Transformación Digital

Agencia de Transformación Digital y Telecomunicaciones

Plan Nacional Ciberseguridad

Diciembre 2025

Plan **Nacional** Ciberseguridad

Diciembre 2025

Este Plan Nacional de Ciberseguridad ha contado con el apoyo técnico del Banco Interamericano de Desarrollo a través de Jorge Mora-Flores y Ariel Nowersztern. Las opiniones expresadas en esta publicación son del autor y no necesariamente reflejan el punto de vista del BID, de su directorio ejecutivo, ni de los países que representa.

Índice

Figuras

Tablas

1. Introducción

El presente Plan Nacional de Ciberseguridad es un instrumento estratégico que guiará a la Administración Pública Federal (APF) en su transformación y fortalecimiento hacia un ecosistema digital confiable y seguro durante el periodo 2025–2030. Su propósito principal es establecer una hoja de ruta integral que permita a toda la APF proteger sus activos digitales y los datos de las personas frente a amenazas de ciberseguridad cada vez más sofisticadas, al mismo tiempo que contribuye a posicionar a México como referente regional en gobernanza de ciberseguridad en América Latina y el Caribe (ALC).

México cuenta con una visión de largo plazo: evolucionar, a partir de 2025, hacia un marco sólido en materia normativa y operativa de ciberseguridad que permita el fortalecimiento y consolidación de capacidades avanzadas de ciberdefensa, la integración segura de tecnologías emergentes, la exportación de servicios especializados en la región de ALC y el liderazgo en el desarrollo de estándares y mejores prácticas que fortalezcan la ciberseguridad regional.

La recién creada Agencia de Transformación Digital y Telecomunicaciones (ATDT), a través de la Dirección General de Ciberseguridad (DGCiber), establece las bases institucionales, regulatorias, técnicas y de cooperación internacional que permitirán alcanzar esta visión. A partir de un proceso progresivo de madurez, la DGCiber impulsará el fortalecimiento de la postura de ciberseguridad federal y, con ello, contribuirá al fortalecimiento nacional y a la proyección internacional de México como actor clave en la ciberseguridad regional.

En la actualidad, la rápida adopción de tecnologías digitales ha incrementado la interconexión global y la dependencia de los sistemas en línea en economías, sociedades, organizaciones y personas. Si bien la digitalización genera beneficios económicos y sociales significativos,

también introduce riesgos crecientes asociados a amenazas cibernéticas globales. Esta realidad se manifiesta con especial intensidad en los países en desarrollo, donde el ritmo de la digitalización supera en ocasiones las inversiones necesarias para consolidar la ciber resiliencia, aumentando la probabilidad de materialización de riesgos cibernéticos.

América Latina y el Caribe se encuentran en el centro de este desafío. El Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) (2020) han señalado el incremento de los ciberataques en la región, evidenciando vulnerabilidades estructurales en el espacio digital. Informes recientes reportan un incremento notable de ataques cibernéticos en México, con un aumento interanual del 78% en 2024 (Riquelme, 2024). Entre los factores que explican esta tendencia se encuentran el mayor uso de dispositivos de internet de las cosas (IoT), el crecimiento del comercio electrónico y una adopción acelerada de soluciones de gobierno digital.

Los países de ALC enfrentan un riesgo mayor que economías más desarrolladas debido a menores niveles de inversión en ciberseguridad, procesos de digitalización acelerada y, en algunos casos, contextos de inestabilidad política y económica.

La Política General de Ciberseguridad para la Administración Pública Federal de 2025 subraya que, en esta era digital, la población, las instituciones y los gobiernos —nacionales e internacionales— se encuentran crecientemente interconectados, con un uso intensivo de las tecnologías de la información y comunicaciones. De acuerdo con el INEGI, ENDUTIH 2024, el 73.6% de los hogares mexicanos cuenta con acceso a internet, lo que representa un incremento de 9.2 puntos porcentuales respecto a lo señalado en el estudio del BID y la OEA de 2020. Este avance es un hito en materia de inclusión digital, pero al mismo tiempo amplía la superficie de exposición y los riesgos asociados a las ciberamenazas actuales.

El país ha realizado esfuerzos significativos para fortalecer su postura de ciberseguridad a nivel global; sin embargo, persisten desafíos relevantes,

particularmente en materia de coordinación legislativa, protección de infraestructuras críticas y mejora de capacidades de respuesta ante ciberataques.

México cuenta con un CSIRT nacional, reconocido en el Reporte de Ciberseguridad 2020 del BID y la OEA: el CERT-MX, integrante de la red CSIRT Américas y con una trayectoria consolidada en funciones de prevención y mitigación de ciberamenazas. Asimismo, el país dispone de CSIRTs de carácter militar, como SEDENA-CSIRT y CSIRT-SEMAR, los cuales también forman parte de la red CSIRT Américas.

A partir del 30 de septiembre de 2024, la Guardia Nacional, órgano a cargo del CERT-MX, se incorporó a la Secretaría de la Defensa Nacional (SEDENA), constituyéndose como un nuevo integrante de las Fuerzas Armadas mexicanas y dotando al Estado de una fuerza de seguridad pública nacional, disciplinada y profesional para enfrentar los desafíos del crimen organizado y otras amenazas a la seguridad.

No obstante, resulta necesario contar con un centro orientado de manera específica a la coordinación integral y transversal que requiere la APF para la protección de sus sistemas, servicios digitales, procesos institucionales y la gestión de incidentes de ciberseguridad.

Por ello, como parte del presente Plan Nacional de Ciberseguridad se han definido dos proyectos de gran importancia para la APF: la creación del CSOC (Centro Nacional de Operaciones en Ciberseguridad – SOC) y del CSIRT Nacional APF (CSIRT-APF), que permitirá contar con una instancia civil, dedicada y técnicamente especializada en la prevención, detección, análisis y respuesta coordinada a incidentes que afecten directamente a las instituciones del Gobierno Federal.

En los últimos años, México ha experimentado múltiples incidentes de ciberseguridad que lo han situado entre los países más atacados de Latinoamérica. El análisis de medios oficiales en el periodo 2022–2025 identificó 16 incidentes críticos de ciberseguridad en sectores como

gobierno, financiero, privado/industrial y educación; adicionalmente, se registraron 5 incidentes en reportes preliminares o filtraciones no oficiales.

Al revisar foros de grupos de ciberdelincuentes de ransomware en la dark web, México se ubica como el segundo país con más víctimas publicadas (155), detrás de Brasil (320), en el periodo de noviembre de 2019 al 1 de septiembre de 2025. De las 155 víctimas, el 60% se concentra en 10 grupos de cibercriminales, lo que refleja la concentración de capacidades ofensivas en actores específicos y la necesidad de respuestas coordinadas y sistemáticas.

La reforma a la Ley Orgánica de la Administración Pública Federal, mediante Decreto del 28 de noviembre de 2024, creó la Agencia de Transformación Digital y Telecomunicaciones (ATDT), que integra dentro de su estructura a la Dirección General de Ciberseguridad (DGCiber), bajo la Coordinación Nacional de Infraestructura Digital. La DGCiber cuenta con 14 atribuciones estratégicas, de gestión de riesgos, auditoría, coordinación, respuesta a incidentes y colaboración, y tiene el mandato de establecer y fortalecer la postura de ciberseguridad de la APF, así como promover mecanismos de cooperación con otras entidades gubernamentales, el sector privado y organismos internacionales, posicionándose como un actor central del ecosistema nacional de ciberseguridad.

Otra reforma relevante establece que la Guardia Nacional, que tiene a su cargo el CERT-MX, fue transferida a la Secretaría de la Defensa Nacional mediante reforma publicada en el Diario Oficial de la Federación (DOF) el 30 de septiembre de 2024. Esta decisión implica la integración de recursos humanos, materiales y financieros de la Guardia Nacional a la SEDENA, como parte del “Plan de Consolidación de la Guardia Nacional” referido en el Primer Informe de Gobierno 2024–2025. La Ley de la Guardia Nacional fue actualizada y, aunque se mantienen sus tareas de seguridad pública, la institución opera ahora bajo mando militar.

2. Diagnóstico de la situación actual

El panorama mundial de la ciberseguridad en 2025 presenta una complejidad superior a la de años anteriores, derivada de tensiones geopolíticas, del auge de tecnologías emergentes —principalmente la inteligencia artificial—, de las interdependencias en las cadenas de suministro y del incremento del cibercrimen, que ha sofisticado sus métodos aprovechando la democratización de la Inteligencia Artificial (IA).

El informe Global Cybersecurity Outlook 2025 del World Economic Forum (WEF) señala que nos encontramos en un punto crítico de inflexión, en el que la convergencia de múltiples factores está redefiniendo el paradigma de la seguridad digital. De acuerdo con este informe, el 72% de las organizaciones a nivel mundial reporta un incremento en los riesgos cibernéticos, siendo el ransomware la principal preocupación, acompañado por la sofisticación creciente de los ciberataques impulsados por la IA generativa (GenIA).

La complejidad del entorno cibernético global tiene implicaciones profundas para las organizaciones y los Estados. Entre los factores que se refuerzan mutuamente y dificultan la gestión de la ciberseguridad se encuentran:

- **Tensiones geopolíticas:** Han generado un entorno incierto en el ciberespacio, donde el ciberespionaje, la pérdida de información sensible o de propiedad intelectual y la interrupción de procesos críticos influyen en las estrategias de ciberseguridad de gobiernos y empresas.
- **Sofisticación del ciberdelito:** Los ciberdelincuentes adaptan continuamente sus tácticas, técnicas y procedimientos (TTPs), elevando el nivel de sofisticación de los ataques. Además del ransomware, cobran relevancia el fraude cibernético, el phishing, el

vishing, los deepfakes basados en IA y el robo de identidad. La IA generativa ya se utiliza en campañas de ingeniería social para hacer los ataques más eficaces.

- **Brecha de habilidades en ciberseguridad:** A nivel global, y de forma más acentuada en ALC, existe una escasez creciente de talento especializado en ciberseguridad, lo que dificulta la gestión efectiva de riesgos. El sector público, responsable de grandes volúmenes de información sensible de la población, enfrenta limitaciones significativas para contar con la fuerza laboral requerida.
- **IA y tecnologías emergentes:** La adopción de tecnologías como la IA o la computación cuántica introduce nuevos riesgos y vulnerabilidades cuando no se contemplan adecuadamente los riesgos de ciberseguridad asociados a su implementación.
- **Requisitos regulatorios:** El desarrollo de marcos regulatorios globales, regionales y nacionales para mitigar riesgos y proteger datos personales ha generado un entorno normativo complejo y, en ocasiones, poco armonizado. Esta superposición de regulaciones impacta la capacidad de las organizaciones, especialmente públicas, para implementar y cumplir con todos los requisitos, considerando sus limitaciones de recursos y personal especializado.
- **Interdependencias en las cadenas de suministro:** El incremento en el uso de tecnologías de información, sistemas interconectados y soluciones digitales en las cadenas de suministro ha ampliado la superficie de ataque y la complejidad del riesgo. Las vulnerabilidades introducidas por terceros y la propagación de incidentes a través del ecosistema muestran la relevancia de contar con mayor visibilidad, supervisión y controles en todos los niveles de conexión con terceros.

Estos factores, que se potencian entre sí, amplían la brecha entre organizaciones grandes y pequeñas, entre sector público y privado y entre economías desarrolladas y en vías de desarrollo. Esta “brecha cibernética”

tiene efectos negativos sobre la resiliencia general del ecosistema global de ciberseguridad. El siguiente gráfico nos resume los principales desafíos de la ciberseguridad (WEF, 2025).

Figura 1: Desafíos de la ciberseguridad. Basado en Global Cybersecurity Outlook 2025, WEF.

El panorama de amenazas también está experimentando una transformación cualitativa. Se observa un incremento en los incidentes de phishing e ingeniería social más sofisticados, así como en la suplantación de identidad por voz que aprovecha avances en IA generativa. Se suman riesgos crecientes para infraestructuras de tecnología operacional (OT), habituales en sectores industriales y en organizaciones públicas que prestan servicios esenciales como electricidad, agua o salud. Estos ataques buscan interrumpir el funcionamiento de sistemas de control, comprometer datos y generar impactos críticos en la población y la economía.

América Latina y el Caribe registra el crecimiento más acelerado del mundo en incidentes de ciberseguridad divulgados públicamente, con una tasa anual de incremento del 25% entre 2014 y 2023 (World Bank, 2024). El uso

extendido de dispositivos IoT en hogares y oficinas, su incorporación en equipos industriales e infraestructuras críticas, el crecimiento del comercio electrónico y la digitalización de los servicios gubernamentales incrementan la superficie de ataque y facilitan la explotación de vulnerabilidades. El informe sobre la Economía de la Ciberseguridad para los Mercados Emergentes del Grupo Banco Mundial indica que aproximadamente el 30% de los incidentes cibernéticos divulgados globalmente corresponden a países en vías de desarrollo.

Desde la perspectiva gubernamental, los costos económicos directos de estos incidentes pueden representar un riesgo real para la estabilidad macroeconómica. El ciberataque de ransomware que afectó a Costa Rica en 2022 impactó a más de 20 instituciones públicas y tuvo efectos significativos en el sector privado, principalmente en el comercio exterior, con pérdidas estimadas en 38 millones de dólares por día durante las primeras semanas. La situación, que se prolongó por alrededor de dos meses, derivó en la primera declaración de emergencia nacional por un incidente cibernético y en un costo aproximado de 2.4% del PIB (World Bank, 2024). Este caso ilustra la magnitud de los riesgos para países en desarrollo que carecen de recursos financieros y humanos suficientes y de controles específicos para proteger sus instituciones.

Las vulnerabilidades de los países de ALC se ven agravadas por la falta de recursos, infraestructura adecuada, profesionales capacitados, vacíos legales e ineficiencias de mercado que favorecen a países de ingresos altos o grandes corporaciones. El mercado mundial de ciberseguridad presenta un sesgo en su demanda: el gasto público per cápita en países de ingresos altos (como Canadá y Estados Unidos) supera los 30 dólares, frente a menos de 1 dólar en países en desarrollo como India y México, según el informe de Economía de la Ciberseguridad para los Mercados Emergentes. A ello se suma la escasez global de profesionales en ciberseguridad, con cerca de 4 millones de puestos vacantes en 2023, afectando especialmente a los

sectores públicos, a las pequeñas y medianas empresas y a los países en desarrollo.

Situación de México en el contexto regional

La situación de México en el contexto regional evidencia un progreso constante en el desarrollo de estrategias e infraestructuras de ciberseguridad, junto con desafíos persistentes en materia de coordinación y marco regulatorio.

En 2017 se publicó la Estrategia Nacional de Ciberseguridad, cuyo propósito era articular la ciberseguridad en el Estado mexicano, resaltando el papel de las TIC como motor de desarrollo político, social y económico, e identificando acciones prioritarias en los ámbitos económico, social y político para promover un uso responsable de las TIC. Este documento fue emitido al final de la administración 2012–2018 y no se encontraron evidencias de actualización durante la administración 2018–2024, por lo que actualmente no se cuenta con una versión vigente de la Estrategia.

El presente Plan Nacional de Ciberseguridad, reconociendo la importancia estratégica de contar con una Estrategia Nacional de Ciberseguridad actualizada, contempla específicamente el desarrollo de una nueva Estrategia para el año 2026.

En cuanto a la formalización de equipos de respuesta a incidentes, el país cuenta con un CSIRT nacional (CERT-MX) y CSIRTs sectoriales como SEDENA-CSIRT y CSIRT-SEMAR, todos miembros de CSIRT Américas. A estas instancias se suma la Dirección General de Ciberseguridad de la ATDT.

A partir de la identificación de estas cuatro entidades federales, se realizó un ejercicio de mapeo de otros sectores que cuentan con centros de respuesta a incidentes informáticos, obteniéndose un total de 68 centros en México, de los cuales 26 forman parte del Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST, por sus siglas en inglés) (https://www.first.org/), incluyendo los tres gubernamentales federales.

La siguiente tabla y gráfico, nos muestran su distribución.

Sector	Cantidad	Porcentaje
Servicios de ciberseguridad	9	13.2%
Académico	8	11.8%
Consultoría	7	10.3%
Gubernamental Federal	4	5.9%
Telecomunicaciones	4	5.9%
Servicios Empresariales de TI	6	8.8%
Sistema Financiero	5	7.4%
Seguridad Pública Estatal	15	22.1%
Energía	3	4.4%
Sectores Especializados	5	7.4%
Tecnología y Software	2	2.9%
TOTAL	**68**	**100%**

Tabla 1 y Figura 2: Cantidad de CERTs y CSIRTs de México. Elaboración propia.

Este mapeo permite visualizar el ecosistema nacional de respuesta a incidentes e identificar oportunidades de mayor coordinación y colaboración entre sectores. Desde una perspectiva geográfica, la Ciudad de México concentra el 62% (42 CERTs/CSIRTs) del total, seguida de Nuevo León con 6 centros, y de Veracruz, Yucatán, Chihuahua y Puebla con 2 centros cada uno. Los 12 centros restantes se distribuyen en otras entidades federativas.

El Reporte Ciberseguridad 2020 presenta una radiografía del progreso de México en ese momento, destacando la Estrategia Nacional de Ciberseguridad de 2017, el reconocimiento de la infraestructura crítica vinculada con servicios esenciales cuya afectación impactaría la seguridad nacional y la existencia del CERT-MX bajo la órbita de la entonces Policía Federal. El reporte también señala que, frente al crecimiento del cibercrimen, las organizaciones mexicanas han incorporado cada vez más especialistas en seguridad y privacidad en la toma de decisiones estratégicas, dando lugar a una gestión más proactiva de los riesgos en proyectos de transformación digital.

En el ámbito académico, se han identificado programas de formación en ciberseguridad a nivel de grado y posgrado, así como iniciativas gubernamentales tales como foros especializados y cursos dirigidos a personas servidoras públicas. No obstante, el marco legal mantiene vacíos normativos: si bien el Código Penal tipifica diversos delitos informáticos, no se cuenta aún con una ley específica de ciberdelitos, lo que limita la respuesta ante este tipo de amenazas. En materia de privacidad, México regula por separado la protección de datos en bases públicas y privadas.

La Estrategia Digital Nacional, derivada del Plan Nacional de Desarrollo 2013–2018, buscó incrementar la digitalización del país mediante la expansión de la infraestructura de telecomunicaciones y la adopción de TIC por parte de la población. Como resultado, se han creado plataformas como el portal gob.mx, que centraliza servicios en línea vinculados con salud, identificación, visados y otros trámites, con el objetivo de fortalecer la relación entre ciudadanía y gobierno.

Entre las principales acciones de la administración actual destaca la reforma a la Ley Orgánica de la Administración Pública Federal que crea la Agencia de Transformación Digital y Telecomunicaciones (ATDT), responsable de planear y conducir sus actividades con base en las políticas definidas por la persona titular del Ejecutivo Federal y alineadas con los objetivos, estrategias y prioridades del Plan Nacional de Desarrollo. Como parte de su estructura se crea la Dirección General de Ciberseguridad (DGCiber), encargada, entre otras funciones, de diseñar, desarrollar, ejecutar y actualizar estrategias y un marco de gobierno para la gestión de la ciberseguridad en la APF. Durante 2025, la DGCiber ha desarrollado la nueva Política General de Ciberseguridad para la Administración Pública Federal.

En relación con el nivel de madurez (CMM) presentado en el reporte Ciberseguridad 2020 del BID y la OEA, para la región de Centroamérica y México, el país mostró la mejor posición, alcanzando, en la mayoría de los criterios, puntajes entre 2 (formativo) y 3 (consolidado) en las cinco dimensiones del Modelo de Capacidad de Ciberseguridad:

- Política y Estrategia,
- Cibercultura y Sociedad,
- Educación/Capacitación/Habilidades en Ciberseguridad,
- Marcos Legales y Regulatorios, y
- Estándares/Organizaciones/Tecnologías.

El análisis más reciente de la Unión Internacional de Telecomunicaciones (UIT), contenido en el Global Cybersecurity Index (GCI) 2024, indica que México se ubica en el "Tier 2 – Avanzado", lo que evidencia un progreso regional y, al mismo tiempo, desafíos pendientes. Esta clasificación refleja un compromiso activo con la ciberseguridad a través de acciones coordinadas impulsadas por el gobierno para evaluar, establecer o implementar medidas de ciberseguridad generalmente aceptadas en la mayoría de los cinco pilares del índice.

México comparte el Tier 2 con países como Canadá, Ecuador y Uruguay en la región de las Américas. Los Tiers del GCI buscan reflejar el nivel de compromiso de los países y reconocer que siempre existen márgenes de crecimiento y adaptación, independientemente de las puntuaciones obtenidas. A continuación, se presenta la gráfica de GSI 2024.

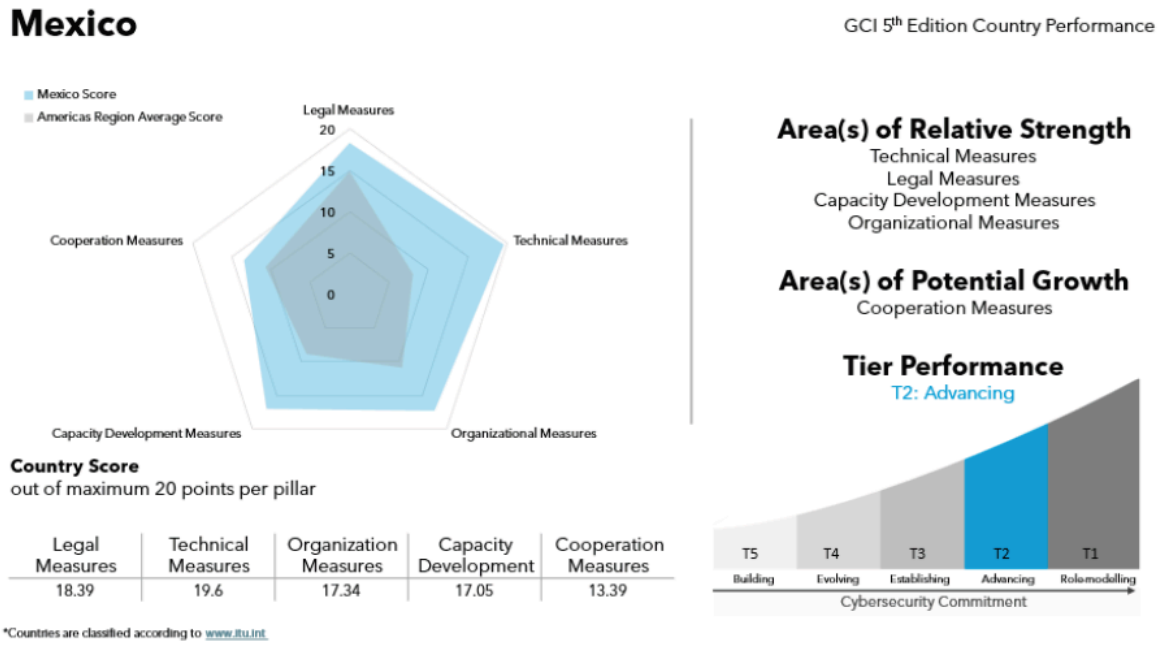


Figura 3: Medición de México en el Global Cybersecurity Index 2024, UIT.

Si bien el índice muestra fortalezas notables en medidas técnicas (19.6 de 20) y legales (18.39 de 20), se identifican oportunidades de mejora en las medidas de cooperación interinstitucional e internacional, esenciales ante los riesgos globales. En cuanto a las medidas organizacionales (17.34 de 20), se subraya la necesidad de fortalecer aún más las estructuras institucionales; la creación de la DGCiber dentro de la ATDT responde, en parte, a esta recomendación.

Vergara Cobos (2024) señala que, durante 2023 y 2024, las instituciones públicas (21%) y las organizaciones financieras (13%) de los países de ALC enfrentaron el mayor número de ciberataques. Estas cifras resultan especialmente relevantes para México, donde tras el incidente que derivó en la exfiltración de datos clasificados de la Secretaría de la Defensa Nacional (SEDENA), se han impulsado estrategias e iniciativas orientadas a mejorar la postura general de ciberseguridad del país.

Brechas de ciberseguridad identificadas

En los últimos años México ha experimentado un crecimiento en el número de incidentes de ciberseguridad, convirtiéndose en uno de los países más atacados en ALC, luego de la investigación realizada en los foros de ransomware para el presente Plan Nacional. Estos incidentes de ciberseguridad críticos han afectado tanto a instituciones del sector público mexicano como a empresas privadas, al sector financiero, a centros educativos, al sector militar y a otros sectores.

Tomando en cuenta comunicados oficiales, conferencias de prensa, y reportes de Banxico que se encuentran públicos en internet, se identificaron 16 incidentes entre 2022 y 2025, clasificados de la siguiente forma:

- Gobierno:
  - SEDENA – Guacamaya Leaks (septiembre 2022).
  - Secretaría de Infraestructura, Comunicaciones y Transportes (SICT) – Ransomware (octubre 2022).
  - CONAGUA – Ransomware BlackByte (abril 2023).
  - Consejería Jurídica de la Presidencia – RansomHub (noviembre 2024).
  - SEP/DGETI (CBTis/CETis) – filtración de datos escolares (abril 2025).
- Sector Financiero:
  - Buró de Crédito – fuga interna confirmada (diciembre 2022 a febrero 2023).
  - Banxico – reporta 4 incidentes graves en bancos y 1 en cooperativa (durante el 2023).
- Sector Privado/Industrial:
  - Mercado Libre – acceso indebido a código y usuarios (marzo 2022).
  - Foxconn (Tijuana) – ransomware (junio 2022).
  - Coca-Cola FEMSA – ataque con exfiltración (abril y mayo 2023).

  - Grupo Bimbo – ransomware Medusa (febrero 2024).
  - Coppel – caída operativa por ataque (abril 2024).
- Sector Educación:
  - UNAM (IIMAS) – exfiltración de correos (marzo 2024).

La siguiente gráfica nos resume estos eventos.

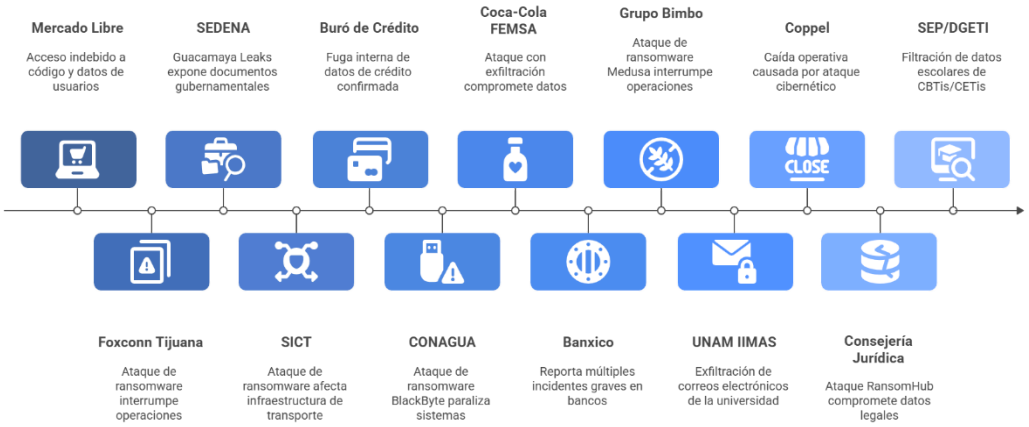


Figura 4: Principales incidentes publicados oficialmente en internet. Elaboración propia.

Adicional a estos incidentes identificados en medios oficiales, se lograron detectar reportes preliminares o anuncios de filtraciones por medios no oficiales con supuestas "evidencias" en foros de ciberdelincuentes, filtraciones en la dark web o denuncias indirectas; pero es importante aclarar que estos casos no fueron confirmados por las autoridades en su momento, contabilizando 5 incidentes preliminares / no oficiales que se detallan a continuación:

- "Chilango Leaks" – 1.3 TB de correos del gobierno de CDMX (abril 2024).
- Sistema de transporte Va y Ven (Yucatán) – presunta intrusión (2024).
- Padrón Electoral filtrado en foros (INE aclaró que era copia entregada a un partido; no un hackeo directo, pero sí fuga de datos) (2023).
- Base de datos de acreditación de prensa de Presidencia – acceso por exfuncionario (enero 2024).
- Universidad Autónoma de Nuevo León – filtración de datos (~5 GB) atribuida a un archivo antiguo (junio de 2023).

La siguiente figura resume los incidentes por año y sector.

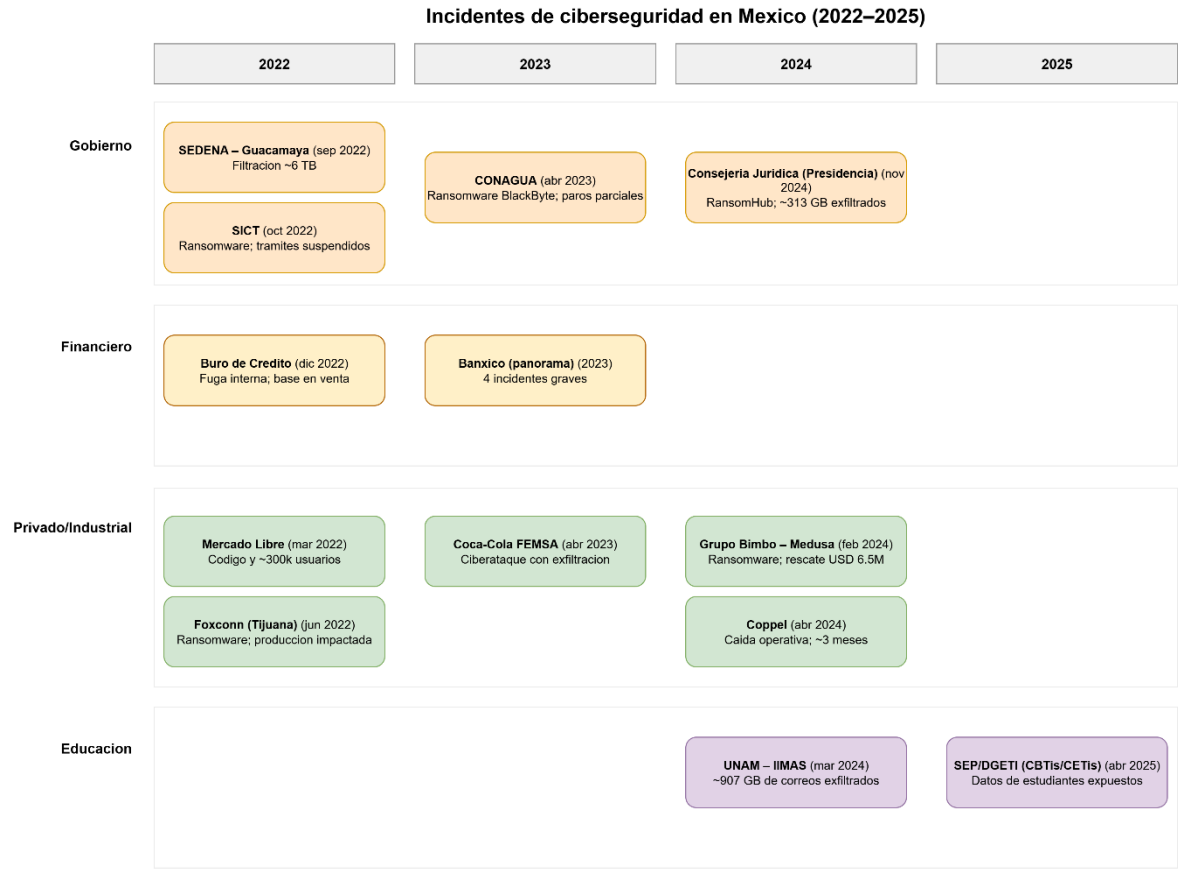


Figura 5: Incidentes de ciberseguridad del 2022 al 2025. Elaboración propia.

Distintos informes del sector privado sugieren que México recibió alrededor de 324 mil millones de intentos de ataque en 2023, lo que representa un aumento del 25% con respecto al año anterior, según datos divulgados por Infochannel Videos (s.f.). Esta alta incidencia coloca al país como uno de los más afectados de la región ALC (Riquelme, 2024), reflejando su considerable atractivo para ciberdelincuentes (Vela-Trevino & Villanueva-Plasencia, 2025), donde una gran parte de los incidentes en países en desarrollo tienen motivaciones políticas, además de financieras, lo que puede reflejar su atractivo para ciberdelincuentes y hacktivistas.

Sin embargo, a la hora de analizar los foros de los ciberdelincuentes de ransomware, este número de 16 incidentes comunicados en medios

oficiales y de 5 incidentes identificados en medios no oficiales, tuvo un incremento de 155 víctimas contabilizadas entre noviembre del 2019 y el 1 de setiembre del 2025, superado únicamente por Brasil con 320 víctimas, de este modo, México se coloca como el segundo país con más víctimas publicadas en los foros de los ciberdelincuentes de ransomware de la región de ALC. La siguiente gráfica nos muestra la cantidad de víctimas por año.

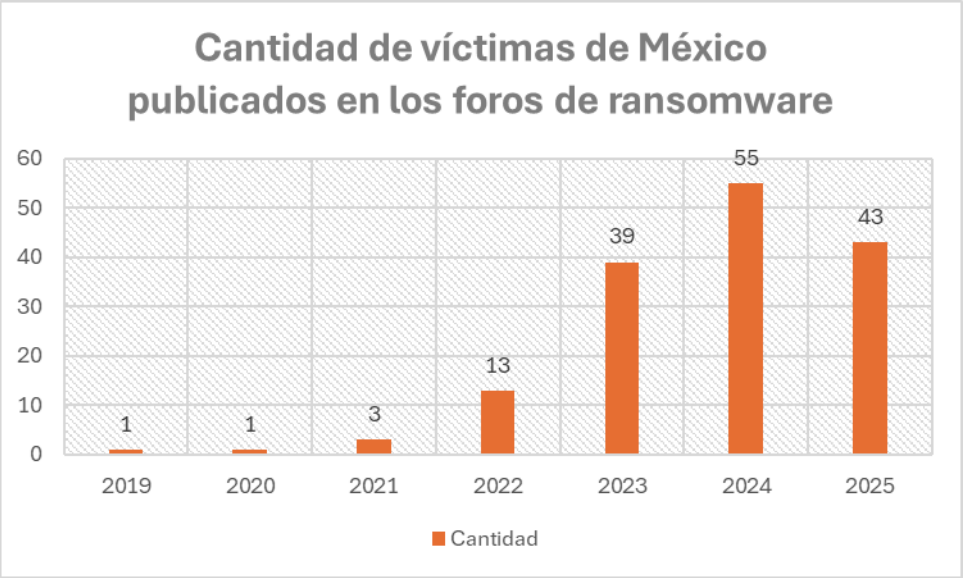


Figura 6: Total de víctimas en foros de ransomware de noviembre 2019 al 1 de septiembre 2025. Elaboración propia.

Al analizar los tipos de ransomware dominantes en México, identificamos que el grupo de ciberdelincuentes Lockbit domina con un 25% (39 de las 155 víctimas) con sus versiones de Lockbit3 y Lockbit2, seguido por los grupos Clop y Ransomhub. Es importante mencionar que no se contabilizan las víctimas de foros de grupos de ciberdelincuentes que se han desarticulado por parte de esfuerzos internacionales, como lo son Maze, Conti y Hive, entre otros. La siguiente gráfica muestra la distribución de los tipos de ransomware en México.

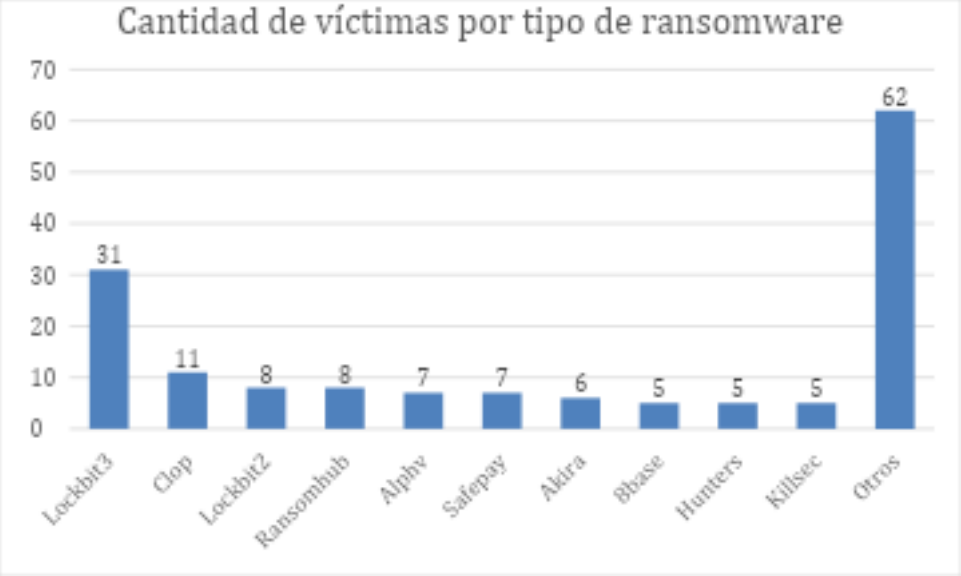


Figura 7: Cantidad de víctimas por tipo de ransomware de noviembre de 2019 al 1 de septiembre de 2025. Elaboración propia.

Se identifican patrones destacados, como el ransomware, como una amenaza recurrente y costosa para las organizaciones en su proceso de recuperación. La filtración de datos confidenciales se produce debido a vulnerabilidades no atendidas por las organizaciones o a accesos internos mal configurados. Una fragilidad en la seguridad pública puede materializarse en la afectación de dependencias gubernamentales que carecen de controles de seguridad robustos o que tienen dependencias en software no actualizado. El impacto económico tangible se puede calcular con los costos ocultos en los procesos de mitigación y recuperación luego de un incidente de ciberseguridad. Otro patrón es el de contar con una respuesta institucional desigual, donde podemos identificar instituciones que han mejorado en transparencia al reportar incidencias y otras que no lo han hecho.

Amenazas específicas

Se han identificado tres amenazas principales para México en el ámbito de la ciberseguridad: el cibercrimen organizado, las amenazas geopolíticas y las amenazas emergentes en la era de la IA.

Incidentes como el de SEDENA (2022) y CONAGUA (2023), así como los actores de amenazas cibernéticas y de estado-nación, muestran la presencia del cibercrimen organizado en el país. Al mismo tiempo, la posición estratégica que tiene México entre Estados Unidos y América Latina expone al país a amenazas geopolíticas como:

- Espionaje industrial y de gobierno.
- Ataques a infraestructuras críticas por potenciales motivaciones geopolíticas.
- Campañas de desinformación en la era de la IA para afectar la imagen del gobierno o durante los procesos electorales.
- Hacktivismo con motivaciones políticas.

A pesar que se espera que la IA tenga un impacto significativo en la prevención y protección en ciberseguridad de las organizaciones públicas y privadas, el sesgo que existe en temas presupuestarios para la adquisición de este tipo de tecnologías avanzadas y promovidas por el sector privado, pone en desventaja al sector público, a las pequeñas y medianas empresas, mientras que los altos ingresos de los ciberdelincuentes les permite tener un acceso temprano a estas tecnologías para desarrollar técnicas avanzadas de ataques. En México, esto podría representar:

- Ataques avanzados de phishing, personalizados con la utilización de la IA generativa.
- Deepfakes para fraudes financieros y manipulación mediática.
- Automatización de ataques con escalación a diferentes organizaciones y diferentes sectores.
- Evasión de los controles de seguridad y sistemas de detección tradicionales o implementados en el sector público.

Cultura de ciberseguridad

Tomando como referencia el GCI 2025 de la UIT y el Reporte Ciberseguridad 2020 de la OEA y el BID, se observa que la cultura de ciberseguridad en el sector público mexicano ha mostrado avances sostenidos, pero aún requiere un fortalecimiento integral y sistemático. En México se han desarrollado diversos eventos y actividades en materia de ciberseguridad, impulsados por los sectores público y privado, así como foros especializados en ámbitos como el financiero e industrial. No obstante, persisten desafíos que es necesario atender, entre los cuales destacan:

- Limitada concientización en los niveles directivos y de alta toma de decisión sobre la importancia estratégica de la ciberseguridad en las organizaciones públicas y privadas.
- Resistencia al cambio tecnológico y a la implementación de controles de ciberseguridad.
- Asignación insuficiente de presupuesto para programas de capacitación continua en ciberseguridad dirigidos a personas servidoras públicas.
- Falta de métricas que permitan evaluar el impacto de las capacitaciones y de la implementación de controles de ciberseguridad en las organizaciones.
- Ausencia de esquemas de certificación obligatoria en ciberseguridad para las personas servidoras públicas que manejan información sensible de la población.

En los últimos años se han incrementado las oportunidades de aprendizaje para la sociedad, particularmente a través de programas de educación superior en universidades líderes de la región, que ofrecen opciones de formación en ciberseguridad tanto a nivel de pregrado como de posgrado.

La penetración de Internet en México para el año 2024 alcanzó aproximadamente 73.6% de la población, y los suscriptores a servicios de

internet móvil representaron el 81.7%, de acuerdo con datos del INEGI (ENDUTIH 2024). Estas cifras abren importantes oportunidades, pero también plantean nuevos desafíos, entre los que se encuentran: la baja percepción del riesgo cibernético en la población general, la sobreexposición de información personal a través de redes sociales, el uso de software no licenciado —que incrementa la probabilidad de vulnerabilidades en los dispositivos— y una educación digital desigual que profundiza la brecha entre zonas urbanas y rurales.

Estos elementos subrayan la necesidad de diseñar e implementar programas de alfabetización digital con componentes específicos de ciberseguridad, dirigidos a los distintos grupos etarios de la población y con cobertura en todo el territorio nacional, como condición fundamental para consolidar una cultura de ciberseguridad robusta e inclusiva.

Creación de la Agencia de Transformación Digital y Telecomunicaciones (ATDT)

La creación de la Agencia de Transformación Digital y Telecomunicaciones (ATDT) representa un hito en la evolución de la gobernanza digital en México. Dentro de su estructura se encuentra la Dirección General de Ciberseguridad (DGCiber), adscrita a la Coordinación Nacional de Infraestructura Digital y constituida como el centro operativo de la estrategia de ciberseguridad de la Administración Pública Federal (APF). La DGCiber funge como autoridad técnica central en materia de seguridad de la información y telecomunicaciones en toda la APF, con facultades para definir los protocolos, lineamientos y disposiciones necesarias en esta materia.

Su mandato integra atribuciones amplias, que abarcan el diseño, desarrollo, ejecución y actualización continua de las estrategias y marcos de gestión de ciberseguridad, así como la formulación de políticas, lineamientos,

reglamentos y procedimientos orientados a asegurar una regulación homologada en la APF. Asimismo, la DGCiber debe coordinar la identificación, el monitoreo y la evaluación de riesgos de ciberseguridad, estableciendo procesos para su mitigación efectiva.

Como parte de sus funciones de supervisión, le corresponde gestionar auditorías y evaluaciones periódicas a fin de garantizar el cumplimiento normativo de las instituciones de la APF, así como emitir recomendaciones y mejores prácticas en materia de ciberseguridad. La DGCiber coordinará, además, el intercambio de información crítica y apoyará la atención y respuesta a incidentes de ciberseguridad que afecten a las instituciones federales.

En el ámbito operativo, la Dirección asume la conducción de la respuesta a incidentes informáticos propios de la ATDT. Entre sus tareas relevantes se encuentran el desarrollo de programas de capacitación para personas servidoras públicas y la coordinación de estudios especializados con sectores público y privado. Asimismo, asiste a la persona titular de la ATDT en la celebración de convenios de cooperación con instituciones nacionales e internacionales.

La DGCiber colabora con la APF en funciones de monitoreo de amenazas, análisis de vulnerabilidades y atención de incidentes mediante el Centro de Operaciones de Ciberseguridad (CSOC). Además de la capacitación y la concientización, tiene bajo su responsabilidad el desarrollo de estrategias, marcos de gobernanza, políticas, regulación y gestión de riesgos, así como la supervisión del cumplimiento de auditorías y obligaciones normativas en ciberseguridad.

Una función estratégica de la DGCiber consiste en brindar apoyo técnico para promover el desarrollo de marcos jurídicos en materia de ciberseguridad, tanto para la APF como para fortalecer las bases de un marco nacional integral, alineado con las mejores prácticas internacionales y adaptado a la realidad federal del país.

El año 2026 representará un desafío adicional debido a la realización del Mundial de Fútbol organizado por la FIFA, cuyas sedes incluirán Canadá, Estados Unidos y México. Dado que este evento se celebrará durante la presente administración, la ATDT y la DGCiber deberán cumplir funciones específicas en un periodo acotado. El Mundial 2026 constituye un evento de alto impacto nacional e internacional, por lo que México debe garantizar la seguridad digital de infraestructuras críticas, servicios esenciales, sistemas financieros, plataformas digitales y demás activos tecnológicos asociados a su realización. La DGCiber integra el grupo de trabajo nacional encargado de la coordinación y seguridad del evento, colaborando con recomendaciones para la identificación de amenazas específicas, la definición de protocolos de ciberseguridad y la protección de sistemas informáticos, incluidos los sistemas digitales e IoT de los estadios, los sistemas de transporte, la infraestructura hotelera, los servicios públicos y otros servicios esenciales.

Durante 2025, la DGCiber definió metas prioritarias para fortalecer el marco regulatorio en ciberseguridad, entre las que destacan:

1. La emisión de una directriz integral de ciberseguridad aplicable a toda la APF.
2. El desarrollo de tres instrumentos normativos con obligaciones institucionales, directrices estratégicas y mecanismos de articulación.
3. La implementación de un instrumento diagnóstico del estado de la ciberseguridad.
4. La creación de una herramienta de valoración basada en parámetros internacionales, destinada a todas las instituciones de la APF.

Estas iniciativas forman parte del proceso de validación del cumplimiento normativo, orientado a supervisar, examinar y garantizar que las instituciones de la APF cumplan con el marco regulatorio establecido en materia de ciberseguridad.

Desde enero de 2025 se encuentra en operación un mecanismo integral de protección cibernética para la APF, que ha generado los siguientes resultados:

- Ejecución de un procedimiento de localización y hallazgo de vulnerabilidades, con más de 750 avisos técnicos emitidos junto con sus medidas preventivas.
- Eliminación de 25 portales fraudulentos que simulaban servicios gubernamentales, evitando posibles estafas y la apropiación indebida de información personal o sensible.
- Fortalecimiento de la postura de ciberseguridad de organismos federales mediante el lanzamiento del primer servicio gubernamental de notificaciones anticipadas sobre potenciales debilidades emergentes.
- Realización de más de 30 evaluaciones de ciberseguridad en plataformas digitales, facilitando la detección de vulnerabilidades en servicios de la ATDT y dependencias de la APF.
- Asistencia especializada en 22 incidentes graves de ciberseguridad en organismos federales, logrando contener los incidentes, reforzar su estructura tecnológica, disminuir impactos y evitar fugas de información.
- Expansión y actualización del Centro de Operaciones de Ciberseguridad (SOC) del INFOTEC, incrementando en 40% su capacidad de detección e identificación de amenazas, y optimizando tiempos y procedimientos de respuesta. Este SOC continúa ofreciendo servicios a sus usuarios actuales. Como parte del fortalecimiento institucional, la ATDT ha definido el proyecto para la creación del CSOC Nacional, encargado de coordinar los SOC de entidades públicas y privadas.

En materia internacional, la ATDT y la DGCiber han fortalecido la presencia y coordinación global mediante actividades relevantes, incluyendo:

- La Asamblea General de la Red Ciberlac, celebrada el 28 de agosto en la Ciudad de México durante la primera escuela de verano de ciberseguridad Ciberlac 2025.
- El CAN WEEK México 2025, realizado del 30 de septiembre al 3 de octubre con apoyo de OEA/CICTE y la red CSIRT Américas, que incluyó:

    - **30 de septiembre:** Entrega al comandante de la Guardia Nacional de la declaración de cumplimiento de la Línea Base de CSIRT Américas del CERT-MX, cuya evaluación tuvo lugar del 5 al 7 de marzo de 2025.
    - **1 y 2 de octubre:** Ejercicio "Tabletop Ejecutivo para la Gestión de Incidentes", coordinado por la ATDT y la DGCiber, dirigido a sectores vinculados con la ciberseguridad y las infraestructuras críticas.
    - **3 de octubre:** Mentoría personalizada para la DGCiber en la creación de un CSIRT conforme a la metodología internacional SIM3 y las buenas prácticas de la red CSIRT Américas.

Análisis FODA del estado de la ciberseguridad

Para finalizar la sección de diagnóstico de la situación actual de México en ciberseguridad se ha desarrollado el siguiente análisis de fortalezas, debilidades, oportunidades y amenazas:

Fortalezas	Debilidades
• Marco institucional renovado con la creación de la ATDT. • Capacidades técnicas sólidas según el GCI 2024. • Marco legal en desarrollo. • Posición geográfica estratégica para la cooperación regional.	• Cooperación internacional limitada (puntuación de 13.39 de 20 en el GCI). • Brecha de talento severa con déficit de profesionales en ciberseguridad. • Ausencia de CSIRT Nacional explícitamente establecido para la APF

• Sector financiero relativamente maduro en estándares de seguridad.	• Fragmentación regulatoria entre sectores y niveles de gobierno.
Oportunidades	**Amenazas**
• Liderazgo regional en ciberseguridad para América Latina. • Nearshoring seguro aprovechando la relación con Estados Unidos. • Desarrollo de la industria nacional de ciberseguridad. • Hub de talento para empresas globales de seguridad. • Innovación en seguridad para mercados emergentes. • Identificar e involucrar a diferentes actores del ecosistema para recuperar la confianza en los procesos de transformación digital y servicios digitales seguros ofrecidos por la APF.	• Cibercrimen organizado transnacional en expansión. • Ataques a infraestructura crítica y afectación a servicios esenciales. • "Weaponización" de IA para ataques sofisticados. • Tensiones geopolíticas manifestadas en el ciberespacio. • Pérdida de competitividad por la inseguridad digital. • Desconfianza de la ciudadanía por los procesos de transformación digital impulsados por el gobierno.

Tabla 2: Análisis FODA del estado de situación de ciberseguridad. Elaboración propia.

El análisis del estado de la ciberseguridad nos muestra que México se encuentra en un momento de transición. La creación de la ATDT ofrece una oportunidad para el fortalecimiento de la Gobernanza Digital, sobre la cual la OCDE ha realizado recomendaciones a las naciones durante los últimos años y que al mismo tiempo brinda la oportunidad de transformar la postura de ciberseguridad del país, para colocarlo como un referente regional en ALC.

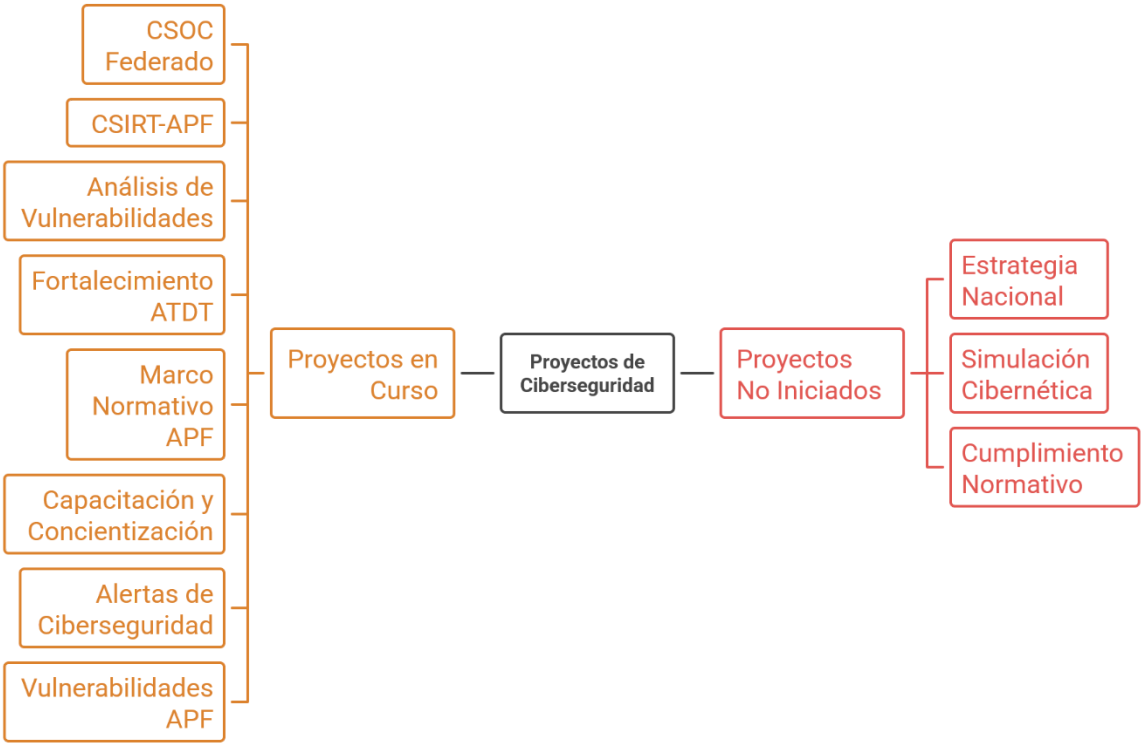
3. Visión a largo plazo

La visión a largo plazo de México para la Administración Pública Federal y Nacional, en materia de ciberseguridad se edifica sobre un proceso de madurez que es progresiva y que abarca del 2025 al 2030. Durante este período, la Administración Pública Federal iniciará un proceso que inicia desde el establecimiento de los fundamentos normativos y de operación hacia el desarrollo de capacidades avanzadas de ciberdefensa que posicionen a México como el referente regional. Este proceso, el cual es evolutivo, responde al mandato dado a la Dirección General de Ciberseguridad (DGCiber) dentro de la Agencia de Transformación Digital y Telecomunicaciones (ATDT), el cual se materializa mediante un portafolio estratégico de proyectos que ayudarán a fortalecer la protección de los activos digitales federales, la gestión integral de los riesgos cibernéticos, y la cooperación nacional e internacional en seguridad del ciberespacio. La arquitectura temporal definida del Plan se estructura en seis fases secuenciales —Fundamento (2025), Expansión (2026), Consolidación (2027), Maduración (2028), Liderazgo (2029) y Transformación (2030)— cada una con objetivos específicos y proyectos articulados que, en su conjunto, permitirán a México alcanzar una posición de vanguardia en la región de América Latina y el Caribe, contribuyendo de forma activa en el fortalecimiento de la ciberseguridad regional mediante el desarrollo de normatividad, la exportación de conocimiento especializado, y el liderazgo en iniciativas de cooperación.

La visión a largo plazo toma el mandato y los objetivos específicos de la Dirección Nacional de Ciberseguridad para definir una hoja de ruta a seis años, mediante un portafolio de proyectos estratégicos que contribuyan al fortalecimiento de la ciberseguridad en las instituciones de la APF.

Inicialmente, se definió una lista de proyectos por parte de la Dirección General de Ciberseguridad, de los cuales la mayoría de ellos se encuentran

en ejecución y cumpliendo su cronograma inicial según lo programado.



Estos proyectos con su estado actual se presentan a continuación.

Figura 8: Proyectos programados. Fuente: ATDT, 2025.

Tomando en cuenta el planteamiento de desarrollar una visión a largo plazo que incorpora un rango de tiempo entre el presente año, 2025 hasta el 2030, se definen un grupo de proyectos a desarrollar para cada año, cada uno con su objetivo, su alcance y metas definidas, las cuales se medirán en la siguiente sección por medio de los indicadores definidos..

Se presentan a continuación a nivel general los proyectos agrupados por año de implementación del Plan Nacional:

2025 – Fundamento

- Marco General de Ciberseguridad para la APF.
- Adhesión formal a LAC4.

- Memorando de Entendimiento (MOU) sobre cooperación en materia de ciberseguridad entre Brasil y la ATDT.

2026 – Expansión

- Integración de Red de CSIRTs para incrementar las capacidades de visibilidad.
- Administración Pública Federal Cibersegura (APF - Cibersegura).
- Identificación de infraestructuras críticas y de los servicios esenciales.
- Programa operativo y de evaluación de vulnerabilidades.
- Estrategia Nacional de Ciberseguridad.
- CSOC (Centro Nacional de Operaciones en Ciberseguridad - SOC).
- CSIRT Nacional APF (CSIRT-APF).
- Academia Virtual Federal para la implementación de políticas y lineamientos.
- RNCC-MX (Red Nacional de Contactos de Ciberseguridad).
- MoUs bilaterales entre el sector privado, el sector público y la academia.
- MoUs de CSIRTs internacionales (países, otros CERTs/CSIRTs).
- Red Federal de CERTs/CSIRTs.
- Sistema de alertas críticas de la APF.

2027 – Consolidación

- Sistema integral de gestión de riesgos (ERM-Cyber ATDT).
- Cyber Range Nacional.

2028 – Maduración

- IA para ciberdefensa.

- Centro Regional LATAM de Respuesta.

2029 – Liderazgo

- Estrategia de exportación de servicios.
- VUIC (Ventanilla Única de Información de Ciberseguridad)
- Observatorio APF de Ciberseguridad.

2030 – Transformación y proyección

- Certificación nacional para el cumplimiento de los lineamientos y protocolos de ciberseguridad de la APF.
- Next-Gen SecOps (IA avanzada y tecnologías emergentes).

La siguiente imagen resume la hoja de ruta de la visión a largo plazo con una descripción para cada uno de los años.

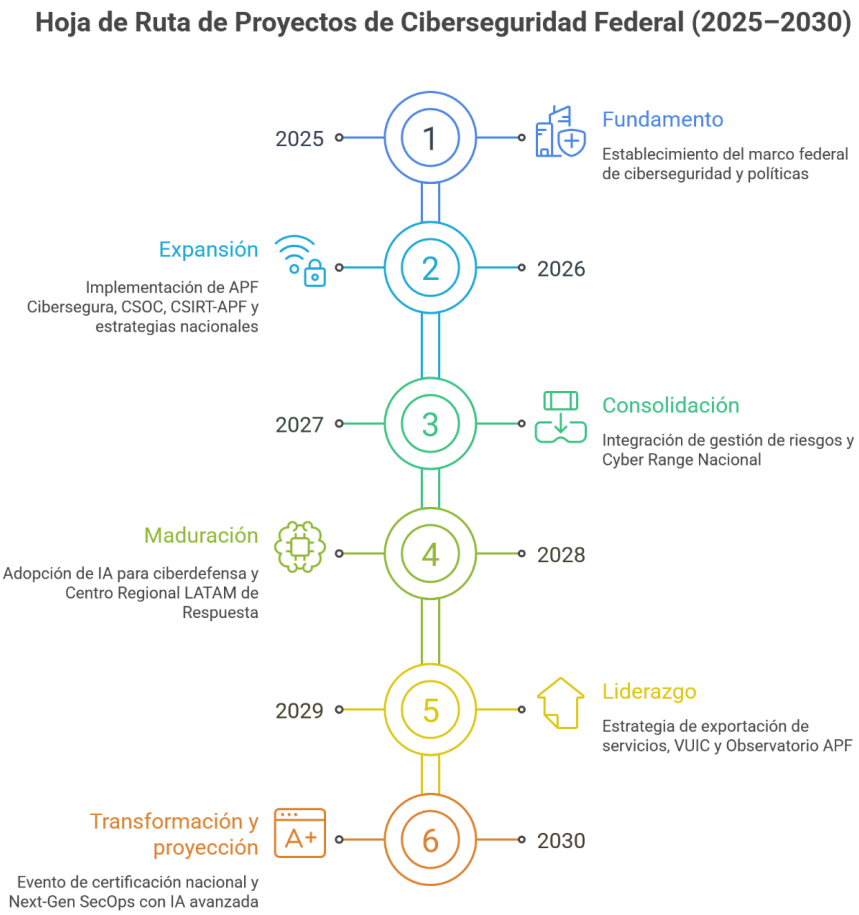


Figura 9: Hoja de ruta Plan Nacional de la DGCIBER. Elaboración propia.

Se ha desarrollado una ficha por proyecto para ofrecer a la persona lectora del Plan Nacional de Ciberseguridad, una idea general del alcance de cada uno de ellos, incluyendo el mandato y objetivo del reglamento de la agencia que justifica su desarrollo. Las fichas se encuentran clasificadas por el año de su implementación.

Año 2025 - Fundamento

2025 - Fundamento

Nombre del Proyecto	Marco General de Ciberseguridad para la APF.
Año de Implementación	2025, 2026 y 2027.
Mandatos y Objetivos del Artículo 19	Art. 19.I, Art. 19.II, Art. 19.III.
Categoría	Gobernanza.
Descripción del Proyecto	Es una iniciativa estratégica fundacional para el establecimiento de un sistema integral de gobernanza de la ciberseguridad en la Administración Pública Federal. El Marco Federal de Ciberseguridad incorpora el desarrollo de la Política General de Ciberseguridad de la APF, así como los lineamientos y protocolos de ciberseguridad definidos por la DGCiber. Como parte de los lineamientos se pueden mencionar a un alto nivel: • La Política General de Ciberseguridad fija las bases para la aplicación de estrategias, modelos de madurez, revisiones, capacitación, adquisiciones, evaluación de proveedores y todos aquellos aspectos básicos de una estrategia interna de ciberseguridad, y responde al Artículo 19, apartado II. Se aplicará a todas las actividades, personas, procesos, servicios, tecnologías, sistemas de información y/o activos digitales que apoyen el cumplimiento de funciones sustantivas y administrativas de las dependencias, sus órganos administrativos desconcentrados y entidades de la APF, así como al tratamiento, almacenamiento, transmisión o protección de información de cualquier tipo. Se incluyen los servicios digitales que presten servicios a la ciudadanía o a otras dependencias, sus órganos administrativos desconcentrados, y entidades de la APF. Finalmente, se aplicará a todas las redes, plataformas, nubes o infraestructuras tecnológicas utilizadas, gestionadas y operadas por dependencias, sus órganos administrados desconcentrados y entidades de la APF. • Lineamiento para la gestión de riesgos y el manejo de incidentes de ciberseguridad, que define con claridad los roles, responsabilidades y protocolos de actuación que todas las instituciones de la APF deben seguir para atender de manera coordinada los incidentes de ciberseguridad. Como extensión de este lineamiento, se desarrolla el Protocolo Nacional de Clasificación y Manejo de Información Sensible de la APF, que adopta y adapta al contexto gubernamental mexicano el Traffic Light Protocol, estándar internacional de manejo de información sensible ampliamente utilizado por comunidades de ciberseguridad y desarrollado por FIRST. Otro de los protocolos

	que se deriva de este lineamiento es el Protocolo Nacional de Notificación, Reporte y Escalamiento de Incidentes de Ciberseguridad para la APF, el cual establece los procedimientos estandarizados, formatos, canales de comunicación, plazos de respuesta y cadenas de mando que deben seguir todas las dependencias y entidades federales al detectar, reportar y escalar incidentes de ciberseguridad. • Lineamiento de capacitación y sensibilización, que promueve y regula la implementación de programas de formación, actualización y concientización en ciberseguridad para todas las personas funcionarias de la APF. • Lineamiento de evaluación de madurez: define la metodología, los criterios, los indicadores y los procedimientos para medir el nivel de madurez y la efectividad de las capacidades de ciberseguridad en las instituciones de la APF. Este lineamiento establece un mecanismo mediante el cual la DGCIBER ejecuta las verificaciones de las auditorías realizadas por terceros a las instituciones de la APF, con el fin de cumplir con políticas, lineamientos, reglamentos y normas en materia de ciberseguridad. Cada uno de los lineamientos puede derivar en una serie de protocolos que guíen a las instituciones de la APF y apoyen su cumplimiento. Estos protocolos se desarrollarán según las necesidades de la APF, a fin de garantizar la aplicación de lo dispuesto en los lineamientos. Este proyecto responde a los mandatos establecidos en el Artículo 19, apartados I, II y III, del Reglamento de la ATDT, considerando elementos como el diseño, el desarrollo y la actualización de estrategias, así como la emisión de políticas públicas, lineamientos, reglamentos y procedimientos de regulación. El marco incluye la definición de estructuras de gobernanza, roles y responsabilidades institucionales, así como mecanismos de coordinación interinstitucional, y la orientación técnica para la implementación efectiva para las instituciones de la APF. Asimismo, establece los fundamentos normativos que regirán la gestión de riesgos, la respuesta ante incidentes y el cumplimiento de los estándares de seguridad de la información a nivel de la APF.

2025 - Fundamento	
Nombre del Proyecto	Adhesión formal a LAC4.
Año de Implementación	2025.
Mandatos y Objetivos del Artículo 19	Art. 19.XII.
Categoría	Cooperación.
Descripción del Proyecto	El proyecto de Adhesión formal al organismo internacional LAC4, representa la incorporación de México a las principales redes regionales de cooperación en ciberseguridad de América Latina y el Caribe, fortaleciendo las capacidades nacionales mediante el intercambio de experiencias, mejores prácticas, información sobre amenazas, y coordinación de respuestas a incidentes de alcance regional. En cumplimiento del Artículo 19, apartado XII, esta iniciativa formaliza la participación de la ATDT en este organismo mediante una nota formal de solicitud de adhesión. Esta iniciativa busca incorporar a México como actor relevante en el ecosistema latinoamericano de ciberseguridad, facilitando el acceso a recursos técnicos, a la inteligencia compartida y a la experiencia colectiva regional.

2025 - Fundamento	
Nombre del Proyecto	Memorando de Entendimiento (MOU) sobre cooperación en materia de ciberseguridad entre Brasil y la ATDT.
Año de Implementación	2025.
Mandatos y Objetivos del Artículo 19	Art. 19.XII.
Categoría	Cooperación.
Descripción del Proyecto	Considerando el incremento acelerado en el desarrollo de nuevas tecnologías y aplicaciones que deja expuestos a los gobiernos, empresas y la sociedad ante la ocurrencia riesgos cibernéticos, los Estados reconocen la importancia de suscribir instrumentos jurídicos

	internacionales que fortalezcan la cooperación bilateral en materia de ciberseguridad, mediante el intercambio de información experiencias, así como la elaboración y aplicación de ordenamientos jurídicos y técnicos. En concordancia con el Artículo 19, apartado XII, la suscripción del Memorando de Entendimiento, formaliza la cooperación y colaboración entre el Gabinete de Seguridad Institucional de la Presidencia de la República Federativa del Brasil y la ATDT. Este proyecto, reafirma el compromiso de los Estados para promover la seguridad y estabilidad en el ciberespacio.

Año 2026 – Expansión

2026 – Expansión	
Nombre del Proyecto	**Integración de Red de CSIRTs para incrementar las capacidades de visibilidad**.
Año de Implementación	2026.
Mandatos y Objetivos del Artículo 19	Art. 19.XIII.
Categoría	Cooperación.
Descripción del Proyecto	Luego de haber identificado 68 CSIRTs privados y públicos de diferentes sectores y con el motivo del desarrollo de un evento masivo como lo es el Mundial de Fútbol 2026 en México, se identifica una excelente oportunidad para desarrollar un proyecto que fortalezca la gobernanza y capacidad de coordinación de la DGCIBER por medio de la creación de una Red de CSIRTs para incrementar las capacidades de visibilidad del Mundial de Fútbol FIFA 2026 y luego de ese evento se continúe la cooperación de la red para otros potenciales eventos de ciberseguridad y coordinación intersectorial. Con base en el Artículo 19, apartado XIII, durante el año 2026 se negocian y suscriben diferentes MoUs diferentes CSIRTs privados, académicos y sectoriales.

2026 – Expansión

Nombre del Proyecto	Administración Pública Federal Cibersegura (APF - Cibersegura).
Año de Implementación	2026, 2027, 2028.
Mandatos y Objetivos del Artículo 19	Art. 19.VIII.
Categoría	Talento y capacitación.
Descripción del Proyecto	El Programa Nacional de Concientización de la Administración Pública Federal Cibersegura "APF - Cibersegura" constituye una iniciativa integral, de alcance a todas las personas funcionarias de la APF, con el objetivo de desarrollar cultura, conocimientos y prácticas seguras en el uso de tecnologías digitales entre los funcionarios públicos federales. En atención al mandato del Artículo 19, apartado VIII, este programa diseña y ejecuta campañas masivas de comunicación en medios tradicionales y digitales de la APF, desarrolla materiales educativos diferenciados por segmentos poblacionales, organiza eventos presenciales y/o virtuales de sensibilización. Los programas se pueden desarrollar por medio de alianzas con instituciones educativas, el sector privado y organismos internacionales. Un objetivo específico es reducir la victimización cibernética de los funcionarios públicos federales, fortalecer la resiliencia digital federal, y generar conciencia de los riesgos y las capacidades de autoprotección en el entorno digital.

2026 - Expansión	
Nombre del Proyecto	Identificación de infraestructuras críticas y de los servicios esenciales.
Año de Implementación	2026.
Mandatos y Objetivos del Artículo 19	Art. 19.IV.
Categoría	Gobernanza.
Descripción del Proyecto	Establece la metodología y ejecuta el proceso de categorización y priorización de los activos tecnológicos, sistemas de información, servicios digitales e infraestructuras que resultan fundamentales para la continuidad de las funciones sustantivas de la APF. Con base en el Artículo 19, apartado IV, este proyecto desarrolla un inventario nacional de la infraestructura crítica y de los servicios esenciales, aplicando criterios de

	criticidad basados en el impacto potencial ante fallas o compromisos de ciberseguridad, el nivel de interconexión, la afectación a los servicios ciudadanos y la relevancia para la seguridad nacional. Los resultados constituyen el fundamento para la asignación diferenciada de recursos de protección, la implementación de controles de seguridad, el diseño de planes de continuidad y recuperación ante desastres específicos para cada infraestructura crítica y servicio esencial.

2026 - Expansión	
Nombre del Proyecto	Programa operativo y de evaluación de vulnerabilidades.
Año de Implementación	2026, 2027, 2028, 2029, 2030.
Mandatos y Objetivos del Artículo 19	Art. 19.IV.
Categoría	Operaciones.
Descripción del Proyecto	El programa operativo y de evaluación de vulnerabilidades tiene un enfoque técnico especializado, con foco en la identificación, análisis, priorización y gestión sistemática de vulnerabilidades en los sistemas de información, aplicaciones, infraestructura tecnológica y redes de comunicaciones de la ATDT y de las instituciones de la APF. En cumplimiento del Artículo 19, apartado IV, este programa implementa metodologías de escaneo automatizado, coordinadas con las instituciones, pruebas de hacking ético, revisiones de código fuente y análisis de configuraciones de seguridad. El proyecto ofrece la posibilidad de establecer alianzas público-privadas (APP) o con el sector educativo para fortalecer el programa operativo y agregar capacidades del sector privado y de las instituciones de educación superior para la evaluación de vulnerabilidades en las instituciones de la APF. El programa establece ciclos continuos de evaluación y sistemas de priorización basados en la criticidad de los activos y el nivel de criticidad de las vulnerabilidades. La operación del programa genera métricas de exposición al riesgo, tendencias de mejora e información para la toma de decisiones estratégicas para el fortalecimiento de la postura de ciberseguridad de la ATDT y las instituciones de la APF.

2026 - Expansión

Nombre del Proyecto	Estrategia Nacional de Ciberseguridad.
Año de Implementación	2026.
Mandatos y Objetivos del Artículo 19	Art. 19.I.
Categoría	Gobernanza.
Descripción del Proyecto	La Estrategia Nacional de Ciberseguridad constituye el documento rector de más alto nivel que articula la visión, objetivos estratégicos, líneas de acción, responsabilidades institucionales y mecanismos de coordinación para la protección del ciberespacio mexicano en los sectores gubernamental, privado, de la academia y social. En cumplimiento del Artículo 19, apartado I, esta estrategia trasciende el ámbito exclusivo de la Administración Pública Federal para establecer un enfoque integral de seguridad cibernética nacional. El documento contempla ejes estratégicos que abarcan el fortalecimiento institucional, la protección de infraestructuras críticas y servicios esenciales nacionales, el desarrollo de capital humano especializado, el fomento de la industria mexicana de ciberseguridad, la cooperación internacional, el marco legal y regulatorio, y la generación de una cultura de ciberseguridad ciudadana. La estrategia establece indicadores nacionales de desempeño, mecanismos de gobernanza multi-actor, y define el modelo de coordinación y transparencia entre los tres órdenes de gobierno, el sector privado, la academia y la sociedad civil para la construcción de un ciberespacio seguro, resiliente y confiable. Para este proyecto, uno de los principales insumos que se han considerado es el reciente documento realizado por la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) que por medio de una serie de contribuciones de la industria desarrollaron un documento de Propuesta de Lineamientos para una Estrategia Nacional de Ciberseguridad para México.

2026 - Expansión	
Nombre del Proyecto	CSOC (Centro Nacional de Operaciones en Ciberseguridad - SOC).
Año de Implementación	2026, 2027, 2028.
Mandatos y Objetivos del Artículo 19	Art. 19.IX.

Categoría	Operaciones.
Descripción del Proyecto	El Centro Nacional de Operaciones en Ciberseguridad representa el siguiente paso del CSIRT-APF hacia una capacidad de comando unificado y operación con monitoreo continuo, correlación de eventos de seguridad, detección proactiva de amenazas, y respuesta coordinada a incidentes cibernéticos que afectan a la APF, siguiente el esquema de NIST donde el CSOC se encarga de las etapas de Identificar, Proteger y Detectar; y el CISRT-APF de Responder y Recuperar, así como otras labores propias definidas. Este proyecto se basa en el artículo 19, apartado IX. El CSOC integra tecnológicamente múltiples fuentes de telemetría de seguridad provenientes de instituciones federales mediante la implementación de un Security Operations Center, equipado con plataformas de SIEM, sistemas de correlación avanzada mediante inteligencia artificial, capacidades de análisis forense automatizado, y herramientas de orquestación de respuesta. El centro mantiene comunicación directa con líderes de ciberseguridad institucionales mediante la RNCC-MX, y coordina respuestas ante ciberataques de impacto en la APF, constituyendo el cerebro operativo del ecosistema nacional de ciberseguridad gubernamental.

2026 – Expansión	
Nombre del Proyecto	CSIRT Nacional APF (CSIRT-APF).
Año de Implementación	2026, 2027.
Mandatos y Objetivos del Artículo 19	Art. 19.VII, Art. 19.IX, Art. 19.XII.
Categoría	Operaciones.
Descripción del Proyecto	El Centro de Respuesta a Incidentes de Ciberseguridad de la ATDT, CSIRT Nacional APF, representa la capacidad institucional rectora para la operación continua, con capacidad de monitoreo, análisis, detección, respuesta y coordinación de incidentes de ciberseguridad a nivel de la APF. En cumplimiento de los mandatos establecidos en el Artículo 19, apartados VII, IX y XII, el CSIRT-APF opera con personal especializado, herramientas de análisis forense digital, sistemas de monitoreo de seguridad, y procedimientos estandarizados de gestión de incidentes. Este centro constituye el punto focal de la APF para la recepción de notificaciones de incidentes, la coordinación de respuestas, la emisión de

	alertas técnicas y boletines de seguridad, así como la articulación con organismos nacionales e internacionales de respuesta a incidentes. Como parte del proceso de creación del CSIRT-APF, se continuará con el proceso de adhesión a CSIRT Americas (OEA/CICTE), mediante el cumplimiento de requisitos, compromisos y procedimientos formales necesarios para la incorporación de México como miembro activo de esta red regional de equipos de respuesta a incidentes de seguridad informática del continente americano. La adhesión a CSIRT Americas proporciona a México acceso a inteligencia colectiva sobre ciberamenazas que afectan la región, facilita la coordinación de respuestas ante incidentes de alcance del continente americano, permite el aprendizaje de experiencias y mejores prácticas de países con mayor madurez en ciberseguridad, y posiciona al país como socio confiable en el ecosistema regional de protección cibernética, fortaleciendo las capacidades nacionales mediante la cooperación con otros CERTs/CSIRTs miembros. Se dará inicio al proceso de adhesión al Forum of Incident Response and Security Teams (FIRST) y al establecimiento de mecanismos de colaboración con la Unión Internacional de Telecomunicaciones (UIT), lo cual representa la estrategia de incorporación de México a los organismos globales de más alto nivel en materia de respuesta a incidentes de ciberseguridad y de regulación de telecomunicaciones seguras.

2026 - Expansión	
Nombre del Proyecto	Academia Virtual Federal para la implementación de políticas y lineamientos.
Año de Implementación	2026, 2027, 2028.
Mandatos y Objetivos del Artículo 19	Art. 19.III.
Categoría	Talento y capacitación.
Descripción del Proyecto	La Academia Virtual Federal para la Implementación de Políticas y Lineamientos, constituye un programa formativo especializado orientado a desarrollar capacidades institucionales del personal responsable de la implementación operativa de políticas, lineamientos y procedimientos de ciberseguridad en dependencias y entidades de la APF. Con base en el Artículo 19, apartado III, este proyecto piloto busca diseñar y ejecutar

	módulos de capacitación práctica sobre la interpretación de las normas desarrolladas para la ATDR y la DGCiber en materia de ciberseguridad. La fase piloto se desarrollará durante el año 2026 y seleccionará un grupo limitado de instituciones de la APF que representen distintos sectores. Durante los años 2027 y 2028 se expandirá a toda la APF. El programa puede establecer alianzas estratégicas con universidades nacionales e internacionales, organismos especializados y proveedores privados de tecnología para garantizar la actualización continua de contenidos y el acceso a certificaciones reconocidas internacionalmente.

2026 - Expansión	
Nombre del Proyecto	RNCC-MX (Red Nacional de Contactos de Ciberseguridad).
Año de Implementación	2026 y 2027.
Mandatos y Objetivos del Artículo 19	Art. 19.VI.
Categoría	Gobernanza.
Descripción del Proyecto	La Red Nacional de Contactos de Ciberseguridad establece un mecanismo institucionalizado de coordinación, comunicación y colaboración entre los responsables de ciberseguridad de todas las dependencias y entidades de la Administración Pública Federal, que se denominan responsables institucionales de ciberseguridad (RIC), constituyendo una red de enlaces que sostiene el ecosistema de la APF. A esta red se pueden integrar puntos de contacto de otros sectores del ecosistema, sea nacional, privado o del sector educativo, por medio de acuerdos de cooperación. En cumplimiento del Artículo 19, apartado VI, la RNCC-MX designa puntos focales oficiales de ciberseguridad en cada institución federal, establece canales seguros de comunicación, implementa protocolos para el intercambio rápido de información sobre amenazas e incidentes y organiza reuniones periódicas de coordinación técnica. La red facilita la difusión ágil de mejores prácticas, alertas de seguridad, boletines técnicos, y recomendaciones de la Dirección General de Ciberseguridad, así como el intercambio de experiencias y soluciones entre instituciones federales y otros actores. La RNCC-MX puede operar grupos de trabajo temáticos sobre desafíos específicos, coordinar respuestas colaborativas ante incidentes que afectan a múltiples instituciones y constituir el mecanismo operativo de coordinación que

	complementa los instrumentos normativos formales, fortaleciendo la cohesión y la efectividad del sistema federal de ciberseguridad.

2026 - Expansión	
Nombre del Proyecto	MoUs bilaterales entre el sector privado, el sector público y la academia.
Año de Implementación	2026, 2027, 2028, 2029, 2030.
Mandatos y Objetivos del Artículo 19	Art. 19.XIII.
Categoría	Cooperación.
Descripción del Proyecto	El proyecto se refiere al establecimiento de Memorandos de Entendimiento bilaterales entre el sector privado, el sector público y la academia, los cuales constituyen un mecanismo formal mediante el cual se definen los alcances de las relaciones de cooperación, intercambio de información y colaboración técnica entre estos tres sectores del ecosistema mexicano de ciberseguridad. Con base en el Artículo 19, apartado XIII, durante el año 2026 se negocian y suscriben diferentes MoUs con empresas tecnológicas líderes, proveedores de servicios de telecomunicaciones, operadores de infraestructura crítica, instituciones financieras, universidades, otras instituciones públicas y centros de desarrollo tecnológico.

2026 - Expansión	
Nombre del Proyecto	MoUs de CSIRTs internacionales (países, otros CERTs/CSIRTs).
Año de Implementación	2026, 2027, 2028, 2029, 2030.
Mandatos y Objetivos del Artículo 19	Art. 19.XII.
Categoría	Cooperación.

Descripción del Proyecto	El programa de Memorandos de Entendimiento (MoUs) con CSIRTs internacionales constituye la estrategia de cooperación internacional de México en materia de respuesta a incidentes de ciberseguridad, estableciendo acuerdos formales de colaboración con equipos de respuesta a incidentes de otros países y organizaciones internacionales especializadas que ante un eventual ataque a infraestructuras críticas o servicios esenciales, se pueda contar con el apoyo y experiencia de otros CSIRTs de la región. En cumplimiento del Artículo 19, apartado XII, esta iniciativa contribuye a la celebración de acuerdos, convenios y mecanismos de colaboración bilateral y multilateral en ciberseguridad.

2026 – Expansión	
Nombre del Proyecto	**Red Federal de CERTs/CSIRTs**.
Año de Implementación	2026, 2027 y 2028.
Mandatos y Objetivos del Artículo 19	Art. 19.VII, Art. 19.IX, Art. 19.XIII.
Categoría	Operaciones.
Descripción del Proyecto	La Red Federal de Centros de Respuesta a Incidentes de Ciberseguridad Estatales, en su Fase 1, representa una estrategia de apoyo para la creación de CSIRTs en diferentes Estados mexicanos, extendiendo la cobertura operativa más allá del ámbito federal hacia los gobiernos de las entidades federativas. En cumplimiento de los mandatos del Artículo 19, apartados VII, IX y XIII, el proyecto establece, durante 2026, CERTs/CSIRTs en un grupo inicial de estados piloto seleccionados por criterios de madurez tecnológica, voluntad política y capacidades institucionales existentes. La iniciativa contempla la transferencia de conocimientos, metodologías y herramientas desde el CSIRT ATDT, la capacitación de equipos estatales de respuesta, el establecimiento de procedimientos de escalamiento y de coordinación operativa con el Centro Nacional de Operaciones de Ciberseguridad, y la implementación de sistemas de comunicación segura para el intercambio de información sobre incidentes y amenazas. La red promueve la cooperación entre diferentes actores, incorporando universidades estatales, el sector privado y organizaciones de la sociedad civil, y construyendo ecosistemas estatales de ciberseguridad que fortalezcan la resiliencia cibernética territorial.

2026 - Expansión	
Nombre del Proyecto	Sistema de alertas críticas de la APF.
Año de Implementación	2026, 2027.
Mandatos y Objetivos del Artículo 19	Art. 19.X
Categoría	Operaciones.
Descripción del Proyecto	El Sistema de Alertas Críticas de la APF constituye una plataforma tecnológica especializada que habilita la capacidad de la DGCiber para requerir, de manera ágil y estructurada, información específica a instituciones de la APF sobre incidentes de seguridad, exposición a vulnerabilidades críticas, adopción de parches de seguridad urgentes, o cualquier otro elemento relevante para la supervisión y fortalecimiento de la ciberseguridad. Con fundamento en el Artículo 19, apartado X, el sistema implementa mecanismos automatizados de distribución de alertas técnicas por niveles de severidad, establece tiempos máximos de respuesta diferenciados según la criticidad, incorpora formatos estandarizados de reporte que facilitan la consolidación de la información y genera paneles de control ejecutivos sobre el estatus de la respuesta institucional.

Año 2027 - Consolidación

2027 - Consolidación	
Nombre del Proyecto	Sistema integral de gestión de riesgos (ERM-Cyber ATDT).
Año de Implementación	2027.
Mandatos y Objetivos del Artículo 19	Art. 19.IV.
Categoría	Gobernanza.
Descripción del Proyecto	El Sistema integral de gestión de riesgos de ciberseguridad (ERM-Cyber ATDT) constituye la implementación de un marco estructurado de

	Enterprise Risk Management especializado en ciberseguridad para la Agencia de Transformación Digital y Telecomunicaciones. En cumplimiento del Artículo 19, apartado IV, este sistema integra la identificación, el análisis, la evaluación, el tratamiento y el monitoreo continuo de los riesgos de ciberseguridad en todos los niveles organizacionales de la Agencia. El proyecto contempla el desarrollo de inventarios actualizados de activos de información, la identificación de amenazas y vulnerabilidades, el análisis de impacto y probabilidad, la evaluación del nivel de riesgo, el diseño de planes de tratamiento, y el establecimiento de indicadores clave de riesgo (KRIs). Integra metodologías reconocidas internacionalmente y establece comités de gestión de riesgos que involucran a todos los niveles de la organización.

2027 - Consolidación	
Nombre del Proyecto	Cyber Range Nacional.
Año de Implementación	2027, 2028, 2029.
Mandatos y Objetivos del Artículo 19	Art. 19.VI, Art. 19.VIII.
Categoría	Talento y capacitación.
Descripción del Proyecto	El Cyber Range Nacional constituye una plataforma de entrenamiento y simulación avanzada que replica infraestructuras críticas, redes de telecomunicaciones, y sistemas de información federales en entornos virtuales controlados, permitiendo la capacitación práctica de equipos de ciberseguridad mediante ejercicios realistas de defensa, detección y respuesta ante ciberataques sofisticados. En cumplimiento del Artículo 19, apartados VI y VIII, esta iniciativa promueve la formación de talento especializado en ciberseguridad, proporcionando entrenamiento avanzado a servidores públicos, operadores de infraestructura crítica, y equipos de respuesta a incidentes mediante simulaciones de escenarios de ataque realistas que replican las tácticas, técnicas y procedimientos (TTPs) de adversarios reales. El Cyber Range implementa ejercicios de red team vs blue team donde equipos atacantes (red team) ejecutan campañas maliciosas contra defensores (blue team) en tiempo real, utilizando escenarios de respuesta a incidentes de ransomware, APTs y

	DDoS, simulaciones de compromisos de infraestructura crítica con consecuencias en el mundo físico, y ejercicios de toma de decisiones para alta dirección ante crisis cibernéticas nacionales. Mediante convenios, el Cyber Range puede ser una plataforma al servicio de los países de América Latina y el Caribe.

Año 2028 - Maduración

2028 - Maduración	
Nombre del Proyecto	IA para ciberdefensa.
Año de Implementación	2028, 2029, 2030.
Mandatos y Objetivos del Artículo 19	Art. 19.IV, Art. 19.IX.
Categoría	Cooperación e investigación y desarrollo (I+D).
Descripción del Proyecto	El proyecto de Inteligencia Artificial para Ciberdefensa constituye una iniciativa de vanguardia tecnológica orientada a revolucionar las capacidades de gestión de riesgos, detección de amenazas, y respuesta automatizada a incidentes de ciberseguridad mediante la aplicación de técnicas avanzadas de machine learning, deep learning, y análisis predictivo. En cumplimiento del Artículo 19, apartados IV y IX, este proyecto fortalece la gestión de riesgos con analítica avanzada capaz de procesar volúmenes masivos de información, identificar patrones anómalos a un menor tiempo que utilizando el análisis humano, predecir vectores de ataque emergentes, y automatizar procesos de respuesta que actualmente requieren intervención manual. El proyecto posiciona a

	la DGCiber a la vanguardia tecnológica global, estableciendo capacidades de ciberdefensa cognitiva que aprenden continuamente de cada incidente y evolucionan para anticipar amenazas futuras.

2028 - Maduración	
Nombre del Proyecto	Centro Regional LATAM de Respuesta.
Año de Implementación	2028, 2029, 2030.
Mandatos y Objetivos del Artículo 19	Art. 19.VII, Art. 19.XIII
Categoría	Cooperación.
Descripción del Proyecto	Promover el desarrollo de un Centro Regional de Respuesta a Incidentes para América Latina representa una iniciativa de alcance regional que posiciona a México como líder en ciberseguridad en el continente americano, estableciendo capacidades de coordinación multinacional para responder a ciberataques de alcance transnacional que afectan a múltiples países de la región. Tomando de base el Artículo 19, apartados VII y XIII, este centro proporciona servicios de coordinación ante incidentes regionales, opera bajo un modelo 24/7 que garantiza respuesta continua, facilita el intercambio de información de amenazas entre CERTs/CSIRTs nacionales latinoamericanos, coordina respuestas conjuntas ante campañas maliciosas de alcance continental, y promueve la cooperación multi actor entre gobiernos, sector privado, academia y organizaciones internacionales. El centro fortalece la resiliencia en ciberseguridad de América Latina y el Caribe, reconociendo que las amenazas cibernéticas no respetan fronteras y requieren respuestas coordinadas entre los países.

Año 2029 - Liderazgo

2029 - Liderazgo

Nombre del Proyecto	Estrategia de exportación de servicios.
Año de Implementación	2029.
Mandatos y Objetivos del Artículo 19	Art. 19.XIII.
Categoría	Cooperación.
Descripción del Proyecto	El proyecto de exportación de servicios representa una iniciativa pionera que transforma a México de receptor de cooperación internacional en ciberseguridad a proveedor de servicios especializados de alto valor agregado para gobiernos de América Latina y el Caribe, generando capacidades de proyección regional a partir de las capacidades institucionales desarrolladas por la Dirección General de Ciberseguridad durante el periodo 2025-2029. En cumplimiento del Artículo 19, apartado XIII, este proyecto establece mecanismos formales de cooperación con entidades gubernamentales y organismos internacionales para la prestación de servicios de consultoría en ciberseguridad, capacitación especializada, transferencia de tecnología, asesoría en el desarrollo de marcos normativos y apoyo en la respuesta a incidentes de gran escala. El proyecto contempla la creación de un catálogo de servicios exportables por parte de la DGCiber, entre ellos el Cyber Range Nacional y otros proyectos e iniciativas desarrollados por la DGCiber que contribuyan al fortalecimiento de las capacidades de ciberseguridad a nivel regional. Este proyecto está diseñado para recibir la cooperación de organismos multilaterales para el financiamiento de viajes de los miembros de CERTs/CSIRTs de otros países, visitas de CSIRT ATDT a otros países o aplicaciones técnicas.

2029 - Liderazgo	
Nombre del Proyecto	VUIC (Ventanilla Única de Información de Ciberseguridad).
Año de Implementación	2029, 2030
Mandatos y Objetivos del Artículo 19	Art. 19.X

Categoría	Cooperación.
Descripción del Proyecto	La Ventanilla Única de Información de Ciberseguridad (VUIC) constituye el mecanismo centralizado y estandarizado para requerir, recopilar, procesar, almacenar y analizar, de manera sistemática, oportuna y segura, información de ciberseguridad de todas las dependencias, órganos administrativos desconcentrados y entidades de la Administración Pública Federal. En cumplimiento del Artículo 19, fracción X, esta plataforma transforma la gestión de la información de ciberseguridad de un modelo fragmentado basado en solicitudes ad hoc a un sistema integrado que proporciona visibilidad holística del estado de ciberseguridad del sector público federal. La VUIC implementa formularios digitales estandarizados para la solicitud de información según tipo de requerimiento (incidentes de seguridad, inventarios de activos, evaluaciones de vulnerabilidades, cumplimiento normativo, indicadores de desempeño), flujos de trabajo automatizados para el procesamiento de solicitudes con plazos de respuesta obligatorios, mecanismos de validación automática de integridad y completitud de información recibida, y protocolos de confidencialidad según clasificación de información. La plataforma integra capacidades de análisis agregado que permiten identificar tendencias nacionales de amenazas, patrones de vulnerabilidades recurrentes, brechas de cumplimiento sistémicas y benchmarking de la madurez en ciberseguridad entre instituciones. Incluye tableros de control ejecutivos que muestran el estado de respuesta a requerimientos de información en tiempo real, la generación automatizada de reportes consolidados para la alta dirección y capacidades de minería de datos para el descubrimiento de insights estratégicos. La VUIC reduce significativamente la carga administrativa asociada a la recopilación de información mediante la automatización de procesos, elimina duplicidades en los requerimientos entre diferentes áreas de la Agencia y asegura que las decisiones estratégicas de ciberseguridad se fundamenten en información actualizada, confiable y exhaustiva del universo completo de instituciones federales.

2029 - Liderazgo	
Nombre del Proyecto	Observatorio APF de Ciberseguridad.
Año de Implementación	2029, 2030.

Mandatos y Objetivos del Artículo 19	Art. 19.XI
Categoría	Cooperación e investigación y desarrollo (I+D).
Descripción del Proyecto	El Observatorio de Ciberseguridad de la Administración Pública Federal constituye un centro permanente de estudios, análisis estratégico, y prospectiva tecnológica en materia de ciberseguridad que genera conocimiento especializado, documenta tendencias, evalúa amenazas emergentes, y produce recomendaciones fundamentadas para la toma de decisiones de política pública en protección del ciberespacio gubernamental. En cumplimiento del Artículo 19, fracción XI, este observatorio elabora informes anuales exhaustivos sobre el estado de la ciberseguridad en el sector público federal que documentan incidentes relevantes, tendencias de amenazas, evolución de la madurez institucional, efectividad de políticas implementadas y desafíos emergentes. El observatorio implementa capacidades de análisis prospectivo mediante la aplicación de metodologías de inteligencia estratégica, análisis de escenarios futuros, evaluación de tecnologías emergentes con implicaciones en ciberseguridad, monitoreo de tendencias globales de cibercrimen y ciberconflicto, y evaluación de impacto de cambios regulatorios internacionales. Produce estudios temáticos especializados sobre áreas prioritarias como seguridad de infraestructuras críticas, protección de datos personales, ciberseguridad en servicios de gobierno digital, amenazas de actores estatales, impacto de la inteligencia artificial en ciberseguridad y preparación ante pandemias cibernéticas. El observatorio mantiene repositorios de conocimiento accesibles que incluyen bibliografía especializada, bases de datos de incidentes históricos, taxonomías de amenazas, inventarios de mejores prácticas internacionales y directorios de expertos nacionales. Genera, además, recomendaciones de política pública, fundamentadas en evidencia, que informan la actualización continua del marco normativo de ciberseguridad, la priorización de inversiones en tecnologías de protección y el diseño de programas de desarrollo de capacidades. El observatorio posiciona a la Dirección General de Ciberseguridad como autoridad intelectual reconocida en materia de ciberseguridad gubernamental, facilita el aprendizaje organizacional mediante la documentación sistemática de experiencias y asegura que la evolución de las políticas de ciberseguridad se base en análisis rigurosos de contextos nacionales e internacionales.

Año 2030 – Transformación y proyección

2030 – Transformación y proyección	
Nombre del Proyecto	Certificación nacional para el cumplimiento de los lineamientos y protocolos de ciberseguridad de la APF.
Año de Implementación	2030.
Mandatos y Objetivos del Artículo 19	Art. 19.VI.
Categoría	Talento y capacitación.
Descripción del Proyecto	La Certificación Nacional de Cumplimiento de los lineamientos y Protocolos de Ciberseguridad de la APF establece un sistema formal de acreditación y certificación que reconoce a las instituciones de la APF que demuestren niveles de implementación de protocolos de seguridad, cumplimiento normativo, y madurez en capacidades de ciberseguridad. Esta certificación tendrá un evento para el reconocimiento de todas las instituciones de la APF que durante 2025 y 2029 tuvieron avances significativos en la aplicación de los lineamientos y protocolos de ciberseguridad, para que sirvan de ejemplo a nivel nacional e internacional de su madurez obtenida. En cumplimiento del Artículo 19, apartado VI, este programa fomenta las mejores prácticas mediante el reconocimiento público de instituciones que alcanzan estándares de excelencia en ciberseguridad, generando incentivos reputacionales por la adopción de controles de seguridad. El programa contempla la definición de niveles de certificación escalonados (básico, intermedio, avanzado, excelencia) con criterios objetivos y medibles de cumplimiento, procesos de evaluación técnica ejecutados por equipos de auditores certificados, requisitos de mantenimiento de la certificación mediante auditorías periódicas de seguimiento, y protocolos de revocación en caso de incidentes graves o incumplimientos materiales. El programa genera un “Sello” o “Galardón” de Ciberseguridad para la institución.

2030 – Transformación y proyección	
Nombre del Proyecto	Next-Gen SecOps (IA avanzada y Tecnologías Emergentes).
Año de Implementación	2030.

Mandatos y Objetivos del Artículo 19	Art. 19.IV, Art. 19.IX
Categoría	Cooperación e investigación y desarrollo (I+D).
Descripción del Proyecto	El proyecto Next-Gen SecOps representa la evolución hacia operaciones de seguridad de próxima generación, fundamentadas en inteligencia artificial avanzada, machine learning profundo, la aplicación de tecnologías emergentes y la automatización cognitiva, que transforman radicalmente las capacidades de gestión de riesgos en tiempo real, la predicción de amenazas futuras y la respuesta autónoma a incidentes de ciberseguridad sin intervención humana. En cumplimiento del Artículo 19, fracciones IV y IX, este proyecto implementa sistemas de IA de vanguardia que aprenden continuamente de cada incidente, evolucionan sus modelos de detección automáticamente, anticipan vectores de ataque emergentes antes de su materialización y ejecutan respuestas defensivas complejas de manera completamente autónoma bajo supervisión estratégica humana. El proyecto contempla la implementación de sistemas de gestión de riesgos en tiempo real que procesan continuamente feeds de inteligencia de amenazas global, correlacionan indicadores de vulnerabilidad con patrones de ataque observados, calculan probabilidades dinámicas de compromiso para cada activo crítico, y ajustan automáticamente prioridades de remediación según la evolución del panorama de amenazas. Incluye capacidades predictivas basadas en modelos de deep learning que analizan series temporales de actividad maliciosa, identifican patrones precursores de campañas de ataque sofisticadas, anticipan tácticas de adversarios mediante análisis de comportamiento histórico, y generan alertas tempranas de amenazas emergentes con semanas o meses de anticipación. El proyecto implementa, además, operaciones de seguridad autónomas mediante plataformas de orquestación inteligente (AI-powered SOAR) que ejecutan playbooks complejos y adaptativos, toman decisiones tácticas de contención sin intervención humana, aprenden de resultados de respuestas previas para optimizar estrategias futuras y escalan únicamente a analistas humanos cuando enfrentan escenarios sin precedentes que requieren juicio experto. Integra sistemas que proporcionan transparencia sobre decisiones automatizadas, mantiene controles de supervisión humana sobre acciones críticas potencialmente disruptivas y asegura la alineación con los principios éticos de uso de la IA en el ámbito de la seguridad. El proyecto posiciona a México a la vanguardia absoluta global en la aplicación de la inteligencia artificial para la ciberdefensa, estableciendo capacidades operativas que rivalizan con las de potencias tecnológicas mundiales y demostrando que los países en desarrollo pueden alcanzar

	la excelencia en tecnologías de frontera mediante una inversión estratégica sostenida.

A continuación, se presenta el cronograma propuesto de proyectos del Plan Nacional de la Dirección Nacional de Ciberseguridad:

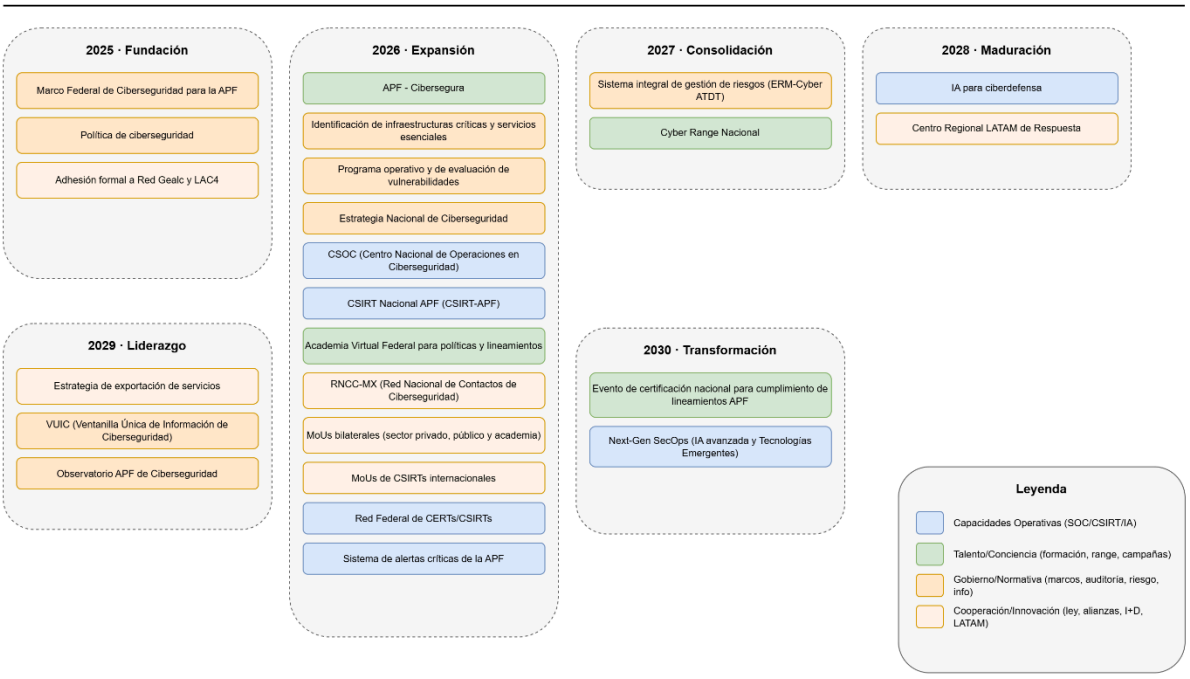


Figura 10: Proyectos de ciberseguridad de la DGCIBER – Plan Nacional de 2025-2030. Elaboración propia.

4. Indicadores y metas

El presente apartado presenta los indicadores y metas para cada uno de los proyectos que se desarrollarán durante el plazo de 2025 a 2030 por parte de la DGCIBER y la ATDT. Se han clasificado los proyectos por su año de inicio de implementación, considerando que algunos requieren continuidad en el año posterior a su inicio y se mantienen en el tiempo.

Año 2025 – Fundamento

Nombre del Proyecto	Descripción Corta	Indicadores	Metas 2025
Marco Federal de Ciberseguridad para la APF	Sistema integral de gobernanza que incluye la Política, los lineamientos (gestión de riesgos, incidentes, capacitación y madurez) y los protocolos (TLP, notificación y escalamiento) para la APF.	1. Política de Ciberseguridad publicada 2. Lineamientos principales desarrollados 3. Protocolos fundamentales establecidos 4. Instituciones priorizadas notificadas	1. Política publicada en DOF (Q4 2025) 2. 100% instituciones APF dentro del alcance identificadas 3. Tres lineamientos principales publicados (incidentes, capacitación, madurez) 4. tres protocolos establecidos (TLP, notificación, escalamiento) 5. 20 instituciones prioritarias formalmente notificadas
Adhesión formal a LAC4	Incorporación de México a redes regionales de cooperación en ciberseguridad de LATAM mediante el intercambio de experiencias, mejores prácticas e información sobre amenazas.	1. Solicitud de adhesión presentada 2. Proceso de membresía completado 3. Participación en eventos regionales 4. Intercambio de información iniciado	1. Notas formales de adhesión enviadas (Q4 2025) 2. Membresía aprobada en ambas redes (Q1 2026) 3. Participación en 2 eventos regionales mínimo (2026) 4. Primer intercambio de información sobre amenazas
Memorando de Entendimiento (MOU) sobre cooperación en materia de ciberseguridad entre Brasil y la ATDT.	Instrumento jurídico de carácter internacional que facilita el intercambio de conocimiento y experiencias en temas de ciberseguridad.	1. Solicitud de suscripción de MOU 2. Proceso de revisión institucional 3. Aprobación y firma 4. Actividades de cooperación iniciadas	1. Posturas institucionales aprobadas (Q4 2025). 2. Suscripción bilateral de MOU (Q4 2025). 3. Inicio de actividades de cooperación.

Año 2026 – Expansión

Nombre del Proyecto	Descripción Corta	Indicadores	Metas 2026
APF Cibersegura	Programa nacional de concientización para funcionarios públicos federales, con campañas, materiales educativos, eventos y alianzas, para desarrollar una cultura y prácticas seguras.	1. Programa formalmente lanzado 2. Campañas de concientización ejecutadas 3. Materiales educativos desarrollados 4. Funcionarios públicos alcanzados 5. Instituciones participantes	1. Lanzamiento oficial del programa (Q2 2026) 2. 4 campañas de concientización en APF 3. 10 tipos de materiales educativos básicos 4. Directriz para que el curso sea obligatorio a todos los funcionarios de la APF (capacitación virtual) 5. 30 instituciones APF participando activamente
Identificación Infraestructuras Críticas y Servicios Esenciales	Metodología y proceso de categorización de activos tecnológicos, sistemas y servicios, fundamentales para la continuidad de la APF, con inventario nacional y criterios de criticidad.	1. Metodología de categorización establecida 2. Inventario nacional iniciado 3. Infraestructuras críticas identificadas 4. Servicios esenciales catalogados 5. Informe de clasificación publicado	1. Metodología aprobada y documentada (Q2 2026) 2. Todo el inventario la cobertura de instituciones de la APF 3. Infraestructuras críticas priorizadas 4. Servicios esenciales catalogados inicialmente 5. Primer informe nacional de IC/SE publicado (Q4 2026)
Programa Operativo Evaluación de Vulnerabilidades	Identificación, análisis y gestión sistemática de vulnerabilidades mediante escaneo automatizado, hacking ético, revisión de código y alianzas público-privadas.	1. Programa operativo establecido 2. Herramientas de evaluación implementadas 3. Evaluaciones realizadas 4. Vulnerabilidades críticas identificadas 5. Alianzas para evaluación formalizadas	1. Programa documentado y operativo (Q1 2026) 2. Herramientas de escaneo implementadas 3. Evaluaciones básicas completadas al primer grupo de instituciones 4. Identificación y clasificación de vulnerabilidades 5. 2 alianzas APP o academia establecidas

Estrategia Nacional de Ciberseguridad	Documento rector de alto nivel que articula visión, objetivos, líneas de acción y coordinación multisectorial para la protección del ciberespacio mexicano.	1. Estrategia desarrollada y aprobada 2. Ejes estratégicos definidos 3. Consulta pública realizada 4. Presentación oficial ejecutada 5. Sectores comprometidos	1. Estrategia Nacional aprobada (Q3 2026) 2. 5 a 7 ejes estratégicos establecidos 3. Consulta con 100+ participantes multisector 4. Presentación oficial de alto nivel realizada 5. Compromisos iniciales de sectores clave definidos
CSOC (Centro Nacional Operaciones)	Comando unificado con SOC para monitoreo 24/7, correlación de eventos, detección proactiva con SIEM, coordinación de respuestas en la APF.	1. Centro establecido con infraestructura 2. Personal operativo contratado 3. Plataforma SIEM implementada 4. Instituciones con conexión inicial 5. Eventos de seguridad monitoreados	1. CSOC operativo en fase inicial (Q4 2026) 2. Equipo base de 10 especialistas contratados 3. Plataforma SIEM con configuración básica 4. 10 instituciones piloto conectadas y la ATDT 5. Monitoreo inicial de eventos establecido
CSIRT Nacional APF	Centro de respuesta a incidentes 24/7 para la APF, con personal especializado, herramientas forenses y coordinación nacional e internacional (CSIRT Americas, FIRST, UIT).	1. CSIRT establecido y operativo 2. Personal especializado integrado 3. Incidentes atendidos 4. Adhesión CSIRT Americas completada 5. Proceso FIRST/UIT iniciado	1. CSIRT operativo 24/7 (Q3 2026) 2. 12 especialistas certificados en el equipo 3. Atención de incidentes con capacidad inicial 4. Membresía CSIRT Americas aprobada (Q4) 5. Solicitudes formales FIRST/UIT presentadas
Academia Virtual Federal Implementación Políticas	Programa formativo virtual especializado para personal responsable de la implementación de políticas y lineamientos de ciberseguridad con fase piloto y expansión.	1. Academia virtual establecida 2. Módulos de capacitación desarrollados 3. Fase piloto ejecutada 4. Funcionarios capacitados 5. Alianzas académicas formalizadas	1. Plataforma virtual operativa (Q2 2026) 2. 3 módulos de capacitación práctica disponibles 3. Piloto con 10 instituciones completado (Q4) 4. 200 capacitados en piloto 5. 2 alianzas con universidades establecidas
RNCC-MX (Red Nacional Contactos)	Red institucionalizada de coordinación entre los responsables de ciberseguridad (RIC) de la APF, con puntos focales, canales seguros y grupos de trabajo.	1. Red formalmente constituida 2. Responsables institucionales designados 3. Canales de comunicación establecidos 4. Reuniones de coordinación realizadas	1. RNCC-MX oficialmente establecida (Q2 2026) 2. RICs designados en 80% instituciones APF 3. Plataforma de comunicación segura activa 4. 6 reuniones nacionales de coordinación 5. 3 grupos de trabajo temáticos iniciados

		5. Grupos de trabajo operando	
MoUs Bilaterales Sector Público-Privado-Academia	Memorandos de entendimiento para la cooperación, el intercambio de información y la colaboración técnica entre sectores del ecosistema mexicano de ciberseguridad.	1. MoUs negociados y firmados 2. Sectores participantes 3. Áreas de cooperación definidas 4. Proyectos colaborativos iniciados 5. Intercambio de información activo	1. MoUs bilaterales firmados en 2026 2. Participación de 3 sectores activos 3. 5 áreas de cooperación prioritarias definidas 4. 3 proyectos colaborativos iniciados 5. Inicio de intercambio de inteligencia
MoUs CSIRTs Internacionales	Acuerdos formales de cooperación con equipos de respuesta a incidentes de otros países para el apoyo mutuo ante ataques a infraestructuras críticas.	1. MoUs con CSIRTs internacionales firmados 2. Países con acuerdos activos 3. Mecanismos de colaboración establecidos 4. Intercambios de información realizados 5. Coordinación de incidentes ejecutada	1. MoUs con CSIRTs internacionales firmados 2. Acuerdos con países (prioritarios de región) 3. Protocolos de colaboración definidos 4. Inicio de intercambio de información 5. Primer caso de coordinación internacional
Red Federal de CERTs/CSIRTs	Apoyo para la creación de CSIRTs estatales en fase piloto con transferencia de conocimientos, capacitación y coordinación con el CSIRT Nacional APF.	1. Estados piloto seleccionados 2. CSIRTs estatales establecidos 3. Personal estatal capacitado 4. Protocolos de coordinación definidos 5. Ecosistemas estatales iniciados	1. 5 estados piloto seleccionados (Q1 2026) 2. 3 CSIRTs estatales operando en fase inicial (Q4) 3. 50 especialistas estatales capacitados 4. Protocolos de escalamiento establecidos 5. Vinculación con universidades estatales iniciada
Sistema de Alertas Críticas APF	Plataforma tecnológica para la distribución ágil de alertas técnicas por severidad con formatos estandarizados, tiempos de respuesta y paneles de control.	1. Sistema de alertas implementado 2. Niveles de severidad definidos 3. Alertas distribuidas 4. Tiempo de respuesta institucional 5. Cobertura de instituciones conectadas	1. Plataforma operativa con funcionalidad básica (Q3 2026) 2. 3 niveles de severidad estandarizados 3. Capacidad de distribución de alertas activa 4. Medición de tiempos de respuesta iniciada 5. 20% instituciones APF conectadas al sistema

Año 2027 - Consolidación

Nombre del Proyecto	Descripción Corta	Indicadores	Metas 2027
Sistema Integral Gestión de Riesgos (ERM-Cyber ATDT)	Marco estructurado de Enterprise Risk Management especializado en ciberseguridad para ATDT, con identificación, análisis, evaluación, tratamiento y monitoreo de riesgos, basado en metodologías internacionales.	1. Sistema ERM implementado 2. Inventario de activos desarrollado 3. Análisis de riesgos completado 4. Planes de tratamiento establecidos 5. Indicadores clave de riesgo (KRIs) definidos 6. Comités de gestión operando	1. Sistema ERM operativo en ATDT (Q3 2027) 2. Inventario de activos críticos de ATDT completo 3. Análisis de riesgos principales documentado 4. Planes de tratamiento para riesgos prioritarios 5. 15 KRIs principales en monitoreo 6. Comité de gestión de riesgos establecido
Cyber Range Nacional	Plataforma de entrenamiento y simulación avanzada que replica infraestructuras críticas para una capacitación práctica mediante ejercicios red team vs blue team, escenarios APT, ransomware y DDoS.	1. Plataforma de Cyber Range establecida 2. Escenarios de simulación desarrollados 3. Ejercicios de entrenamiento ejecutados 4. Profesionales entrenados 5. Infraestructura técnica operativa 6. Alianzas regionales establecidas	1. Cyber Range operativo en fase inicial (Q4 2027) 2. 4 escenarios de ataque realistas disponibles 3. 3 ejercicios nacionales ejecutados 4. 100 profesionales federales entrenados 5. Infraestructura virtual para simulación activa 6. 2 convenios con países de LATAM para uso regional

Año 2028 - Maduración

Nombre del Proyecto	Descripción Corta	Indicadores	Metas 2028
IA para Ciberdefensa	Aplicación de machine learning, deep learning y análisis predictivo para revolucionar la gestión de riesgos, la detección de amenazas y la respuesta automatizada con capacidades cognitivas.	1. Proyecto de IA iniciado 2. Modelos de ML/DL desarrollados 3. Integración con sistemas existentes 4. Casos de uso implementados 5. Mejora en detección de amenazas (%) 6. Alianzas tecnológicas establecidas	1. Proyecto de IA formalmente lanzado (Q1 2028) 2. 3 modelos piloto de ML en desarrollo 3. Integración inicial con CSOC/CSIRT 4. 5 casos de uso de detección implementados 5. 30% mejora en velocidad de detección (piloto) 6. 2 alianzas con sector tecnológico/academia
Centro Regional LATAM de Respuesta	Centro multinacional 24/7 para la coordinación de respuestas ante ciberataques transnacionales en LatAm con intercambio de inteligencia y cooperación multiactor gobierno-privado-academia.	1. Proyecto del Centro promovido 2. Países de la región comprometidos 3. Marco de cooperación regional establecido 4. Infraestructura y recursos identificados 5. Hoja de ruta desarrollada 6. Eventos de promoción realizados	1. Propuesta formal del Centro presentada (Q2 2028) 2. Países clave de LATAM con interés expresado 3. Marco de cooperación multilateral en desarrollo 4. Evaluación de requerimientos completada 5. Hoja de ruta 2029-2030 aprobada 6. 2 eventos regionales de promoción ejecutados

Año 2029 - Liderazgo

Nombre del Proyecto	Descripción Corta	Indicadores	Metas 2029
Estrategia de Exportación de Servicios	Transformación de México en proveedor regional de servicios especializados: consultoría, capacitación, transferencia tecnológica, marcos normativos y respuesta a incidentes para LATAM.	1. Estrategia de exportación desarrollada 2. Catálogo de servicios exportables creado 3. Países clientes identificados 4. Contratos o acuerdos firmados 5. Servicios prestados 6. Financiamiento multilateral gestionado	1. Estrategia aprobada y publicada (Q2 2029) 2. Catálogo con servicios exportables definidos 3. 2 países de LATAM identificados como beneficiarios potenciales 4. Primeros acuerdos de servicio firmados 5. Inicio de prestación de servicios (Cyber Range, consultoría, capacitación) 6. Acuerdo con algún

			organismo multilaterales para financiamiento
VUIC (Ventanilla Única Información Ciberseguridad)	Plataforma centralizada para requerir, recopilar, procesar y analizar información de ciberseguridad de toda la APF mediante formularios estandarizados, flujos automatizados y tableros ejecutivos.	1. Plataforma VUIC desarrollada e implementada 2. Instituciones APF integradas al sistema 3. Tipos de requerimientos estandarizados 4. Solicitudes de información procesadas 5. Tableros de análisis operativos 6. Tiempo promedio de respuesta (días)	1. VUIC operativa en fase inicial (Q3 2029) 2. 40% instituciones APF integradas al sistema 3. 6 tipos de requerimientos estandarizados 4. Capacidad de procesamiento de solicitudes activa 5. Tablero ejecutivo con indicadores básicos 6. Reducción 40% en tiempo de respuesta vs modelo anterior
Observatorio APF de Ciberseguridad	Centro permanente de estudios, análisis estratégico y prospectiva que genera informes anuales, estudios temáticos, repositorios de conocimiento y recomendaciones de política pública.	1. Observatorio formalmente establecido 2. Informe anual de ciberseguridad publicado 3. Estudios temáticos desarrollados 4. Repositorio de conocimiento implementado 5. Recomendaciones de política emitidas 6. Eventos de difusión realizados	1. Observatorio inaugurado oficialmente (Q2 2029) 2. Primer informe anual del estado de ciberseguridad APF 3. 4 estudios temáticos especializados publicados 4. Repositorio digital con documentos accesibles 5. Recomendaciones de política pública emitidas 6. 2 eventos de difusión de conocimiento realizados

Año 2030 – Transformación y proyección

Nombre del Proyecto	Descripción Corta	Indicadores	Metas 2030
Certificación Nacional Cumplimiento Lineamientos APF	Sistema formal de certificación que reconoce instituciones APF con excelencia en la implementación de protocolos con niveles escalonados, Sello/Galardón de ciberseguridad y evento de reconocimiento.	1. Sistema de certificación operativo 2. Niveles de certificación implementados 3. Instituciones evaluadas y certificadas 4. Evento nacional de certificación ejecutado 5. Sellos de ciberseguridad otorgados 6. Benchmarking nacional publicado	1. Sistema de certificación plenamente operativo 2. 4 niveles certificación implementados (básico a excelencia) 3. Primeras instituciones APF evaluadas y certificadas 4. Evento nacional de alto nivel realizado (Q4 2030) 5. Diseño y entrega de Sellos/Galardones de ciberseguridad otorgados 6. Reporte nacional de madurez por institución publicado

Next-Gen SecOps (IA Avanzada y Tecnologías Emergentes)	Operaciones de seguridad de próxima generación con IA avanzada, ML profundo, predicción de amenazas, respuesta autónoma, gestión de riesgos en tiempo real y capacidades de vanguardia a nivel global.	1. Proyecto Next-Gen SecOps implementado 2. Sistemas de IA avanzada operativos 3. Capacidades predictivas activas 4. Respuestas autónomas ejecutadas 5. Gestión de riesgos en tiempo real 6. Mejora en capacidades operativas (%)	1. Next-Gen SecOps operativo en CSOC (Q3 2030) 2. Sistema(s) de IA avanzada integrados y activos 3. Predicción de amenazas con 3-4 semanas de anticipación 4. 50% respuestas de nivel 1-2 completamente autónomas 5. Dashboard de riesgos en tiempo real operativo 6. 60% mejora en tiempo de detección y respuesta vs 2025

5. Vinculación internacional

En este apartado se desarrolla la importancia acerca de la cooperación y la vinculación internacional que los países y las agencias a cargo de la materia de ciberseguridad deben impulsar, como elementos fundamentales y críticos para la lucha contra el cibercrimen y la promoción de una ciberseguridad global, especialmente ante los grandes desafíos de las amenazas actuales como lo indica la *WEF* en su reporte *Global Cybersecurity Outlook 2025*. Otro elemento para considerar es cómo las sociedades se han ido incorporando y generando dependencias del buen funcionamiento de los sistemas y servicios digitales, con millones de personas y dispositivos interconectados, lo que hace que la ciberseguridad requiera una responsabilidad compartida que no tiene fronteras.

La comunidad internacional, desde hace algunos años, viene trabajando colectivamente para fortalecer la resiliencia en ciberseguridad, sin embargo para lograr el éxito en este fortalecimiento se requiere que los países, las organizaciones, el sector privado, la academia y la sociedad civil, trabajen de una forma colaborativa y con acciones claras como el intercambio de información de inteligencia, recursos y mejores prácticas entre los países y los sectores y la participación multisectorial del ecosistema. La Unión Internacional de Telecomunicaciones (UIT) reconoce formalmente la

cooperación como uno de los cinco pilares esenciales que miden el compromiso de un país con la ciberseguridad, y que es utilizado en la medición de su Índice Global de Ciberseguridad (GCI).

Para lograr promover la cooperación es necesario definir la existencia de asociaciones, marcos de colaboración, redes de intercambio de información a nivel nacional, regional y global por medio de instrumentos habilitadores, como pueden ser Memorándums de Entendimiento (MoU), convenios interinstitucionales, Directrices, Decretos o Leyes, por mencionar algunos. A nivel mundial, 166 países mantienen acuerdos internacionales de ciberseguridad. Estos esfuerzos incluyen:

1. **Marcos legales internacionales**: Entre los principales instrumentos se pueden identificar el Convenio de Budapest sobre la Ciberdelincuencia, iniciado en el año 2004, y el Convenio sobre la Ciberdelincuencia de la Organización de las Naciones Unidas, que buscan promover y mejorar la cooperación entre los países para responder judicialmente a los criminales cibernéticos. Un desafío es armonizar los marcos legales de los diferentes países para investigar y llevar a juicio los delitos que trascienden las fronteras.
2. **Acuerdos bilaterales y regionales**: La generación de acuerdos bilaterales entre países centrados en el intercambio de información y el desarrollo de capacidades forman parte de los instrumentos de cooperación y vinculación internacional. Para la región de América Latina y el Caribe (ALC), la Organización de los Estados Americanos (OEA) por medio de CICTE y CSIRT Américas, programas que cuentan con el apoyo de la Unión Europea como EU Cybernet, LAC4 y EU-LAC Digital Alliance – Policy Dialogs, así como organismos multilaterales como el Banco Interamericano de Desarrollo (BID) y el Grupo Banco Mundial (WBG), han intensificado, en los últimos años, sus esfuerzos para el desarrollo de capacidades cibernéticas en la región.
3. **Redes de Centros de Respuesta a Incidentes**: Plataformas como CSIRT Américas de CICTE/OEA, que opera activamente desde el año

2016, promueve la cooperación regional y el entrenamiento para mejorar las capacidades y los niveles de madurez de los equipos nacionales y gubernamentales de gestión de incidentes de ciberseguridad.

4. Alianzas Público-Privadas (APP): Una oportunidad que trasciende al "trabajo en silos" de las instituciones gubernamentales y que puede colaborar para atender la complejidad de los riesgos cibernéticos es la generación de alianzas público-privadas por medio de marcos normativos habilitantes, como lo pueden ser los MoU o normativas legales.

Para que la cooperación sea plenamente efectiva, los países de ALC deben invertir en el desarrollo de capacidades y talento especializados, sentando las bases para que contribuyan activamente a los esfuerzos globales de ciberseguridad, promoviendo la confianza y la seguridad.

La estrategia de vinculación internacional de México se estructura por medio de un proceso en un plazo de tres años (2025-2027), diseñado para integrar sistemáticamente al país en los principales ecosistemas regionales e internacionales de cooperación en materia de ciberseguridad. Este enfoque aplica las mejores prácticas identificadas por organismos multilaterales y permite un desarrollo de capacidades sostenible y alineado con los objetivos de posicionamiento regional de México.

Las etapas de vinculación internacional se presentan a continuación:

Q4 2025:

- Carta de intención de adhesión a LAC4:
    - El Centro de Competencia Cibernética de América Latina y el Caribe (LAC4) representa una de las principales plataformas regionales de formación y entrenamiento en ciberseguridad, implementado por EU CyberNet y financiado por la Unión Europea desde su establecimiento en 2022 en Santo Domingo, República Dominicana (LAC4, 2025). LAC4 ha demostrado ser un

catalizador fundamental para el desarrollo de capacidades regionales, ofreciendo infraestructura de entrenamiento híbrida, laboratorios de forense digital y un cyber range especializado (EU CyberNet, 2023). La adhesión de México a LAC4 proporcionará acceso a programas de capacitación técnica, política y estratégica, así como oportunidades para participar en ejercicios de simulación y en la red de expertos conformada por más de 600 profesionales que contribuyen activamente a las misiones cibernéticas de la Unión Europea y la región.

  - El Centro LAC4 actualmente cuenta con 16 países miembros, incluyendo recientemente a Colombia, Costa Rica y las Bahamas, lo que posiciona a la iniciativa como el principal foro regional para el intercambio de conocimientos y el desarrollo de capacidades en ciberseguridad. Los eventos emblemáticos como CyberWeek@LAC4, que en su edición 2025 reunió a expertos de 30 países bajo el tema "Construyendo resiliencia sin fronteras", representan oportunidades estratégicas para que México participe activamente en el diálogo birregional sobre amenazas emergentes.

- Posturas institucionales aprobadas y suscripción de MOU entre Brasil y la ATDT:
  - Como parte de los avances en la cooperación regional en materia de ciberseguridad, resulta indispensable contar con mecanismos que promuevan el intercambio de experiencias y conocimiento desde la perspectiva de cada Estado en relación con su legislación, regulación, estrategias y mejores prácticas en dicha materia. La suscripción del MOU entre el Gabinete de Seguridad Institucional de la Presidencia de la República Federativa del Brasil y la Agencia de Transformación Digital y Telecomunicaciones es el mecanismo que habilita la cooperación y colaboración entre los Estados.

- La suscripción de este instrumento jurídico permite que los Estados entre otras actividades, puedan compartir experiencias en relación con la aplicación de su respectivo marco regulatorio en temas de ciberseguridad, así como la adopción, desarrollo e implementación de estándares de ciberseguridad. Además facilita las consultas e intercambio de información en relación con nuevos desafíos relacionados con incidentes y amenazas en materia de ciberseguridad y plantea la posibilidad de realizar talleres y seminarios.

- Solicitud de información sobre el avance y siguientes pasos de EU-LAC Digital Alliance:"

  - La Alianza Digital UE-LAC fue creada en el marco de la estrategia Global Gateway de la Unión Europea, y representa la primera asociación digital regional entre la UE y los países de América Latina y el Caribe, buscando fortalecer el compromiso compartido hacia una visión de la economía y sociedad digital centrada en el ser humano.

  - Con un respaldo inicial de €145 millones del Equipo Europa, incluyendo €50 millones del presupuesto de la UE, la Alianza ha desarrollado una hoja de ruta de Diálogos Políticos que abarca gobernanza de datos, gobernanza electrónica, ciberseguridad, conectividad e inteligencia artificial. México, como uno de los 20 países signatarios originales de la Declaración Conjunta adoptada durante la Cumbre UE-CELAC de julio 2023, tiene la oportunidad de participar en iniciativas concretas como la extensión del cable de fibra óptica BELLA, la implementación de estrategias regionales de Copernicus para observación de la Tierra, y el establecimiento del Acelerador Digital UE-LAC para fomentar la colaboración multisectorial y la innovación.

- El primer Diálogo Político de Alto Nivel sobre Ciberseguridad de la Alianza se realizó en febrero 2024 en Santo Domingo, reuniendo a más de 150 altos representantes gubernamentales para abordar ciberdiplomacia, ecosistemas resilientes, desarrollo de capacidades y protección de infraestructuras críticas, estableciendo precedentes importantes para la participación mexicana en futuros diálogos birregionales.

2026:

1. Incorporación a CSIRT Americas (OEA/CICTE):
    - CSIRT Americas constituye la red hemisférica de Equipos de Respuesta a Incidentes Cibernéticos gubernamentales de los Estados Miembros de la Organización de Estados Americanos (OEA), creada en 2016 como el impulsor principal del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE/OEA).
    - La red conecta actualmente a 55 CSIRTs gubernamentales de 22 países de la región, proporcionando una plataforma para el intercambio de información sobre alertas de ciberseguridad 24/7, programas de asistencia técnica especializada, y oportunidades de desarrollo profesional continuo para sus miembros (OEA, 2023). En el último año, CSIRT Americas ha compartido información crítica de millones de credenciales expuestas en foros y mercados de la Dark Web, de las cuales muchas de ellas pertenecían a instituciones públicas de los países miembros, demostrando la relevancia operativa de la red para la protección de infraestructuras estatales.

- La incorporación de la DGCiber a CSIRT Americas permitirá a México beneficiarse de iniciativas como la evaluación bajo la metodología de Línea Base de CSIRT Americas, programas especializados de capacitación incluyendo la CSIRT Américas Week que fortalece el factor humano en la gestión de respuestas a incidentes, y acceso a la Guía Práctica para CSIRTs desarrollada por la red que presenta recomendaciones basadas en las mejores prácticas regionales y globales. Por medio del CSIRT Americas, se realizó un ejercicio de mesa (tabletop exercises - TTX) para la gestión de incidentes enfocados en sectores críticos, en el contexto del Mundial de FIFA 2026, durante la CAN WEEK 2025.

2. Acercamiento a organismos multilaterales para explorar cooperaciones técnicas y fuentes de financiamiento para proyectos:

    - El desarrollo de capacidades de ciberseguridad requiere inversión sostenida y asistencia técnica especializada. Los organismos multilaterales de desarrollo han incrementado significativamente sus cooperaciones en los países de América Latina y el Caribe, reconociendo la brecha de inversión existente entre la región y las economías desarrolladas. El Banco Interamericano de Desarrollo (BID), a través de iniciativas como la Red de Excelencia en Ciberseguridad de Latinoamérica y el Caribe (Red Ciberlac) y el programa Reporte Ciberseguridad 2020 en colaboración con la OEA, ha demostrado su compromiso con el fortalecimiento regional.

    - El Grupo Banco Mundial, en su informe "Economía de la Ciberseguridad para los Mercados Emergentes" (2024), ha identificado que aproximadamente el 30% de los incidentes cibernéticos divulgados a nivel mundial pertenecen a países en vías de desarrollo, con costos que pueden alcanzar el 2.4% del PIB en casos críticos como el experimentado por Costa Rica en

2022. Esta evidencia sustenta la necesidad de cooperaciones técnicas que incluyan transferencia de conocimiento, desarrollo de capital humano, y financiamiento para proyectos de infraestructura crítica de ciberseguridad.

3. Desarrollo de programas de CSIRT Americas:
    - La participación en los programas de desarrollo de capacidades de CSIRT Americas permitirá a los profesionales de la DGCiber acceder a entrenamientos especializados en metodologías internacionales como SIM3 (Security Incident Management Maturity Model), análisis forense digital, gestión avanzada de incidentes de ransomware, threat intelligence, y coordinación multisectorial para la respuesta a incidentes que afectan infraestructuras críticas de la APF.
4. Inicio de acciones para guías de implementación con la UIT:
    - La Unión Internacional de Telecomunicaciones (UIT) reconoce formalmente la Cooperación como uno de los cinco pilares esenciales que miden el compromiso de un país con la ciberseguridad en su Índice Global de Ciberseguridad (GCI). El inicio de acciones con la UIT permitirá a México acceder a marcos de referencia técnicos y guías de implementación que han posicionado exitosamente a países de la región en el ranking global, facilitando, además, la alineación con estándares internacionales y la participación en iniciativas como el Programa de Mentoría para Mujeres en Ciberseguridad que la UIT coorganiza con FIRST.

2027:

- Incorporación a FIRST:
    - El Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST, por sus siglas en inglés) representa la organización

internacional líder con un reconocimiento mundial en respuesta a incidentes, fundada en 1990 y conformada por más de 600 organizaciones de más de 100 países en las Américas, Asia, Europa, África y Oceanía (FIRST, 2025). FIRST reúne equipos de respuesta a incidentes de seguridad de gobiernos, entidades comerciales y organizaciones educativas, con el objetivo de fomentar la cooperación y coordinación en la prevención de incidentes.

- La membresía en FIRST proporciona acceso a servicios de valor agregado que incluyen: desarrollo y mantenimiento de estándares internacionales como el Common Vulnerability Scoring System (CVSS) que es el estándar para expresar el impacto de vulnerabilidades de seguridad; el Traffic Light Protocol (TLP) para clasificar información sensible; y el Exploit Prediction Scoring System (EPSS) para predecir cuándo las vulnerabilidades de software serán explotadas. La organización también mantiene el marco de Servicios de CSIRT (CSIRT Services Framework) que describe de manera estructurada una colección de servicios de ciberseguridad y funciones asociadas que los equipos de respuesta a incidentes pueden proveer.
- La incorporación a FIRST posicionará a México en la red global de confianza para respuesta a incidentes, facilitando la colaboración con pares internacionales en la gestión de amenazas transnacionales, acceso a conferencias especializadas que ayudan a los equipos de respuesta a incidentes con responsabilidad nacional a ganar mayor integración con la comunidad internacional de respuesta a incidentes.

A continuación, se presenta una gráfica que resume las etapas de la vinculación internacional.

Figura 11: Cronograma de vinculación internacional 2025-2027. Fuente: elaboración propia.

6. Recomendaciones

El desarrollo y la implementación del Plan Nacional de Ciberseguridad de México 2025-2030 representa un esfuerzo para transformar la postura de ciberseguridad de la Administración Pública Federal, que busca posicionar al país como un referente regional. Tomando en cuenta el diagnóstico realizado, el análisis del panorama internacional de amenazas, y las atribuciones de la Dirección General de Ciberseguridad (DGCiber) de la Agencia de Transformación Digital y Telecomunicaciones (ATDT), el presente capítulo formula una serie de recomendaciones estratégicas, operativas y de gobernanza que buscan maximizar el impacto del Plan y garantizar su implementación de forma efectiva.

Estas recomendaciones se presentan en seis ejes temáticos que reflejan las dimensiones críticas identificadas durante el desarrollo del Plan: **gobernanza y marco institucional**, **desarrollo de capacidades humanas**, **cooperación y vinculación internacional**, **gestión de riesgos e identificación de infraestructuras críticas**, **innovación y adopción tecnológica**, y **sostenibilidad presupuestaria y financiera**. Cada eje presenta recomendaciones específicas basadas en las mejores prácticas internacionales y evidencia empírica de casos comparables en la región.

1. **Gobernanza y Marco Institucional**

La creación de la ATDT y los mandatos integrales que han sido asignados a la DGCiber representan un avance para establecer un modelo de gobernanza de ciberseguridad integral y efectivo. Se recomienda:

- Formalización de un Consejo Nacional de Ciberseguridad decreto presidencial o reforma legislativa, presidido por el titular de la ATDT e integrado por representantes de las dependencias y entidades de la Administración Pública Federal (APF) con responsabilidades en seguridad nacional, infraestructuras críticas, servicios esenciales, y protección de datos.

- Definición de roles y responsabilidades intersectoriales por medio del desarrollo de una matriz RACI (Responsible, Accountable, Consulted, Informed) que defina con precisión las responsabilidades de cada actor del ecosistema de la APF de ciberseguridad. El modelo debe evitar duplicidades funcionales, establecer protocolos claros de escalamiento, y garantizar flujos eficientes de información.
- Fortalecimiento del marco legal y regulatorio: Impulsar la agenda legislativa para subsanar los vacíos normativos identificados, particularmente la ausencia de una ley específica de ciberseguridad.
- Articulación multinivel: federal, estatal y municipal. Desarrollo de programas de colaboración e intercambio de información entre los diferentes niveles del sector público mexicano.

2. **Desarrollo de Capacidades Humanas y Cultura de Ciberseguridad**

Es importante que el Plan Nacional con sus proyectos desarrollen un camino para lograr una estrategia nacional de desarrollo de talento en ciberseguridad. La escasez global de profesionales de ciberseguridad, estimada en 4 millones de vacantes a nivel mundial (World Bank, 2024), representa un riesgo para México que debe abordarse mediante una estrategia integral, en la cual se pueden incluir propuestas como:

- Programa Nacional de Becas en Ciberseguridad.
- Fortalecimiento de la oferta académica nacional por medio de la Secretaría de Educación Pública y la Red Ciberlac del BID para expandir y estandarizar la oferta académica en ciberseguridad en universidades públicas de todo el país.
- Certificaciones profesionales para el sector público.

Otra acción consiste en el desarrollo de una concientización y cultura de ciberseguridad, en la cual se sugieren acciones como:

- Campaña Nacional de Concientización en Ciberseguridad, dirigida a la población general, abordando riesgos cibernéticos cotidianos tales

como: phishing, ingeniería social, deepfakes, protección de datos personales en redes sociales, y uso seguro de servicios financieros digitales. La campaña debe adaptarse a diferentes grupos demográficos y considerar la brecha digital entre zonas urbanas y rurales.

- Programa de alfabetización digital con enfoque en ciberseguridad el cual puede ser desarrollado en coordinación con la SEP
- Cultura de Ciberseguridad en la APF, implementando un programa obligatorio de concientización para todos los funcionarios públicos federales, con cursos diferenciados según nivel jerárquico y acceso a información.

3. Cooperación y Vinculación Internacional

México debe avanzar decididamente hacia liderazgo regional por medio de la diplomacia digital segura, se sugiere valorar:

- Designar un Embajador o Coordinador Nacional para Asuntos Digitales Seguros o Cibernéticos como lo ha realizado de forma exitosa países como Estonia y República Dominicana.
- Participación en el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio de la OEA
- Consolidación de la participación en redes regionales e internacionales.

4. Gestión de Riesgos e Identificación de Infraestructuras Críticas

México debe avanzar decididamente en el desarrollo de un Marco Federal y Nacional de Identificación y Protección de Infraestructuras Críticas, para lo cual es necesario:

- Definir un Catálogo Nacional de Infraestructuras Críticas y Servicios Esenciales mediante metodologías estandarizadas a nivel internacional

- Definir los Requisitos de Seguridad Diferenciados por Nivel de Criticidad.
- Desarrollo de ejercicios en la APF de resiliencia en ciberseguridad por medio de table-top exercises o cyber drills de forma periódica cada año, que involucren operadores de infraestructuras críticas, dependencias gubernamentales, y el sector privado.

5. Innovación y Adopción Tecnológica

México debe trabajar en el aprovechamiento e integración de las tecnologías emergentes como parte de una estrategia de adopción tecnológica y desarrollo de innovación que permita el aumento de la competitividad del país y el fortalecimiento de la ciberseguridad sobre la APF. Para esto se propone:

- Aplicación de la Inteligencia Artificial para ciberdefensa con un enfoque ético y responsable de las capacidades que la IA nos ofrece. Se recomienda establecer un comité ético de IA en ciberseguridad que supervise el desarrollo e implementación de estas tecnologías.
- El desarrollo de un Cyber Range Nacional, dado su valor para entrenamiento de personal, pruebas de tecnologías de seguridad, y ejercicios de simulación.

6. Sostenibilidad Presupuestaria y Financiera

La ATDT y la DGCiber deben liderar las conversaciones para lograr de forma escalonada y planificada un incremento progresivo de inversión en ciberseguridad, estableciendo una meta explícita de incrementar progresivamente la inversión pública en ciberseguridad, considerando que el gasto público per cápita en México es menor a $1.00 USD comparado con más de $30.00 USD en países de ingresos altos (World Bank, 2024). Se recomienda una meta intermedia per cápita para 2030.

Se recomienda valorar mecanismos de financiamiento complementarios por medio de organismos multilaterales de desarrollo tales como el BID, Banco Mundial, CAF, y otros organismos multilaterales para acceder a financiamiento concesional, de proyectos específicos, asistencia técnica, y transferencia de conocimiento.

Conclusión

La implementación exitosa del Plan Nacional de Ciberseguridad 2025-2030 requiere compromiso sostenido al más alto nivel político, asignación de recursos adecuados, coordinación efectiva entre múltiples actores, y adaptación continua en un entorno de amenazas en constante evolución. Las recomendaciones presentadas buscan maximizar las probabilidades de éxito mediante el fortalecimiento de la gobernanza, inversión en capital humano, profundización de la cooperación internacional, implementación de tecnologías avanzadas, y establecimiento de mecanismos robustos de financiamiento y seguimiento.

México cuenta con elementos fundamentales para alcanzar su visión de largo plazo de convertirse en referente regional en ciberseguridad: una base institucional sólida con la creación de la ATDT y la DGCiber, un ecosistema de respuesta a incidentes que incluye 68 centros identificados con presencia en múltiples sectores, capacidades académicas en crecimiento con universidades líderes en la región de América Latina y el Caribe, y la voluntad política demostrada mediante la formulación de este Plan Nacional.

La implementación del Plan Nacional de Ciberseguridad y el desarrollo de los proyectos formulados, posicionará a México en la vanguardia de la ciberseguridad regional, contribuyendo no solo con la protección de sus propios activos digitales y de su población, sino también con el fortalecimiento de la ciberseguridad regional en América Latina y el Caribe.

7. Referencias

ADN Sureste. (2024, 4 abril). *Chilango Leaks: hackers cumplen amenaza contra el gobierno de CDMX y filtran millones de correos privados.* https://www.adnsureste.info/chilango-leaks-hackers-cumplen-amenaza-contra-el-gobierno-de-cdmx-y-filtran-millones-de-correos-privados-1100-h/

Agencia de Transformación Digital y Telecomunicaciones (ATDT). (2025). *Primer informe de labores de la Agencia de Transformación Digital y Telecomunicaciones*. Ciudad de México, México.

Animal Político. (2022, 30 septiembre). *Guacamaya: el grupo de hackers que atacó a la Sedena y otros ejércitos latinoamericanos.* https://animalpolitico.com/verificacion-de-hechos/te-explico/grupo-hackers-guacamaya-ciberataque-sedena-ejercitos-latinos

Arghire, I. (2022, 3 junio). *Foxconn Confirms Ransomware Hit Factory in Mexico.* SecurityWeek. https://www.securityweek.com/foxconn-confirms-ransomware-hit-factory-mexico/

Associated Press. (2024, 20 noviembre). *Mexico's president says government is investigating reported ransomware hack of legal affairs office.* https://apnews.com/article/a97fa044850ba05f574f71d2af3d67c8

Banco de México. (2025, enero). *Informe anual sobre el ejercicio de las atribuciones de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros (julio 2023–junio 2024).* https://sil.gobernacion.gob.mx/Archivos/Documentos/2025/01/asun_4827302_20250108_1736359622.pdf

Banco de México. (2025, 15 mayo). *Informe anual sobre las infraestructuras de los mercados financieros y los sistemas de pagos 2024.* https://www.banxico.org.mx/publicaciones-y-prensa/informe-anual-sobre-las-infraestructuras-de-los-me/%7BE0085475-B1D7-DED0-60AF-05ED88153BDC%7D.pdf

BleepingComputer. (2022, 2 junio). *Foxconn confirms ransomware attack disrupted production in Mexico.* https://www.bleepingcomputer.com/news/security/foxconn-confirms-ransomware-attack-disrupted-production-in-mexico/

Comparitech. (2024, 6 junio). *Bread maker Bimbo confirms data breach; hackers demanded $6.5 million.*

https://www.comparitech.com/news/bread-maker-bimbo-confirms-data-breach-hackers-demand-6-5-million/
Cracking.org. (2023, 31 mayo). *Database – Universidad Autónoma de Nuevo León (UANL).*
https://cracking.org/threads/universidad-autonoma-de-nuevo-leon-uanl-m%C3%A9xico.266756/
Crónica de Xalapa. (2024, 4 abril). *Chilango Leaks: hackers cumplen amenaza contra el gobierno de CDMX y filtran millones de correos privados.*
https://cronicadexalapa.com.mx/chilango-leaks-hackers-cumplen-amenaza-contra-el-gobierno-de-cdmx-y-filtran-millones-de-correos-privados/
DPL News. (2022, 1 noviembre). *Por hackeo, SICT suspende trámites el resto de 2022.*
https://dplnews.com/por-hackeo-sict-suspende-tramites-el-resto-de-2022/
El Economista. (2023, 5 marzo). *Buró de Crédito lo confirma: no fue hackeo.*
https://www.eleconomista.com.mx/opinion/Buro-de-Credito-lo-confirma-no-fue-hackeo-20230305-0009.html
El Economista. (2025, 29 abril). *México recibió 324,000 millones de intentos de ciberataques en 2024: Fortinet.*
https://www.eleconomista.com.mx/tecnologia/mexico-recibio-324-000-millones-intentos-ciberataques-2024-fortinet-20250429-756919.html
El Financiero. Calderón, C. (2024, 5 septiembre). *Coppel admite que hackeo en 1,800 tiendas limitó sus operaciones por 3 meses.*
https://www.elfinanciero.com.mx/empresas/2024/09/05/tuviste-problemas-con-coppel-admite-que-hackeo-en-1800-tiendas-limito-sus-operaciones-por-3-meses/
Expansión. (2022, 7 marzo). *Mercado Libre confirma hackeo y acceso a datos de 300,000 usuarios.*
https://expansion.mx/tecnologia/2022/03/07/mercado-libre-hackeado
Expansión. (2023, 12 junio). *El ciberataque a Coca-Cola Femsa vulneró datos de su operación en Latinoamérica.*
https://expansion.mx/empresas/2023/06/12/el-ciberataque-a-coca-cola-femsa-vulnero-datos-de-su-operacion-en-latinoamerica
Forum of Incident Response and Security Teams (FIRST). (2024). About FIRST.
https://www.first.org/about/
Fortinet / FortiGuard Labs. (2025, 28 abril). *Global Threat Landscape Report 2025 (comunicado).*

https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2025/fortinet-threat-report-reveals-record-surge-in-automated-cyberattacks
Gómez Villaseñor, I. (2024, 23 marzo). *UNAM expuesta: hacker accede a casi 1 TB de correos del IIMAS.* Publimetro México. https://www.publimetro.com.mx/noticias/2024/03/22/unam-expuesta-hacker-accede-a-mas-de-900-gigabytes-de-correos-del-instituto-de-matematicas-aplicadas/
Gómez Villaseñor, I. (2024, 26 marzo). *Megahackeo a la UNAM: hacker de Mexican Mafia vendió los 2.3 millones de archivos robados del IIMAS.* Publimetro México. https://www.publimetro.com.mx/noticias/2024/03/26/megahackeo-a-la-unam-hacker-de-mexican-mafia-vendio-los-23-millones-de-archivos-robados-del-iimas/
Hackmanac (X/Twitter). (2024, 19 febrero). *CyberAttack Alert #Mexico – Grupo Bimbo: Medusa ransomware group demands $6,500,000.* https://x.com/H4ckManac/status/1759622481638244352
Infobae. (2023, 22 febrero). *La base de datos del Buró de Crédito podría haberse vendido en la web profunda desde 2016.* https://www.infobae.com/mexico/2023/02/22/la-base-de-datos-del-buro-de-credito-podria-haberse-vendido-en-la-web-profunda-desde-2016/
Inter-American Development Bank, Organization of American States, & Global Cyber Security Capacity Centre, University of Oxford. (2020). *CYBERSECURITY: Risks, Progress, and the Way Forward in Latin America and the Caribbean.* Inter-American Development Bank; Organization of American States; Global Cyber Security Capacity Centre, University of Oxford.
International Telecommunication Union. (2024). *Global Cybersecurity Index 2024 (5th ed.).* ITU Publications.
International Telecommunication Union. (2025). *Measuring digital development: The ICT Development Index 2025.* ITU Publications.
International Telecommunication Union, & United Nations Development Programme. (2023). *SDG Digital Acceleration Agenda.* International Telecommunication Union; United Nations Development Programme.
IT Masters Mag. (2023, 27 abril). *Ciberataque a Coca-Cola Femsa: empresa afirma que nunca perdió control de sus sistemas IT.* https://www.itmastersmag.com/transformacion-digital/ciberataque-a-coca-cola-femsa-empresa-afirma-que-nunca-perdio-control-de-sus-sistemas-it/

IT Masters Mag. (2023, 5 septiembre). *Más de 67 mdp perdidos por ciberataques al sistema financiero en primer semestre de 2023.* https://www.itmastersmag.com/transformacion-digital/mas-de-67-mdp-perdidos-por-ciberataques-al-sistema-financiero-en-primer-semestre-de-2023/
Juárez, E. (2024, 16 julio). *Este año se han presentado dos incidentes cibernéticos a financieras por 140.5 millones de pesos.* El Economista. https://www.eleconomista.com.mx/sectorfinanciero/Este-ano-se-han-presentado-dos-incidentes-ciberneticos-a-financieras-por-140.5-millones-de-pesos-20240716-0101.html
La Jornada. (2023, 30 mayo). *Conagua amplía por tercera ocasión suspensión de trámites por hackeo.* https://www.jornada.com.mx/notas/2023/05/30/politica/conagua-amplia-por-tercera-ocasion-suspension-de-tramites-por-hackeo/
LAC4. (2024). Informe: Gobiernos de América Latina y el Caribe demuestran compromiso inquebrantable para fortalecer sus capacidades en ciberseguridad. https://www.lac4.eu/es/informe-gobiernos-de-america-latina-y-el-caribe-demuestran-compromiso-inquebrantable-para-fortalecer-sus-capacidades-en-ciberseguridad/
LAC4. (2025). Centro de Competencia Cibernética de América Latina y el Caribe. https://www.lac4.eu/es/
López Obrador, A. M. (2022, 30 septiembre). *AMLO confirma hackeo contra Sedena; son datos de dominio público, señala.* Capital 21. https://www.capital21.cdmx.gob.mx/noticias/?p=33439
Organización de los Estados Americanos (OEA). (2023). Guía Práctica para CSIRTs. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf
Organización de los Estados Americanos (OEA). (2024). CICTE: Ciberseguridad. https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp
Organization for Economic Co-operation and Development. (2024). *2023 OECD Digital Government Index: Results and Key Findings.* OECD Publishing.
Page, C. (2022, 2 junio). *Foxconn confirms ransomware attack disrupted operations at Mexico factory.* TechCrunch. https://techcrunch.com/2022/06/02/foxconn-ransomware-attack-mexico-factory/

Publimetro México. (2025, 8 abril). *Ciberataque sin precedentes expone a escuelas públicas de México: "Peligra toda la red".* https://www.publimetro.com.mx/noticias/2025/04/08/ciberataque-sin-precedentes-expone-a-escuelas-publicas-de-mexico-peligra-toda-la-red/
R3D: Red en Defensa de los Derechos Digitales. (2024, 24 abril). *Coppel guarda silencio sobre el "incidente de ciberseguridad" que afectó a sus sistemas.* https://r3d.mx/2024/04/24/coppel-guarda-silencio-sobre-el-incidente-de-ciberseguridad-que-afecto-a-sus-sistemas/
R3D: Red en Defensa de los Derechos Digitales. (2024, 28 noviembre). *Consejería Jurídica de la Presidencia sufre ciberataque; filtran más de 200 GB.* https://r3d.mx/2024/11/28/consejeria-juridica-de-la-presidencia-sufre-ciberataque-filtran-mas-de-200-gb-de-contratos-y-datos-personales/
Red de Gobierno Electrónico de América Latina y el Caribe (RedGEALC). (2020). Ciberseguridad: Uruguay lidera en América Latina y el Caribe. https://www.redgealc.org/contenido-general/noticias/ciberseguridad-uruguay-lidera-en-america-latina-y-el-caribe/
Red de Gobierno Electrónico de América Latina y el Caribe (RedGEALC). (2024). Marco de Ciberseguridad: nueva versión disponible. https://www.redgealc.org/contenido-general/noticias/marco-de-ciberseguridad-nueva-version-disponible/
Reporte Índigo. (2023, 26 abril). *Coca-Cola FEMSA sufre un ataque cibernético; la empresa activó sus protocolos de ciberseguridad.* https://www.reporteindigo.com/nacional/Coca-Cola-Femsa-sufre-un-ataque-cibernetico-la-empresa-activo-sus-protocolos-de-ciberseguridad-20230426-0085.html
Riquelme, R. (2022, 3 octubre). *Varios hackers ya habían infectado a la Sedena antes de Guacamaya.* El Economista. https://www.eleconomista.com.mx/tecnologia/Varios-hackers-ya-habian-infectado-a-la-Sedena-antes-de-Guacamaya-20221003-0070.html
Riquelme, R. (2022, 2 noviembre). *La SICT suspende trámites en lo que resta del año por hackeo.* El Economista. https://www.eleconomista.com.mx/empresas/La-SICT-suspende-tramites-en-lo-que-resta-del-año-por-hackeo-20221102-0005.html
Rodríguez, D. (2023, 4 febrero). *Hackeo o sustracción: la gravedad de la filtración de datos personales del Buró de Crédito en México.* El País.

https://elpais.com/mexico/2023-02-04/hackeo-o-sustraccion-la-gravedad-de-la-filtracion-de-datos-personales-del-buro-de-credito-en-mexico.html
Vergara Cobos, E. (2024). *Economía de la ciberseguridad para los mercados emergentes, panorama general.* Banco Mundial. https://openknowledge.worldbank.org/bitstreams/9ebee657-5ead-40e7-9d13-1836c6d4cd48/download
WeLiveSecurity (ESET). Harán, J. M. (2022, 8 marzo). *Mercado Libre confirma acceso indebido y robo de parte de su código fuente.* https://www.welivesecurity.com/la-es/2022/03/08/mercadolibre-confirma-acceso-indebido-sistemas-robo-codigo-fuente/
WIRED en Español. (2024, 22 abril). *Hackeo en Coppel: ¿qué pasó con las cuentas y dónde puedes pagar deudas?* https://es.wired.com/articulos/hackeo-en-coppel-que-paso-con-las-cuentas-y-en-donde-puedes-pagar-deudas
World Economic Forum. (2025). *Global Cybersecurity Outlook 2025.* World Economic Forum.
World Economic Forum. (2025). *The Global Risks Report 2025 (20.ª ed.).* World Economic Forum. https://www.weforum.org/publications/global-risks-report-2025/