, 2017), creando así un incentivo para que las organizaciones privadas implementen medidas de seguridad efectivas contra las amenazas cibernéticas.

Mientras que para el sector público, la LGPDPPSO en su artículo 31 establece la obligatoriedad de la protección de la información y datos sensibles de los responsables públicos:

> Artículo 31. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad. (LGPDPPSO, 2017, pág. 13)

El artículo 163 de esta ley señala como causa de sanción el incumplimiento del deber de confidencialidad por parte de las instituciones públicas. Para estas infracciones, el artículo 164 establece que se dará vista a la autoridad competente para que imponga o ejecute la sanción correspondiente y que pueden generarse responsabilidades en distintos ámbitos legales (administrativo, civil y penal) con cada una de estas responsabilidades determinas por separado, siguiendo sus propios procedimientos específicos según las leyes correspondientes según el artículo 165 (LGPDPPSO, 2017).

Asú pues, en los instumentos normativos del Estado mexicano la inclusión del derecho a la protección de datos personales en la CPEUM o la facultad del Congreso de la Unión para legislar en materia penal federal permiten estructurar la acción gubernamental para enfrentar las amenazas cibernéticas desde una perspectiva de seguridad pública, aunque tienendo la particularidad de que ninguno de estos ordenamientos utiliza explícitamente los términos "ciberdelito" o "delito cibernético" para la aproximación directa al fenómeno.

A partir de esta identificación de los instrumentos normativos expuestos, se puede afirmar que el Estado mexicano sí cuenta con una base legal que habilita y obliga el diseño e implementación de acciones de ciberseguridad enfocadas tanto en la protección de derechos humanos de la población como en la persecución de delitos cometidos en entornos digitales. La traducción en planes y acciones concretas, la dotación de recursos especializados y de la articulación operativa y los sectores involucrados son aspectos que se exploran en los apartados siguientes.

3.2.2 Instrumentos organizativos

Los instrumentos organizativos durante el sexenio de Andrés Manuel López Obrador en materia de ciberseguridad en la seguridad pública, enlistados en la Tabla 8, constituyen las estructuras institucionales diseñadas para coordinar la acción pública en el ámbito de la ciberseguridad. De acuerdo con Rosas (2021), estos instrumentos se refieren a las organizaciones y mecanismos creados o modificados para implementar políticas públicas, garantizando la coordinación interinstitucional y la ejecución de estrategias en materia de seguridad cibernética.

Empezando por la Guardia Nacional (GN), fue la institución que AMLO estableció para sustituir a la Policía Federal a partir de la reforma constitucional del 26 de marzo de 2019, para que este organismo fuera la institución policial de carácter civil adscrita a la Secretaría de Seguridad y Protección Ciudadana (SSPC), cuyo análisis de capacidades instituionales se desarrolla en el capítulo siguiente, "que formulará la Estrategia Nacional de Seguridad Pública, los respectivos programas, políticas y acciones' (DOF, 2019a, pág. 12), con los fines de "salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social' (DOF, 2019a, pág. 12), y para la "coordinación y colaboración con las entidades federativas y municipios, así como la salvaguarda de los bienes y recursos de la Nación" (DOF, 2019a, pág. 12).

Tabla 8. Instrumentos organizativos de la acción pública del Estado en ciberseguridad en materia de seguridad pública

Organización			**Descripción**
Secretaría de Seguridad y Protección Ciudadana	Guardia Nacional (2019, antes Policía Federal)	Dirección General Científica (Previa existencia dentre de la Policía Federal desde 2010)	Unidad especializada de la Guardia Nacional encargada de coordinar los servicios técnico-científicos y laboratorios criminalísticos, así como de implementar acciones de vigilancia, identificación y monitoreo en Internet y apoya en la investigación y esclarecimiento de ciberdelitos.
		Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) (Previa existencia dentre de la Policía Federal desde 2012)	Adscrito a la Dirección General Científica de la Guardia Nacional. Actúa como equipo de respuesta a incidentes cibernéticos (CIRT), evaluando, documentando y respondiendo a incidentes de seguridad informática. Apoya en la investigación forense digital y el análisis técnico-policial en coordinación con el Ministerio Público, y emite alertamientos a la ciudadanía sobre peligros cibernéticos.
Presidencia de la República	Coordinación de Estrategia	Comisión Intersecretarial de Tecnologías de la Información y	Órgano colegiado que coordina las políticas federales en materia de tecnologías de la información,

	Digital Nacional (desde 2013)	Comunicación y de la Seguridad de la Información (CITICSI) (2023)	comunicación y seguridad de la información.
		Comisión permanente de Seguridad de la Información (2023)	Comisión permanente de la CITICSI sobre Seguridad de la Información, establece lineamientos y acciones para proteger los datos y sistemas en la Administración Pública Federal.
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)			Órgano constitucionalmente autónomo que garantiza el derecho a la transparencia, acceso a la información pública y protección de datos personales, vigila el cumplimiento de la LFPDPPP y la LGPDPPSO, y ha colaborado institucionalmente con el IFT y la GN en materia de ciberseguridad en cumplimiento de sus funciones.
Instituto Federal de Telecomunicaciones (IFT)			Órgano constitucionalmente autónomo que regular y supervisa las telecomunicaciones, radiodifusión y competencia en el sector. Teniendo una función de apoyo en los instrumentos programáticos del Ejecutivo en materia de telecomunicaciones e Internet, en el que se incluye la ciberseguridad y que puede colaborar con otras institciones para ello.

Fuente: Elaboración propia

Dentro de su estructura, la Guardia Nacional cuenta con unidades especializadas con el objetivo principal proponer lineamientos, mecanismos y técnicas generales para la investigación de delitos, la atención a mandamientos ministeriales y judiciales, y el aseguramiento de bienes relacionados con hechos delictivos (Reglamento de la Ley de la Guardia Nacional, 2020).

La unidad especializada encargada de proponer políticas y procedimientos institucionales para la actuación en contra de la ciberdelincuencia es la Dirección General Científica, cuyo objetivo es la:

> Aplicación de estrategias con contra la ciberdelincuencia, la investigación criminalística y desarrollo científico-tecnológico para la implementación de las acciones que apoyen las investigaciones en materia de prevención del delito, así como el esclarecimiento de hechos delictivos competencia de la Guardia Nacional. (Reglamento de la Ley de la Guardia Nacional, 2020).

Entre las funciones de la Dirección General Científica se encuentra la implementación de acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet con el fin de prevenir conductas delictivas. Asimismo, esta dirección establece mecanismos y protocolos para el registro de la información obtenida durante las investigaciones, fortaleciendo la confidencialidad e integridad de los datos. También propone lineamientos internos orientados a la emisión de opiniones técnicas y políticas en materia de servicios técnico-científicos, con el objetivo de modernizar y optimizar las metodologías y herramientas de ciberseguridad utilizadas por las unidades administrativas de la Guardia Nacional (Reglamento de la Ley de la Guardia Nacional, 2020).

Despúes de la transición a la Guardia Nacional, se mantuvo en adscripción en esta dirección el CERT-MX (Centro Nacional de Respuesta a Incidentes Cibernéticos), creado en 2012 durante el sexenio de Felipe Calderón (Noticias 24 Horas, 2012). Este órgano funciona como un CIRT (Cyber Security Incident Response Team), es decir, un grupo de expertos especializados en evaluar, documentar y responder a incidentes cibernéticos con el objetivo de garantizar que las redes afectadas no solo se recuperen rápidamente, sino que también se implementen medidas para prevenir incidentes futuros (U.S. Department of Homeland Security, 2024).

Además del CERT-MX, otras instituciones en materia de seguridad en México cuentan con sus propios equipos de respuesta a incidentes: la Secretaría de la Defensa Nacional opera el SEDENA-CSIRT y la Secretaría de Marina opera el CSIRT-SEMAR, responsables de proteger las infraestructuras críticas relacionadas con la defensa nacional, asegurando que los sistemas y redes bajo su custodia estén resguardados contra ciberataques que puedan comprometer la seguridad del país (SEDENA, 2024; SEMAR, 2024).

Sin embargo, a diferencia de los equipos de la SEDENA y SEMAR que se solo enfocan en la defensa nacional a través de las fuerzas armadas, el CERT-MX actúa en el ámbito de

la seguridad nacional en el resguardo de la ciberseguridad dentro de la administración pública federal y de la seguridad pública respondiendo a incidentes cibernéticos que afectan a la población y a instituciones gubernamentales no relacionadas directamente con la defensa.

El CERT-MX tiene como objetivo:

> "Brindar los servicios de apoyo en la respuesta a incidentes cibernéticos que afectan a las instituciones en el país que cuentan con infraestructura crítica de información, que incluye la identificación de amenazas y modus operandi de la ciberdelincuencia para el alertamiento a la ciudadanía, mediante la gestión de incidentes de seguridad informática, fungiendo como el único punto de contacto y coordinación dentro y fuera del territorio nacional y actuando en la investigación forense digital y el análisis técnico policial en apoyo al Ministerio Público. (Guardia Nacional-CERT-MX, s.f)

Bajo el gobierno de López Obrador, este centro fue instruido para desempeñar funciones específicas dentro de *Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos* en sus fases de detección, respuesta y recuperación ante incidentes cibernéticos, así como en la actualización y mejora continua de capacidades institucionales (Guardia Nacional, 2021).

Otro organismo fue la Comisión Intersecretarial de Tecnologías de la Información y Comunicación y de la Seguridad de la Información (CITICSI, a partir de ahora), que fue creada en enero de 2023 mediante un decreto emitido por el Presidente de la República para susituir al CIDGE (Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico) previamente en funcionamiento, fundamentándose en una necesidad de coordinar de forma colegiada las políticas federales en materia de tecnologías de la información, comunicación y de su seguridad, enmarcadas dentro del Plan Nacional de Desarrollo 2019-2024 y la Estrategia Digital Nacional 2021-2024 (Diario Oficial de la Federación, 2023a).

Este órgano intersecretarial fue establecido dependiente directamente del titular del Poder Ejecutivo Federal (Presidencia de la República), con el presidido del titular de la Coordinación de Estrategia Digital Nacional (CEDN) adscrita a la Oficina de la Presidencia, y conformado por los titulares de las Unidades de Tecnologías de la Información y Comunicación (o los equivalentes) de las secretarías de Estado, del Servicio de

Administración Tributaria (SAT), del Consejo Nacional de Ciencia y Tecnología (CONACyT), del Instituto Mexicano del Seguro Social (IMSS), del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), de Petróleos Mexicanos (PEMEX), de la Comisión Federal de Electricidad (CFE) y del Centro Nacional de Inteligencia, así como del titular de la empresa productiva subsidiaria de la CFE, CFE Telecomunicaciones e Internet para Todos, y del titular de la Comisión Nacional de Mejora Regulatoria (Diario Oficial de la Federación, 2023a).

Las funciones de la CITICSI son:

I. Fungir como instancia de coordinación entre las autoridades responsables de la implementación y desarrollo de acciones en materia de tecnologías de la información y comunicación, así como de la seguridad de la información, en la Administración Pública Federal;
II. Participar en la implementación de estrategias y acciones interinstitucionales para el uso de las tecnologías de la información y comunicación, y de la seguridad de la información;
III. Impulsar y coordinar con los sectores público, privado, académico y social el desarrollo de estudios y actividades relacionadas con el aprovechamiento de las tecnologías de la información y comunicación, y de la seguridad de la información;
IV. Emitir los lineamientos para su organización y funcionamiento;
V. Crear las subcomisiones y grupos de trabajo que estime necesarios para el cumplimiento de sus funciones;
VI. Emitir los manuales o, en su caso, los lineamientos de organización y funcionamiento de las subcomisiones y grupos de trabajo que con motivo del objeto del presente Decreto sean creados por la Comisión;
VII. Solicitar a las subcomisiones y grupos de trabajo que para tal efecto instaure, la elaboración de documentos, estudios, proyectos, y lineamientos necesarios para mejorar las tecnologías de la información y comunicación, y de la seguridad de la información en la Administración Pública Federal;
VIII. Recibir y analizar los informes de actividades y, en su caso, aprobar los acuerdos, informes y documentación que les sean presentados por las subcomisiones y grupos de trabajo creados por la Comisión, y
IX. Las demás que sean necesarias para el cumplimiento de su objeto. (DOF, 2023a).

La CITICSI se organiza en tres subcomisiones permanentes, cada una con funciones especializadas. Entre ellas, la Subcomisión de Seguridad de la Información**,** que juega el papel de la ciberseguridad. Esta subcomisión establece mecanismos de coordinación entre las instituciones responsables de la protección de la información e impulsa el diseño y la

implementación de estrategias y protocolos orientados a prevenir, detectar y responder a incidentes cibernéticos (DOF, 2023a).

Mientras que dentro de las organizaciones constitucionalmente autónomas se encuentran el INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) y el IFT (Instituto Federal de Telecomunicaciones). Ambos, aunque específicamente no tienen funciones específicas sobre la ciberseguridad ni sobre seguridad pública, sus estatutos orgánicos hacen que estos puedan denunciar ante las autoridades correspondientes (FGR) asuntos de su competencia y pueden participar en la implementación de la Estrategia Digital Nacional del Ejecutivo.

El primer organismo, el INAI es el:

> organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento de los derechos de acceso a la información pública y de protección de datos personales… (DOF, 2017, pág. 8)

Que dentro de su estatuto orgánico le da función a su *Dirección General de Asuntos Jurídicos* para:

> Presentar denuncias de hechos, querellas, desistimientos y otorgar perdones ante el Ministerio Público u otras autoridades competentes, coadyuvar en la integración de las averiguaciones previas y en el trámite de los procesos que afecten al Instituto o en los que éste tenga interés jurídico. (DOF, 2017, pág. 29)

Es decir, que en caso de romperse alguna ley de las cuales el INAI es encargado de vigilar, puede interponer la denuncia al Ministerio Público para su sanción. También su estatuto orgánico le otorga una función a su *Dirección General de Promoción y Vinculación con la Sociedad* de fomentar el ejercicio de los derechos de acceso a la información y protección de datos personales a través de actividades de divulgación, colaboración interinstitucional y desarrollo de herramientas tecnológicas (DOF, 2017, pág. 41), siendo así posible que esta organización haya tenido participaciones con la Guardia Nacional y el IFT en actividades de

promoción ciudadana de ciberseguridad para la ciudadanía dentro del periodo de AMLO (INAI, 2021).

Por otro lado, el IFT es el "órgano público autónomo, independiente en sus decisiones y funcionamiento, con personalidad jurídica y patrimonio propio, que tiene por objeto regular y promover la competencia y el desarrollo eficiente de las telecomunicaciones y la radiodifusión" (DOF, 2014, pág. 2).

De la cual, su Dirección General de Desarrollo de las Telecomunicaciones y la Radiodifusión tiene como una función la de:

> Proponer al Pleno las acciones necesarias para contribuir, en el ámbito de competencia del Instituto, al logro de los objetivos de la política de inclusión digital universal y cobertura universal establecida por el Ejecutivo Federal; así como a los objetivos y metas fijados en el Plan Nacional de Desarrollo y los demás instrumentos programáticos relacionados con los sectores de radiodifusión y telecomunicaciones, además de fomentar el desarrollo eficiente del ecosistema de Internet. (DOF, 2014, pág. 21)

Dicha función permite que pueda haber colaboraciones del IFT con las dependencias del Ejecutivo para la implementación de sus instrumentos programáticos, pero también con otros órganos constitucionales autónomos, siendo función de la *Coordinación General de Vinculación Institucional* establecer, fomentar, fortalecer y dar seguimiento a las relaciones institucionales para el cumplimiento de las funciones del IFT. Haciendo que esta organización haya podido tener participaciones en materia de ciberseguridad para la segruidad ciudadana con la Guardia Nacional y el INAI durante el periodo de AMLO (IFT, 2023).

En conclusión, la identificación de los instrumentos organizativos dentro del sexenio de López Obrador sobre ciberseguridad en materia de seguridad pública muestra que no se produjeron cambios. A excepción de la creación de la CITICSI en 2023 para sustituir al CIDGE, la administración mantuvo las estructuras preexistentes y no creó nuevas organizaciones en materia de ciberseguridad.

Cabe destacar que la creación de la CITICSI ocurrió tres meses después del incidente de ciberseguridad dentro de los sistemas de información de la SEDENA que resultó en la

sustracción ilegal de 6 terabytes de información confidencial (*Guacamaya Leaks*). Aunque la SEDENA tiene su propio CERT, la proximidad temporal sugiere que su creación pudo responder, al menos en parte, a dicho evento. De no haber sido por esta sustitución del CIDGE, el gobierno federal habría operado durante todo el sexenio exclusivamente con las estructuras heredadas de administraciones anteriores, sin introducir ajustes organizativos en el ámbito de la ciberseguridad aplicada a la seguridad pública.

3.2.3 Instrumentos programáticos

Los instrumentos programáticos durante el sexenio de Andrés Manuel López Obrador, enlistados en la Tabla 9, constituyen los documentos gubernamentales que orientaron y delimitaron las acciones estatales en materia de ciberseguridad como parte de la seguridad pública. De acuerdo con Rosas (2021), estos instrumentos definen los lineamientos estratégicos y operativos para abordar los ciberdelitos, articulando la acción gubernamental mediante planes y programas que establecen objetivos, prioridades y mecanismos de implementación.

Tabla 9. Instrumentos programáticos de la acción pública del Estado en ciberseguridad en materia de seguridad pública

Año	Programa	Descripción
2019	Estrategia Nacional de Seguridad Pública	Primera estrategia nacional de AMLO en la que su Estrategia D priorizó recursos para tecnología policial (equipamiento, interconexión de sistemas, REPUVE y videovigilancia), sentando bases para políticas de ciberseguridad.
2019	Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024.	Con el Objetivo 4 buscó modernizar infraestructuras críticas, gestionar riesgos cibernéticos y homologar sistemas en materia de ciberseguridad.
2021	Estrategia Digital Nacional 2021-2024	Incluyó el Objetivo 5 en materia de seguridad de la información en instituciones públicas para implementar el protocolos homologados, evaluaciones de riesgos ante ciberataques y alianzas con CERT-MX.

2021	Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.	Obligó a las dependencias públicas a crear Marcos de Gestión de Seguridad (MGSI) con controles mínimos, análisis de riesgos y respuestas a ciberataques, e institutionalizó prácticas alineadas al Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.
2022	Programa Nacional de Seguridad Pública 20 22-2024	Enfocado en el combare de ciberdelincuencia organizada (Estrategia 3.4): rastreo de sitios web ilícitos, detección de ciberataques y búsqueda acuerdos internacionales. No contó con metas, pero reconoció el ciberespacio como ámbito estratégico para la segruidad pública.

Fuente: Elaboración propia

El primer instrumento programático propio del periodo presidencial de Andrés Manuel López Obrador que aperturó la ejecución estratégica y operativa del gobierno federal en materia de ciberseguridad fue la Estrategia Nacional de Seguridad Pública (ENSP, en adelante), publicada en 2019, con base en el artículo 21 constitucional que establece la responsabilidad del Estado sobre la seguridad pública (DOF, 2019b).

Dentro de la ENSP, se establecieron nueve estrategias específicas para atender los desafíos en materia de seguridad pública y prorizar “la prevención del delito, la procuración e impartición de justicia, el restablecimiento del estado de derecho y la reinserción de infractores" (DOF, 2019b).

Siendo la estrategia D, “Nuevos criterios de distribución de los recursos federales en materia de seguridad”, la que aunque explicitamente no fue relacionada con la ciberseguridad pero sí recupera la importancia de la estructura tecnológica nacional para el combate al delito (y ciberdelito implícitamente), permitió la posterior creación en ese mismo año de otro instrumento programático en el que sí especifica explícitamente objetivos de ciberseguridad con la recuperación de los criterios 2, 6, 7, 8 y 9 de esta estrategia D. Estos criterios fueron los lineamientos que definieron los programas para la asignación y administración del Fondo de Aportaciones para la Seguridad Pública (FASP) para fortalecer las capacidades institucionales en materia de seguridad pública.

Empezando por el criterio 2, relacionado con el equipamiento policial y de instituciones, fue el que reconoció la precariedad y obsolecencia del equipamiento policial de las instutuciones para enfrentar la delincuencia, por lo que como prioridad se debían destinar mayores recursos de los fondos federales para el equipamiento de las corporaciones con el fin de que las policías contaran con mejor condiciones para el desarrollo de su trabajo, incluyendo "mejores uniformes, mejor protección, mejores vehículos y mejor armamento" (DOF, 2019b).

El criterio 6, referente a la interconexión tecnológica de los sistemas de información federal, estatal y municipal, reconoció que la falta de acuerdos de colaboración y coordinación interinstitucional había limitado su eficacia en el combate del crímen. Para atender esta problemática, se planteó el fortalecimiento de la Plataforma México (la plataforma digital que contiene todas las bases de datos relativas a la seguridad pública del país) con el objetivo de lograr una interconexión eficiente entre los diferentes niveles de gobierno (DOF, 2019b).

El criterio 7, sobre la actualización y fortalecimiento de la Red Nacional de Radiocomunicación, señaló que su estado presentaba un alto nivel de obsolescencia y abandono, además de estar afectado por la existencia de un monopolio, esta situación limitando su desarrollo organizado y articulado. Ante ello, el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, en conjunto con la Secretaría de Seguridad y Protección Ciudadana, debían de establecer medidas para garantizar su operación y vigencia a largo plazo, contemplando específicamnte la libre competencia en la provisión de infraestructura y servicios, la actualización e integración distintas tecnologías de comunicación usados por el Estado y sus instituciones de seguridad para optimizar la su conexión entre sistemas de rario y de satélite (MEXSAT MORELOS III) y robustecer la capacidad de respuesta garantizando una comunicación segura y continua en el marco de la seguridad pública (DOF, 2019b).

El criterio 8 relacionado con el fortalecimiento tecnológico del Registro Vehicular (REPUVE) abordó la problemática del robo de vehículos y se subrayó que las experiencias previas en materia de registro de vehículos habían sido insatisfactorias, por lo que se impulsó la consideración del REPUVE como un instrumento de seguridad destacando su utilidad en el combate al delito, ya que facilitaba la identificación rápida de los responsables a través del seguimiento de los vehículos involucrados en el crimen (DOF, 2019b).

Finalmente, el criterio 9 relacionado con el fortalecimiento de los sistemas de videovigilancia y geolocalización señaló que, en gran parte de las ciudades y municipios del país, los sistemas existentes no estaban operando adecuadamente. Además, se identificó la falta de un esquema adecuado de mantenimiento y capacitación para los sistemas ya instalados, lo que limitaba su efectividad. A pesar de estas deficiencias, se reconoció que los sistemas de videovigilancia y geolocalización habían demostrado ser efectivos para reducir la criminalidad, lo que justificó su fortalecimiento y mejora en el ámbito nacional (DOF, 2019b).

Posteriormente un año después, en 2020, estos criterios fueron retomados dentro del objetivo 4 del Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024 con la finalidad de establecer estrategias y acciones específicas relacionadas con la seguridad de la infraestructura y de ciberseguridad (DOF, 2020).

Este programa señaló que la deficiencia tecnológica del Estado había facilitado el incremento de delitos cibernéticos, generando nuevos espacios para la actividad delictiva y afectando especialmente a grupos vulnerables, quienes podían convertirse tanto en víctimas como en replicadores de violencia (DOF, 2020), mencionando que en los anteriores seis años a su publicación, se habían atendido "más de 260 mil incidentes y 68 mil reportes ciudadanos, neutralizando alrededor de 26 mil sitios web identificados con actividades ilícitas", y se habían "realizado 4,500 colaboraciones internacionales", por lo que se requería una atención prioritaria (DOF, 2020).

El Objetivo 4 fue el aquel que se centró en fortalecer las capacidades tecnológicas de las instituciones de seguridad en los tres órdenes de gobierno para la protección de las instituciones públicas y para la persecución del delito, dentro del cual se establecieron cuatro estrategias prioritarias con acciones puntuales dirigidas a mejorar la infraestructura de ciberseguridad de las instituciones de seguridad pública y para el combate del ciberdelito.

La primera de ellas, fue la estrategia 4.1 "Actualizar la infraestructura en materia de tecnologías de la información y comunicaciones para que las instituciones de seguridad de los tres órdenes de gobierno mantengan la disponibilidad de los servicios tecnológicos" (DOF, 2020).

La estrategia priorizó la modernización de infraestructuras críticas con medidas como la actualización de la Red Nacional de Radiocomunicación mediante sistemas cifrados (acción puntual 4.1.1), la interconexión segura de plataformas gubernamentales a través de redes cifradas (4.1.3), y la incorporación de tecnologías para el almacenamiento y transmisión segura de datos (4.1.4), con el fin garantizar la disponibilidad y confidencialidad de la información institucional.

La segunda estrategia 4.2 fue "Implementar procesos de gestión de riesgos para la protección de los sistemas de información y telecomunicaciones de las plataformas tecnológicas que permitan a las instituciones de seguridad de los tres órdenes de gobierno proteger la información ante la presencia de ciberataques" (DOF, 2020).

La estrategia se enfocó en la protección proactiva contra ciberataques. Esto incluyó la implementación de protocolos de seguridad informática para prevenir intrusiones de ciberataques (4.2.1), la promoción de acuerdos con el sector público, privado e instituciones internacionales para la prevención, investigación y persecución del ciberdelito (4.2.2 y 4.2.4) y programas de capacitación en herramientas de ciberseguridad para funcionarios públicos (4.2.3). Además, el diseño de campañas de concientización sobre riesgos digitales dirigidas a instituciones públicas (4.2.5), tal como detalla el DOF (2020).

La tercera estrategia 4.3 "Actualizar y desarrollar los sistemas informáticos que permitan la optimización, homologación e interoperabilidad entre los sistemas de las instituciones de seguridad de los tres órdenes de gobierno para generar inteligencia en la prevención, investigación y persecución del delito", estableció la estrategia 4.3.3 para la homologación de sistemas para la validación segura de identidades en bases de datos institucionales con el fin de prevenir fraudes y accesos no autorizados.

Finalmente la cuarta estrategia, "4.4 Mejorar los procesos de interconexión tecnológica entre las instituciones de seguridad de los tres órdenes de gobierno para facilitar la generación de inteligencia en la prevención, investigación y persecución del delito", estableció la estrategia 4.4.1 para la homologación de bases de datos entre instituciones para el intercambio seguro de información, evitando vulnerabilidades cibernéticas derivadas de la fragmentación de los sistemas.

Posteriormente en 2021, fue publicado otro instrumento programático del periodo presidencial de AMLO que retomó el tema de la ciberseguridad en materia de seguridad pública, la Estrategia Digital Nacional 2021-2024, la cual se orientó a la necesidad de “el uso y el desarrollo de las TIC al bienestar social del pueblo mexicano" con una visión humanista y bajo los principios de "austeridad republicana, transparencia" y el "privilegio de lo público y el uso o desarrollo nacional de tecnologías de acceso abierto" buscando conducir el potencial transformador de las tecnologías hacia el fortalecimiento de los programas sociales y su impacto en la población beneficiaria (DOF, 2021b).

La Estrategia Digital Nacional 2021-2024 (EDN 2021-2024, a partir de ahora) contempló dentro de su objetivo específico 5 titulado “Promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales”, las medidas de ciberseguridad en las instuciones públicas para la seguridad de los ciudadanos.

Siendo este el primer instrumento programático del gobierno de AMLO en el que existió una estrategia específica con todas sus lineas de acción destinadas a la ciberseguridad. La lista completa de estrategias adoptadas se presenta a continuación.

- Promover una política general de seguridad de la información que procure la preservación de la confidencialidad, disponibilidad e integridad de la información resguardada por las Instituciones.
- Promover la implementación de un protocolo homologado para la gestión de incidentes cibernéticos entre las instituciones.
- Coordinar evaluaciones de seguridad en las Instituciones para la detección de amenazas y mejorar la gestión de riesgos de seguridad de la información.
- Fortalecer la coordinación entre autoridades para mejorar los procesos de prevención y atención de incidencias cibernéticas.
- Promover buenas prácticas de prevención y reacción a través de la colaboración con el Centro Nacional de Respuesta a Incidentes Cibernéticos [CERT-MX].
- Proponer la adopción de acciones clave para fortalecer los mecanismos de seguridad de la información que prevengan riesgos y amenazas a la información e infraestructura institucional. (DOF, 2021b)

Como parte de la implementación de estas estrategias, fue publicado en septiembre de ese mismo año, 2021, el "*Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal*", en el que en su capítulo cuarto establecen las políticas tecnológicas aplicables a los proyectos de Tecnologías de la Información y Comunicación (TIC) y de Seguridad de la Información (SI) (DOF, 2021c).

Dentro del cual, el capítulo VI es específica para la política general de "Seguridad de la Información", en la que se centra en la creación de un Marco de Gestión de Seguridad de la Información (MGSI) que garantice altos niveles de confidencialidad, integridad y disponibilidad de los datos en las instituciones públicas. En este sentido, el artículo 75 establece de política que cada dependencia y entidad integrante de la administración pública federal debe alinear su MGSI a esta política general de Seguriad de la Información contenida en el capítulo, procurando que dicho marco contribuya al cumplimiento de objetivos institucionales, tecnológicos, regulatorios, organizacionales, operativos y culturales para asegurar la continuidad y la integridad de la información (DOF, 2021c).

Asimismo, el artículo 76 detalla los elementos indispensables que debe incorporar cada MGSI. Entre ellos se encuentran la definición de objetivos claros, la identificación y clasificación de procesos y activos críticos, y la realización de un análisis de riesgos que permita detectar amenazas y vulnerabilidades cibernéticas.

Además, se exige la implementación de controles mínimos de seguridad basados en estándares técnicos, el desarrollo de un programa de gestión de vulnerabilidades, y la instauración de un protocolo de respuesta ante incidentes cibernéticos, que incluye la conformación de un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC), alineado con lo que posteriormente se conocería y formalizaría en el *Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos* un mes después, en octubre de 2021 (DOF, 2021c).

Este modelo asignaría responsabilidades específicas al CERT-MX de la Guardia Nacional y a la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), la cual,

en 2023, fue reemplazada por la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información (CITICSI).

Finalmente, el último instrumento programático de AMLO fue el Programa Nacional de Seguridad Pública 2022-2024, publicado en 2022, en el que se inserta la prevención de conductas delictivas en el ciberespacio relacionadas con la delincuencia organizada, junto con el combate en el robo a autotransporte y pasajeros en carreteras y el combate al mercado ilícito de hidrocarburos en el objetivo pioritario 3 “Disminuir los delitos vinculados con la delincuencia organizada en las regiones del país”, el cual reconoce que “la actividad criminal se diversifica por medio de nuevas formas para la comisión de ilícitos y traslada sus actividades hacia el ciberespacio y plataformas como el Internet” (DOF, 2022).

Para el caso de la prevención de las conductas delictivas en el ciberespacio, la estrategia prioritaria 3.4 "Fortalecer los mecanismos de investigación para prevenir las conductas delictivas en los sitios web" estableció cinco acciones puntuales para lograrlo y delegando su ejecución y seguimiento en la Secretaría de Seguridad y Protección Ciudadana (DOF, 2022).

La primera de ellas, la acción 3.4.1, estableció que se debían realizar acciones de rastreo en la red pública de Internet sobre sitios web con el fin de prevenir conductas delictivas que atentaran contra la integridad de niñas, niños, adolescentes, jóvenes y adultos mayores (DOF, 2022).

La segunda acción, 3.4.2, estableció que se implementaran mecanismos de detección de ataques en ciberseguridad sobre la infraestructura tecnológica, con el objetivo de asegurar y resguardar la información contenida en las plataformas tecnológicas (DOF, 2022).

La tercera acción, 3.4.3, estableció que se diseñaran e implementeran medidas y protocolos de operación que permitieran prevenir delitos cibernéticos y proteger a los usuarios del ciberespacio durante el intercambio de información en materia de seguridad (DOF, 2022).

La cuarta acción, 3.4.4, estableció la necesidad de establecer acuerdos con organismos nacionales e internacionales, tanto públicos como privados, para generar medidas que faciliten la prevención, investigación y persecución del delito en materia de ciberseguridad (DOF, 2022).

Finalmente, la quinta acción, 3.4.5, estableció que se diseñaran e implementaran mecanismos para dar respuesta a incidentes de ciberseguridad, así como para dar seguimiento a las acciones propuestas para su mitigación y prevención (DOF, 2022).

Al final del documento se definen compromisos puntuales sobre resultados a alcanzar para el año 2024, adoptando una visión a mediano plazo sobre los objetivos, además de establecer metas anuales para dar seguimiento y la detección oportuna de acciones de mejora. Sin embargo, a diferencia de lo establecido para la prevención de robos a pasajetos y delitos relacionados con el mercado ilícito de hidrocarburos, la estrategia para prevenir delitos en el ciberespacio no incluyó metas o parámetros específicos.

3.2.4 Instrumentos financieros

Los instrumentos financieros realizados durante el sexenio de Andrés Manuel López Obrador en materia de ciberseguridad en la seguridad pública, enlistados en la Tabla 10, son aquellos que movilizaron recursos económicos para implementar las acciones y lograr sus objetivos gubernamentales planteados (Rosas, 2021).

Tabla 10. Instrumentos financieros de la acción pública del Estado en ciberseguridad en materia de seguridad pública

Instrumento	Descripción
Presupuestos de Egresos de la Federación 2019-2024	Asignó presupuesto federal a los instrumentos organizativos en sus rubros generales, sin partidas específicas para los los dependientes de cada uno, imposibilitando cuantificar gasto específico.
Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal (FASP)	Financió el Modelo Homologado de Policía Cibernética en los estados, para la capacitación, equipamiento tecnológico y creación de las unidades estatales.

Durante el sexenio de Andrés Manuel López Obrador, los recursos económicos asignados a los organismos en materia de ciberseguridad en la seguridad pública se canalizaron a través

de dos instrumentos financieros: el Presupuesto de Egresos de la Federación (PEF) de los años 2019 a 2024 y el Fondo de Aportaciones para la Seguridad Pública (FASP).

Sin embargo, dentro de los Presupuestos de Egresos de la Federación aprobados por la Cámara de Diputados, no se identificaron partidas, programas o ejes presupuestales específicos o explícitos para para la ciberseguridad o el combate del ciberdelito etiquetados dentro de sus estructuras presupuestales. Los únicos datos disponibles corresponden a los montos totales recibidos por cada institución que el gobierno de AMLO utilizó como instrumentos organizativos para estos rubros (SSPC, GN, Presidencia de la República, INAI e IFT), que se detallan en la Tabla 11 excluyendo la inflación con base 2019.

No existe un desglose público que permita determinar qué porcentaje de esos recursos se destinó exclusivamente a sus organismos adscritos en materia de ciberseguridad o en la participación de cada instrumento programático.

Para la Secretaría de Seguridad y Protección Ciudadana (SSPC), su presupuesto inició hasta 2020, puesto que en 2019 "no se presupuestaron recursos originalmente por tratarse de una dependencia de nueva creación" (Transparencia Presupuestaria, 2019, pág.1). Sin embargo, su financiamiento real aumentó progresivamente, pasando de 57.402 millones de pesos en 2020 a 86.866 mdp en 2024.

En el caso de la Guardia Nacional (GN), este comenzó a recibir recursos directamente a partir de 2021 en un rubro específico para la "operación de la Guardia Nacional para la prevención, investigación y persecución de delitos" (Cámara de Diputados, 2021), ya que en 2020 el presupuesto de la SSPC incluyó los fondos destinados a la transición de la Policía Federal a la GN. Su asignación para la prevención, investigación y persecución de delitos creció de 25,521 millones de pesos en 2021 a 31,032 millones en 2024. Por otro lado, la Oficina de la Presidencia de la República tuvo paulatinamente una reducción real, de 876 millones de pesos en 2021 a 725 millones de pesos en 2024.

En cuanto a los órganos autónomos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) presentó un incremento presupuestal, pasando de 900 millones en 2019 a 1,318 millones en 2024. En contraste, el Instituto Federal

de Telecomunicaciones (IFT) sufrió una reducción, con un presupuesto de 864 millones de pesos en 2024, inferior al de los años anteriores.

Tabla 11. Evolución real del presupuesto en pesos (deflactado base 2019) asignado a Ciberseguridad en Seguridad Pública en el PEF (2019–2024)

Año	Secretaría de Seguridad y Protección Ciudadana	Guardia Nacional	Oficina de la Presidencia de la República	INAI	IFT
2019	-	-	1,569,844,550	900,151,692	1,500,000,000
2020	57,402,254,392.31	-	876,605,634.94	837,342,721.01	1,470,820,582.09
2021	57,906,258,036.59	25,521,594,972.85	734,784,326.55	826,343,316.96	1,378,249,506.40
2022	80,079,349,302.90	25,558,444,432.34	715,095,388.59	842,908,973.26	1,337,807,614.77
2023	82,097,387,126.34	28,336,292,151.44	718,573,946.17	859,467,584.89	1,364,088,313.12
2024	86,866,037,999.31	31,032,562,933.31	725,080,389.46	1,318,204,768.64	861,033,673.67

Fuente: Elaboración propia con información del PEF 2019-2024 (Cámara de Diputados, 2019, 2020, 2021, 2022, 2023, 2024)

El segundo instrumento financiero, el Fondo de Aportaciones para la Seguridad Pública de los Estados y el Distrito Federal (FASP), que ha mantuvo durante el perido de AMLO como subprograma el "Modelo Homologado de Unidades de Policía Cibernética", que fue aquel que destinó recursos federales a las entidades federativas para:

> …sentar las bases de coordinación para incrementar la capacidad del estado mexicano en la prevención y atención de Delitos Cibernéticos proponiendo un modelo de operación para las Policías Cibernéticas Estatales, así como los canales de comunicación que sirvan como marco de implementación para la creación y fortalecimiento de las Policías Cibernéticas del país mediante la capacitación y especialización de policías activos. (SSPC y GN, 2023, pág. 2)

El subprograma estableció que los estados deben llevar registros y métricas del actuar de sus unidades de policía cibernética como entregables a la Federación y al FASP, así mismo la

medición del desempeño a través de métricas o indicadores de desempeño del subprograma para “medir sus avances en diferentes dimensiones: ejercicio de recursos, metas alcanzadas, propósitos logrados y contribución a mejorar la seguridad pública dentro del Programa con Prioridad Nacional” (SSPC y GN, 2023, pág. 21).

Finalmente, cada año es publicado el *Informe Nacional de Evaluación del Fondo de Aportaciones para la Seguridad Pública (FASP)*, que resume todas las métricas realizadas por los estados en cada uno de los programas y subprogramas durante el año pasado, así como los montos asignados y acordados entre la federación y los gobiernos locales. Aunque este informe no desglosa exclusivamente las aportaciones federales, la Tabla 12 sintetiza los montos totales del financiamiento conjunto (federal + estatal) destinados al subprograma *Modelo Homologado de Policía Cibernética* hasta 2023, siendo el último informe publicado a la fecha de redacción de este trabajo.

Según los datos financieros, en 2019, el monto asignado fue de aproximadamente 23 millones de pesos, experimentando una disminución del 7% para 2020, cuando se redujo a cerca de 21 millones de pesos. Sin embargo, 2021 marcó un cambio drástico con un incremento del 80%, elevando el financiamiento a casi 39 millones de pesos, lo que podría interpretarse como una respuesta a la creciente amenaza cibernética durante la pandemia. Este impulso continuó en 2022, aunque a menor ritmo, con un crecimiento del 27% que llevó el monto a 49 millones. Para 2023, se observa una considerable desaceleración en el incremento, con solo un 4.68%. Esta evolución puede interpretarse como un un reconocimiento inicial de la importancia de fortalecer las capacidades en materia de policía cibernética, seguido de una disminución en el ritmo de crecimiento de la inversión hacia el final del sexenio

Los datos muestran que la estrategia de financiamiento para enfrentar el problema de los delitos cibernéticos siguió un camino desigual. Por un lado, instituciones como la Guardia Nacional y la Secretaría de Seguridad recibieron aumentos constantes en sus presupuestos, mientras que los órganos autónomos (INAI y el IFT) enfrentaron recortes, a pesar de su papel fundamental en la protección de datos personales y la regulación de infraestructura crítica.

Tabla 12. Evolución real (deflactado base 2019) del monto pagado a las entidades federativas en pesos para el subprograma 7 en financiamiento conjunto del "Modelo Homologado de Unidades de Policía Cibernética" del FASP

Año	Monto ($)	Incremento porcentual anual
2019	22,948,139.37	-
2020	21,369,146.71	-6.88%
2021	38,565,847.75	80.47%
2022	49,040,261.80	27.16%
2023	51,337,264.29	4.68%

Elaboración propia con información de SSPC y SESNSP (2020, pág. 3; 2021, pág. 42; 2022, pág. 152; 2023, pág. 101; 2024, pág. 59)

Esta disparidad no es casual. Refleja el enfoque preferencial del gobierno de López Obrador, que priorizó sistemáticamente a las instituciones de seguridad nacional sobre aquellos organismos autónomos. Resulta paradójico que, a lo largo del sexenio, el INAI y el IFT hayan sido objeto de constantes cuestionamientos públicos por parte del presidente, cuando en la práctica colaboraron activamente para el problema de la ciberseguridad y los delitos cibernéticos con las propias dependencias de seguridad de su administración.

El patrón presupuestal tiene una visión de la ciberseguridad como un tema exclusivamente vinculado a la defensa nacional, más que como una política de Estado integral. Mientras se inyectaban recursos a instituciones de carácter policial-militar, se debilitaba deliberadamente a los organismos constitucionalmnte autónomos encargados de asegurar transparencia, rendición de cuentas y protección de derechos en el espacio digital.

En la revisión de instrumentos de acción pública, se identificaron acciones que no pueden ser clasificados dentro de la tipología recuperada para la reconstrucción de la política pública (instrumentos normativos, organizativos, programáticos ni financieros). Siendo que estos nuevos documentos que operacionalizan la acción gubenamental articulando todos los instrumentos para la ciberseguridad de la seguridad pública, estos son el *Modelo Homologado de Policía Cibernética* y el *Protocolo Nacional Homologado de Gestión de*

Incidentes Cibernéticos, de los que podemos decir que fueron los instrumentos operativos del gobierno de López Obrador para el problema de la ciberseguridad en la seguridad pública.

El primero de ellos, el *Modelo Homologado de Policía Cibernética*, fue formulado en el periodo presidencial de Enrique Peña Nieto y continuado por López Obrador en su implementación nacional con recursos del Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal (FASP).

La información disponible sobre la implementación del Modelo Homologado de Policía Cibernética se ha documentado únicamente en los informes oficiales de la Guardia Nacional de 2020 y 2024. El informe de 2020 representa el primer y único ejercicio que actualiza el mapeo de los niveles de maduración de las unidades estatales desde el diagnóstico inicial de 2016, mientras que el reporte de 2024 se limita a detallar el gasto de recursos del FASP sin evaluar capacidades operativas (SSPC y GN, 2020; SSPC y GN, 2024).

El principal problema radica en que el informe de 2020 no sirve para comparar con el diagnóstico de 2016 porque utilizan criterios totalmente distintos para medir los niveles de madurez, los criterios de evaluación utilizados en 2020 responden a los estándares definitivos del Modelo Homologado, los cuales difieren de los aplicados en el diagnóstico de 2016. Por ejemplo, lo que en 2016 se consideraba nivel 2 (procesos intermedios documentados) dista del nivel 2 de 2020 (capacidades forenses especializadas). El mapeo de 2020 debe entenderse como la línea base definitiva del modelo con los estándares oficiales, no como una continuación del diagnóstico incial.

Para 2020, las entidades federativas muestran una distribución desigual en los niveles de madurez alcanzados. La mayoría de las entidades federativas (53%) se encuentran en el nivel 0 que corresponde a unidades con capacidades básicas de prevención. Este grupo incluye 17 entidades federativas, es decir, en 2020, más de la mitad de los estados apenas contaban con los fundamentos operativos mínimos establecidos por el modelo.

Un 22% de las entidades (7 estados) alcanzaron el nivel 1, que implica funciones de atención ciudadana y ciberpatrullaje. Cuatro años después de la implementación del modelo solo una minoría de estados había logrado desarrollar capacidades operativas intermedias.

Tabla 13. Mapeos oficiales del estado de maduración de las unidades cibernéticas estatales de policía cibernética (2016 y 2020)

Diagnóstico incial para la creación del Modelo Homologado de Policía Cibernética (2016)			**Avances de la implementación del Modelo Homologado De Unidades De Policía Cibernética (2020)**		
Nivel de Maduración	**Entidades Federativas**	**%**	**Nivel de Maduración**	**Entidades Federativas**	**%**
0 (no cuentan con una Unidad Cibernética)	Baja California Sur, Chiapas, Colima, Durango, Guerrero, Morelos, Oaxaca, Puebla, Quintana Roo, Sinaloa y Tamaulipas.	35%	**0** (capacidades básicas de prevención)	Baja California, Baja California Sur, Sinaloa, Durango, Nuevo León, Tamaulipas, Zacatecas, Nayarit, Aguascalientes, Gauanajuato, Hidalgo, Campeche, Yucatán, Quintana Roo, Oaxaca, Sonora y Colima	53%
1 (operación básica y no documentada en materia de delitos cibernética)	Aguascalientes, Baja California, Campeche, Coahuila, Nayarit, San Luis Potosí, Sonora, Tabasco, Yucatán y Zacatecas.	32%	**1** (funciones de atención ciudadana y ciberpatrullaje)	Coahuila, San Luis Potosí, Veracruz, Puebla, Guerrero, Tabasco y Chiapas.	22%
2 (operación básica–intermedia y procesos repetitivos en materia de delitos cibernéticos)	Chihuahua, Ciudad de México, Jalisco, Estado de México, Michoacán, Nuevo León, Querétaro y Veracruz.	25%	**2 (**capacidades especializadas de investigación y análisis forense**)**	Chihuahua, Jalisco, Michoacán, Querétaro, Estado de México y Ciudad de México.	19%
Sin información	Guanajuato, Tlaxcala e Hidalgo.	8%	**Sin información**	Tlaxcala y Morelos.	6%

Fuente: Elaboración propia con información de (SSPC y GN, 2023; SSPC y GN, 2024)

El nivel más avanzado (nivel 2), correspondiente a capacidades especializadas de investigación y análisis forense, solo fue alcanzado por seis entidades federativas (19% del total): Chihuahua, Jalisco, Michoacán, Querétaro, Estado de México y Ciudad de México. Podemos decir que esta "élite tecnológica" representa menos de una quinta parte del total

nacional, evidenciando las marcadas desigualdades en el desarrollo de capacidades cibernéticas entre estados y los desafíos pendientes en materia de ciberseguridad a nivel local.

No obstante el informe de 2024 expresa como objetivo a desarrollar dentro de ese año "Identicar el nivel de madurez de cada Unidad de Policia Cibernética del Páis con la finalidad de promover el fortalecimiento de las capacidades nacionales" (SSPC y GN, 2024, pág. 7) es desconocido si se llevó a cabo, puesto que no hubo información o informes publicados posteriormente haciendo referencia a la evolución del modelo.

Por otro lado, el *Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos* fue desarrollado en 2021 por la Coordinación de Estrategia Digital Nacional en colaboración con la Guardia Nacional teniendo como objetivo:

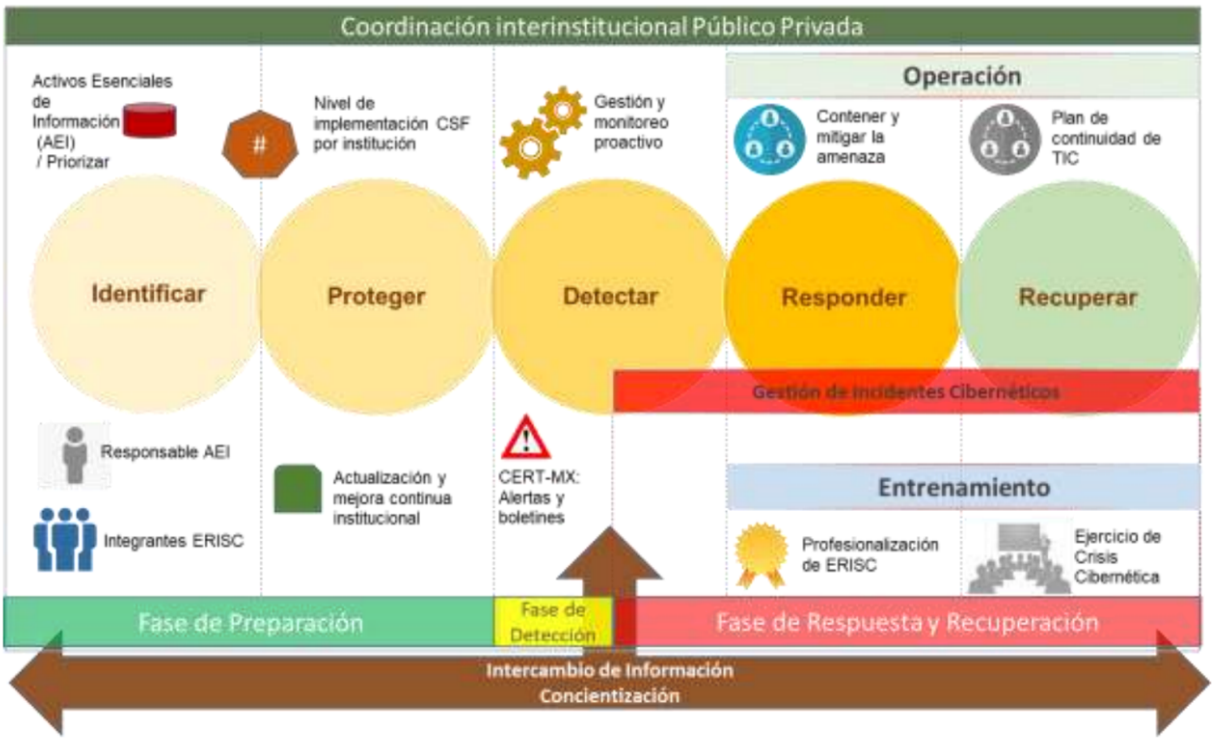
> Establecer y operar el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, que permita fortalecer la Ciberseguridad en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país, con la finalidad de alcanzar los niveles de riesgo aceptables en la materia, contribuyendo al mantenimiento del orden constitucional, la preservación de la democracia, el desarrollo económico, social y político del país, así como al bienestar de las mexicanas y los mexicanos. (CEND y GN, 2021, pág. 3)

Siendo su modelo de operación basado en cinco funciones conectadas a lo largo de tres fases (preparación, detección, respuesta y recuperación ante incidentes cibernéticos) como se muestra en la figura 1, donde en cada fase, el protocolo cumple una función específica y asigna responsabilidades específicas tanto a los Múltiples Involucrados como al CERT-MX de la Guardia Nacional y a la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), la cual, en 2023, fue reemplazada por la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información (CITICSI).

La primera de ellas, Identificar, se orientó en la identificación del contexto de las instituciones de la administración pública federal, entidades federativas, organismos constitucionales autónomos, academia e instancias del sector privado del país (los llamados "Múltiples Involucrados"); sus activos esenciales de información que soportan los servicios

esenciales; y sus riesgos en materia de Ciberseguridad con el propósito de desarrollar una estrategia de gestión de riesgos alineada a las necesidades de cada institución (CEND y GN, 2021, pág. 12).

Figura 1. Modelo de operación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos



Fuente: Recuperado de (CEND y GN, 2021, pág. 12).

La segunda función, Proteger, se "orienta en el desarrollo de un plan apropiado de seguridad que garantice la entrega de los servicios esenciales proporcionados por los activos esenciales de información", con el fin de "establecer estrategias para limitar o contener el impacto de un eventual ataque cibernético" (CEND y GN, 2021, pág. 12).

La tercera función, Detectar, se "orienta en el desarrollo de acciones apropiadas para la detección de eventos que afecten la Ciberseguridad de los activos esenciales de información y en consecuencia puedan afectar los servicios esenciales que prestan", siendo esta detección oportuna ante ataque cibernéticos (CEND y GN, 2021, pág. 13).

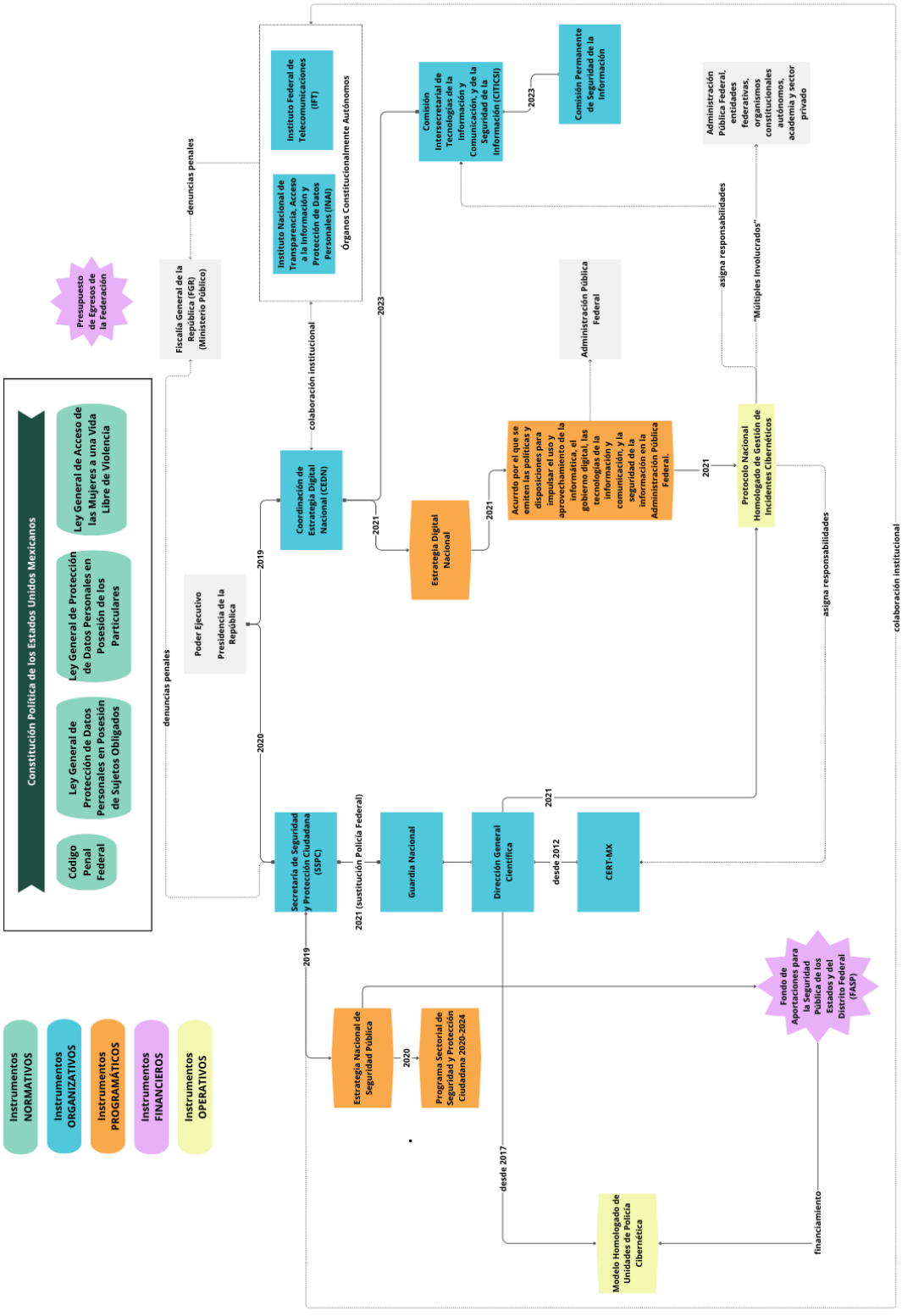
La cuarta función, Responder, se "orienta en el desarrollo e implementación de acciones apropiadas respecto de la atención de eventos de Ciberseguridad que puedan afectar los servicios esenciales", es decir, "la habilidad para contener el impacto de un ataque cibernético" (CEND y GN, 2021, pág. 13).

La quinta y última función, Recuperar, se "orienta en el desarrollo e implementación del plan de resiliencia que permita la restauración en el menor tiempo posible de cualquier capacidad o servicio esencial que haya sido impactado por un ataque cibernético para reducir la afectación en los activos esenciales de información" (CEND y GN, 2021, pág. 13).

Finalmente, la identificación de estos tipos de instrumentos que no corresponden a la tipología teórica recuperada, sugieren la necesidad de expandir las tipologías clásicas de instrumentos de política pública para incorporar esta categoría operativa. A diferencia de otros instrumentos, estos instrumentos fueron diseñados para operar inmediatamente como manuales de acción. El Protocolo especifica detalladamente las cinco funciones críticas y las fases de operación, mientras que el Modelo establece los parámetros concretos para homologar y evaluar capacidades estatales. Esta característica los convierte en herramientas únicas para la política de ciberseguridad.

La identificación de estos instrumentos permite mapear la acción gubernamental frente a la problemática de los ciberdelitos y la ciberseguridad en México. La Figura 2 sintetiza los instrumentos detectados, representando el conjunto de acciones emprendidas por el Estado mexicano en esta materia en el periodo presidencial de López Obrador.

Figura 2. Instrumentos de política pública en materia de ciberdelitos y ciberseguridad en México (2018–2024)



Fuente: elaboración propia.

Capítulo 4. Identificación y evaluación de las preferencias y capacidades institucionales del Estado mexicano en ciberseguridad en el periodo obradorista (2018-2024)

El presente capítulo constituye la segunda y última parte del núcleo analítico de esta investigación, con el objetivo de evaluar las capacidades institucionales desarrolladas en el periodo de AMLO sobre la política de ciberseguridad para la seguridad pública en México haciendo uso de la matriz de evaluación preferencias y capacidades institucionales propuesto en el capítulo 1.

Para ello, este capítulo se organiza en cuatro secciones que corresponden a las variables clave para evaluar las capacidades institucionales de México en materia de ciberseguridad. La evaluación se realiza con base en el marco analítico desarrollado en el apartado 1.3 Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos, el cual establece indicadores específicos para medir las preferencias y capacidades del Estado.

La primera sección analiza la estructura organizacional en ciberseguridad, evalúa las preferencias institucionales sobre los organismos responsables y sus mecanismos de coordinación. La segunda evalúa el enfoque de la normativa vigente, considerando su alcance y adecuación frente a los desafíos digitales actuales. La tercera sección estudia las políticas de respuesta a incidentes cibernéticos y persecución del ciberdelito, incluyendo protocolos de acción y herramientas programáticas. Finalmente, la cuarta sección aborda la cooperación internacional en el combate a ciberdelitos, revisando los mecanismos de vinculación con estándares globales.

4.1 Estructura organizacional en ciberseguridad

Como se identificó en el Capítulo 3, la estructura organizacional de la ciberseguridad en México en materia de seguridad ciudadana se caracteriza por la dispersión de responsabilidades entre diversas entidades. Esta característica distribuye competencias entre múltiples organismos gubernamentales, cada uno con roles específicos dentro de un esquema de atribuciones compartidas.

Es decir, que dentro de las preferencias institucionales del gobierno mexicano, el indicador de la *Ausencia de organismos estatales* en la que no existe una secretaría de Estado o un organismo designado responsable de las políticas de ciberseguridad nacionales, no aplica a México dentro de este periodo analizado.

En el ámbito del Poder Ejecutivo Federal, la Secretaría de Seguridad y Protección Ciudadana representa la única secretaría de Estado con atribuciones directas en materia de ciberseguridad. Esta secretaría, a través de la Guardia Nacional, incorporó las capacidades técnicas especializadas en este campo, específicamente dentro de su Dirección General Científica que tiene como responsabilidades la actuación en contra de la ciberdelincuencia (Reglamento de la Ley de la Guardia Nacional, 2020).

Bajo la estructura de la aquella direccion opera el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), constituyendo su técnicidad dentro del esquema organizacional. Su adscripción a la Guardia Nacional lo sitúa dentro del ámbito de seguridad pública, lo que define en gran medida su enfoque y prioridades operativas.

Paralelamente, la Presidencia de la República participa en este esquema institucional a través de la Coordinación de Estrategia Digital Nacional (CEDN). Esta coordinación representa el componente de alto nivel en la estructura organizacional que incide en aspectos de política pública relacionados con el entorno digital, incluyendo elementos de ciberseguridad.

En el segundo nivel de la CEDN se encuentra la Comisión Intersecretarial de Tecnologías de la Información y Comunicación y de la Seguridad de la Información (CITICSI). Esta comisión constituye el mecanismo de coordinación que integra a representantes de todas secretarías de Estado y otras entidades del ejecutivo, buscando articular esfuerzos entre distintas dependencias federales para la implementación de las políticas en materia de tecnologías de la información, comunicación y seguridad de la información, y conteniendo en su estructura orgánica una subcomisión de Seguridad de la Información para dedicada a diseñar e implementar estrategias de prevención, detección y respuesta a incidentes cibernéticos.

La estructura gubernamental se complementa con la participación de órganos constitucionalmente autónomos que, si bien no dependen jerárquicamente del Poder

Ejecutivo, intervienen en aspectos relevantes para la ciberseguridad. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) constituye un ejemplo de estos organismos. Su autonomía constitucional le otorga un carácter particular dentro del esquema organizacional, aportando una dimensión adicional a la dispersión de responsabilidades en materia de ciberseguridad, particularmente en lo relacionado con la protección de datos personales.

De manera similar, el Instituto Federal de Telecomunicaciones (IFT) participa en el esquema organizacional desde su ámbito de competencia en telecomunicaciones y radiodifusión. Como órgano constitucionalmente autónomo, el IFT mantiene independencia operativa respecto a las entidades del Poder Ejecutivo, lo que añade otra dimensión a la estructura organizacional en materia de ciberseguridad.

Adicionalmente, un aspecto distintivo de esta estructura organizacional es la existencia de competencias superpuestas entre diversas entidades. Esta superposición se manifiesta en varios ámbitos de la ciberseguridad donde dos o más instituciones comparten atribuciones similares o complementarias sin una clara delimitación de responsabilidades.

En el ámbito de la respuesta a incidentes cibernéticos, tanto el CERT-MX de la Guardia Nacional como la Comisión Permanente de Seguridad de la Información de la CITICSI tienen atribuciones relacionadas con la gestión de incidentes de seguridad informática. Mientras el CERT-MX enfoca su actuación desde una perspectiva operativa y de investigación, la Comisión Permanente lo hace desde un enfoque más administrativo y de política pública, generando áreas donde sus competencias se traslapan.

En el ámbito de la protección de datos personales, el INAI mantiene competencias específicas derivadas de su mandato constitucional. Sin embargo, aspectos operativos relacionados con incidentes que comprometen datos personales también entran en el ámbito de actuación del CERT-MX. Esta situación deriva en una superposición parcial de competencias donde ambas entidades pueden intervenir desde diferentes perspectivas ante un mismo incidente.

De manera similar, en aspectos relacionados con la seguridad de las telecomunicaciones e Internet, el IFT y la Guardia Nacional comparten espacios de actuación. Mientras el IFT regula y supervisa aspectos técnicos de las telecomunicaciones desde su mandato como

órgano regulador, la Guardia Nacional interviene desde la perspectiva de seguridad pública cuando estos aspectos se relacionan con posibles conductas delictivas en el ciberespacio.

El resultado es una estructura donde la ciberseguridad no recae en una sola entidad dedicada, sino que se distribuye en la coexistencia de organismos del Poder Ejecutivo, comisiones intersecretariales y órganos autónomos que operan con mandatos específicos propios y realizan funciones dentro de sus respectivos ámbitos de competencia sin liderazgo total y que configuran un esquema organizacional donde las responsabilidades en materia de ciberseguridad se encuentran distribuidas y parcialmente superpuestas entre múltiples actores organizacionales.Aunque la Secretaría de Seguridad y Protección Ciudadana (SSPC) se configura como la principal dependencia del Estado mexicano responsable de abordar los temas de ciberseguridad y delitos cibernéticos, pues cuenta con las capacidades más robustas en comparación con las demás dependencias, en la destaca el poder accionar sus capacidades ante un delito cibernético en las fases de prevención (antes), reactiva (durante) y de resiliencia (despues).

La conclusión descrita, la coexistencia fragmentada de organismos con responsabilidades distribuidas y superpuestas, se alinea directamente con la preferncia gubernamental de un andamiaje organizacional fragmentado en varias dependencias. Por ello para la variable estructura organizacional en ciberseguridad, se le asigna un puntaje de 1. Pues aunque la SSPC, si bien constituye la dependencia principal para abordar la ciberseguridad, opera dentro de un andamiaje institucional fragmentado. Este andamiaje se caracteriza por: (1) la coexistencia de organismos autónomos y no autónomos aunque con competencias superpuestas; (2) la ausencia de un liderazgo unificado; y (3) la dispersión de responsabilidades en materia de ciberseguridad.

4.2 Enfoque de la normativa sobre ciberseguridad

Dentro de la variable del enfoque de la normativa mexicana sobre ciberseguridad, la materia se encuentra distribuida en diversos ordenamientos jurídicos que en conjunto establecen no solo un marco regulatorio para castigar ciberdelitos, sino para implementar medidas preventivas, definir requisitos de seguridad para organizaciones, fortalecer instituciones y proteger infraestructuras críticas ante ciberataques. Siendo que esta preferencia institucional

del gobierno mexicano comprende el indicador de *Políticas y marcos jurídicos con enfoque integral.*

Empezando con un marco regulatorio base que rige el actuar del Estado ante la comisión de ciberdelitos es la Constitución, como se mencionó en el apartado anterior, la ciberseguridad se encuentra vinculada a derechos humanos, la privacidad y la seguridad pública. Sin embargo, la falta de una referencia explícita a la ciberseguridad como una función del Estado deja su desarrollo a interpretaciones normativas y a la asignación de responsabilidades entre diversas instituciones. Esta ambigüedad ha dado lugar a un enfoque normativo fragmentado en el que múltiples actores, desde el ámbito penal hasta el de protección de datos personales, intervienen en la respuesta gubernamental ante amenazas cibernéticas (ver apartado, 3.2.1 Instrumentos normativos).

En el ámbito penal, el marco jurídico vigente establece sanciones aplicables a quienes cometan ciberdelitos, aunque sin tipificar explícitamente dichas conductas bajo un concepto uniforme de "ciberdelito". Por ejemplo, el acceso no autorizado a sistemas informáticos, la revelación o uso indebido de información confidencial, el fraude informático y otros actos que atentan contra la integridad de los datos pueden ser sancionados a partir de figuras jurídicas ya establecidas, como la revelación de secretos o la violación de la Ley General de Protección de Datos Personales. Sin embargo, la falta de una clasificación clara y homogénea dificulta la labor del Ministerio Público, que debe argumentar cada caso con base en la normatividad vigente, lo que puede generar inconsistencias en la aplicación de la justicia.

Por ejemplo, Luque-Ruiz (2024), señala que la ausencia de una legislación específica en materia de ciberseguridad y la falta de actualización en la normativa jurídica han dificultado en México la investigación, persecución y sanción efectiva de los ciberdelitos. Propone la incorporación de un catálogo de delitos cibernéticos con definiciones claras y tipificaciones específicas para fortalecer el marco jurídico y enfrentar de manera efectiva las consecuencias de estos actos delictivos.

Asimismo, se ha destacado la necesidad de regular el ciberespacio y definir conceptos como la identidad digital argumentando que, sin una delimitación clara de estos elementos, es

complicado tipificar y sancionar adecuadamente delitos relacionados, como la vulneración, el robo o la usurpación de identidad (Gallegos, 2022).

Desde una perspectiva preventiva, tanto el sector público como el privado tienen la obligación de implementar medidas de seguridad de la información y gestión de riesgos conforme a las leyes de protección de datos personales. En el gobierno de Andrés Manuel López Obrador, se impulsó la implementación obligatoria de marcos de gestión de información en todas las organizaciones y dependencias del Poder Ejecutivo Federal, con el objetivo de fortalecer la protección de datos y establecer requisitos mínimos de seguridad en sus sistemas informáticos.

En cuanto al fortalecimiento institucional, los documentos programáticos del Modelo Homologado de Unidades de Policía Cibernética establecieron la necesidad de fortalecer continuamente las capacidades operativas de las unidades estatales dedicadas a la investigación y persecución de ciberdelitos. Por ello el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) y la Guardia Nacional han señalado, a través de solicitudes de transparencia (INAI, 2025a; INAI, 2025b), que participa en iniciativas internacionales para el combate al ciberdelito y al ciberterrorismo. Estas colaboraciones incluyen:

1. La participación activa en organismos multilaterales como la Organización de los Estados Americanos (OEA), INTERPOL y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), donde se comparte inteligencia sobre amenazas cibernéticas y se desarrollan capacidades técnicas conjuntas y hay un fortalecimiento de capacidades en la identificación y mitigación de ataques cibernéticos.
2. La integración en redes especializadas de respuesta a incidentes, específicamente en CSIRT Américas (iniciativa de la OEA que busca fortalecer las capacidades de respuesta ante incidentes de ciberseguridad en los países de la región), que permite el intercambio de alertas tempranas y buenas prácticas entre equipos de seguridad cibernética de la región.
3. La colaboración con otros equipos internacionales de respuesta de incidentes miembros del Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST, por

sus siglas en inglés), para fortalecer la capacidad de respuesta y recuperación ante incidentes.

4. La asistencia regular a foros internacionales como el Tercer Congreso Internacional de Investigación e Inteligencia y las reuniones del Grupo de Trabajo de Ciberseguridad de la OEA, espacios donde se discuten protocolos y estrategias contra el cibercrimen.
5. El desarrollo de ejercicios de simulación y capacitaciones conjuntas con otros países para mejorar la preparación ante posibles ataques cibernéticos y el monitoreo continuo de amenazas en Internet a través del CERT-MX, utilizando protocolos estandarizados internacionalmente para la detección y análisis de riesgos digitales.
6. La participación dentro de la Iniciativa Global contra el Terrirismo Cibernético con actividades relacionadas al monitoreo de amenazas cibernéticas en la red pública de Internet a través del CERT-MX para detectar eventos hacktivistas y ciberyihadistas, el capacitación y entrenamiento en técnicas avanzadas de detección y respuesta ante ataques cibernéticos en colaboración con organismos internacionales, y la participación de ejercicios de simulación para la mejora de coordinación en la respuesta de incidentes cibernéticos de carácter internacional.

Es decir, que dentro del marco normativo vigente en México son reflejados los enfoques en la gestión de la ciberseguridad los cuales han permitido estructurar una respuesta tanto punitiva como preventiva ante los ciberdelitos y las amenazas digitales. Por un lado, el enfoque punitivo establece sanciones para conductas ilícitas en el entorno digital, utilizando figuras legales ya existentes para su persecución. Aunque no hay una tipificación única de los ciberdelitos, este enfoque ha permitido aplicar sanciones a través de normativas como la Ley General de Protección de Datos Personales y diversas disposiciones del Código Penal Federal. Por otro lado, el enfoque preventivo se ha fortalecido en los últimos años con la adopción de marcos de gestión de información en el sector público, la implementación de estándares de seguridad en organismos gubernamentales y la promoción de medidas orientadas a la resiliencia institucional.

En este contexto, la matriz de identificación de preferencias y capacidades institucionales indica que México cumple con los criterios de un enfoque integral, logrando una calificación

de 4 puntos en esta categoría. La combinación de esfuerzos en la persecución de delitos cibernéticos y el fortalecimiento institucional ha permitido avanzar en la consolidación de una estrategia de ciberseguridad que abarca tanto la respuesta ante incidentes como la prevención de riesgos en el entorno digital.

4.3 Enfoque de las políticas asociadas a las respuestas ante incidentes informáticos, a la protección de la infraestructura crítica y a la persecución del ciberdelito

Para el caso de la varieble que expica cómo México responde ante incidentes informáticos, se identificó en el apartado *3.3.3 Instrumentos organizativos* que el país cuenta con el Centro de Respuesta a Incidentes Cibernéticos (CERT-MX), que funge como el equipo especializado en atender este tipo de situaciones. Este organismo opera bajo un modelo homologado de gestión de incidentes cibernéticos que contempla diversas fases diseñadas para abordar los ataques de manera integral. En primer lugar, se busca prevenir los incidentes mediante medidas proactivas. Sin embargo, en caso de que estas medidas no sean suficientes y ocurra un ataque, la siguiente etapa se centra en la contención del mismo, con el objetivo de mitigar al máximo los daños ocasionados.

El modelo implementado por el CERT-MX también incluye la colaboración activa de múltiples partes interesadas. Entre estas se encuentran actores del sector privado, instituciones académicas y otras organizaciones relevantes a las que llama “múltiples involucrados” . Este enfoque colaborativo permite que tanto las infraestructuras críticas del sector público como las del sector privado puedan ser protegidas de manera más efectiva. En caso de un incidente, el CERT interviene para contenerlo y, una vez superada la emergencia, facilita una fase posterior orientada al aprendizaje y la resiliencia organizacional. Esto último para fortalecer las capacidades preventivas y reactivas frente a futuros ataques.

También, la institucionalización de las políticas de ciberseguridad en México ha estado marcada por la Estrategia Nacional de Ciberseguridad (2017) y la implementación del Modelo Homologado de Unidades de Policía Cibernética, el cual comenzó a desarrollarse en 2016 con la colaboración de la Policía Federal y el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. Este modelo estableció estándares para la capacitación de

unidades estatales, promoviendo la formación de policías cibernéticas en las entidades federativas, lo que permitió mejorar la capacidad de respuesta ante incidentes cibernéticos

El diagnóstico realizado en 2016 sobre las unidades cibernéticas estatales identificó un desarrollo desigual en términos normativos, operativos y de infraestructura. Mientras que algunas entidades ya contaban con unidades funcionales y normativa específica, otras carecían completamente de estos elementos. Como respuesta, el Modelo Homologado estableció un marco gradual de madurez para la consolidación de las unidades estatales, con niveles progresivos de capacitación, equipamiento y desarrollo operativo. Esto permitió fortalecer la respuesta a ciberdelitos y mejorar la protección de la infraestructura crítica mediante un enfoque coordinado

Además, el Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024 (DOF, 2020) enfatiza la necesidad de acuerdos con organismos nacionales e internacionales para la prevención y persecución del ciberdelito. Estrategias como la 4.2.2 promueven alianzas público-privadas para fortalecer capacidades técnicas, mientras que la 4.4.1 busca homologar bases de datos entre instituciones, facilitando el flujo seguro de información. Estas acciones evidencian un modelo que trasciende el ámbito gubernamental, integrando a actores externos en la protección del ciberespacio.

Es decir, las políticas mexicanas en esta materia adoptan un enfoque colaborativo, donde no se le niega o no se le considera la participación al sector privado y a otros interesados la creación e implementación de la política de ciberseguridad, en la respuesta de incidentes cibernéticos, en el intercambio de información y en el combate del ciberdelito. Siendo que cumple con las características del indicador de un *Enfoque multisectorial*, se asigna la calificación de 2 puntos en esta categoría, al cumplirse la característica de una participación amplia.

4.4 Cooperación internacional

Como última categoría, la cooperación internacional busca identificar cómo el Estado mexicano se vincula internacionalmente mediante acuerdos internaciones que tienen como tema central la cooperación en el combate del ciberdelito.

Aunque los indicadores recuperados señalan como una preferencia institicional mejor calificada el hecho de que México estuviera alineado a un acuerdo internacional sobre delitos cibernéticos al firmarlo o ratificarlo, la realidad muestra que el país no ha establecido compromisos vinculantes en materia de ciberseguridad y ciberdelincuencia mediante la ratificación de algún tratado internacional.

Según información oficial proporcionada por la Secretaría de Relaciones Exteriores mediante solicitudes de información (INAI, 2025b), el país no forma parte algun convenio o tratado internacional sobre delitos ciberneticos, es decir que no forma parte del Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa y tampoco se han adoptado los estándares regulatorios propuestos por otros bloques regionales como la Unión Europea o la Organización para la Cooperación de Shanghái.

La SRE también menciona que la participación mexicana se ha limitado principalmente a espacios de diálogo y cooperación técnica, donde destacó la intervención mexicana en el Comité ad hoc de las Naciones Unidas encargado de elaborar una Convención Integral contra el Ciberdelito, cuyas labores concluyeron en 2024 (INAI, 2025b). Sin embargo, hasta el momento no se ha concretado la ratificación de este instrumento. En el ámbito regional, el país forma parte de iniciativas como el Directorio de Puntos Focales de la Organización de los Estados Americanos (OEA) y la red CSIRT Americas (INAI, 2025b).

El indicador de que el Estado mexicano no suscribe acuerdos internacionales específicos en materia de ciberdelitos y ciberseguridad resulta en una calificación de 0 en la matriz de preferencias y capacidades institucionales, ubicandose en la preferencia institucional de *Sin un alineamiento internacional.*

4.5 Valoración cuantitativa

A partir de la evaluación de los indicadores seleccionados y su respectiva ponderación, se obtuvo un puntaje total de 8 en una escala de 0 a 10, donde 0 representa capacidades iniciales y 10 indica capacidades avanzadas en la implementación de políticas de ciberseguridad, representandose en la Tabla 13.

Tabla 13. Puntuación de las capacidades institucionales en ciberseguridad en materia de seguridad pública del periodo obradorista (2018-2024)

Variable	Preferencia institucional	Indicador de la capacidad institucional	Evidencia	Valor
Estructura organizacional en ciberseguridad	Andamiaje organizacional fragmentado	Existen múltiples secretarías de Estado u organismos (con o sin autonomía, técnicos o políticos) que implementan políticas de ciberseguridad, sin que exista un ente único designado como responsable principal.	Las responsabilidades se distribuyen entre la SSPC, GN y CERT-MX, CITICSI, INAI e IFT.	1
Enfoque de la normativa sobre ciberseguridad	Políticas y marcos jurídicos con enfoque integral	Políticas y marcos jurídicos con enfoque integral	Uso de leyes existentes (Código Penal Federal, LGAMVLV, LFPDPPP y LFPDPPSO) para sancionar ciberdelitos y la implementación de marcos de gestión de riesgos en el sector público para la resiliencia y protección de infraestructuras críticas e información.	4
Enfoque de las políticas asociadas a las respuestas ante incidentes informáticos, a la protección de la infraestructura crítica y a la persecución del ciberdelito	Enfoque multisectorial	Existencia de políticas públicas contemplando la participación del sector público y privado y otras partes interesadas en para la respuesta a ciberincidentes, intercambio de información, protección de infraestructuras críticas y el combate al ciberdelito.	El Programa Sectorial de Seguridad 2020-2024 (Estrategias 4.2.2 y 4.4.1) y el Protocolo Nacional Homolo gado de Gestión de Incidentes Cibernéticos establecen el enfoque tanto público como privado para la creación e implementación de las medidas de la ciberseguridad en la seguridad pública.	3

Cooperación Internacional	Sin alineamiento internacional	Ausencia de tratados vinculantes	México no ha firmado algún tartado internacional en materia de ciberseguridad y ciberdelito.	0
			Total	**8/10**

Fuente: Elaboración propia

En estructura organizacional, se asignó 1/1 al identificarse un *andamiaje organizacional fragmentado*. La evidencia muestra que las responsabilidades en ciberseguridad están distribuidas entre múltiples entidades, como la Secretaría de Seguridad y Protección Ciudadana (SSPC), la Guardia Nacional, el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), la Comisión Intersecretarial de Tecnologías de la Información y Comunicación (CITICSI), el Instituto Nacional de Transparencia (INAI) y el Instituto Federal de Telecomunicaciones (IFT). Si bien la existencia de estos organismos evita un escenario de ausencia total de estructura (0/1), la superposición de competencias y la falta de un ente rector único limitan la coordinación única a niver federal.

El enfoque normativo obtuvo la máxima puntuación (4/4), alineado con *políticas y marcos jurídicos con enfoque integral*. El marco legal combina medidas punitivas, como la aplicación del Código Penal Federal y la Ley General de Protección de Datos Personales, con acciones preventivas, como la obligatoriedad de contar con estándares de gestión de riesgos en el sector público y protocolos para proteger sus infraestructuras críticas.

En políticas asociadas a incidentes informáticos, a la protección de la infraestructura crítica y a la persecución del ciberdelito, se alcanzó 3/3, correspondiente a un *enfoque multisectorial*. Programas como el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos y las estrategias del Programa Sectorial de Seguridad 2020-2024 integran la participación de actores públicos, privados y académicos. Estas iniciativas demuestran una búsqueda por la colaboración multisectorial para responder a incidentes, proteger infraestructuras críticas y combatir el ciberdelito.

En contraste, la cooperación internacional registró 0/2, categorizada como *sin alineamiento internacional*. Aunque México participa en espacios técnicos como CSIRT Américas y foros

de la ONU, la falta de ratificación de tratados vinculantes como el Convenio de Budapest o la adopción de estándares regulatorios internacionales lo distancia de las capacidades avanzadas en este ámbito.

El puntaje total (8/10) indica que el Estado mexicano cuenta con bases institucionales y normativas operativas, cercanas a un nivel avanzado. La proximidad al máximo se sustenta en la existencia organismos especializados (aunque con roles fragmentados), un marco jurídico integral que combina prevención y sanción, y políticas multisectoriales para la gestión de incidentes. No obstante, la distancia con el 10 se explica por la ausencia de compromisos internacionales formales para el combate al ciberdelito.

En contraste, un escenario cercano a 0, caracterizado por vacíos normativos de normas, de políticas y una inexistencia de organismos especializados queda descartado evidenciando que México ha tiene capacidades avanzadas medibles.

Conclusiones

Esta investigación partió de las preguntas: ¿en la administración de Andrés Manuel López Obrador se desarrolló una política de seguridad cibernética en materia de seguridad pública? y ¿qué fortalezas y debilidades institucionales tiene? Tras el análisis realizado en esta investigación, podemos concluir que durante el sexenio 2018-2024 sí se implementaron acciones orientadas a una política de seguridad pública de ciberseguridad, aunque con un desarrollo temporal desigual.

El sexenio obradorista se caracterizó más por la continuidad que por la innovación. La administración federal operó mayoritariamente con estructuras heredadas de gobiernos anteriores, con la única excepción notable de la creación de la CITICSI en 2023, que sustituyó al CIDGE, aparentemente como respuesta reactiva al incidente de ciberseguridad conocido como "Guacamaya Leaks". A diferencia del sexenio anterior, no se desarrolló una Estrategia Nacional de Ciberseguridad propia. En su lugar, se abordó el tema de manera fragmentada en instrumentos programáticos como la Estrategia Digital Nacional 2021-2024 y el Programa Sectorial de Seguridad y Protección Ciudadana, que carecieron de metas específicas y recursos etiquetados dentro del PEF.

Además de los hallazgos principales, se identificó un tipo de instrumento no considerado en la tipología inicial de Rosas (2021), los instrumentos operativos, entre los que destaca el *Modelo Homologado de Policía Cibernética*, que a pesar de su implementación desde el sexenio anterior y su continuidad durante el gobierno de López Obrador, la falta de transparencia en los informes anuales de la Guardia Nacional impide evaluar su evolución real. Pues no se cuenta con datos públicos detallados sobre el avance en los niveles de maduración de las unidades estatales.

Las fortalezas identificadas fueron que México cuenta con marco normativo integral (valorado con 4/4 puntos) que combina adecuadamente medidas punitivas y preventivas, y políticas asociadas a incidentes informáticos con enfoque multisectorial (3/3) que integran la participación de actores públicos, privados y académicos.

La mayor debilidad identificada corresponde a la cooperación internacional (0/2), evidenciada por la nula adopción de estándares regulatorios internacionales. Esta situación

limita la capacidad del Estado mexicano para vincularse internacionalmte ante amenazas transnacionales y beneficiarse de la colaboración internacional en la materia.

Es importante destacar que esta investigación se enfocó exclusivamente en la identificación y análisis de los instrumentos de política pública en materia de ciberseguridad y ciberdelitos en la seguridad pública, sin evaluar su eficacia real para cumplir con los propósitos para los que fueron creados. El incremento del 372% en incidentes cibernéticos entre 2017 y 2023 sugiere que estos instrumentos podrían no estar logrando contener efectivamente las amenazas digitales, pero determinar la relación causal entre las políticas implementadas y los resultados observados requiere estudios adicionales. Determinar con precisión la eficacia real de cada instrumento identificado queda como una tarea pendiente para futuras investigaciones.

A partir de los hallazgos de esta investigación, se propone la creación de una Ley General de Ciberseguridad que establezca la base jurídica específica para la política de Estado en esta materia. Esta normativa deberá contemplar la obligatoriedad de diseñar e implementar una Estrategia Nacional de Ciberseguridad con objetivos definidos en seguridad pública, defensa nacional y protección de derechos digitales. La estrategia resultante debe articularse de manera coherente con la Estrategia Digital Nacional y los programas sectoriales existentes, garantizando la participación coordinada de todos los niveles de gobierno, así como del sector privado, la academia y demás interesados.

Así mismo, se recomienda una actualización del Código Penal Federal para incluir figuras delictivas digitales como el secuestro de datos digitales, el robo de identidad y los ataques a infraestructura crítica, a la vez de fortalecer la cooperación internacional al alinearse con tratados sobre ciberseguridad y armonizándose la legislación federal con aquellos estándares.

Estas propuestas buscan transformar el enfoque actual de la ciberseguridad en México, pasando de un modelo fragmentado a uno integral y alineado con los estándares internacionales, que mediante una política de Estado bien estructurada, coordinada entre todos los actores y con visión de largo plazo será posible garantizar la seguridad digital de los ciudadanos, las instituciones y la infraestructura del país frente a las crecientes y cambiantes amenazas del ciberespacio.

Bibliografía

Aguilar Villanueva, L. F. (2012). *Política pública*. Biblioteca básica de Administración Pública. Siglo XXI Editores.

Arteaga, R. A. D. Ciberdelitos, alarma mundial y políticas de información en ciberseguridad: un acercamiento al contexto de Tamaulipas. *Problemas sociales de información, comunicación e interacción en espacios digitales: panorama expuesto en una sociedad pandémica*, 9.

BBC. (2018a, diciembre 1). *Toma de protesta de AMLO: López Obrador, investido presidente de México*. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-46414847

BBC. (2018b, julio 5). *Elecciones en México: el único estado de los 32 de México en el que no ganó López Obrador*. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-44689634

Bustos Frati, G., & Aguerre, C. (2022). Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos. Centro Latam Digital. https://centrolatam.digital/wp-content/uploads/2022/05/Marco-anali%CC%81tico_ciberseguridad-en-argentina.pdf

Cámara de Diputados. (2019). Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2019. https://www.diputados.gob.mx/LeyesBiblio/abro/pef_2019/PEF_2019_abro.pdf

Cámara de Diputados. (2020). Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2021. https://www.diputados.gob.mx/LeyesBiblio/abro/pef_2020/PEF_2020_abro.pdf

Cámara de Diputados. (2021). Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2021. https://www.diputados.gob.mx/LeyesBiblio/abro/pef_2021/PEF_2021_abro.pdf

Cámara de Diputados. (2022). Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2022. https://www.diputados.gob.mx/LeyesBiblio/abro/pef_2022/PEF_2022_abro.pdf

Cámara de Diputados. (2023). Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2023. https://www.diputados.gob.mx/LeyesBiblio/abro/pef_2023/PEF_2023_abro.pdf

Cámara de Diputados. (2024). Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2024. https://www.diputados.gob.mx/LeyesBiblio/pdf/PEF_2024.pdf

Código Penal Federal [CPF], Reformado, Diario Oficial de la Federación [D.O.F.], 7 de junio de 2024, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Constitución Política de los Estados Unidos Mexicanos [C.P.E.U.M.], Reformada, Diario Oficial de la Federación [D.O.F.], 17 de enero de 2025, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Coordinación de Estrategia Digital Nacional y Guardia Nacional. (2021). Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

Cruz, E. V. (2015). *Retos y oportunidades de la Estrategia Digital Nacional – u-GOB*. https://u-gob.com/retos-y-oportunidades-de-la-estrategia-digital-nacional/

Diario Oficial de la Federación. (2013, mayo 20). Plan Nacional de Desarrollo 2013-2018. https://www.dof.gob.mx/nota_detalle.php?codigo=5299465&fecha=20/05/2013#gsc.tab=0

Diario Oficial de la Federación. (2014, septiembre 4. Estatuto Orgánico del Instituto Federal de Telecomunicaciones. https://www.ift.org.mx/conocenos/estatuto-organico

Diario Oficial de la Federación. (2014a, abril 30). Programa para la Seguridad Nacional 2014-2018. https://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014#gsc.tab=0

Diario Oficial de la Federación. (2014b, abril 30). Programa Nacional de Seguridad Pública 2014-2018. https://www.dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014#gsc.tab=0

Diario Oficial de la Federación. (2017, enero 17). Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://www.diputados.gob.mx/LeyesBiblio/regla/n42.pdf

Diario Oficial de la Federación. (2019a, 26 de marzo). *Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional*. Primera sección, p. 11. https://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_235_26mar19.pdf

Diario Oficial de la Federación. (2019b, 16 de mayo). *Decreto por el que se aprueba la Estrategia Nacional de Seguridad Pública del Gobierno de la República.* https://www.dof.gob.mx/nota_detalle.php?codigo=5560463&fecha=16/05/2019#gsc.tab=0

Diario Oficial de la Federación. (2019c, julio 12). Plan Nacional de Desarrollo 2019-2024. https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019#gsc.tab=0

Diario Oficial de la Federación. (2020, 2 de julio). *Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024.* https://dof.gob.mx/nota_detalle.php?codigo=5596028&fecha=02/07/2020#gsc.tab=0

Diario Oficial de la Federación. (2021a, 1 de junio). *Decreto por el que se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal.* https://www.dof.gob.mx/nota_detalle.php?codigo=5619905&fecha=01/06/2021#gsc.tab=0

Diario Oficial de la Federación. (2021b, 6 de septiembre). *Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024.* https://www.dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

Diario Oficial de la Federación. (2021c, septiembre 6). *Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.* https://www.dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021#gsc.tab=0

Diario Oficial de la Federación. (2022, diciembre 5). Programa Nacional de Seguridad Pública 2022-2024. https://www.dof.gob.mx/nota_detalle.php?codigo=5673252&fecha=05/12/2022#gsc.tab=0

Diario Oficial de la Federación. (2023a, 10 de enero). *Decreto por el que se crea la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información.* https://www.dof.gob.mx/nota_detalle.php?codigo=5676645&fecha=10/01/2023#gsc.tab=0

Diario Oficial de la Federación. (2023b, 3 de abril). *Acuerdo por el que se emiten los Lineamientos para la Integración, Organización y Funcionamiento de la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información.* https://www.dof.gob.mx/nota_detalle.php?codigo=5684585&fecha=03/04/2023#gsc.tab=0

Edeza, M. Á. R. (2018). La elección de 2018 en méxico y la maduración de la democracia: el voto del hartazgo. *LA ELECCIÓN DE LA TRANSFORMACIÓN: LO QUE AMLO SE LLEVÓ*. https://www.academia.edu/45592928/La_elecci%C3%B3n_de_la_transformaci%C3%B3n_lo_que_AMLO_se_llev%C3%B3?sm=b

Fonfría, A., & Duch-Brown, N. (2020). Elementos para una política de ciberseguridad efectiva. *Análisis del Real Instituto Elcano (ARI)*, *127*, 2020. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari127-fonfriaduchbrown-elementos-para-politica-de-ciberseguridad-efectiva.pdf

Forbes México. (2018, abril 16). *AMLO rebasa el 40% de preferencias en encuesta de SDPNoticias*. https://forbes.com.mx/amlo-rebasa-el-40-de-preferencia-en-encuesta-de-sdpnoticias/

Gallegos, R. (2022, October 15). *México carece de legislación y funcionarios especializados en delitos cibernéticos*. https://laverdadjuarez.com/2022/10/15/mexico-carece-de-legislacion-y-funcionarios-especializados-en-delitos-ciberneticos

Gobierno de México. (2017a). Estrategia Nacional de Ciberseguridad. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno de México. (2017b). Comunicado 187: Sesiona la Comisión Intersecretarial para el desarrollo del gobierno electrónico. https://www.gob.mx/sfp/prensa/sesiona-la-comision-intersecretarial-para-el-desarrollo-del-gobierno-electronico

Gobierno de México. (2018). Memoria y Recomendaciones ENCS. https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf

Gobierno de México. (s.f.). Modelo Homologado de Unidades de Policía Cibernética. https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf

Guardia Nacional y Coordinación de Estrategia Digital Nacional. (2021). Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

Guardia Nacional-CERT-MX. (s.f).*¿Qué es CERT-MX?* gob.mx. https://www.gob.mx/gncertmx?tab=%C2%BFQu%C3%A9%20es%20CERT-MX?

Guardia Nacional. (2021). Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. https://www.gob.mx/gncertmx/documentos/94081

Herrera, C. y Urrutia, A. (2012, diciembre 3). Peña Nieto, PRD, PAN y PRI firman el Pacto por México. *La Jornada*. https://www.jornada.com.mx/2012/12/03/politica/002n1pol

https://www.bbc.com/mundo/noticias-america-latina-46410722

Illades, C. (2018, junio 27). AMLO y la oportunidad histórica de la izquierda. *The New York Times*. https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/

INE. (2018a, mayo 28). *Define INE Lista Nominal y Padrón Electoral para #Elecciones2018*. Central Electoral. https://centralelectoral.ine.mx/2018/05/28/define-ine-lista-nominal-y-padron-electoral-para-elecciones2018/

INE. (2018b, julio 1). *Tercer Mensaje en Cadena Nacional de Lorenzo Córdova relativo al resultado del conteo rápido para la elección presidencial*. Central Electoral. https://centralelectoral.ine.mx/2018/07/01/tercer-mensaje-en-cadena-nacional-de-lorenzo-cordova-relativo-al-resultado-del-conteo-rapido-para-la-eleccion-presidencial/

INE. (2018c, julio 6). *Da a conocer INE resultados del cómputo de la elección presidencial 2018*. Central Electoral. https://centralelectoral.ine.mx/2018/07/06/da-conocer-ine-resultados-del-computo-de-la-eleccion-presidencial-2018/

INEGI. (2024). Censo Nacional de Seguridad Pública Federal 2024. Presentación de resultados generales. https://www.inegi.org.mx/contenidos/programas/cnspf/2024/doc/cnspf_2024_resultados.pdf

Instituto Federal de Telecomunicaciones. (2023). *El IFT y la Guardia Nacional llevarán levarán a cabo "Conferencias de Ciberseguridad 2023" (Comunicado de prensa) 23 de octubre*. https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-ift-y-la-guardia-nacional-llevaran-cabo-conferencias-de-ciberseguridad-2023-comunicado-de-prensa

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2025a). Respuesta a solicitud de información (Folio 332259825000220).

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2021). Comunicado INAI/249/21, CRIMEN ORGANIZADO, INVOLUCRADO EN VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-249-21.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2025b). Respuesta a solicitud de información (Folio 332259825000221).

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2025c). Respuesta a solicitud de información (Folio 330026824004114).

International Telecommunication Union (ITU). (2018). Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf

Internet Watch Foundation (2023). *"Self Generated" child sex abuse - 2022's trends & Data*. https://annualreport2022.iwf.org.uk/trends-and-data/self-generated-csam/

Islas, O. (2018). Ciberseguridad nacional: errores, omisiones y lo que falta…. Proceso. https://www.proceso.com.mx/opinion/2018/6/16/ciberseguridad-nacional-errores-omisiones-lo-que-falta-206894.html

Latinus_us. (2022, septiembre 29). *Loret capítulo 96* [Video]. YouTube. https://www.youtube.com/watch?v=fjtWvZNr4bY

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, [L.F.P.D.P.P.P], Reformada, Diario Oficial de la Federación [D.O.F.], 26 de enero de 2017, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados, [L.F.P.D.P.P.S.O], Publicación original, Diario Oficial de la Federación [D.O.F.], 26 de enero de 2017, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ley General de Acceso de las Mujeres a Una Vida Libre de Violencia, [L.G.A.M.V.L.V.], Reformada, Diario Oficial de la Federación [D.O.F.], 16 de diciembre de 2024, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf

Luque-Ruiz, B., A. (2024). *CIBERDELITOS Y CIBERSEGURIDAD: la necesidad de actualizar la legislación penal en México.* NODOS 2024. https://nodos.org/ponencia/ciberdelitos-y-ciberseguridad-la-necesidad-de-actualizar-la-legislacion-penal-en-mexico/

Meny, I. y Thoenig, J. C. (1992), *Políticas Públicas,* Barcelona, Ariel.

Nilson Report. (2023). Total value of losses due to card fraud, either credit card fraud or debit card fraud, worldwide from 2014 to 2022. In Statista. Retrieved October 17, 2024, from https://statista.uam.elogim.com/statistics/1394119/global-card-fraud-losses/

Norton. (2012). Norton Cybercrime Report 2012. https://icma.org/documents/2012-norton-cybercrime-report

Norton. (2016). Norton Cyber Security Insights Report 2016. https://www.nortonlifelock.com/us/en/newsroom/press-kits/ncsir-2016/

Noticias 24 Horas. (2012, Marzo 9). Arranca División Científica de la Policía Federal. https://24-horas.mx/policias/calderon-y-garcia-luna-inauguran-unidad-de-division-de-la-pf/

Ochoa, M., & Fernanda, M. (2019). La evolución de la política de ciberseguridad de Canadá entre 2010 y 2018. https://ddd.uab.cat/record/213467

ONUDC. (2013). Estudio exhaustivo sobre el delito cibernético. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Organización de los Estados Americanos. (2017). Comunicado de Prensa C-049/17, OEA entregó al gobierno de México recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad. https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-049/17

Organization for Economic Co-operation and Development. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. OECD Publishing. https://ccdcoe.org/uploads/2018/11/OECD-121116-CybersecurityPolicyMaking.pdf

Reglamento de la Ley de la Guardia Nacional, Reformado, Diario Oficial de la Federación [D.O.F.], 11 de diciembre de 2020, (México). https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGN_111220.pdf

Rodríguez, C. (2018). *Ciberseguridad: ¿En qué debe poner atención el gobierno de Andrés Manuel López Obrador?* Derechos Digitales. https://www.derechosdigitales.org/12659/ciberseguridad-en-que-debe-poner-atencion-el-gobierno-de-andres-manuel-lopez-obrador/

Rosas, A. (2021). Propuestas metodológicas para un mismo fin: el análisis de políticas públicas. En R. Hernández Mar, M. G. Martínez Tiburcio, J. E. Culebro Moreno, & A. Navarro (Eds.), *Experiencias, retos y desafíos de la enseñanza de las políticas públicas en México* (pp. 257-267). UAM.

Santos Vidal, M. D. (2022). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento: respuestas del Estado ecuatoriano en el período 2013-2022 (Master's thesis, Quito, EC: Universidad Andina Simón Bolívar, Sede Ecuador). https://repositorio.uasb.edu.ec/handle/10644/9076

Secretaría de Gobernación. (2013). Estrategia Digital Nacional. https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf

Secretaría de la Defensa Nacional. (2024). *Equipo de Respuesta a Incidentes Cibernéticos*. gob.mx. https://www.gob.mx/defensa/es/articulos/equipo-de-respuesta-a-incidentes-ciberneticos-sedena-354440

Secretaría de Marina. (2024). Cartilla de Ciberseguridad de la Secretaría de Marina. https://www.gob.mx/semar/documentos/productos-de-seguridad-en-el-ciberespacio-para-la-comunidad-maritima-y-portuaria

Secretaría de Seguridad y Protección Ciudadana y Guardia Nacional. (2023). *Subprograma "Infraestructura Y Equipamiento De Las Instituciones De Seguridad Pública Y Procuración De Justicia" Anexo D. "Modelo Homologado De Unidades De Policía Cibernética"*. https://www.gob.mx/cms/uploads/attachment/file/791905/5.Anexo_D_Modelo_Homologado_de_Unidades_de_Polic_a_Cibern_tica.PDF

Secretaría de Seguridad y Protección Ciudadana y Guardia Nacional. (2020). AVANCES DE LA IMPLEMENTACIÓN DEL MODELO HOMOLOGADO DE UNIDADES DE POLICÍA CIBERNÉTICA. https://www.gob.mx/cms/uploads/attachment/file/527384/13_GUARDIA_NAL_POL_CIBERNe_TICA_CAPACITACI_N_2020.pdf

Secretaría de Seguridad y Protección Ciudadana y Guardia Nacional. (2024). AVANCES DE LA IMPLEMENTACIÓN: MODELO HOMOLOGADO DE UNIDADES DE POLICÍA CIBERNÉTICA. https://www.gob.mx/cms/uploads/attachment/file/891117/14_CIBERN_TICA.pdf

Secretaría de Seguridad y Protección Ciudadana y Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2023). Informe Nacional de Evaluación del Fondo de Aportaciones para la Seguridad Pública para los estados y el Distrito Federal: FASP 2022.

https://www.gob.mx/cms/uploads/attachment/file/884031/INE_FASP_2022_compressed..pdf

Secretaría de Seguridad y Protección Ciudadana y Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2021). INFORME NACIONAL DE EVALUACIÓN DEL FONDO DE APOTACIONES PARA LA SEGURIDAD PÚBLICA 2020. https://www.gob.mx/cms/uploads/attachment/file/671795/Informe_Nacional_de_Evaluacio_n_del_FASP_2020_vc.pdf

Secretaría de Seguridad y Protección Ciudadana y Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2020). Informe nacional de evaluación del fondo de apotaciones para la seguridad pública: FASP 2019. https://app.powerbi.com/view?r=eyJrIjoiMjMzMjU2ODgtMGM5Yi00ZGQ0LWI5NWItYmU3Y2YxNDE3ODllIiwidCI6IjViMDQyN2M3LTgxYTUtNDgwZC1iZTQ5LWUyM2ViNjExMTRlNyJ9

Secretaría de Seguridad y Protección Ciudadana y Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2022). Informe Nacional de Evaluación del Fondo de Aportaciones para la Seguridad Pública (FASP) 2021. https://www.gob.mx/cms/uploads/attachment/file/949389/INE_FASP_2021.pdf

Secretaría de Seguridad y Protección Ciudadana y Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2024). Informe Nacional de Evaluación del Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal: FASP 2023. https://www.gob.mx/cms/uploads/attachment/file/947720/INE_FASP_2023_30-09-24_compressed.pdf

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. International Journal of Computer Science and Information Security, 14(1), 129-136. https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies

Suprema Corte de Justicia de la Nación. (2025). *Constitución Política de los Estados Unidos Mexicanos, que reforma la de 5 de Febrero de 1857 (Compilación Cronológica de sus Modificaciones)*. TITULO PRIMERO. https://www.scjn.gob.mx/sites/default/files/cpeum/documento/CPEUM-021_2.pdf

Transparencia Presupuestaria. (2019). Cuenta pública 2019: seguridad y protección ciudadana. https://www.transparenciapresupuestaria.gob.mx/work/models/CP/2019/tomo/III/Print.R36.03.AEPE.pdf

U.S. Department of Homeland Security. (2024). *Cyber Security Incident Response Teams.* https://www.dhs.gov/archive/science-and-technology/csd-csirt

Ureste, M. (2018, junio 28). *Con un festival musical, AMLO cierra campaña en el Estadio Azteca y promete erradicar la corrupción*. Animal Politico. https://animalpolitico.com/2018/06/con-un-festival-musical-amlo-cierra-campana-en-el-estadio-aztecay-promete-erradicar-la-corrupcion

Vallés, J. (2006). *Ciencia Política. Una introducción*. 6ª edición, Ariel.

Verizon. (2024). Number of cyber incidents in the financial industry worldwide from 2013 to 2023. *Statista*. https://statista.uam.elogim.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/