

# Propuesta de Lineamientos para una Estrategia Nacional de Ciberseguridad para México

Contribuciones de la industria para  
un entorno digital más seguro y  
confiable para toda la población  
mexicana

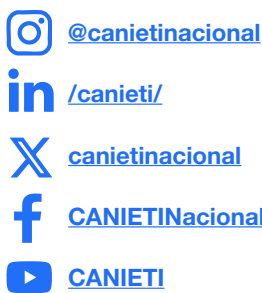
---

Noviembre 2025



La Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) es un organismo empresarial que representa la alta tecnología, la innovación y la digitalización en México. Fundada en 1935, es una institución autónoma de interés público, con personalidad jurídica y patrimonio propio, conformada por más de 1.000 empresas en todo el país. Contamos con seis sedes regionales y nueve oficinas de representación.

Nuestra labor es representar y defender los intereses del sector, promoviendo su desarrollo en un entorno global con servicios de alta calidad. Impulsamos el crecimiento de las industrias de Electrónica, Telecomunicaciones y Tecnologías de la Información para que impacten en el crecimiento económico-social, convirtiendo a nuestro país en un polo digital y de innovación.



La Vicepresidencia Nacional de Ciberseguridad de CANIETI expresa su profundo agradecimiento a todos los integrantes de la Cámara que contribuyeron activamente con compartir su experiencia y conocimientos para la elaboración de este documento. En especial, reconocemos la participación activa de los equipos de Cisco y Apple para la elaboración del presente documento para la construcción de un ecosistema digital en México más ciberseguro, y ciberresiliente.

### Autor:



Es una firma de estrategias de tecnología y asuntos públicos digitales enfocada en América Latina. Hoy esta sirviendo a empresas y organizaciones internacionales líderes a entender y actuar en el complejo contexto regional en temas como tecnologías 4.0, innovación, plataformas, infraestructura digital, educación virtual, ciberseguridad, medio ambiente y políticas institucionales para la transformación digital.

#SURFTTHELATAMDIGITALPOLICYSCENE

Para más información, visite [www.smplusconsulting.com](http://www.smplusconsulting.com)



Esta obra se encuentra sujeta a una licencia Creative Commons Atribución-NoComercial 4.0 Internacional (CC BY-NC 4.0) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo a los autores.



LICENCIA DE DISTRIBUCIÓN CC

# Prólogo

En la era digital, el ciberespacio se ha convertido en la columna vertebral de nuestra economía, comercio y vida social. En esta sociedad hiperconectada, la ciberseguridad ya no es una opción, sino un pilar de profunda importancia estratégica y de seguridad nacional.

La urgencia de actuar es innegable. El costo económico global de los ataques cibernéticos alcanzó los 9.5 billones de dólares en 2024 y se proyecta que escale a 10.5 billones en 2025 (Cybersecurity Ventures). Este incremento es impulsado por la creciente sofisticación de los ataques, que emplean inteligencia artificial y otras tecnologías emergentes para explotar una superficie de ataque digital en constante expansión. Este cálculo incluye pérdidas por robo de datos, interrupciones operativas, pagos de rescate, litigios, recuperación de sistemas, y otros impactos financieros derivados de incidentes cibernéticos.

Lamentablemente, la preparación no ha ido a la par de la amenaza. A nivel mundial, la gran mayoría de las empresas (70%) se encuentra estancada en etapas iniciales de madurez cibernética, y solo un 4% ha alcanzado un nivel "Maduro" (Cisco Cybersecurity Readiness Index 2025). Esta situación es aún más crítica en México, donde las evaluaciones (Cisco Cybersecurity Readiness Index 2025) reflejan que apenas el 2% de las organizaciones alcanza ese nivel, dejando a un preocupante 76% en fases de "Principiante" o "Formativa". Esta brecha de madurez hace que las entidades de gobierno, las MiPyMEs y los ciudadanos de México sean altamente vulnerables ante ciberataques potencialmente devastadores.

Las amenazas actuales son ataques altamente sofisticados y persistentes, donde los riesgos externos se conjugan con

vulnerabilidades internas. En este escenario, es imperativo entender que el cibercrimen se ha globalizado; ningún país puede enfrentarlo solo. Por ello, el éxito de cualquier estrategia depende de un modelo de colaboración y responsabilidad compartida que trascienda las fronteras institucionales y geográficas, haciendo de la ciber-diplomacia una herramienta esencial.

Frente a esta realidad, la elaboración de una Estrategia Nacional de Ciberseguridad es una necesidad impostergable. La ciberseguridad debe ser vista como una decisión estratégica del más alto nivel para proteger nuestro desarrollo económico y social. No es un fin en sí mismo, sino un medio para garantizar la efectividad de los derechos humanos y las libertades fundamentales en el entorno digital, incluyendo la privacidad y la protección de datos personales.

Por ello, desde la CANIETI, organismo empresarial que representa a los sectores de alta tecnología, innovación y digitalización en México, ponemos a disposición del Gobierno de México este documento. Su propósito es ofrecer lineamientos estratégicos claros para preservar la continuidad de los servicios esenciales, las infraestructuras críticas, la seguridad pública, la estabilidad económica y, al mismo tiempo, salvaguardar la gestión soberana de los recursos digitales.

Esta propuesta es fundamental para alinear prioridades y crear políticas públicas robustas. Con ella, buscamos contribuir decididamente al desarrollo de un entorno digital más seguro y hacer de México un país ciberseguro y resiliente.



**Rafael Sánchez Loza**  
Presidencia  
Nacional  
de CANIETI



**Adriana Servín**  
Vicepresidencia  
Nacional de  
Ciberseguridad

# LA OPORTUNIDAD PARA UN MÉXICO CIBERSEGURO: NECESIDAD DE ACCIÓN



LA TRANSFORMACIÓN DIGITAL IMPULSA EL CRECIMIENTO ECONÓMICO Y LA COMPETITIVIDAD DE MÉXICO, CONSOLIDANDO A LA CIBERSEGURIDAD COMO UN HABILITADOR ESTRATÉGICO DEL DESARROLLO SOSTENIBLE Y DE LA GESTIÓN SOBERANA DE LOS RECURSOS DIGITALES.

Por primera vez en la historia de México, el eje de la ciberseguridad fue plasmado en el Plan Nacional de Desarrollo 2025-2030 y en el Plan México de la Presidenta Claudia Sheinbaum como una prioridad para garantizar la protección de la infraestructura digital y la privacidad de los ciudadanos, así como el fortalecimiento de la infraestructura crítica y de los servicios esenciales digitales, capacitación y educación a funcionarios y a la ciudadanía, colaboración internacional, regulación y legislación.



ESTA PROPUESTA ES UNA HOJA DE RUTA PARA CONSTRUIR UNA ARQUITECTURA NACIONAL DE CIBERSEGURIDAD ROBUSTA, RESILIENTE Y COORDINADA, BASADA EN LA COLABORACIÓN GENUINA Y SOSTENIDA ENTRE EL SECTOR PÚBLICO Y PRIVADO.

Consideramos que estamos en el momentum perfecto para dar respuesta a los desafíos en términos de ciberseguridad que sin duda requiere de una visión integral, con coordinación efectiva entre el sector público, la industria, la academia y la sociedad civil. Las empresas que integran CANIETI poseen la experiencia técnica y el conocimiento operativo para traducir los principios estratégicos en soluciones implementables. La ciberseguridad es una condición estructural para el desarrollo sostenible, la gestión soberana de los recursos digitales y la confianza en el futuro del país.

## PRINCIPIOS GUÍA PARA UNA FUTURA ESTRATEGIA DE CIBERSEGURIDAD DE MÉXICO

### CORRESPONSABILIDAD

Cada actor del ecosistema digital, gobierno, empresas, academia y ciudadanos, tiene un rol definido y una responsabilidad activa en la construcción y el mantenimiento de un ciberespacio seguro.

### PROTECCIÓN DE DERECHOS DIGITALES

Toda acción en materia de ciberseguridad debe salvaguardar los derechos fundamentales, incluyendo la privacidad, la libertad de expresión y el acceso.

### COOPERACIÓN PÚBLICO-PRIVADA

La colaboración efectiva entre gobierno, empresas y academia es esencial para desarrollar capacidades, compartir información y responder ante incidentes.

### SOBERANÍA

México debe fortalecer su capacidad para proteger sus infraestructuras críticas y servicios esenciales digitales, sus datos y sus procesos estratégicos, asegurando independencia tecnológica y control sobre sus activos digitales.



### PROTECCIÓN DE IDENTIDAD DIGITAL

Reforzar el cumplimiento de la legislación vigente y promover la adopción de las más altas prácticas internacionales para la salvaguarda de la identidad e información personal de todos los mexicanos. Siempre evitando la falsa dicotomía entre protección e innovación y promoción de la inversión.

### TRANSPARENCIA Y RENDICIÓN DE CUENTAS

Las políticas y acciones de ciberseguridad deben implementarse bajo principios de apertura, trazabilidad y responsabilidad institucional.

### RESILIENCIA E INNOVACIÓN

Fomentar la capacidad de anticipar, resistir y recuperarse de incidentes, impulsando la adopción de tecnologías, seguras e innovadoras.

### INCLUSIÓN Y TALENTO

Promover la formación de capacidades en todos los niveles, con especial atención a jóvenes, mujeres y PyMEs.



**MÉXICO TIENE LA OPORTUNIDAD HISTÓRICA DE CONSTRUIR UN MARCO DE CIBERSEGURIDAD QUE SUPERE LA FRAGMENTACIÓN INSTITUCIONAL ACTUAL Y PROTEJA INFRAESTRUCTURAS CRÍTICAS Y SERVICIOS ESENCIALES DIGITALES.**

Este marco debe evitar la falsa dicotomía entre protección e innovación. Normativas muy prescriptivas que alteren la integridad de productos o servicios digitales, como es hoy el caso europeo, son una fuente de vulnerabilidades y riesgos.



**EL FORTALECIMIENTO DE LA CIBERSEGURIDAD ES UN MOTOR DE CONFIANZA QUE ATRAE INVERSIÓN, PROMUEVE LA COMPETITIVIDAD INTERNACIONAL Y CATALIZA LA INNOVACIÓN TECNOLÓGICA EN EL PAÍS.**

Los enfoques rectores para esta estrategia deben ser:

- inclusivos y transversales al sector público y privado;
- centrados en el ser humano (protegiendo derechos y libertades fundamentales en el espacio cibernético);
- y basados en la gestión de riesgos (priorizando acciones por impacto y probabilidad).

La armonización, la previsibilidad y la consulta a múltiples actores involucrados son principios clave para también guiar la definición de marcos de ciberseguridad alineados con las mejores prácticas internacionales, como el enfoque de seguridad digital que promueve la OCDE.

## LOS LINEAMIENTOS PROPUESTOS PLANTEAN OBJETIVOS DE CORTO, MEDIANO Y LARGO PLAZO

- En el corto plazo, consideramos necesaria una Coordinación Nacional de Ciberseguridad que funcione como un mecanismo de transición hacia una gobernanza nacional y que defina la Estrategia Nacional de Ciberseguridad 2026-2030 (ENC) que integre esfuerzos gubernamentales y privados.
- A mediano plazo, el objetivo es la creación de una Ley Nacional de Ciberseguridad e Infraestructura Crítica que unifique y fortalezca el marco regulatorio nacional, y acompañe la ENC.
- Para el largo plazo, se espera que esta Estrategia Nacional de Ciberseguridad sienta las bases de una política más desarrollada y madura para el quinquenio 2031-2035.

## HITOS CLAVE HACIA ADELANTE

### OBJETIVO DE LA ESTRATEGIA 2026-2030

Funcionar como hoja de ruta para la creación de un marco de ciberseguridad robusto, resiliente y coordinado en el ecosistema nacional mexicano, con participación del sector público, privado y la academia.



**canieti** Sin un marco consultivo y participativo de todos los sectores involucrados no será posible la implementación de una Estrategia Nacional de Ciberseguridad efectiva y sostenible en el tiempo.

## HACIA UN NUEVO MARCO DE GOBERNANZA

La transición institucional se iniciaría con la creación inmediata de una Coordinación Nacional de Ciberseguridad dotada de liderazgo político y técnico, integrando lo público y lo privado. Esta Coordinación tendría la función de ordenar y articular los esfuerzos y actores, garantizando la participación plena del sector privado y estableciendo reglas claras de operación.

Creemos fundamental que la Coordinación trabaje en tres ejes, que van desde el marco institucional y de gobernanza hasta la cultura, la promoción de talento y la sensibilización. Dichos ejes, a su vez, se despliegan en 11 objetivos generales, con sus correspondientes acciones.

## PRINCIPALES ROLES Y OBJETIVOS DE LA FIGURA DE TRANSICIÓN



LA CONSOLIDACIÓN DE UN MARCO INSTITUCIONAL REQUIERE DE UN ANDAMIAJE NORMATIVO CLARO, COHERENTE Y PROGRESIVO.

<p><b>LEY GENERAL DE CIBERSEGURIDAD</b></p> <ul style="list-style-type: none"> <li>Objeto, alcance y definiciones</li> <li>Autoridad competente en la coordinación y colaboración multi-actores</li> <li>Definición y catálogo de Infraestructuras críticas y servicios esenciales digitales</li> <li>Gestión de Incidentes y prevención vulnerabilidades</li> <li>Transparencia y rendición de cuentas</li> </ul>	<p><b>PROTECCIÓN DE LA IDENTIDAD DIGITAL</b></p> <ul style="list-style-type: none"> <li>Establecer obligaciones claras para prestadores de servicios críticos, incluyendo la exigencia de autenticación multifactor y contraseñas robustas</li> <li>Considerar la integración de la privacidad desde el diseño</li> <li>Minimizar recolección de datos</li> <li>Asegurar protección de datos en todo su ciclo de vida</li> <li>Asegurar operaciones verificables y transparentes</li> </ul>	<p><b>REVISIÓN DE NORMATIVA PENAL</b></p> <ul style="list-style-type: none"> <li>Evaluar la pertinencia de actualizar el marco penal vigente de forma independiente a la Ley que se propone</li> <li>Incorporar tipologías delictivas que respondan a los desafíos contemporáneos, como el ransomware, el robo de identidad digital, la ingeniería social y el uso de la Inteligencia Artificial o tecnologías emergentes</li> </ul>	<p><b>T-MEC Y COORDINACIÓN INTERNACIONAL</b></p> <ul style="list-style-type: none"> <li>T-MEC: revisión del capítulo de ciberseguridad (centrado en cooperación, y no en obligaciones) para adecuarlo a la realidad actual, considerando avances tecnológicos y aumento de amenazas de actores extra regionales desde 2018</li> <li>Cooperación Internacional: adhesión al Convenio de Budapest y a la Convención de la ONU sobre ciberdelincuencia, junto con protocolos adicionales y buenas prácticas legales internacionales</li> </ul>
--	---	--	---

MÉXICO REQUIERE DAR UN SALTO CUALITATIVO EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y SERVICIOS ESENCIALES DIGITALES

Las infraestructuras críticas y los servicios esenciales digitales constituyen un campo de trabajo de importancia estratégica, cuya afectación podría representar una catástrofe de niveles impredecibles.

La Coordinación Nacional tendría el encargo de liderar la definición de sectores clave y la elaboración de un Catálogo de Infraestructuras Críticas Cibernéticas y Servicios Esenciales Digitales.

HOJA DE RUTA PROPUESTA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS Y SERVICIOS ESENCIALES DIGITALES



**A PARTIR DE LA DEFINICIÓN DE SECTORES DE INFRAESTRUCTURAS CRÍTICAS Y SERVICIOS ESENCIALES DIGITALES SE DEBEN ESTABLECER LAS INFRAESTRUCTURAS CIBERNÉTICAS**

## ES FUNDAMENTAL FORTALECER LA RESPUESTA A INCIDENTES, CON EL APOYO DE UNA MAYOR COOPERACIÓN INTERNACIONAL

Es vital construir un liderazgo nacional que promueva y coordine una red de confianza de Equipos de Respuesta a Incidentes (CERT/CSIRT) con adhesión voluntaria.

Esta red debe servir como un instrumento eficaz para divulgar información de alertas sobre vulnerabilidades críticas y amenazas de manera rápida, alcanzando a MiPyMEs e instituciones en todo el territorio nacional.

### RESPONSABILIDADES DEL COORDINADOR DE CERTS & CSIRTS



**LA GESTIÓN DE CRISIS CIBERNÉTICAS DEBE FORTALECERSE MEDIANTE LA IDENTIFICACIÓN DE ESCENARIOS NACIONALES DE ALTO IMPACTO Y LA PLANIFICACIÓN DE EJERCICIOS DE SIMULACIÓN**



**LA COOPERACIÓN INTERNACIONAL (CIBERDIPLOMACIA) DEBE SER UN PRINCIPIO RECTOR DE TRABAJO, BUSCANDO LA COLABORACIÓN EN LA DETECCIÓN Y RESPUESTA A AMENAZAS TRANSFRONTERIZAS.**

México debe fortalecer sus capacidades de ciberdiplomacia y establecer acuerdos de asistencia mutua con naciones de confianza para el intercambio de información y la coordinación de la agenda en foros internacionales en materia de prevención de incidentes.

## NECESITAMOS PRIORIZAR EL DESARROLLO DE TALENTO Y LA PROMOCIÓN DE UNA CULTURA DE CIBERSEGURIDAD



**MÉXICO ENFRENTA UN DÉFICIT SIGNIFICATIVO EN LA FUERZA LABORAL ESPECIALIZADA, POR LO QUE LA GESTIÓN DE TALENTO DEBE SER UNA PARTE CENTRAL DE LA ESTRATEGIA NACIONAL.**

Se propone la creación urgente de un Consejo Nacional de Talento en Ciberseguridad para articular la oferta de formación relevante y actual, tanto pública como privada. Este Consejo tendría la tarea de realizar un diagnóstico actualizado de la brecha laboral y adaptar el Marco NICE del NIST a la realidad mexicana para estandarizar terminología, competencias y perfiles profesionales.

Se necesita elaborar un catálogo de credenciales y micro-credenciales apilables que guíen las trayectorias de carrera, aprovechando la experiencia del sector privado, como el [CANIETI Talent Hub](#).

ACCIONES ESTRATÉGICAS A TENER EN CUENTA EN UN PLAN NACIONAL DE TALENTO

ESTÁNDARES Y FRAMEWORKS DE CIBERSEGURIDAD



**CATALOGO DE CREDENCIALES Y ESTÁNDARES:** elaboración de un catalogo de estándares, credenciales y micro-credenciales apilables con mayor demanda en el mercado laboral de ciberseguridad.

**HACKÁTHONES:** realización de hackáthones con participación del sector privado y las universidades para promover carreras de formación en ciberseguridad.

**CORTO PLAZO**

CERTIFICACIONES Y CREDENCIALES EN CIBERSEGURIDAD



**PLATAFORMA DIGITAL EDUCATIVA:** creación de una plataforma digital que recopile cursos y diplomaturas en ciberseguridad del sector privado y universitario.

**PROGRAMAS DUALES:** promoción de programas de educación dual entre el sector privado y la academia para robustecer y acelerar la formación específica en ciberseguridad de estudiantes universitarios.

**MEDIANO PLAZO**

**PROGRAMA DE RE-SKILLING Y UP-SKILLING DEL SECTOR PÚBLICO:** elaboración de un programa orientado a la capacitación y perfeccionamiento de la formación de trabajadores del sector público con habilidades digitales.

**CARRERAS ESPECÍFICAS EN CIBERSEGURIDAD:** promover la puesta en oferta de carreras de grado y posgrado específicas de ciberseguridad en el ámbito universitario.

**LARGO PLAZO**

LA ESTRATEGIA DEBE GARANTIZAR LA RESILIENCIA DE LAS MIPYMES.

Las MiPyMEs representan más del 99,8% del tejido empresarial y son el eslabón más débil, lo que representa un riesgo sistémico para toda la economía.



ACCIONES ESTRATÉGICAS

**GUÍAS DE CIBERSEGURIDAD PARA MIPYMES:** elaborar y poner a disposición guías y kits que puedan utilizar las MiPyMEs para formar y concientizar a sus empleados en elementos básicos y buenas prácticas de ciberseguridad.

**CORTO PLAZO**

**PROGRAMAS DE ASESORÍA:** desarrollar programas de asesoría para ayudar a las MiPyMEs a poner a punto la protección de su infraestructura tecnológica y digital.

**MEDIANO PLAZO**

**LÍNEA DE ATENCIÓN DEL CERT:** poner a disposición de las MiPyMEs una línea de atención y respuesta a ciberincidentes.

**LARGO PLAZO**

**LA INNOVACIÓN (I+D) EN CIBERSEGURIDAD ES CLAVE PARA ANTICIPAR AMENAZAS Y GENERAR SOLUCIONES LOCALES QUE FORTALEZCAN Y COMPLEMENTEN LAS TECNOLOGÍAS EXTERNAS**

## ES ESENCIAL DESARROLLAR CAMPAÑAS MASIVAS DE SENSIBILIZACIÓN PARA FOMENTAR HÁBITOS DE CIBERHIGIENE

Campañas de comunicación robustas y bien dirigidas serán la piedra angular para construir una cultura de ciberseguridad nacional. Un componente prioritario será la ciberprevención dirigida a adultos mayores y las infancias, debido a su uso intensivo y exposición a los riesgos en línea.

### MENSAJES DE SENSIBILIZACIÓN POR GRUPO POBLACIONAL

MENSAJES MASIVOS		MENSAJES DIRIGIDOS		
<p><b>CAMPAÑAS PARA TODA LA CIUDADANÍA:</b></p> <p>realizar campañas de campaña en medios masivos para la ciudadanía en general.</p>	<p><b>NÚMERO TELEFÓNICO NACIONAL DE ASESORÍA CIBERNÉTICA:</b></p> <p>implementar un número de orientación inmediata y confidencial a personas afectadas por incidentes cibernéticos, fraudes, acoso digital o vulneraciones de datos.</p>	<p><b>GUÍAS EN EDUCACIÓN PRIMARIA:</b></p> <p>elaborar una guía para el desarrollo de talleres de ciber higiene en educación primaria.</p>	<p><b>PLATAFORMAS PARA NIÑOS Y ADOLESCENTES:</b></p> <p>establecer alianzas estratégicas con plataformas digitales para sensibilizar niños y adolescentes en temas de ciberseguridad.</p>	<p><b>TALLERES PARA ADULTOS MAYORES:</b></p> <p>desarrollar talleres dirigidos a adultos mayores en ciberseguridad, prevención de estafas e identificación de tácticas de ingeniería social.</p>

**LA CIBERSEGURIDAD ES UNA RESPONSABILIDAD COMPARTIDA, ES CLAVE ALINEAR LOS MENSAJES PARA CADA SEGMENTO DE LA POBLACIÓN**

### PROPONEMOS LÍNEAS DE ACCIÓN CONCRETAS

A continuación listamos las líneas de acción propuestas agrupadas según el eje de trabajo y su horizonte temporal, identificando también los posibles éxitos tempranos (en Anexo se presenta mayor detalle de cada una de ellas).

Éxitos tempranos

	CORTO		MEDIANO		LARGO
<b>1 INSTITUCIONALIDAD</b>	Crear órgano rector		Instalar mesas de trabajo temáticas		
<b>2 BASE LEGAL</b>			Promover Ley Nacional de Ciberseguridad	Revisar marco penal existente	
<b>3 INFRA. CRÍTICAS</b>	Asignar responsabilidades para la definición de normas		Definir categorías de infraestructuras críticas		Definir criterios y metodologías para la identificación de las infraestructuras críticas
<b>4 COOP. INTERNACIONAL</b>			Participar en foros	Suscribir a acuerdos de asistencia mutua	Crear un foro interinstitucional para coordinar la agenda internacional de ciberseguridad
<b>5 RESPUESTA A INCIDENTES</b>	Definir y establecer marco institucional		Establecer programa de adhesión voluntaria para divulgar alertas		
<b>6 MADUREZ</b>	Identificar escenarios de ciber crisis con alto impacto		Planificar y ejecutar ejercicios nacionales de simulación de ciberataques		
<b>7 TALENTO</b>	Crear el Consejo Nacional de Talento en Ciberseguridad		Realizar un diagnóstico de la brecha laboral	Adaptar el marco NICE a las necesidades	Elaborar un plan de acciones estratégicas para la formación laboral en ciberseguridad
<b>8 SIST. EDUCATIVO</b>	Elaborar catálogo de credenciales de ciberseguridad	Coordinar con el sector privado en formación	Impulsar convenios entre instituciones educativas y empresas tecnológicas		
<b>9 MIPYMES</b>	Desarrollar kits de concientización	Desarrollar guías para diseño de políticas internas			Implementar programas de créditos y exenciones fiscales
<b>10 FOMENTO I+D</b>			Crear becas y fondos concursables	Establecer mecanismos de apoyo económico	Establecer un sistema de mecanismos de apoyo económico para promover la colaboración
<b>11 SENSIBILIZACIÓN</b>	Desarrollar campañas masivas sobre ciber higiene	Lanzas campañas en medios para prevenir fraudes	Elaborar guías, kits educativos y recursos didácticos sobre ciber higiene para escuelas		Implementar encuestas y análisis de redes sociales

CORTO

MEDIANO

LARGO

HORIZONTE TEMPORAL



# Contenidos

<b>Introducción: La oportunidad para un México ciberseguro.....</b>	<b>11</b>
Propósito y alcance	11
La ciberseguridad como habilitador estratégico del desarrollo sostenible y de la gestión soberana de los recursos digitales	12
Diagnóstico y antecedentes	13
Tendencias clave de la gobernanza e institucionalidad de la ciberseguridad	17
<b>Marco estratégico .....</b>	<b>21</b>
Por qué México necesita una Estrategia Nacional de Ciberseguridad	21
Visión y enfoques rectores	22
Retos y desafíos	23
<b>Propuesta de Lineamientos para una Estrategia Nacional de Ciberseguridad .....</b>	<b>26</b>
<b>I. Hacia un nuevo marco de gobernanza .....</b>	<b>26</b>
1. Transición hacia una gobernanza nacional de ciberseguridad en México	26
2. Normativa requerida para la implementación del marco institucional de ciberseguridad en México	29
3. Protección de infraestructuras críticas y servicios esenciales digitales	30
4. Bases para fortalecer la cooperación internacional	33
<b>II. Fortalecimiento del Sistema Nacional de Gestión de Crisis y Respuesta a Incidentes Cibernéticos .....</b>	<b>35</b>
5. Construir liderazgo y fortalecimiento de la gestión de incidentes a nivel nacional	35
6. Asegurar capacidades para abordar crisis cibernéticas como prueba de la madurez en la respuesta a incidentes	39
<b>III. Priorización del desarrollo de talento y de la promoción de una cultura en ciberseguridad .....</b>	<b>40</b>
7. Creación de un Consejo Nacional de Talento para una oferta de formación relevante y actual	40
8. Desarrollo de credenciales y habilidades en ciberseguridad	43
9. Claves para atender la especificidad de las MiPyMEs	45
10. Fomento a la Investigación y Desarrollo	47
<b>IV. Cultura, sensibilización y comunicación .....</b>	<b>48</b>
11. La ciberseguridad como cultura	48
<b>Conclusiones .....</b>	<b>51</b>
<b>Anexo: Plan de acción consolidado .....</b>	<b>52</b>
<b>Fuentes.....</b>	<b>55</b>



# Introducción: La oportunidad para un México ciberseguro

## Propósito y alcance

La transformación digital ha redefinido la competitividad y la seguridad económica de los países. En este contexto, la ciberseguridad se consolida como un habilitador estratégico para garantizar el desarrollo sostenible y la gestión soberana de los recursos digitales. México enfrenta el desafío de fortalecer su capacidad institucional, técnica y humana frente a amenazas cada vez más sofisticadas, que afectan por igual a gobiernos, empresas y ciudadanía. Por primera vez en la historia de México, el eje de la ciberseguridad fue plasmado en el Plan Nacional de Desarrollo 2025-2030 y en el Plan México de la Presidenta Claudia Sheinbaum. Consideramos que estamos en el momentum perfecto para dar respuesta a los desafíos en términos de ciberseguridad que sin duda

requiere de una visión integral, con coordinación efectiva entre el sector público, la industria, la academia y la sociedad civil.

La Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), como organismo de representación empresarial establecido por la Ley de Cámaras Empresariales y sus Confederaciones, asume el compromiso de contribuir al diseño de políticas públicas que fortalezcan el ecosistema digital del país. Este documento constituye una propuesta técnica y de colaboración con el Gobierno de México, sustentada en el análisis de expertos y la experiencia de empresas líderes globales del sector.

## Enfoque y metodología

El documento se estructura como una hoja de ruta para construir una arquitectura nacional de ciberseguridad robusta y coordinada. Propone un modelo de gobernanza basado

en la cooperación multiactor, articulado en torno a tres dimensiones interdependientes:

**1** Infraestructura crítica, orientada a proteger los sistemas y servicios esenciales digitales para el funcionamiento del país.

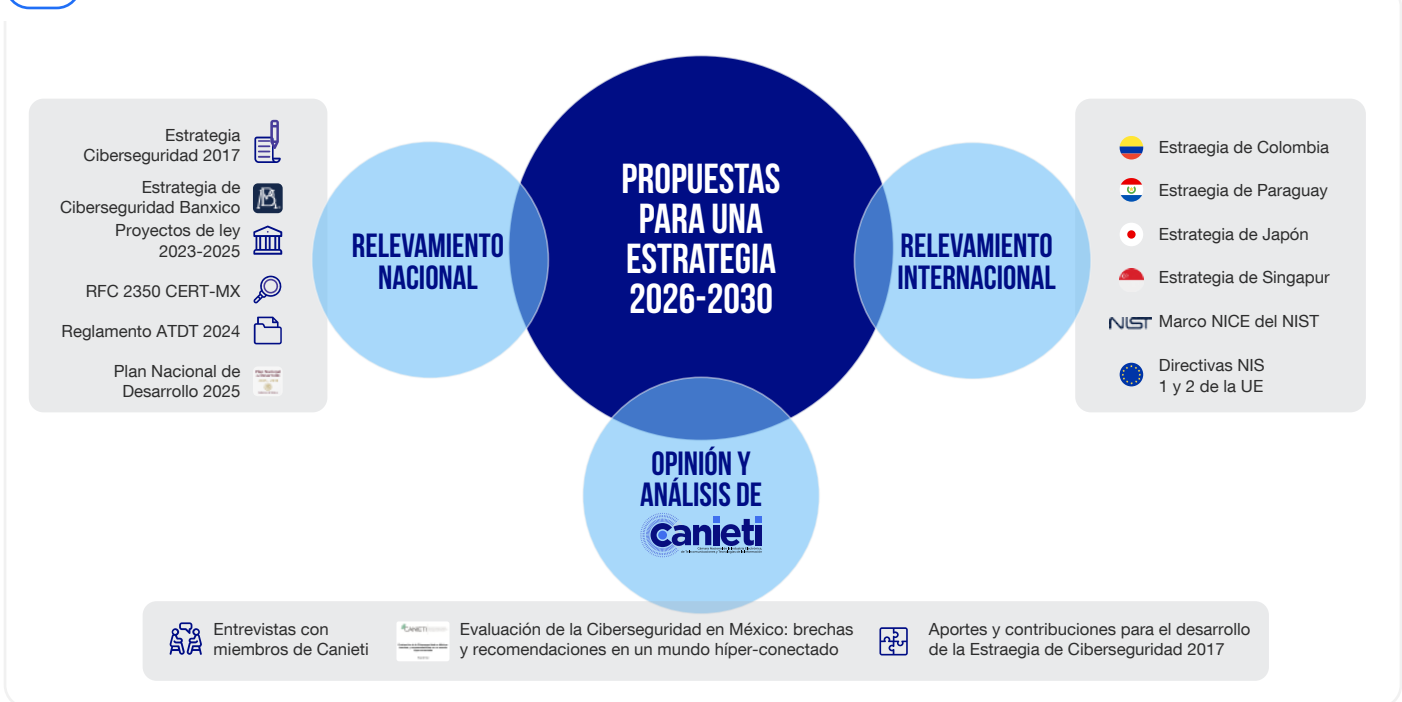
**2** Datos e identidad digital, que aseguren la integridad y privacidad de la información.

**3** Continuidad operativa, centrada en la resiliencia de las instituciones y empresas ante incidentes de ciberseguridad.

Estas dimensiones fueron definidas a partir de un análisis comparado internacional y entrevistas con actores clave del ecosistema nacional, afiliados a la CANIETI. La propuesta

incorpora buenas prácticas y estándares reconocidos por organismos internacionales, junto con las lecciones aprendidas de países que han logrado madurez en la materia.

I/01 Elementos analizados para la realización de la propuesta



Fuente: elaboración propia

## La ciberseguridad como habilitador estratégico del desarrollo sostenible y de la gestión soberana de los recursos digitales

En el entorno actual, contar con una Estrategia Nacional de Ciberseguridad actualizada no es solo una medida operativa, sino una condición estructural para el desarrollo sostenible, la

gestión soberana de los recursos digitales y la confianza en el futuro del país.

### La ciberseguridad como habilitador estratégico del desarrollo económico

La ciberseguridad debe entenderse como habilitador del crecimiento económico y la transformación digital. Su fortalecimiento asegura la continuidad de la economía, fomenta la innovación y genera un clima de confianza para consumidores, empresas e inversionistas. La protección efectiva de los entornos digitales reduce el fraude y los ataques financieros, aumentando la credibilidad de los mercados y la competitividad nacional.

Asimismo, la seguridad digital impulsa la adopción de tecnologías emergentes al ofrecer garantías sólidas de

protección de datos e infraestructura. Los países que demuestran resiliencia digital son percibidos como socios confiables dentro de las cadenas de suministro globales; con una estrategia moderna y coordinada, México puede consolidarse como un hub digital regional capaz de atraer inversión tecnológica y alianzas estratégicas.

Finalmente, el desarrollo de este ecosistema impulsa la formación de talento especializado y la generación de empleo de alto valor, promoviendo una economía del conocimiento más inclusiva y competitiva.

### Protección de la soberanía y la estabilidad social y económica

Más allá de su valor económico, la ciberseguridad constituye un pilar de la soberanía nacional. Proteger la infraestructura crítica y los servicios esenciales digitales equivalen a proteger el funcionamiento y resiliencia del Estado y la estabilidad

de la sociedad. Una estrategia robusta debe identificar vulnerabilidades, prevenir riesgos y asegurar respuestas rápidas y planes de recuperación efectivos frente a incidentes.

## Los recientes ataques en la región evidencian la magnitud de esta amenaza

**2022** En 2022, Costa Rica fue blanco de un ataque de ransomware perpetrado por el grupo Conti, el que paralizó ministerios, al sistema de salud, aduanas, afectó salarios, pensiones y exportaciones, llevando al gobierno a declarar la emergencia nacional.

**2023** En 2023, un ataque de ransomware a IFX Networks paralizó servicios digitales de más de 30 entidades estatales en **Colombia**, interrumpiendo trámites, páginas oficiales y operaciones gubernamentales.

A medida que la inestabilidad geopolítica se acrecienta, estas situaciones pueden volverse aún más recurrentes y México ser uno de los objetivos por el importante lugar que ocupa en el escenario regional y global.

## Diagnóstico y antecedentes

### La evolución de la ciberseguridad en México (1999–2025)

La evolución de la ciberseguridad en México ha sido gradual y fragmentada, marcada por transiciones institucionales que han limitado la consolidación de una gobernanza unificada. Desde sus inicios, el país ha operado bajo un modelo de cooperación interinstitucional con enfoque policial, lo que permitió ciertos avances, aunque persisten vacíos en la respuesta a amenazas a nivel nacional.

El primer hito normativo fue la reforma al Código Penal Federal de 1999, que tipificó el acceso ilícito a sistemas y datos y alineó a México con los futuros estándares internacionales en materia de delitos informáticos. Sin embargo, el marco legal en materia penal ha cambiado poco, generando rezagos frente a amenazas emergentes como el ransomware o los ataques a infraestructuras críticas<sup>1</sup>.

Durante los años 2000, las capacidades institucionales eran aún incipientes, sin equipos de respuesta a incidentes plenamente operativos. En 2010, se creó la Dirección General de Prevención de Delitos Cibernéticos en la entonces Policía Federal<sup>2</sup> y se estableció el CERT-MX<sup>3</sup>, lo que marcó el inicio de una respuesta más estructurada. La Estrategia Nacional de Ciberseguridad de 2017 representó un esfuerzo multisectorial para alinear principios y objetivos con buenas prácticas internacionales, aunque su implementación fue limitada<sup>4</sup> por la falta de un ente rector con facultades y presupuesto propios.

Con el cambio de administración en 2018, la política digital se reorientó hacia la independencia tecnológica, la coordinación interinstitucional y la emisión de un protocolo de seguridad digital a través del CERT-MX<sup>5</sup>, cuyas funciones pasaron posteriormente a la Guardia Nacional<sup>6</sup>.

El T-MEC (2018)<sup>7</sup> incorporó la ciberseguridad en su artículo 19.15, estableciendo compromisos en cooperación,

intercambio de información y gestión de riesgos. Entre 2020 y 2022, se fortaleció la cooperación internacional con la publicación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, la adhesión a la Counter Ransomware Initiative<sup>8</sup> y la creación del Working Group on Cyber Issues<sup>9</sup> junto con EE. UU. y Canadá<sup>10</sup>.

Sin embargo, es importante reconocer que el T-MEC fue negociado en un contexto económico y tecnológico propio de 2018, y que la realidad actual del comercio y los servicios digitales ha cambiado de forma sustancial. La acelerada adopción tecnológica, la innovación de los últimos años y la incorporación de tecnologías emergentes, junto con las nuevas amenazas en materia de ciberseguridad, especialmente aquellas provenientes de actores maliciosos fuera de la región, exigen una actualización profunda.

En este sentido, la revisión conjunta del acuerdo representa una oportunidad clave para fortalecer su capítulo digital y de ciberseguridad, asegurando su vigencia frente a los desafíos del futuro. América del Norte debe asumir un liderazgo regional en ciberseguridad, promoviendo la cooperación y la armonización regulatoria que le permitan consolidarse como una región cibersegura y ciberresiliente.

Finalmente, el Plan Nacional de Desarrollo 2024–2030<sup>11</sup>, el Plan México y el Programa Sectorial de la Agencia de Transformación Digital y Telecomunicaciones (ATDT) 2025–2030<sup>12</sup> incorporan la ciberseguridad como eje estratégico para fortalecer la confianza digital y la protección de sistemas gubernamentales. La ATDT asume un rol coordinador dentro de la Administración Pública Federal, aunque persiste el desafío de articular al ecosistema nacional (incluyendo otros niveles de gobierno, operadores de infraestructura crítica y el sector privado) bajo una arquitectura integral y coherente.

1. ENISA. (2024). [Panorama de amenazas 2024: Amenazas y tendencias emergentes](#). Agencia de la Unión Europea para la Ciberseguridad.

2. Diario Oficial de la Federación. (2010, 17 de mayo). Reglamento de la Ley de la Policía Federal (Art. 65).

3. FIRST. (2023, March 13). [CERT-MX \(Team profile\)](#). Forum of Incident Response and Security Teams (FIRST).

4. Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad (ENCS 2017).

5. Coordinación de Estrategia Digital Nacional. (2018, diciembre). [Proceso de planeación de la Estrategia Digital Nacional y de la Política Tecnológica](#). Oficina de la Presidencia de la República.

6. Diario Oficial de la Federación (DOF). (2019, 26 de marzo). Decreto por el que se crea la Guardia Nacional.

7. Gobierno de México, Secretaría de Economía. (s. f.). [Tratado entre México, Estados Unidos y Canadá \(T-MEC\)](#), Capítulo 19: Comercio digital — Artículo 19.15: Ciberseguridad.

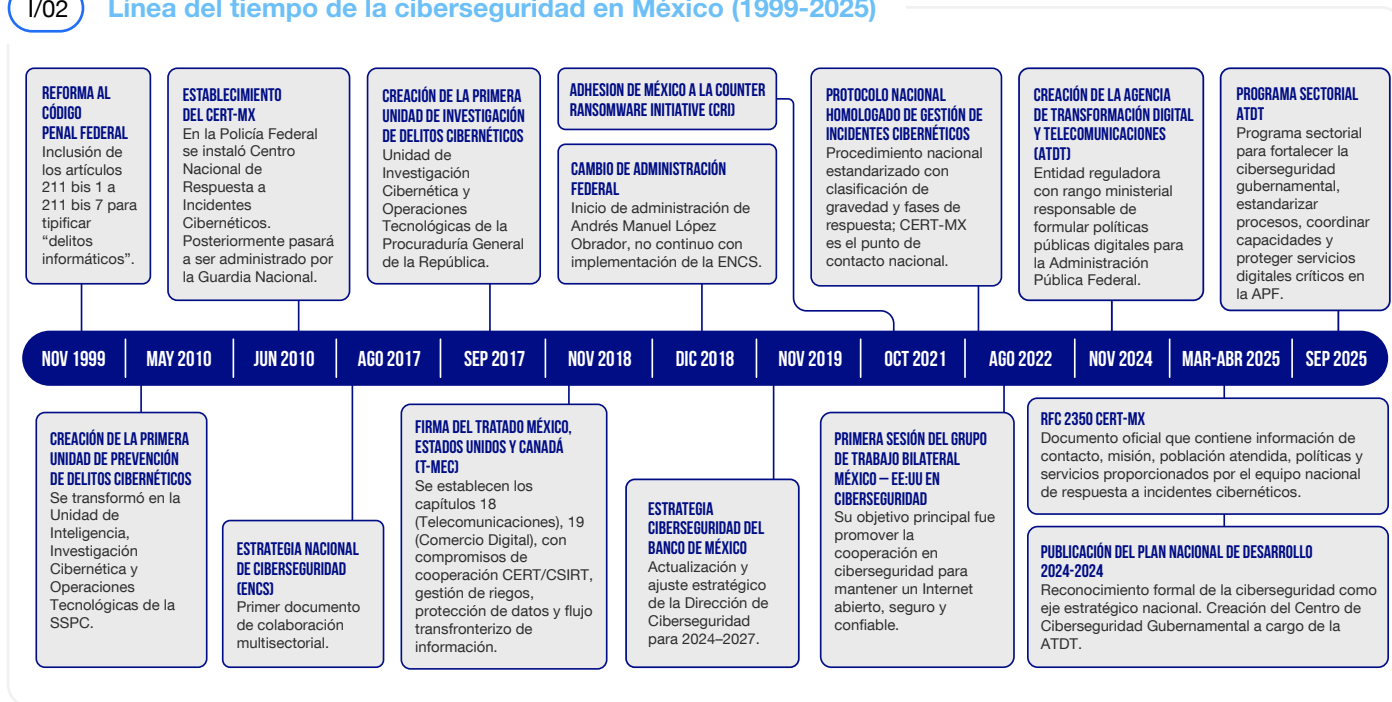
8. Counter Ransomware Initiative. (s. f.). [About the CRI](#).

9. Secretaría de Relaciones Exteriores. (2022, 18 de agosto). [Mexico – U.S. Working Group on Cyber Issues](#).

10. Government of Canada, Prime Minister. (2021, 18 de noviembre). [Joint Statement by North American Leaders](#).

11. Presidencia de la República. (2024). Plan Nacional de Desarrollo 2024–2030.

12. Presidencia de la República. (2025, 19 de septiembre). Programa Sectorial 2025–2030 de la Agencia de Transformación Digital y Telecomunicaciones (ATDT).



Fuente: elaboración propia a partir de la sistematización de eventos y documentos oficiales (1999-2025)

## Marco Institucional de la Ciberseguridad en el México actual

Las responsabilidades en materia de ciberseguridad en México están distribuidas por sectores y niveles de gobierno, con mayores avances en seguridad pública, defensa y el sistema financiero. A nivel federal, sin embargo, coexisten dos cabezas funcionales que dificultan la coordinación nacional y

la construcción de una estrategia integral.

Por un lado, la ATDT concentra la conducción normativa dentro de la Administración Pública Federal (APF). Sus acciones se articulan en tres ejes:

• Un marco normativo y de cumplimiento (lineamientos, diagnósticos y el Sistema de Cumplimiento Normativo en Ciberseguridad).

• La operación de centros nacionales de ciberseguridad (entre ellos el CSOC Federado y el CSIRT Nacional) con monitoreo continuo, inteligencia de amenazas y gestión de incidentes.

• Un programa integral de resiliencia gubernamental, que incluye el Modelo Nacional de Madurez en Ciberseguridad, el ETSEC, el Cyber Range MX y programas de formación.

No obstante, este diseño aún no constituye un sistema nacional de gobernanza ya que carece de un órgano rector con alcance transversal y de mecanismos que integren sistemáticamente al sector privado, incluidas las empresas que operan infraestructuras críticas y las MiPyMEs.

Por otro lado, la Secretaría de Seguridad y Protección Ciudadana (SSPC) y la Guardia Nacional, que opera el CERT-MX, concentran la capacidad técnico-operativa para la gestión de incidentes y el análisis de inteligencia, en coordinación con el Centro Nacional de Inteligencia (CNI).

Esta estructura refuerza la necesidad de una mayor articulación interinstitucional para evitar duplicidades y vacíos de coordinación entre los frentes normativo (ATDT) y operativo (SSPC-GN).

El sector financiero destaca como el más avanzado en ciberresiliencia, con liderazgo del Banco de México, la CNBV y la CNSF, y con instrumentos como la Estrategia de Ciberseguridad del Banco de México y los protocolos de respuesta colaborativa.

Un punto crítico de gobernanza es la protección de infraestructuras críticas. El marco vigente alude a sectores estratégicos, pero carece de una definición operativa y transversal de "infraestructura crítica", lo que dificulta priorizar riesgos, coordinar vulnerabilidades y exigir controles comparables a operadores y proveedores. Mientras no se precise este concepto, los perímetros de acción de los CSIRTs/CERTs seguirán difusos, con riesgo de solapamientos y brechas en la respuesta nacional.

En México existen aproximadamente 40 equipos especializados en la gestión de incidentes de ciberseguridad (CSIRTs/CERTs) en ámbitos gubernamentales, académicos y privados, los cuales presentan una madurez dispareja, lo que pudiera estar restringiendo las sinergias. El reto inmediato consiste en homologar estándares, métricas y esquemas de coordinación nacional (por ejemplo, tiempos medios de detección, contención y recuperación; umbrales de severidad; ejercicios de mesa y ciber-simulacros compartidos), de modo que esta densidad institucional se traduzca en una resiliencia nacional efectiva, medible y sostenible.

**GOBERNANZA DE CIBERSEGURIDAD EN MÉXICO**

Estructura fragmentada por dominios, con islas de alta madurez en seguridad pública/defensa y en el sistema financiero; el reto central es orquestar coordinación, estándares e interoperabilidad entre niveles de gobierno y sector privado.

**INFRAESTRUCTURAS CRÍTICAS Y SERVICIOS ESENCIALES DIGITALES**

En México, las infraestructuras críticas y los servicios esenciales digitales se asocian principalmente con funciones estatales de seguridad y provisión de servicios públicos. Sin embargo, el país carece de una definición precisa y transversal, lo que deja en una zona gris a sectores esenciales como la manufactura crítica, los alimentos y la agricultura. Esta ausencia normativa abre la oportunidad de avanzar hacia una definición estandarizada y un catálogo nacional que abarque todas las infraestructuras críticas, permitiendo establecer criterios claros de protección, priorización y coordinación.

**CSIRTS/CERTS: "DENSIDAD ALTA, COORDINACIÓN PENDIENTE"**

México tiene muchos CSIRTS/CERTS, pero con madurez dispar; el reto es homologar estándares, métricas y coordinación para que la densidad se traduzca en resiliencia nacional.

GOBERNANZA ACTUAL DE LA CIBERSEGURIDAD

ADMINISTRACIÓN PÚBLICA FEDERAL

SEGURIDAD PÚBLICA Y PROTECCIÓN CIUDADANA

DEFENSA NACIONAL

SECTOR FINANCIERO

GOBIERNOS ESTATALES Y MUNICIPALES

PRIVADOS CON INFRAESTRUCTURAS CRÍTICAS

INFRAESTRUCTURAS CRÍTICAS Y SERVICIOS ESENCIALES DIGITALES

**IMPACTO ECONÓMICO Y PRODUCTIVO**

Energía Eléctrica  
Hidrocarburos y Gas Natural  
Servicios Financieros y pagos  
Transporte y Logística  
Alimentos y Agricultura  
Minería y Metalurgia  
Industria Metal-mecánica y manufactura crítica  
Industria química y petroquímica

**IMPACTO SOCIAL Y VITAL**

Salud  
Agua y Saneamiento  
Seguridad Pública y emergencias  
Gobierno Digital  
Fiscal y Aduanero  
Gestión Ambiental y de residuos

**IMPACTO ESTRATÉGICO Y SOBERANO**

Defensa Nacional  
Energía nuclear  
Procesos electorales  
Telecomunicaciones y Servicios Satelitales

CERTS/CSIRTS: +40

5 PÚBLICOS

+23 PRIVADOS

5 PRIVADOS INTERNACIONALES

7 ACADÉMICOS

Fuente: elaboración propia con base en el directorio de equipos miembros de FIRST (CSIRTS/CERTS), el [inventario nacional de equipos](#), y la clasificación sectorial del INEGI (SCIAN 2023) para agrupar las infraestructuras críticas por impacto económico, social y estratégico

## El marco normativo y los intentos de una Ley de Ciberseguridad en México

El marco normativo mexicano en ciberseguridad es fragmentado y sectorial, sin una ley general que articule y coordine las responsabilidades del Estado, el sector privado y la sociedad. Aun así, existen pilares que han sentado bases relevantes.

El Plan Nacional de Desarrollo reconoce la ciberseguridad como prioridad de Estado, otorgándole legitimidad política y ubicándola en la agenda de seguridad nacional y desarrollo digital. Por su parte, las leyes de protección de datos personales (tanto en el sector público como en el privado) constituyen el marco más consolidado, al imponer obligaciones administrativas, técnicas y físicas para el tratamiento de datos y la gestión de riesgos<sup>13</sup>. No obstante, su alcance se limita a los datos personales, dejando fuera otros activos críticos para la continuidad de los servicios esenciales digitales.

El Programa Sectorial<sup>14</sup> de la Agencia de Transformación Digital y Telecomunicaciones (ATDT) 2025–2030 traduce la política digital del Estado en acciones concretas dentro de la APF. Entre sus metas destacan el fortalecimiento de la infraestructura tecnológica, la soberanía de datos y la ciberseguridad gubernamental mediante la creación de una Nube de Gobierno, una política general de ciberseguridad y servicios centralizados de protección digital.

En paralelo, el sector financiero posee un andamiaje normativo robusto, con instrumentos como la Estrategia de Ciberseguridad del Banco de México (2024–2027), las Bases de Coordinación en Materia de Seguridad de la Información (2018) y el Anexo 72 de la Circular Única Bancaria (CUB), lo que lo convierte en uno de los ámbitos más avanzados en materia de ciberresiliencia<sup>15 16 17</sup>.

Sin embargo, el marco actual evidencia vacíos estructurales: México carece de una ley marco de ciberseguridad, de un catálogo legal de infraestructuras críticas y servicios esenciales digitales, y de un deber general de notificación de incidentes. Tampoco existen estándares transversales para la gestión de riesgos o la detección de vulnerabilidades. La falta de definiciones operativas impide priorizar sectores estratégicos (como alimentos o manufactura) y limita la coordinación nacional.

No debe pasarse por alto que la identidad digital emerge como un nuevo eje normativo, esencial para la digitalización gubernamental y la cooperación internacional. Mientras, las tecnologías emergentes plantean desafíos regulatorios que exigen revisar los tipos penales y actualizar los marcos de protección.

En este contexto, es importante reconocer que las Fuerzas Armadas han desarrollado capacidades operativas relevantes

13. Secretaría de Gobernación – Sistema de Información Legislativa (SIL). (2025). [Iniciativa: que expide la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares](#) [Ficha de asunto 4840758].

14. Gobierno de México. (2025, 19 de septiembre). [Decreto por el que se aprueba el Programa Sectorial de la Agencia de Transformación Digital y Telecomunicaciones 2025–2030](#). Diario Oficial de la Federación.

15. Banco de México. (2019). [Disposiciones de carácter general aplicables a las instituciones de crédito \(Circular Única de Bancos – Anexo 72: Ciberseguridad\)](#). Banco de México.

16. Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAAR). (2018, 4 de junio). [Bases de coordinación en materia de seguridad de la información](#). Gobierno de México.

17. Comisión Nacional Bancaria y de Valores (CNBV). (s. f.). Anexo 72. [Indicadores de seguridad de la información](#) (Disposiciones de carácter general aplicables a las instituciones de crédito – CUB).

en materia de ciberseguridad. La Secretaría de la Defensa Nacional (SEDENA) y la Secretaría de Marina (SEMAR) cuentan con unidades especializadas como el Centro de Operaciones del Ciberespacio y la Coordinadora General del Ciberespacio, respectivamente. Ambas participan en una estrategia conjunta de ciberdefensa y colaboran con la Agencia de Transformación Digital y Telecomunicaciones (ATDT), el Centro Nacional de Inteligencia (CNI) y la Secretaría de Seguridad y Protección Ciudadana (SSPC) para fortalecer la protección del ciberespacio nacional<sup>18</sup>.

Por su parte, la Guardia Nacional opera el CERT-MX, responsable de atender incidentes cibernéticos en el ámbito civil. Estas instituciones han sido clave frente a ciberataques recientes y representan capacidades que deben integrarse formalmente en el futuro marco de gobernanza. Su articulación efectiva con los actores civiles es esencial para construir un sistema nacional de ciberseguridad funcional y resiliente<sup>19</sup>. En el ámbito legislativo, México ha intentado aprobar una Ley de Ciberseguridad en múltiples ocasiones, sin éxito. En el Congreso y el Senado se discuten al menos tres proyectos recientes. Estas iniciativas coinciden en la necesidad de un órgano coordinador nacional, la definición de conceptos técnicos, la creación de un catálogo de infraestructuras críticas y la regulación de la gestión de incidentes. Sin embargo, difieren en su modelo de gobernanza

y suelen carecer de metodologías claras de gestión de riesgos o criterios de actualización. Las divergencias sobre quién debe liderar han frenado su avance<sup>20</sup>.

Como resultado, México sigue sin una Ley General de Ciberseguridad ni una Estrategia Nacional actualizada, lo que mantiene un andamiaje disperso basado en normas sectoriales (protección de datos, regulaciones financieras, lineamientos de la APF y protocolos de seguridad pública). Esta fragmentación ha permitido avances puntuales, pero no un sistema nacional coherente con obligaciones claras y capacidades comunes de respuesta.

Hoy la coyuntura es crítica. La ciberseguridad ya es una prioridad de Estado, y el desafío no es solo cuándo se aprobará una ley, sino bajo qué modelo de gobernanza y con qué nivel de articulación y coordinación entre actores federales, estatales, privados y sociales. Para lograrlo, resulta indispensable contar con una Estrategia Nacional de Ciberseguridad, de modo que combine la flexibilidad adaptativa de la estrategia con la fuerza vinculante de una ley integral. Solo esa convergencia permitirá construir un marco que sea a la vez adaptable y exigible, capaz de responder a los desafíos presentes y futuros del ecosistema digital mexicano.



18. Secretaría de Marina (2022). Acuerdo Secretarial Núm. 335/2022 por el que se crea la Coordinadora General del Ciberespacio. DOF, 15 agosto.

19. Guardia Nacional (2023). Informe del CERT-MX y panorama de amenazas cibernéticas. SSPC. OEA-CICTE (2024). Ejercicio de gestión de crisis cibernética - México 2024.

20. No obstante, el 21 de octubre de 2025 el Senado creó la Comisión Ordinaria de Ciberseguridad, un paso institucional que envía una señal positiva hacia la construcción de un marco general que podría acelerar consensos en la LXVI Legislatura. Senado de la República. (2025, 21 de octubre). Crean la Comisión de Ciberseguridad en el Senado (Comunicado). Coordinación de Comunicación Social.

# Tendencias clave de la gobernanza e institucionalidad de la ciberseguridad

## El imperativo estratégico de la gobernanza en materia de ciberseguridad a nivel nacional

En este contexto, una gobernanza sólida y estratégica resulta esencial para resguardar infraestructuras críticas y servicios esenciales digitales, la economía digital, libertades y derechos fundamentales como la privacidad y la intimidad. Esta comprende las interacciones y responsabilidades entre gobierno, sector privado, academia y sociedad civil, orientadas a una gestión integral de riesgos y a la cooperación interinstitucional. Los países que lideran la transformación digital han construido sus modelos sobre principios de coordinación, claridad funcional y distribución eficiente de recursos, combinando instrumentos ejecutivos (como decretos presidenciales) y leyes de alto nivel. Una gobernanza consolidada es, por tanto, indicador de madurez institucional,

y debe figurar como objetivo estratégico dentro de una Estrategia Nacional.

La gobernanza efectiva se articula en tres niveles. En primer lugar, el nivel estratégico, donde se definen políticas, prioridades a largo plazo y mecanismos de interacción entre los actores clave. En segundo lugar, el nivel táctico, encargado de traducir la estrategia en programas concretos, gestión de recursos y coordinación de oficinas con experiencia en ciberseguridad. En tercer lugar, el nivel operativo, enfocado en la ejecución diaria, la gestión de incidentes y la transferencia de conocimiento entre equipos especializados.

### I/04 Niveles que se deben considerar en la gobernanza nacional



Fuente: elaboración propia basado en las mejores prácticas internacionales, tales como el Marco de Gobernanza para Estrategias Nacionales de Ciberseguridad de la Agencia de la Unión Europea para la Ciberseguridad.

A nivel comparado, los modelos más avanzados tienden a la centralización, asignando a una autoridad nacional la coordinación técnica, la formulación de políticas y la protección de infraestructuras críticas. Países como Estados Unidos, Reino Unido, Corea del Sur y Japón adoptaron este enfoque desde los años 2000, consolidando marcos institucionales robustos que integran la ciberseguridad como política de Estado.

México tiene la oportunidad histórica de construir un marco de ciberseguridad que supere la fragmentación institucional

actual y proteja infraestructuras críticas y servicios esenciales digitales. Este marco debe evitar la falsa dicotomía entre protección e innovación. Normativas muy prescriptivas que alteren la integridad de productos o servicios digitales, como es hoy el caso europeo, son una fuente de vulnerabilidades y riesgos. La armonización, la previsibilidad y la consulta a múltiples actores involucrados son principios clave para también guiar la definición de marcos de ciberseguridad alineados con las mejores prácticas internacionales, como el enfoque de seguridad digital que promueve la OCDE.

PAÍS, LOGO Y AÑO DE CREACIÓN	ENTIDAD QUE FUNCIONA COMO AUTORIDAD EN CIBERSEGURIDAD NACIONAL	INDICADOR DE AVANCE
<b>SINGAPUR (2015)</b> 	La Agencia de Ciberseguridad de Singapur (Cyber Security Agency -CSA) se creó en 2015 <a href="https://www.csa.gov.sg/about-csa/who-we-are/">https://www.csa.gov.sg/about-csa/who-we-are/</a>	Proteger el ciberespacio de Singapur.
<b>REINO UNIDO (2016)</b> 	Centro Nacional de Seguridad Cibernética (National Cyber Security Centre – NCSC), parte del GCHQ. <a href="https://www.ncsc.gov.uk/section/about-ncsc/what-we-do">https://www.ncsc.gov.uk/section/about-ncsc/what-we-do</a>	Ayuda a las empresas, al sector público y a las personas a proteger los servicios y dispositivos en línea.
<b>COREA DEL SUR (2009)</b> 	KISA Korea Internet and Security Agency <a href="https://www.kisa.or.kr/EN">https://www.kisa.or.kr/EN</a>	Tiene como objetivo construir una red de protección de datos infalible mediante un sistema avanzado de detección y respuesta, y asegurar la estabilidad de la infraestructura digital ante diversos desastres.
<b>ESTADOS UNIDOS (2018)</b> 	CISA, Cybersecurity and Infrastructure Security Agency <a href="https://www.cisa.gov/about/leadership">https://www.cisa.gov/about/leadership</a>	CISA es un componente del Departamento de Seguridad Nacional de los Estados Unidos (DHS) responsable de la ciberseguridad y la protección de las infraestructuras en todos los niveles del gobierno.
<b>UNIÓN EUROPEA (2004)</b> 	ENISA, Agencia Europea de ciberseguridad. <a href="https://www.enisa.europa.eu/topics">https://www.enisa.europa.eu/topics</a>	Lograr un alto nivel común de ciberseguridad en toda Europa

Fuente: elaboración propia

## La construcción de la gobernanza en la región

En los últimos años, varios países de la región se han dedicado a debatir el marco de gobernanza necesario para coordinar las distintas áreas de la ciberseguridad nacional. Sin embargo, han diferido en sus enfoques y diseños.

Chile abordó la discusión de la gobernanza en ciberseguridad a través del Congreso, lo que terminó derivando en la aprobación de la Ley Marco de Ciberseguridad. Mediante esta ley, se creó la Agencia Nacional de Ciberseguridad (ANCI) como un ente funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, y de naturaleza técnica con poder regulatorio y sancionatorio. Por esto último la ANCI es actualmente un caso único en la región. Por mandato legal, la agencia chilena tiene alcance normativo sobre una amplia diversidad de actores tanto públicos como privados. Los sujetos obligados son definidos por la legislación como proveedores de servicios esenciales y operadores de importancia vital<sup>21</sup>. Los primeros deben cumplir obligaciones generales, como implementar medidas de prevención, gestión y reporte de incidentes significativos

al CSIRT Nacional, mientras que los segundos están sujetos a deberes reforzados, que incluyen la elaboración y certificación periódica de planes de continuidad operacional, auditorías, simulacros, designación de un delegado de ciberseguridad y programas de capacitación permanente, entre otros. Además, la ANCI tiene a su cargo la Red de Conectividad Segura del Estado, la coordinación del CSIRT Nacional y la presidencia del Comité Interministerial sobre Ciberseguridad.

El caso de Brasil ilustra la complejidad de implementar un modelo de gobernanza unificado en un sistema federal grande y descentralizado. Desde hace ya algunos años, Brasil debate la creación de una Agencia Nacional de Ciberseguridad (ANCiber). Sin embargo por limitaciones presupuestarias su creación se ha postergado<sup>22</sup>. Actualmente, la Estrategia Nacional de Ciberseguridad (E-Ciber) publicada por Decreto 12.573 de Agosto de 2025 provee un marco estratégico que aborda la gobernanza, la cual recae en el Gabinete de Seguridad Institucional de la Presidencia (GSI). Específicamente dentro del GSI, el Comité Nacional de

21. Los Operadores de Importancia Vital se encuentran actualmente en proceso de designación por la ANCI, la cual emitió la primera lista borrador el 16 de Septiembre de 2025.

22. Recientemente el Comité Nacional de Ciberseguridad (CNCiber) creó un grupo de trabajo encargado de retomar este debate, evaluando la viabilidad de una agencia u otros diseños de gobernanza.

Ciberseguridad o CNCiber (un órgano colegiado que reúne a 25 instituciones, entre organismos del Gobierno Federal, representantes de entidades de la sociedad civil, instituciones científicas y del sector empresarial relacionados con el ámbito de la ciberseguridad) es el encargado de elaborar el Plan Nacional de Ciberseguridad que delimitará las acciones estratégicas concretas hasta 2031 desprendidas de la Estrategia.

Finalmente, a través del decreto 338 de 2022, Colombia desagregó su modelo de gobernanza en cinco instancias<sup>23</sup> de acuerdo a tres niveles de acción: estratégico, táctico y operacional. En primer lugar, asumiendo el rol estratégico se encuentra la Coordinación Nacional de Seguridad Digital, designada por el Presidente de la República, y responsable de coordinar los asuntos estratégicos a nivel del Gobierno

Nacional. En segundo lugar, el Comité Nacional de Seguridad Digital (CNSD), el cual recomienda al gobierno políticas y medidas estratégicas a nivel nacional, apoya la articulación y propone acciones para fortalecer las capacidades de las múltiples partes interesadas. Incluye representantes de varios ministerios, la Dirección Nacional de Inteligencia, y un representante de las autoridades de cada sector titular de infraestructura crítica cibernética o servicios esenciales. En tercer lugar, a nivel táctico, se encuentran los Grupos de Trabajo de Seguridad Digital encargados de coordinar y asesorar al Comité Nacional de Seguridad Digital desde el punto de vista táctico y procedimental en torno a la seguridad digital a nivel nacional. Finalmente, a nivel operativo, el modelo colombiano creó las Mesas de Trabajo de Seguridad Digital y Puestos de Mando Unificado de Seguridad Digital.

## I/06 Agencias centrales de ciberseguridad en la región

AUTORIDAD CENTRAL	NATURALEZA	BASE LEGAL	ENFOQUE
 <p>CHILE</p> <p><b>AGENCIA NACIONAL DE CIBERSEGURIDAD (ANCI)</b></p>	<p><b>Descentralizada y técnica;</b> con intermediación del Ministerio de Seguridad Pública</p>	<p>Ley 21.663 Marco de Ciberseguridad</p>	<p>Estratégico y operativo</p>
 <p>BRASIL</p> <p><b>GABINETE DE SEGURIDAD INSTITUCIONAL (GSI) + COMITÉ NACIONAL DE CIBERSEGURIDAD (CNCIBER)</b></p>	<p><b>Híbrida;</b> el GSI depende de Presidencia pero el CNCiber es un órgano colegiado con participación de diversos actores.</p>	<p>Decreto 11.856 de 2023</p>	<p>Estratégico</p>
 <p>COLOMBIA</p> <p><b>COORDINACIÓN NACIONAL DE CIBERSEGURIDAD</b></p>	<p><b>Presidencial;</b> el Presidente es el encargado de designar al Coordinador</p>	<p>Decreto 338 de 2022</p>	<p>Estratégico</p>

Fuente: elaboración propia

## Las estrategias: el puntapié necesario para abordar la ciberseguridad nacional

En el último año, cinco países de la región publicaron Estrategias Nacionales de Ciberseguridad, destacando la enorme importancia que tienen para articular una agenda proactiva de mediano y largo plazo en la materia. Entre estos países se encuentran, además de Brasil y Colombia, Paraguay, Uruguay y Perú (este último, en consulta pública, y prevé aprobarla en 2026).

El tratamiento de las infraestructuras críticas y los servicios esenciales digitales deben ocupar un lugar central en todas las estrategias. Se promueve su identificación, clasificación y protección mediante auditorías, ejercicios y marcos sectoriales. Otro eje compartido es la promoción de una cultura nacional de ciberseguridad, con campañas ciudadanas y programas de capacitación para servidores públicos. La formación del talento y fuerza laboral constituye un eje central en todas las estrategias, buscando cerrar brechas y fomentar la certificación profesional. Además, todas las estrategias

priorizan la cooperación internacional, tanto a nivel regional como en foros globales, junto con la adopción de estándares de gestión de riesgos para la respuesta coordinada a incidentes.

Más allá de estas similitudes, cada Estrategia presenta particularidades. Por ejemplo Brasil, con el decreto 12.573 de 2025, es el único país que institucionaliza su estrategia mediante una norma con fuerza jurídica inmediata, y proyecta un Plan Nacional posterior para detallar la ejecución. Su enfoque es pragmático, centrado en ciudadanía, infraestructura crítica y servicios esenciales digitales, cooperación público-privada y la gestión soberana de los recursos digitales. Introduce instrumentos distintivos como una lista nacional de alto riesgo, un sello de certificación nacional para indicar el nivel de seguridad de los activos cibernéticos y un sistema de seguros contra incidentes.

23. Al igual que Brasil, Colombia también ha estado debatiendo políticamente la creación de una agencia. En 2023, el Ministerio de Tecnologías de la Información y las Comunicaciones envió al Congreso un proyecto de ley para crear una Agencia de Seguridad Digital y Asuntos Aeroespaciales. Sin embargo, por limitaciones de presupuesto y resquemores en torno a su diseño el proyecto de ley se paralizó luego de su aprobación en primer debate. La Estrategia Nacional de 2025 retoma este objetivo; sin embargo, el gobierno colombiano aún no ha presentado el proyecto de ley correspondiente.

Colombia amplía el marco de la seguridad digital, integrando derechos digitales, privacidad y confianza. Su estrategia incorpora perspectiva de género, prevención de violencia digital y uso responsable de IA bajo principios éticos, además de su uso como herramienta para la mejora de los sistemas de defensa y respuesta a incidentes. Propone la creación de una entidad nacional, un observatorio y un marco contra el ransomware, además de fortalecer las infraestructuras críticas de la información y los servicios esenciales digitales con arquitectura Zero Trust, además de evaluar la madurez de los CSIRTs con modelos como SIM3.

Paraguay, al igual que Colombia, presta especial atención al ransomware como amenaza junto al cibercrimen. Además reconoce como prioridad la creación de una ley integral de protección de datos y es el único país aquí analizado que propone la creación de un Marco Nacional de Competencias y Roles de Ciberseguridad, alineado con la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) del Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST).

Perú se distingue por alinear explícitamente su Estrategia al Marco de Seguridad Digital de la OCDE. Además, busca

operacionalizar las directrices derivadas de su Ley 30.999 de Ciberdefensa. Entre sus acciones estratégicas destacadas, establece la creación de un registro nacional de riesgos y un Sistema Nacional de Gestión de Ciber crisis. Además proyecta una transición hacia la criptografía post-cuántica.

La Estrategia de Uruguay, finalmente, se distingue por su marco de cocreación amplia que incluyó a más de 120 instituciones públicas, privadas y académicas. Además, enfatiza la coordinación interinstitucional, la interoperabilidad y la promoción del ecosistema nacional de ciberseguridad, incluyendo MiPyMEs e industria local.

La implementación de las Estrategias continúa siendo el mayor reto que enfrentan los países. Actualmente existen otras Estrategias activas en la región (Costa Rica 2023-2027, Ecuador 2022-2025 y República Dominicana 2022-2030) pero no presentan indicios concretos de avance. Sin embargo, casos como el de Brasil parecen indicar que aquellos que abordan la ciberseguridad involucrando a todos los actores relevantes del ecosistema han logrado dar pasos prudentes pero importantes que contemplan la complejidad del reto.





# Marco estratégico

## Por qué México necesita una Estrategia Nacional de Ciberseguridad

México requiere con urgencia una Estrategia Nacional de Ciberseguridad que consolide los esfuerzos dispersos, otorgue coherencia a las políticas públicas y establezca un marco de acción común entre los sectores público, privado, académico y social.

En la era de la interconexión global, hiperconectividad de la sociedad y la competencia geopolítica digital, la ciberseguridad ha trascendido su origen técnico para convertirse en un pilar fundamental estratégico de la soberanía nacional, la estabilidad económica y la confianza social. Las naciones líderes han comprendido que una postura cibernética robusta no es solo una medida defensiva, sino un requisito esencial para el desarrollo, la prosperidad y la influencia internacional. Para México, una de las economías más grandes del mundo e integrante clave de cadenas de valor globales, adoptar un enfoque fragmentado y reactivo ante las ciberamenazas ya no es una opción viable; representa una vulnerabilidad estratégica de primer orden.

El principal obstáculo para la consolidación de una ciber-resiliencia nacional es la actual fragmentación institucional y la falta de coordinación entre actores. Esta bifurcación estructural, sin un mecanismo formal de articulación superior, genera vacíos de coordinación y potenciales duplicidades. Más preocupante aún, el diseño vigente excluye sistemáticamente al sector privado, a la academia y a otros

órdenes de gobierno, actores que poseen capacidades técnicas, inteligencia de amenazas y que operan gran parte de la infraestructura crítica del país. La consecuencia de esta desarticulación es palpable: la propia ATDT ha reconocido públicamente<sup>24</sup> la falta de capacidad de respuesta a incidentes en el gobierno, una brecha que solo se mitiga parcialmente gracias a proveedores tecnológicos del sector privado.

La necesidad de unificar estos esfuerzos no es un diagnóstico reciente. Desde 2017, la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) ha recomendado la creación de una agencia nacional de ciberseguridad y el desarrollo de un marco legislativo integral. El hecho de que estas recomendaciones sigan siendo vigentes casi una década después subraya que el desafío no radica en la falta de diagnóstico, sino en la necesidad de superar los obstáculos estructurales que han impedido su implementación efectiva.

Por tanto, una Estrategia Nacional de Ciberseguridad (ENC) se convierte en el instrumento indispensable para superar esta inercia, no solo para fortalecer las capacidades institucionales, sino también para establecer un marco de corresponsabilidad nacional. Su propósito es funcionar como una hoja de ruta unificadora que permita coordinar a los actores con distintos mandatos, cerrar las brechas de responsabilidad y establecer un lenguaje y prioridades comunes para toda la

24. Véase artículo del 25 de septiembre de 2025 de El Economista: "[No hay capacidad de respuesta a incidentes de ciberseguridad en el gobierno: ATDT](#)".

nación, similar al principio de “Unidad de Acción” adoptado por España o el principio de “defender como uno solo” mediante una gobernanza unificada y una red de cooperación interinstitucional del Reino Unido.

Los lineamientos aquí propuestos no buscan reemplazar las capacidades existentes, sino articularlas bajo una visión compartida, sentando las bases para, en un futuro, dotar al país de un marco legal específico, coherente y unificado, que armonice las normas existentes (protección de datos, delitos informáticos, seguridad pública, infraestructura crítica y

servicios esenciales digitales), y que garantice la resiliencia y la seguridad de México en el siglo digital.

El sector privado mexicano, con su experiencia operativa y tecnológica, debe ser un socio estratégico en esta nueva gobernanza, aportando capacidades, inteligencia y recursos para fortalecer la seguridad nacional.

Sobre esta base, la Estrategia propuesta plantea una visión compartida y unos principios rectores que orientarán su implementación hacia 2030.

## Visión y enfoques rectores

La presente propuesta de lineamientos para una Estrategia Nacional de Ciberseguridad de México se fundamenta en una visión clara y ambiciosa para el futuro del país, guiada por enfoques y principios que aseguran un desarrollo digital equilibrado, seguro e inclusivo.

Para materializar esta visión, se adoptan los siguientes enfoques rectores, alineados con las mejores prácticas internacionales y regionales:

### VISIÓN DE CANIETI 2030

Hacer de México un líder en el ámbito digital, reconocido por su ciberseguridad robusta, su resiliencia ante las amenazas y la confianza que genera en ciudadanos, empresas e inversionistas, garantizando la soberanía nacional, la protección de los derechos fundamentales en el ciberespacio y el impulso al desarrollo económico.

● **Enfoque inclusivo y transversal:** por el que se reconoce que la ciberseguridad requiere la participación activa de todos los sectores: gobierno, empresas, academia y ciudadanía.

● **Enfoque centrado en el ser humano:** que pone a la persona en el centro de la política digital, garantizando la protección de sus derechos, la privacidad y la confianza en el entorno digital.

● **Enfoque basado en la gestión de riesgos:** que prioriza las acciones según su impacto y probabilidad, asignando recursos estratégicamente para reducir las vulnerabilidades más críticas.

1/07

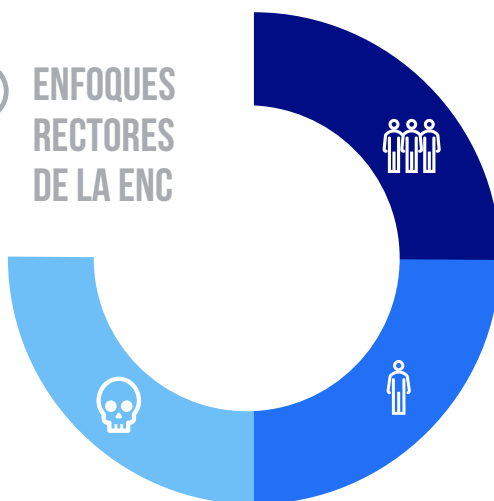
### Enfoques rectores



#### ENFOQUES RECTORES DE LA ENC

##### ENFOQUE BASADO EN LA GESTIÓN DE RIESGOS

Se propone una transición de un modelo reactivo, centrado en el cumplimiento normativo, a uno proactivo y dinámico. Este enfoque se basa en la identificación, evaluación, mitigación y monitoreo continuo de los riesgos cibernéticos, permitiendo priorizar recursos y esfuerzos en la protección de los activos más críticos para la nación y la sociedad.



##### ENFOQUE INCLUSIVO Y TRANSVERSAL

Se reconoce que la ciberseguridad es una responsabilidad compartida que trasciende al gobierno. Su éxito depende de la colaboración activa, estructurada y coordinada del sector, el sector privado, la academia, la sociedad civil y la ciudadanía en general.

##### ENFOQUE CENTRADO EN EL SER HUMANO

La tecnología y las medidas de seguridad deben estar al servicio de las personas. Este enfoque prioriza la protección de los derechos digitales, la privacidad, la seguridad de los datos personales y la dignidad humana en todas las acciones derivadas de la estrategia, asegurando que la ciberseguridad sea un habilitador de libertades y no un pretexto para su restricción.

Fuente: elaboración propia

Adicionalmente, la estrategia debe sustentarse en un conjunto de principios guía para su implementación y evaluación, que constituyen el marco ético y operativo.

## I/08 Principios guía de la Estrategia Nacional de Ciberseguridad de México



Fuente: elaboración propia

Estos enfoques y principios permitirán que la Estrategia Nacional de Ciberseguridad de México no solo aborde la protección frente a amenazas, sino que promueva un





desarrollo digital sostenible, donde la confianza y la seguridad sean motores de crecimiento sostenible.

## Retos y desafíos

Para que la Estrategia Nacional de Ciberseguridad sea efectiva, debe partir de un diagnóstico honesto de los obstáculos que enfrenta el país. Estos retos no son barreras insuperables, sino los problemas concretos que esta hoja

de ruta está diseñada para resolver de manera estructural y coordinada. La siguiente tabla resume los principales desafíos que deben abordarse de manera prioritaria para garantizar la eficacia de la Estrategia.

## T/01 Principios guía de la Estrategia Nacional de Ciberseguridad de México

DESAFIO	DESCRIPCIÓN
 INSTITUCIONAL	La ausencia de una instancia nacional de coordinación impide articular una política integral. Sin un punto central que integre al sector público, privado y académico, la respuesta ante incidentes de gran escala sería lenta, desorganizada e ineficaz.
 NORMATIVO	México carece de un marco jurídico integral y actualizado en materia de ciberseguridad. Las normas actuales solo cubren aspectos parciales, como protección de datos o delitos informáticos, y no contemplan la protección de infraestructuras críticas, servicios digitales esenciales, gestión de incidentes ni cooperación público-privada. Un marco moderno debe ser flexible, basado en riesgo y alineado con estándares internacionales como el Convenio de Budapest <sup>25</sup> , el de la ONU contra la Ciberdelincuencia y el Marco NIST.
 CULTURAL Y DE TALENTO	La ciberseguridad aún no forma parte del ADN institucional ni ciudadano. La escasez de profesionales en ciberseguridad limita la implementación de políticas públicas. Sin una fuerza laboral suficiente y capacitada, y sin una cultura de ciberseguridad arraigada en la ciudadanía y en el tejido empresarial, las mejores tecnologías y las regulaciones más avanzadas resultarán insuficientes.
 SISTÉMICO	Existe una marcada brecha de madurez en ciberseguridad entre grandes corporaciones, especialmente en sectores regulados, y las vulnerables MiPyMEs. Esta asimetría representa un riesgo sistémico, ya que tanto empresas como dependencias públicas dependen de cadenas de suministro donde las MiPyMEs suelen ser el eslabón más débil.

Fuente: elaboración propia

25. [Resolución ex Secretaría de Modernización 1523/2019](#), de la Jefatura de Gabinete de Ministros

Superar estos desafíos requerirá liderazgo político, coordinación y colaboración interinstitucional y un compromiso sostenido del sector privado para traducir la estrategia en resultados tangibles.

La función de la Estrategia Nacional de Ciberseguridad será marcar la visión y los objetivos de país en la materia, así como definir los principios rectores que guiarán la acción pública y privada. Esta estrategia debe partir de un diagnóstico nacional que identifique capacidades, brechas y riesgos prioritarios, y proponer un modelo de gobernanza nacional que articule a las instituciones federales, estatales, gobiernos municipales, el sector privado, la academia y la sociedad civil.

Asimismo, debe incorporar los compromisos multilaterales que México ha asumido en foros internacionales y regionales para

poder identificar a qué está obligado y como puede mejorar la cooperación internacional, y establecer ejes transversales que aseguren sostenibilidad: cultura de ciberseguridad, formación de talento, impulso a la investigación y desarrollo, y considerar desde luego las tecnologías emergentes, como la Inteligencia Artificial o el cómputo cuántico o cualquiera que esté asequible para los que amenacen el ciberespacio. Un componente esencial de la estrategia será el marco de cooperación público-privada e intercambio de información, que permita generar confianza entre sectores y garantizar la circulación oportuna de alertas y buenas prácticas. Al ser un documento flexible y evolutivo, la estrategia deberá contar con mecanismos de actualización periódica, de modo que pueda adaptarse a la rápida transformación tecnológica y a la evolución de las amenazas.

## Objetivos: una visión para 2026-2030

La visión de la Estrategia propuesta es servir como una hoja de ruta para crear un marco de ciberseguridad robusto, resiliente y coordinado en México, con la participación activa del sector público, privado y académico.

En el corto plazo, consideramos necesaria una Coordinación Nacional de Ciberseguridad que funcione como un mecanismo de transición hacia una gobernanza nacional y que defina la Estrategia Nacional de Ciberseguridad 2026-2030 (ENC) que integre esfuerzos gubernamentales y privados.

A mediano plazo, el objetivo es la creación de una Ley Nacional de Ciberseguridad e Infraestructura Crítica que unifique y fortalezca el marco regulatorio nacional, y acompañe la ENC.

Para el largo plazo, se espera que esta Estrategia Nacional de Ciberseguridad sienta las bases de una política más desarrollada y madura para el quinquenio 2031-2035.

1/09

### Hitos clave hacia adelante

#### OBJETIVO DE LA ESTRATEGIA 2026-2030

Funcionar como hoja de ruta para la creación de un marco de ciberseguridad robusto, resiliente y coordinado en el ecosistema nacional mexicano, con participación del sector público, privado y la academia.

COORDINACIÓN  
NACIONAL DE  
CIBERSEGURIDAD

ESTRATEGIA  
NACIONAL DE  
CIBERSEGURIDAD  
PARA ESTE QUINQUENIO  
(2026-2030)

LEY GENERAL DE  
CIBERSEGURIDAD E  
INFRAESTRUCTURA CRÍTICA

EVOLUCIÓN  
DE LA ESTRATEGIA NACIONAL DE CIBERSE-  
GURIDAD PARA EL  
SIGUIENTE QUINQUENIO  
(2031-2035)



CORTO PLAZO



MEDIANO PLAZO



LARGO PLAZO



Sin un marco consultivo y participativo de todos los sectores involucrados no será posible la implementación de una Estrategia Nacional de Ciberseguridad efectiva y sostenible en el tiempo.

Fuente: elaboración propia

Resulta importante destacar que el alcance de esta propuesta es holístico y abarca a toda la sociedad mexicana. La Estrategia cubre de manera integral:

• El sector público, incluyendo no solo a la Administración Pública Federal, sino también a los otros poderes y órdenes de gobierno, así como a toda su cadena de suministro, un punto clave para garantizar la resiliencia del Estado.

• El sector privado, desde los grandes operadores de infraestructuras críticas y servicios esenciales digitales hasta las MiPyMEs, reconociendo su papel fundamental en la economía y como parte de las cadenas de valor sistémicas.

• La ciudadanía, con un enfoque en la protección de sus derechos digitales, la salvaguarda de sus identidades digitales y el fomento de una cultura nacional de ciberseguridad que les permita aprovechar las oportunidades del mundo digital de manera segura y confiable.

Respecto a este último punto, la cultura de ciberseguridad debe entenderse como un pilar transversal de la Estrategia Nacional, al mismo nivel que la infraestructura, el talento y la gobernanza. Ningún avance técnico será sostenible sin una ciudadanía, una fuerza laboral y un sector empresarial conscientes de los riesgos digitales y comprometidos con su prevención. La cultura de ciberseguridad implica transformar hábitos cotidianos y percepciones sociales: pasar de la reacción ante el incidente a la práctica sistemática de la ciberhigiene. Requiere campañas permanentes de sensibilización, educación digital desde la escuela básica hasta la formación especializada en todos los niveles del Estado y del sector privado, y la incorporación de prácticas seguras en la operación de las MiPyMEs. Promover esta cultura no solo reduce vulnerabilidades, sino que fortalece la confianza social y empresarial en el entorno digital,

potenciando la competitividad y la resiliencia nacional frente a las amenazas emergentes.

Esta Estrategia debe concebirse como un proceso evolutivo, con mecanismos de monitoreo y evaluación periódica que permitan su actualización continua ante los cambios tecnológicos y de las amenazas.

Los lineamientos aquí propuestos pueden ayudar a definir la dirección, principios y objetivos sobre los cuales se articularán los ejes, líneas de acción y mecanismos de implementación de la Estrategia Nacional de Ciberseguridad. A partir de este marco, México puede avanzar hacia un modelo de ciberseguridad que combine soberanía, resiliencia y desarrollo sostenible.





# Propuesta de Lineamientos para una Estrategia Nacional de Ciberseguridad

La propuesta está estructurada en tres grandes ejes que van desde el marco institucional y de gobernanza hasta la cultura, la promoción de talento y la sensibilización. Dichos ejes, a su vez, se despliegan en once objetivos generales, con sus correspondientes acciones para lograrlos en un horizonte temporal de corto, medio o largo plazo, e indicadores

concretos para evaluar el avance en esa línea. Se aspira a que los lineamientos aquí sugeridos sean un aporte que contribuya a la discusión plural y el avance hacia el establecimiento de una Estrategia Nacional de Ciberseguridad que como se señaló combine una gestión soberana de los recursos digitales, resiliencia y desarrollo sostenible.

## I. Hacia un nuevo marco de gobernanza

### **1** **Objetivo** Transición hacia una gobernanza nacional de ciberseguridad en México

México enfrenta una brecha institucional significativa en ciberseguridad que excluye parte del ecosistema digital,

limita la capacidad de respuesta ante incidentes y debilita la confianza de ciudadanía y empresas.

#### **A. Crear un órgano rector que articule la gobernanza nacional en ciberseguridad**

Para cerrarla, la transición institucional se iniciaría con la creación inmediata de una Coordinación Nacional de Ciberseguridad dotada de liderazgo político y técnico, integrando lo público y lo privado. Esta Coordinación tendría

la función de ordenar y articular los esfuerzos y actores, garantizando la participación plena del sector privado y estableciendo reglas claras de operación.

## B. Instalar mesas de trabajo temáticas

Esta Coordinación operará mediante cinco mesas público-privadas con objetivos concretos y resultados medibles:

- 1 Mejores prácticas y estándares, para alinear a México con marcos internacionales.
- 2 Red de confianza CERT/CSIRT, que facilite el intercambio ágil de información y alertas.
- 3 Protección de infraestructuras críticas y servicios esenciales digitales frente a una ciber crisis nacional, con un protocolo común y una Mesa Conjunta de Ciber crisis y Resiliencia.
- 4 Vulnerabilidades e incidentes, dedicada a homologar metodologías y playbooks.
- 5 Talento y capacitación, enfocada en educación, concientización y apoyo a grupos vulnerables y MiPyMEs.

Cada mesa contará con líderes designados, miembros permanentes e invitados rotativos según los temas tratados. Esta arquitectura permitirá combinar liderazgo político, soporte técnico y participación multisectorial. Estas

mesas deberán funcionar como instancias ejecutivas, con responsables, plazos y entregables públicos, asegurando transparencia y rendición de cuentas.

## C. Proponer un Marco Nacional de Ciberseguridad

A partir de ello, se recomienda elaborar un Marco Nacional de Ciberseguridad destinado a ordenar la institucionalidad fragmentada y generar insumos para una futura Ley de Ciberseguridad. Este marco integrará a todos los actores del ecosistema y definirá los componentes centrales de una Estrategia Nacional, incluyendo la protección de la identidad digital, un catálogo de infraestructuras críticas y servicios esenciales digitales y la actualización del marco penal frente a nuevos delitos informáticos. Asimismo, impulsará una agenda internacional basada en los compromisos del T-MEC y otros instrumentos multilaterales, garantizando una ruta de largo plazo hacia una política nacional robusta y alineada con las mejores prácticas globales.

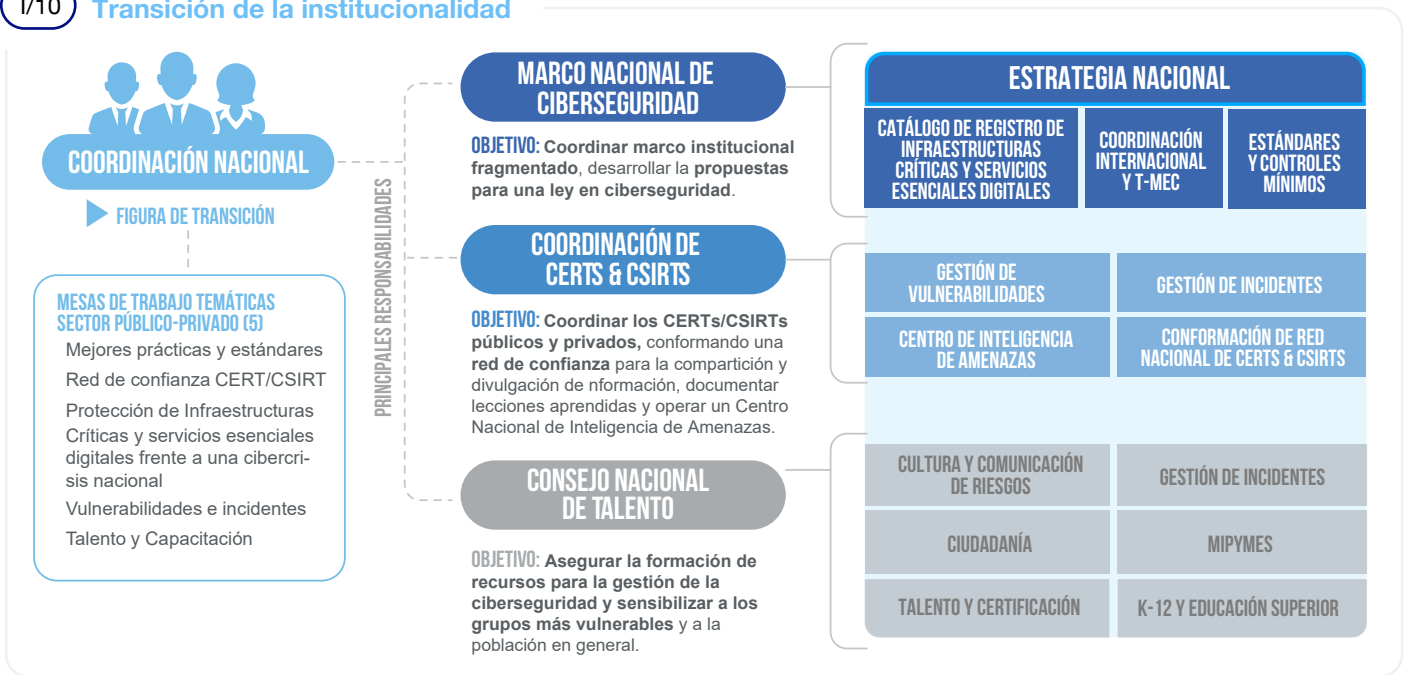
Un componente clave será la coordinación de los CERT/CSIRT. Una red federada de confianza entre equipos públicos, privados y académicos permitirá compartir información, documentar lecciones aprendidas y operar un Centro Nacional de Inteligencia de Amenazas como repositorio de tácticas e indicadores. Esta red deberá estandarizar la gestión de incidentes mediante playbooks comunes y promover la interoperabilidad técnica para responder de forma coordinada a ataques de diversa magnitud. Su eficacia dependerá de estímulos económicos claros y entornos seguros para el intercambio de información sensible.

En el marco de la planeación estratégica para combatir el ciberdelito, se propone fortalecer los mecanismos nacionales de prevención y alerta temprana mediante la creación de sistemas antiscam que permitan identificar y bloquear de manera proactiva sitios fraudulentos y campañas de suplantación de identidad. Asimismo, se recomienda la implementación de listas blancas de páginas y servicios digitales verificados, administradas por la Coordinación Nacional de Ciberseguridad en colaboración con el sector financiero y las empresas de tecnologías de la información y las telecomunicaciones. Estas acciones deben complementarse con un sistema nacional de alertas de amenazas, que difunda de forma oportuna información sobre riesgos emergentes.

Finalmente, se propone crear un Consejo Nacional de Talento en Ciberseguridad, encargado de asegurar la formación de especialistas y fomentar una cultura nacional de ciberseguridad. Este Consejo articulará la capacitación del sector público, la cultura y comunicación hacia la ciudadanía y las MiPyMEs, la incorporación de contenidos en todos los niveles educativos y el desarrollo de un sistema de certificaciones, insignias y microcredenciales alineado con las necesidades del mercado laboral. Así se garantizará tanto la disponibilidad de talento técnico como la construcción de una ciudadanía digital informada y resiliente.



I/10 Transición de la institucionalidad



Fuente: elaboración propia

A través de mesas de trabajo, un marco nacional, una red de confianza CERT/CSIRT, un consejo de talento y una gobernanza multinivel, el país puede sentar las bases de una política pública integral y sostenible. La combinación de ganancias rápidas con entregables estratégicos permitirá avanzar simultáneamente en los temas que ameritan atención inmediata, como la concientización o la capacitación, y en la

construcción de capacidades de largo plazo. Con ello, México no solo cerrará su brecha institucional, sino que también se posicionará como un actor confiable y resiliente en el ecosistema digital global.

Se presentan a continuación las líneas de acción propuestas relativas a la institucionalidad de la estrategia propuesta.

T/02 Líneas de acción institucionalidad

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>INSTITUCIONALIDAD</b>				
1.1	Crear un órgano rector que articule la gobernanza nacional en ciberseguridad	Establecer por decreto la Coordinación Nacional de Ciberseguridad, con secretaría técnica y reglas de operación definidas	00	Coordinación instalada y reglas de operación publicadas
1.2	Instalar mesas de trabajo temáticas	Conformar y formalizar cinco mesas de trabajo (mejores prácticas; red de confianza CERT/CSIRT; ciber crisis nacional; vulnerabilidades e incidentes; talento y capacitación)	00	Actas de instalación y publicación de planes trimestrales de trabajo
1.3	Proponer un Marco Nacional de Ciberseguridad	Elaborar y presentar insumos técnicos para la Estrategia Nacional	00	Insumos publicados y entregados a actores políticos de alto nivel

Fuente: elaboración propia

## Normativa requerida para la implementación del marco institucional de ciberseguridad en México

La consolidación de un marco institucional de ciberseguridad en México requiere de un andamiaje normativo claro, coherente y progresivo, que permita ordenar la institucionalidad fragmentada y dotar al país de una ruta clara de largo plazo. Como parte de la Estrategia Nacional de Ciberseguridad, de carácter flexible y evolutivo, se sugiere

promover una Ley General de Ciberseguridad que establezca las bases jurídicas obligatorias para todos los actores del ecosistema. A ello se suma la necesidad de actualizar el marco penal vigente y de armonizar la legislación nacional con compromisos internacionales, reconociendo que la ciberseguridad trasciende fronteras.

### A. Promover la Ley Nacional de Ciberseguridad

Se requiere la promulgación de una Ley General de Ciberseguridad que establezca un marco general que incluya los fundamentos jurídicos para una gobernanza nacional. Esta ley debe contener, como mínimo, un objeto, alcance y definiciones que delimiten con claridad su aplicación; la designación de una autoridad competente en la coordinación y colaboración multi-actores y la definición de roles y responsabilidades; la identificación y catálogo de infraestructuras críticas y servicios esenciales digitales, incluyendo las cibernéticas; y un marco de gestión de incidentes y vulnerabilidades basado en riesgos. Asimismo, debe contener disposiciones para fortalecer la resiliencia nacional, al incorporar a todos los sectores críticos del país, así como garantizar la transparencia y rendición de cuentas en la actuación de las autoridades. La ley debe ser lo suficientemente robusta para ordenar y articular las capacidades actuales, pero al mismo tiempo incorporar un enfoque prospectivo que impulse la innovación, fomente la cooperación multisectorial y asegure su vigencia frente a la

evolución tecnológica y de las amenazas, evitando quedar anclada en esquemas desactualizados.

Un tema central dentro de este marco normativo debe ser la protección de la identidad digital. La ley y la Estrategia Nacional de Ciberseguridad deben establecer obligaciones claras para los prestadores de servicios críticos, incluyendo la exigencia de autenticación multifactor y contraseñas robustas, la privacidad como configuración predeterminada, la minimización de la recolección de datos, y la obligación de asegurar la protección de la información en todo su ciclo de vida. Además, deben garantizar que las operaciones digitales sean verificables y transparentes, de modo que los usuarios puedan confiar en la integridad de los sistemas y servicios que utilizan. La identidad digital debe ser reconocida como un activo estratégico de la ciudadanía y del Estado, cuya protección es indispensable para la seguridad nacional y la confianza en la economía digital.

I/11

### Marco normativo necesario para la ciberseguridad en México



#### LEY GENERAL DE CIBERSEGURIDAD

- Objeto, alcance y definiciones
- Autoridad competente en la coordinación y colaboración multi-actores
- Definición y catálogo de Infraestructuras críticas y servicios esenciales digitales
- Gestión de Incidentes y prevención vulnerabilidades
- Transparencia y rendición de cuentas



#### PROTECCIÓN DE LA IDENTIDAD DIGITAL

- Establecer obligaciones claras para prestadores de servicios críticos, incluyendo la exigencia de autenticación multifactor y contraseñas robustas
- Considerar la integración de la privacidad desde el diseño
- Minimizar recolección de datos
- Asegurar protección de datos en todo su ciclo de vida
- Asegurar operaciones verificables y transparentes



#### REVISIÓN DE NORMATIVA PENAL

- Evaluar la pertinencia de actualizar el marco penal vigente de forma independiente a la Ley que se propone
- Incorporar tipologías delictivas que respondan a los desafíos contemporáneos, como el ransomware, el robo de identidad digital, la ingeniería social y el uso de la Inteligencia Artificial o tecnologías emergentes



#### T-MEC Y COORDINACIÓN INTERNACIONAL

- T-MEC: revisión del capítulo de ciberseguridad (centrado en cooperación, y no en obligaciones) para adecuarlo a la realidad actual, considerando avances tecnológicos y aumento de amenazas de actores extra regionales desde 2018
- Cooperación Internacional: adhesión al Convenio de Budapest y a la Convención de la ONU sobre ciberdelincuencia, junto con protocolos adicionales y buenas prácticas legales internacionales

Fuente: elaboración propia

### B. Revisar el marco penal existente

Para que la normativa sea efectiva, no basta con prevenir incidentes: también es necesario contar con un marco que permita la persecución y sanción de los delitos informáticos.

En este sentido, se debe evaluar la pertinencia de actualizar el marco penal vigente de forma independiente a la Ley que se propone, incorporando tipologías delictivas que respondan a

los desafíos contemporáneos, como el ransomware, el robo de identidad digital, la ingeniería social y el uso de la Inteligencia Artificial o tecnologías emergentes. Estas adecuaciones deben realizarse en armonía con la cooperación internacional, reconociendo que los delitos cibernéticos rara vez se circunscriben a un solo territorio. En este contexto, resulta fundamental considerar la adhesión de México al Convenio de Budapest sobre Ciberdelincuencia y a la Convención de las Naciones Unidas contra la ciberdelincuencia, incluyendo otros protocolos adicionales y mejores prácticas legales internacionales, lo que permitiría al país integrarse a un esquema global de cooperación judicial y persecución policial en la materia.

En suma, la implementación del marco institucional de ciberseguridad requiere de un esquema normativo integral que combine visión estratégica, bases jurídicas sólidas, protección de la identidad digital y actualización penal. La Estrategia Nacional aportará la flexibilidad y la visión de largo plazo; la Ley General de Ciberseguridad establecerá las obligaciones necesarias; y la adecuación del marco penal, junto con la adhesión a instrumentos internacionales, garantizará la capacidad de sancionar conductas ilícitas en un entorno transnacional. Con este andamiaje, México podrá avanzar hacia una gobernanza nacional de ciberseguridad robusta, resiliente y alineada con las mejores prácticas internacionales.

### T/03 Líneas de acción propuestas para la base normativa

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>BASE LEGAL</b>				
2.1	Promover la Ley Nacional de Ciberseguridad	Generar insumos para su construcción (definiciones y principios; gobernanza y autoridades; catálogo de infraestructuras críticas y servicios esenciales digitales; enfoque basado en riesgos; derechos digitales; identidad digital; cooperación público-privada e internacional)		Insumos incorporados a un anteproyecto de ley
2.2	Revisar el marco penal existente	Conformar un grupo de expertos para revisar las normas penales y proponer actualizaciones conforme a nuevas realidades delictivas		Generación de insumos y análisis técnico-jurídico

Fuente: elaboración propia

## 3 Protección de infraestructuras críticas y servicios esenciales digitales

Dentro de las urgencias para la protección del ecosistema digital de un país, las infraestructuras críticas y los servicios esenciales digitales constituyen un campo de trabajo de

importancia estratégica, cuya afectación podría representar una catástrofe de niveles impredecibles.

### A. Adoptar un marco normativo para infraestructuras críticas y servicios esenciales digitales

Las infraestructuras críticas son aquellos activos estratégicos, sistemas, instalaciones físicas y servicios esenciales digitales para el funcionamiento de la sociedad, la economía y el funcionamiento de los Estados. Incluyen sectores como energía, transporte, salud, agua, telecomunicaciones, finanzas y administración pública. La indisponibilidad o interrupción de estos servicios que se originen en un incidente de ciberseguridad pueden comprometer gravemente la seguridad nacional, el bienestar ciudadano, la reputación del gobierno y la estabilidad económica, razones por las que requieren una protección puntual.

Es clave este concepto amplio e integral de las infraestructuras críticas que incluye también los servicios esenciales digitales, entendidos como aquellos sistemas y plataformas cuya interrupción comprometería la continuidad de funciones sociales, financieras o económicas vitales (como los servicios de salud, energía, comercio digital, transporte, telecomunicaciones, de nube o identidad digital). Esto permite

reconocer que, en la era digital, la indisponibilidad o alteración de un servicio en línea puede tener impactos equivalentes a los de una infraestructura física. En consecuencia, el marco nacional de protección debe definir tanto los sectores críticos tradicionales como los servicios esenciales digitales y sus interdependencias, establecer umbrales de severidad y obligaciones de reporte, e integrar mecanismos de supervisión y respuesta coordinada.

De la misma manera, las infraestructuras críticas cibernéticas o de información están conformadas por un subconjunto de infraestructuras relacionadas con las redes, sistemas y servicios de tecnologías de la información y las comunicaciones (TIC). Comprenden tanto las redes de telecomunicaciones, centros de datos, servicios en la nube y sistemas de control industrial, como plataformas digitales que sostienen la operación de sectores estratégicos.

En este sentido, regiones como la Unión Europea han optado

por la designación de infraestructuras críticas y a partir de esta definición surgen los sectores y subsectores, constituidos por los Sistemas de información, las redes y la infraestructura TIC, es decir, las infraestructuras críticas cibernéticas o de información de cada infraestructura crítica identificada. En el caso de Argentina, las definiciones y la designación de los 11 sectores fueron establecidos por Resolución 1523/2019<sup>26</sup> y la designación de una Infraestructura crítica de Información, en este caso el GDE, el Sistema de Gestión Documental Electrónica de la Administración Pública Nacional fue directamente establecida a partir del Sector Administración pública por Resolución 36 de 2020.

Por otro lado, Colombia definió 13 sectores de infraestructuras crítica en 2015, y el ColCERT (Centro nacional de respuesta ante incidentes) emitió lineamientos y lidera el proceso de identificación de las infraestructuras críticas cibernéticas, con base en el Decreto 338 de 2022

En el caso de Estados Unidos, la definición de los sectores se dio primero mediante la Directiva presidencial Nro 7 en 2003<sup>27</sup>, con el objetivo de que los departamentos y agencias federales

identifiquen y prioricen la infraestructura crítica y los recursos clave de los Estados Unidos y los protejan de ataques terroristas, y luego la Directiva 21 de 2013 estableció una política nacional para fortalecer la seguridad y resiliencia de la infraestructura crítica como una responsabilidad compartida entre los niveles de gobierno federal, estatal, local, tribal y territorial, junto con los propietarios y operadores públicos y privados de dicha infraestructura.

El propósito central de la Directiva 21(en EE. UU.) fue asegurar sistemas y activos vitales, como la energía y las comunicaciones, contra todas las amenazas, incluyendo ataques físicos y cibernéticos, para que puedan resistir y recuperarse rápidamente de interrupciones, incluyendo al Secretario de Seguridad Nacional como guía estratégico, y designar Agencias Específicas Sectoriales para 16 sectores de infraestructura distintos, promoviendo una unidad de esfuerzo nacional a través de la coordinación, el análisis integrado y el intercambio eficiente de información<sup>28</sup>. Este lineamiento fue ratificado y ampliado por la Ley de Protección de Infraestructuras críticas de 2014<sup>29</sup>.

## I/12 Sectores prioritarios para Estados Unidos, Colombia y Argentina



### ESTADOS UNIDOS 2014 16 SECTORES

ESTABLECIMIENTO DESDE 2001 DE LA DEFINICIÓN, DESDE 2007 DE 16 SECTORES POR LEY:

- Química
- Instalaciones comerciales
- Comunicaciones
- Manufactura crítica
- Presas
- Base industrial de defensa
- Servicios de emergencia
- Energía
- Servicios financieros
- Alimentación y agricultura
- Instalaciones gubernamentales
- Atención médica y salud pública
- Tecnologías de la información
- Reactores nucleares, materiales y residuos
- Sistemas de transporte
- Sistemas de agua y aguas residuales



### COLOMBIA 2015 13 SECTORES

ESTABLECIMIENTO DE SECTORES DESDE 2015 E ICC POR DTD. 338 DE 2022:

- Alimentación Y Agricultura
- Agua
- Comercio, Industria, Turismo
- Defensa
- Educación
- Electricidad
- Financiero
- Gobierno/Estado
- Recursos Naturales-Medio Ambiente
- Recursos Minero-Energéticos
- Salud y Protección Social
- Tecnologías de la Información y Comunicaciones
- Transporte



### ARGENTINA 2019 11 SECTORES

ESTABLECIMIENTO DESDE 2019 DEFINICIONES Y SECTORES POR RES. SGM 1523/ 2019:

- Energía
- Tecnologías de Información y Comunicaciones
- Transportes
- Hídrico
- Salud
- Alimentación
- Finanzas
- Nuclear
- Químico
- Espacio
- Estado

Fuente: elaboración propia

Es así como el fortalecimiento en ciberseguridad de los sectores identificados como críticos podría ser abordado para los aspectos cibernéticos por los organismos públicos reguladores o con competencia en la materia con recomendaciones o normativas sectoriales. No obstante, la coordinación de los niveles estratégicos es necesaria tanto para tener una visión general de gestión de riesgos de todos los sectores, como para el establecimiento de canales de coordinación, para que una vez fortalecidos dichos

instrumentos, puedan establecerse protocolos para una respuesta a las crisis.

Un ejemplo claro de madurez se da en el ámbito financiero, uno de los sectores históricamente más afectados en materia de ciberataques, que en todos los países es uno de los que más trabajo ha invertido en el mejoramiento de ciberseguridad, dada la naturaleza del activo en custodia tanto propio como de la ciudadanía.

26. [Resolución ex Secretaría de Modernización 1523/2019](#), de la Jefatura de Gabinete de Ministros.

27. [Directiva Presidencial de Seguridad Nacional 7](#), de 2003.

28. [Directiva Presidencial 21](#) de Estados Unidos de 2013.

29. [H.R.3696](#) - National Cybersecurity and Critical Infrastructure Protection Act of 2014.

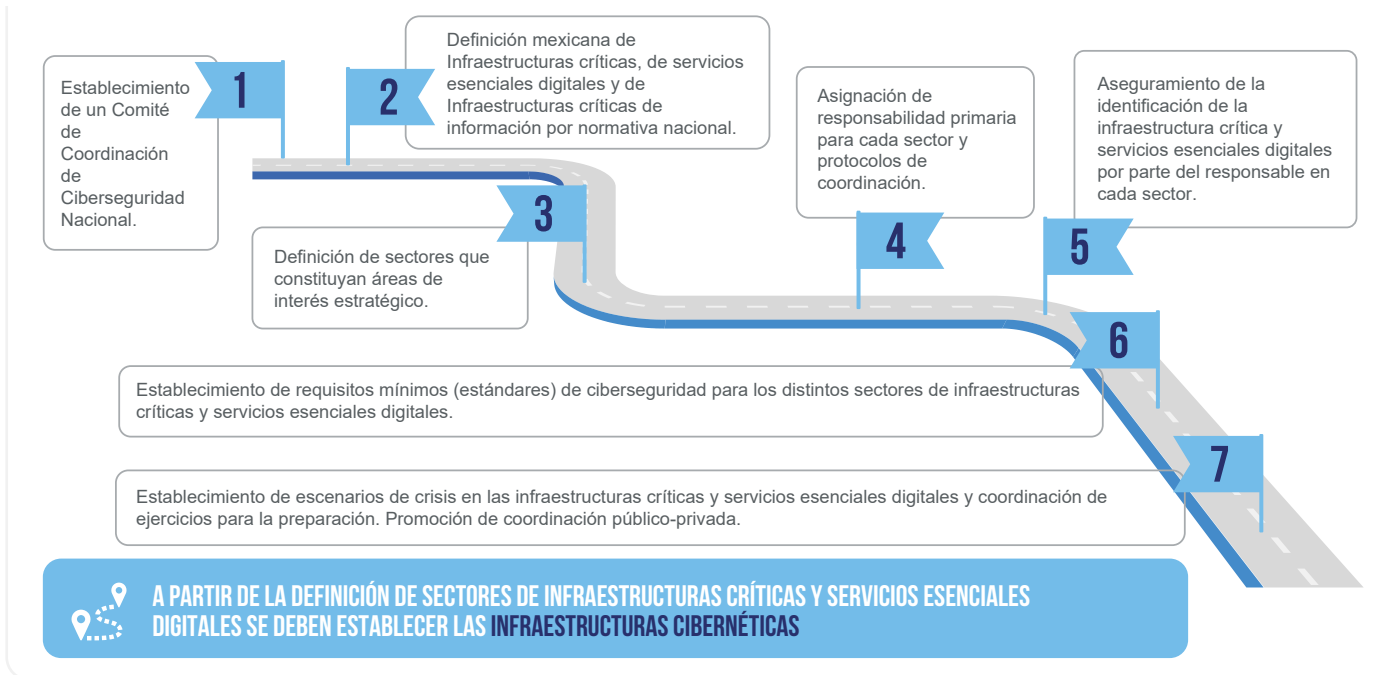
## B. Establecer definiciones, criterios, y catálogos de infraestructuras críticas y servicios esenciales digitales

Entre las acciones institucionales que los países realizan en el camino hacia la madurez está la definición de las infraestructuras críticas y los servicios esenciales digitales, la identificación de los diferentes sectores y el establecimiento de responsabilidades por ley, así como la implementación

de medidas mínimas de ciberseguridad y notificación de incidentes. Luego de las definiciones de los sectores se debe establecer lineamientos o metodologías que permitan identificar las infraestructuras críticas cibernéticas o de información.

I/13

### Hoja de ruta propuesta para el fortalecimiento de la ciberseguridad en infraestructuras críticas y servicios esenciales digitales



Fuente: elaboración propia

Analizando el panorama internacional, se sugiere establecer un rol de responsable de la protección de infraestructuras críticas y servicios esenciales digitales que establezca las definiciones básicas realizando una amplia convocatoria para buscar consensos de las partes interesadas, con participación pública y privada. Definir los sectores que consideran críticos y los subsectores tal como el Sector de la Energía y los subsectores, electricidad, petróleo y gas, de acuerdo a los intereses estratégicos y de soberanía. Algo común en todos

los casos analizados es el establecimiento de medidas de protección para las infraestructuras críticas dentro de los sectores dadas las similitudes internas.

También se deberán establecer los umbrales de criticidad para las infraestructuras críticas y servicios esenciales digitales, así como metodologías de identificación dentro de cada sector y subsector. Entre los criterios observados se encuentra el tipo de impacto que puede tener un incidente:

**En la vida humana:** riesgo de pérdida de vida o grave amenaza a la salud e integridad física.

**Económico:** daño o amenaza de daño grave a la estructura productiva y/o financiera del país.

**En el medio ambiente:** afectación negativa o daño grave al espacio en el que se desarrolla la vida de los seres vivos.

**En el ejercicio de los derechos humanos y de las libertades individuales:** restricción o coartación indebida y colectiva del pleno ejercicio de los derechos.

**Impacto público o social:** acontecimientos susceptibles de provocar grave conmoción en una parte significativa de la población.

**En el ejercicio de las funciones del Estado:** afectación sustancial del normal desempeño de los poderes Ejecutivo, Legislativo o Judicial.

**En la soberanía nacional:** cuestionamiento o restricción del poder del Estado Nacional en el territorio.

**En la integridad territorial nacional:** vulneración de las fronteras territoriales, marítimas o espaciales

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS, INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y SERVICIOS ESENCIALES DIGITALES</b>				
3.1	Adoptar un marco normativo para infraestructuras críticas de información	Asignar responsabilidades para la definición de normas de protección por sector		Propuesta de roles para funciones de PIC
3.2	Establecer definiciones, criterios, y catálogos de infraestructuras críticas y servicios esenciales digitales	Definir formalmente las categorías de infraestructuras críticas y servicios esenciales digitales y sus sectores y subsectores		Propuesta normativa consensuada entre sector público y privado
3.3	Establecer definiciones, criterios, y catálogos de infraestructuras críticas y servicios esenciales digitales	Definir criterios y metodología para la identificación de las ICC		Propuesta normativa consensuada para la identificación de las ICC

Fuente: elaboración propia

## OBJETIVO

## 4

## Bases para fortalecer la cooperación internacional

La cooperación internacional se considera fundamental y esencial debido a la naturaleza transfronteriza y global de las ciberamenazas, el ciberdelincuencia y la ciberseguridad. Este enfoque debería constituir un principio rector de la estrategia

de la ciberseguridad, buscando fortalecer la seguridad digital nacional a través de alianzas estratégicas y la integración con la comunidad global.

## A. Establecer líneas de cooperación internacional

Entre los propósitos se puede mencionar: aunar esfuerzos y colaborar para la detección y respuesta a amenazas, incidentes y ataques, y el combate al ciberdelincuencia; fomentar la confianza entre naciones y el sector privado, contribuyendo a la resiliencia, estabilidad, la paz y la seguridad internacional; mejorar la capacidad de resiliencia global y nacional frente a incidentes transnacionales, promover el desarrollo de la ciberseguridad mediante el intercambio de buenas prácticas, tecnologías y asistencia técnica en foros internacionales especializados como FIRST y finalmente posicionar al país como un actor clave y confiable en la gobernanza del ciberespacio.

El abordaje de la cooperación internacional se puede llevar adelante a través de diversos mecanismos formales e informales, involucrando a múltiples partes interesadas.

Es fundamental armonizar los esfuerzos nacionales e internacionales mediante instrumentos jurídicos y diplomáticos que fortalezcan la cooperación en materia de ciberdelincuencia. Destacan el Convenio de Budapest sobre la Ciberdelincuencia<sup>30</sup>, principal instrumento global para la cooperación penal y transfronteriza en la investigación de delitos informáticos, y el Convenio de las Naciones Unidas sobre la Ciberdelincuencia (2024)<sup>31</sup>, recientemente aprobado por la Asamblea General, que amplía el alcance de la cooperación internacional bajo los principios de soberanía, proporcionalidad y respeto de los derechos humanos.

Para asegurar la efectividad de la Estrategia, se recomienda adoptar como referencia los 18 Controles Críticos de Seguridad (CIS Critical Security Controls v8) del Center for Internet Security (CIS), reconocidos internacionalmente como buenas prácticas para la gestión de riesgos cibernéticos.

30. [Convenio sobre la ciberdelincuencia](#), Budapest, 2001.

31. [Convención de las Naciones Unidas contra la Ciberdelincuencia](#): Fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de Tecnología de la Información y las Comunicaciones y para la Transmisión de Pruebas en Forma Electrónica de Delitos Graves.



Fuente: elaboración propia




Sería deseable que se promueva activamente el intercambio de información de ciberinteligencia y la coordinación de respuestas, reconociendo que el conocimiento es clave para la preparación ante amenazas emergentes, mediante sistemas de Intercambio de información cibernética y de

vulnerabilidades (a menudo utilizando plataformas como MISP) entre actores nacionales e internacionales, también a través de la coordinación de CSIRT y la realización de ejercicios conjuntos de simulacro de ciberseguridad y de crisis a escala nacional e internacional.

## B. Fortalecer las capacidades de ciberdiplomacia

Adicionalmente, la cooperación internacional (ciberdiplomacia) debe ser un principio rector de trabajo, buscando la colaboración en la detección y respuesta a amenazas transfronterizas.

México debe fortalecer sus capacidades de ciberdiplomacia y establecer acuerdos de asistencia mutua con naciones de confianza para el intercambio de información y la coordinación de la agenda en foros internacionales en materia de prevención de incidentes.

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>COOPERACIÓN INTERNACIONAL</b>				
4.1	Establecer líneas de cooperación internacional	Participar activamente en foros transnacionales prioritarios en materia de ciberseguridad		Participación anual en foros transnacionales (#)
4.2	Establecer líneas de cooperación internacional	Suscribir acuerdos de asistencia mutua para el intercambio de información sobre amenazas		Convenios vigentes con entidades de confianza o proveedores de seguridad
4.3	Fortalecer las capacidades de ciberdiplomacia	Crear un foro interinstitucional para que la cancillería coordine la agenda internacional de ciberseguridad		Propuesta de mecanismos de coordinación interinstitucional sistemática

Fuente: elaboración propia

## II. Fortalecimiento del Sistema Nacional de Gestión de Crisis y Respuesta a Incidentes Cibernéticos

OBJETIVO

5

### Construir liderazgo y fortalecimiento de la gestión de incidentes a nivel nacional

La ampliación de capacidades nacionales de gestión ante incidentes cibernéticos representa el punto de apoyo para la construcción de los mecanismos técnicos necesarios en

materia de instituciones expertas para un entorno público que genere confianza digital para la sociedad en su conjunto.

#### A. Construir liderazgo y fortalecer la gestión de incidentes a nivel nacional

Consideramos que sería valioso el diseño de un marco institucional que brinde las competencias para la elaboración de políticas para crear y fortalecer una red de confianza de equipos de respuesta ante incidentes cibernéticos que reúna a entidades públicas y privadas para que pueda ser un

instrumento de contención en momento en que los incidentes ocurran y como medio para compartir información de calidad en materia de ciberseguridad. Con esta finalidad sería necesario establecer de puntos de confianza y compromisos consensuados.

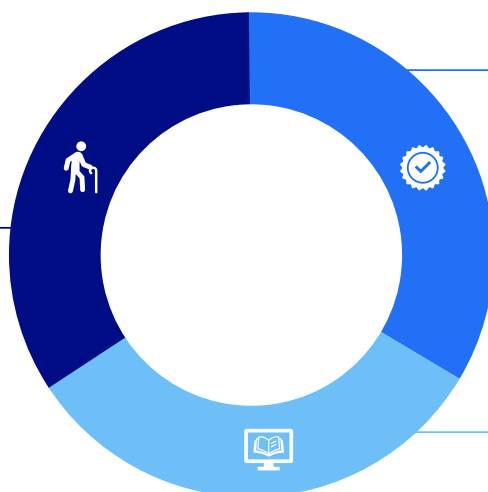
I/15

#### Aspectos clave para el ecosistema de ciberseguridad

##### ASPECTOS CLAVE:

###### MADUREZ DEL ECOSISTEMA

- Desarrollo de cursos de formación y servicios de consultoría.
- Auditorías, elaboración de guías técnicas y promoción de buenas prácticas.
- Criterios y estándares internacionales comunes para una eficiente coordinación entre los equipos de gestión de crisis públicos (CERT MX) y privados.



###### RED DE CONFIANZA OPERATIVA

- Establecimiento de puntos de confianza para compartir y divulgar información de amenazas mediante un programa de adhesión voluntaria
- Fomento de la cooperación público-privada.
- Intercambio de amenazas, incidentes y vulnerabilidades en tiempo real.

###### IMPULSO A CAPACIDADES LOCALES

- Promoción y fortalecimiento de nuevos equipos de respuesta a incidentes (CERTs/CSIRTs).
- Fomento de la colaboración interinstitucional y territorial.

Fuente: elaboración propia

Hasta tanto se puedan obtener los consensos legislativos para contar con un marco regulatorio, se considera oportuno la conformación de una red de confianza mediante un programa de adhesión voluntaria para compartir información de alertas de ciberseguridad y de amenazas, para que las novedades puedan circular de manera rápida y por canales respaldados por la red a una mayor cantidad de organizaciones de distinto tipo y tamaño.

La emisión y circulación de alertas nacionales en materia de vulnerabilidades técnicas y de amenazas desde una autoridad nacional en ciberseguridad constituye hoy una necesidad urgente para evitar que sean aprovechadas por actores maliciosos y de esta manera evitar incidentes. En particular, lograr la más amplia distribución con la mayor capilaridad sectorial y territorial también debería ser un objetivo. Poder llegar a las pequeñas y medianas empresas, a las escuelas e instituciones educativas de todos los niveles,

las clínicas y otras entidades que brindan servicios de salud y a otros sectores debería ser un objetivo para proteger los servicios digitales y a las personas usuarias. Por otro lado, la información de amenazas que circula también representa una oportunidad para evitar nuevos incidentes desde el análisis e investigación de piezas de malware y su comportamiento en distintos entornos. El análisis exhaustivo y direccionado a los distintos sectores puede ser una barrera de prevención eficaz.

Entendemos que construir una red de confianza requiere de tiempo y trabajo para el que consideramos importante crear un liderazgo nacional que permita coordinar los esfuerzos tanto de las administraciones públicas como de la industria. En este sentido se propone una coordinación que pueda desempeñar ese liderazgo para analizar, compartir y establecer estándares de trabajo así como buenas prácticas respecto de los distintos servicios que los equipos puedan brindar.

I/16 **Responsabilidades del coordinador de CERTs & CSIRTs**



**AUTORIDAD TÉCNICA ESPECIALIZADA**

- Organismo designado con conocimiento técnico en ciberseguridad.
- Experto en estándares internacionales y buenas prácticas de respuesta a incidentes.
- Ejercicios de simulación de crisis.



Fuente: elaboración propia

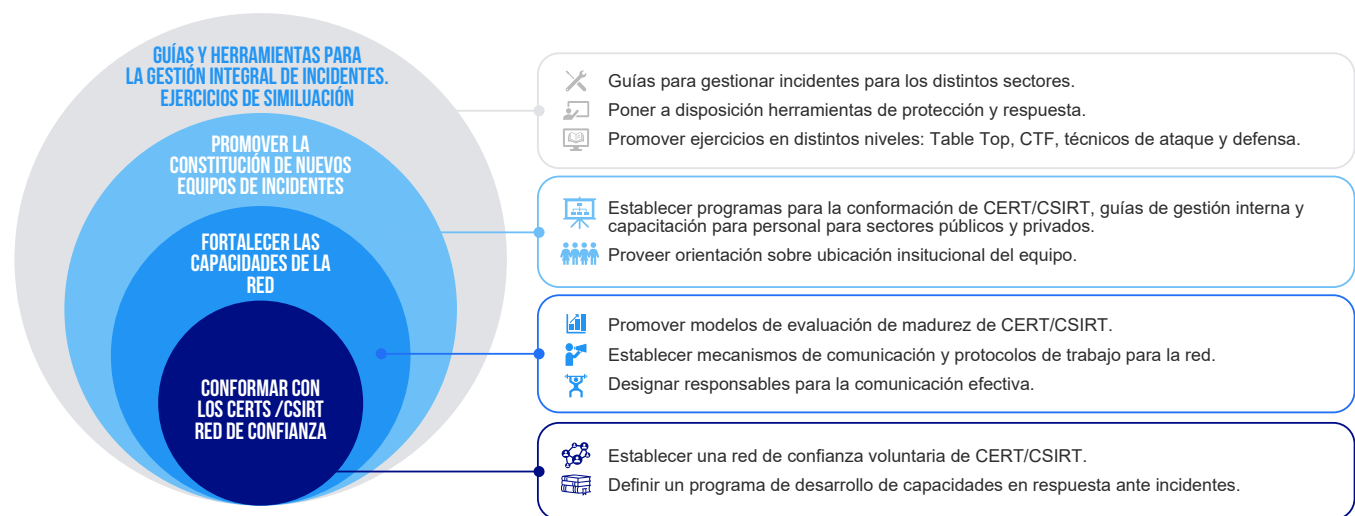
México cuenta con un conjunto de CSIRT que le permitiría construir una red de confianza desde una base firme para avanzar tanto en el fortalecimiento y mejoras de capacidades o áreas de servicios de aquellos equipos existentes, así como de cantidad, para lograr mayor cobertura en cuanto al territorio y las características particulares de cada región. Es decir, una red de confianza que pueda brindar servicios a los distintos sectores o comunidades de atención como indican las buenas prácticas. En este sentido a modo de guía internacional y de referencia pueden seguirse las publicaciones de FIRST y en particular su framework sobre área de servicios para CSIRT, promovido por los expertos en la materia.

Dado que el país cuenta a la fecha con 27 CERT/CSIRT públicos y privados registrados en la organización internacional especializada FIRST, surge que podría realizarse una convocatoria voluntaria para formar una red que permita crecer y fortalecerse de manera colaborativa. En todos los aspectos de la ciberseguridad la participación del sector privado y en especial de la industria de tecnologías de la información es central y en materia de prevención y respuesta ante incidentes también. Los servicios especializados así como los recursos de la industria pueden aportar conocimiento e innovación al ecosistema potenciando las capacidades.

**27** equipos CERT/CSIRT entre públicos y privados en México en la red First\*

\* Aunque son más de 40 considerando los que no pertenecen a First

I/17 **Responsabilidades del coordinador de CERTs & CSIRTs**



LA GESTIÓN DE CRISIS CIBERNÉTICAS DEBE FORTALECERSE MEDIANTE LA IDENTIFICACIÓN DE ESCENARIOS NACIONALES DE ALTO IMPACTO Y LA PLANIFICACIÓN DE EJERCICIOS DE SIMULACIÓN

Fuente: elaboración propia

Por otro lado consideramos que promover programas de formación en esta temática brindaría recursos humanos calificados para alimentar a los elementos de esta red. Cada área de servicio conforma un área de expertise en la que se pueden mejorar los procesos, las herramientas y las habilidades de las personas.

Como hoja de ruta para el fortalecimiento de capacidades sería muy valioso que se puedan adoptar marcos de

evaluación internacional para los servicios de las unidades que brindan respuesta ante incidente y para ello la realización de programas de autoevaluación puede ser un camino para mejorar de manera continua y sistemática. La Open CSIRT Foundations mantiene un modelo de madurez denominado SIM3 que puede ser utilizado para este tipo de evaluaciones que mide la eficacia con la que un equipo gestiona, documenta y realiza sus funciones.

## Marco de Servicios de Gestión de incidentes para equipos de Respuesta

El Marco de Servicios para Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), desarrollado por expertos de la comunidad FIRST, describe buenas prácticas para

facilitar el establecimiento y la mejora de las operaciones de los CERT/CSIRT. El conjunto de áreas de servicio fundamentales que se recomienda adoptar se compone de:

### GESTIÓN DE EVENTOS.

Se trata de identificar proactivamente incidentes mediante el análisis y la correlación de eventos de seguridad provenientes de diversas fuentes de datos que deberían analizarse en sus contextos.

### GESTIÓN DE INCIDENTES.

Está en el corazón de cualquier CSIRT y es vital para ayudar a integrantes de la comunidad de atención durante un incidente o ataque. Adoptarla garantiza una respuesta estructurada y experta.

Incluye:

- **Análisis de incidentes:** se trata de obtener una comprensión profunda del incidente confirmado y su impacto actual o potencial, identificando las causas raíz (vulnerabilidades o debilidades). El resultado es un mayor conocimiento de los detalles clave del incidente (alcance, impacto, ataques/exploits y remediaciones), fundamental para una mitigación efectiva.
- **Mitigación y recuperación:** se trata de contener el incidente, limitar el número de víctimas y asistir en la recuperación de los daños causados. Además, se restaura la integridad de los sistemas y la capacidad de servicio de la red y los sistemas que hayan sido comprometidos.
- **Coordinación de incidentes:** consiste en garantizar la distribución oportuna de notificaciones y de información precisa, así como en realizar un seguimiento efectivo del estado de las actividades de respuesta, asegurando una coordinación exitosa gracias a que los participantes y las partes interesadas se mantienen bien informados.

### GESTIÓN DE VULNERABILIDADES.

Se encarga de manejar vulnerabilidades tanto desconocidas como conocidas, con el fin de prevenir su explotación.

Incluye:

- **Descubrimiento e investigación:** Buscar activamente o aprender sobre nuevas vulnerabilidades (previamente desconocidas).
- **Coordinación:** Intercambiar información y coordinar actividades con participantes involucrados en un proceso de divulgación coordinada de vulnerabilidades (CVD).
- **Difusión:** Compartir información sobre vulnerabilidades conocidas a la comunidad. Los destinatarios del servicio podrán evitar la potencial explotación de vulnerabilidades conocidas, detectarlas y mitigarlas.
- **Respuesta:** Accionar de manera activa sobre la información de vulnerabilidades conocidas para prevenirlas, detectarlas y remediarlas/mitigarlas, de esta manera se previene o reduce la exposición a la amenaza de explotación de una vulnerabilidad.



### LA DIVULGACIÓN COORDINADA DE VULNERABILIDADES (CVD)

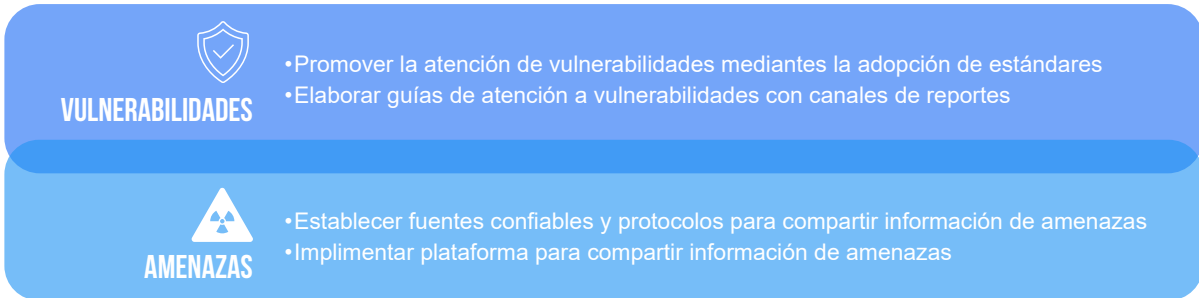
consiste en que, cuando un investigador detecta una falla, la reporta de forma confidencial al fabricante o a un **CSIRT/CERT**, en lugar de hacerla pública de inmediato. El equipo de respuesta coordina con la organización afectada para analizar el fallo, desarrollar un parche y, solo después de corregido, divulgar la información técnica y las medidas de mitigación. Estas acciones contribuyen al marco internacional ya que se reduce la exposición a ataques y fortalece la confianza entre actores públicos y privados, fomentando la responsabilidad compartida y la resiliencia global, especialmente frente a vulnerabilidades que afectan infraestructuras críticas interconectadas.

## CONCIENCIA SITUACIONAL.

Entender el entorno de amenazas, las vulnerabilidades y los riesgos para actuar de forma proactiva. Es fundamental para monitorear continuamente la postura de seguridad, evaluar riesgos, detectar ataques y coordinar respuestas adecuadas que protejan los activos críticos y garanticen la continuidad del negocio. Requiere integrar información de múltiples fuentes, analizarla en tiempo real y visualizar de forma clara y actualizada.

I/18

### Vulnerabilidades y amenazas a considerar en la visibilidad de los CSIRT



Fuente: elaboración propia

## TRANSFERENCIA DE CONOCIMIENTO.

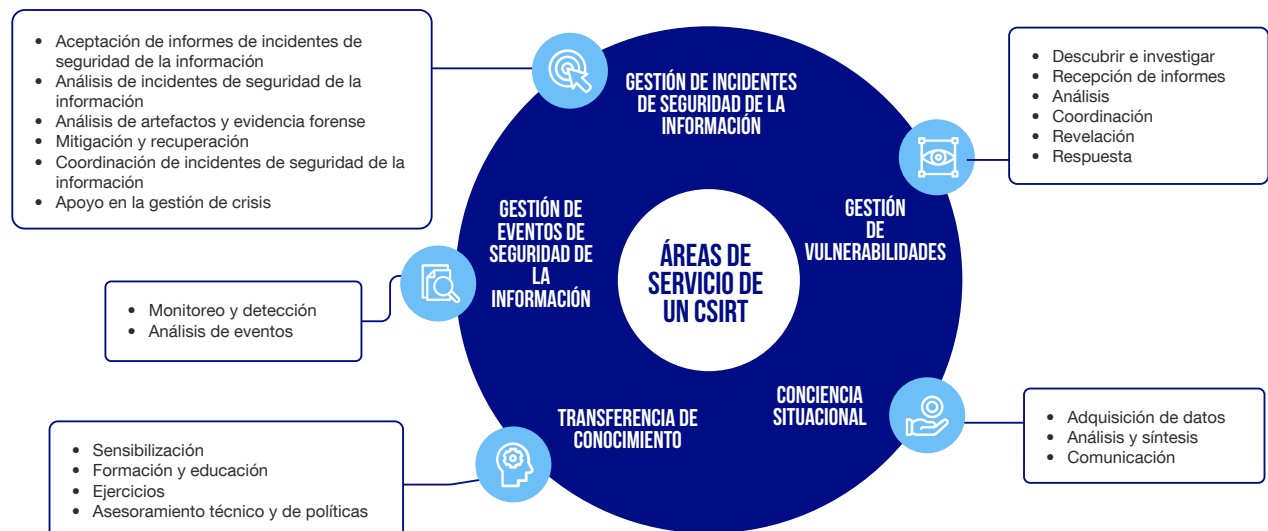
Los CSIRT deben garantizar la difusión sistemática del conocimiento adquirido (incluyendo análisis, tendencias y evaluación de riesgos) con el fin de fortalecer la ciberseguridad colectiva y promover mejores prácticas operativas dentro de su comunidad.

Esta función abarca:

- **Capacitación, educación y cultura:** Se trata de generar instancias de capacitación e impulsar cultura en temas de ciberseguridad y gestión de incidentes. Un programa consistente en formación permite adquirir métodos para detectar, prevenir o responder a amenazas.
- **Desarrollo de conciencia:** Aumenta la cultura de seguridad general de la comunidad, asegurando que sus integrantes están informados sobre los eventos, actividades y tendencias que pueden afectar su capacidad de operar de manera segura, y los pasos a seguir para prevenir y mitigar amenazas.
- **Ejercicios:** Se trata de realizar simulacros para evaluar y mejorar la efectividad y eficiencia de los servicios y funciones de ciberseguridad. Esto resulta en una mejora de la efectividad y eficiencia de los servicios y la identificación de oportunidades para futuras mejoras.
- **Asesoramiento técnico y de políticas:** Asegura que las políticas y procedimientos incluyan consideraciones apropiadas de gestión de incidentes. De esta manera, los integrantes de la comunidad pueden tomar decisiones organizacionales basadas en las mejores prácticas de seguridad que incorporan continuidad del negocio y recuperación ante desastres.

I/19

### Áreas de servicio de los CSIRT



Fuente: elaboración propia a partir de [FIRST CSIRT Services Framework](#)

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>COORDINACIÓN DE RESPUESTA A INCIDENTES</b>				
5.1	Construir liderazgo y fortalecer la gestión de incidentes a nivel nacional	Definir y establecer un marco institucional que promueva, dirija y coordine prevención y respuesta a incidentes	00	Plan nacional de coordinación con responsabilidades y estrategias definidas
5.2	Construir liderazgo y fortalecer la gestión de incidentes a nivel nacional	Establecer puntos de confianza mediante un programa de adhesión voluntaria para divulgar alertas y compartir información sobre vulnerabilidades críticas	00	Cantidad de CERT/CSIRT adheridos a la red nacional de confianza

Fuente: elaboración propia

## 6 Asegurar capacidades para abordar crisis cibernéticas como prueba de la madurez en la respuesta a incidentes

Una óptima respuesta a una crisis nacional originada por un incidente de ciberseguridad requiere de capacidades (CERT/CSIRT) disponibles en todos los sectores y en todo el territorio nacional, con recursos técnicos y competencias operativas

y de comunicación de manera tal de asistir cuando se las convoque. En un modelo ideal se cuenta con protocolos de actuación, ejercicios que se han probado y un rol de coordinador nacional.

### A. Construir capacidades para abordar escenarios de crisis cibernéticas a nivel nacional

Es deseable primero fortalecer las capacidades de respuesta ante incidentes y ampliar la cantidad de equipos de la manera más capilar posible (para más detalle, ver el apartado de Respuesta ante incidentes). No obstante, sería recomendable que, con las capacidades existentes, se realice una planificación de ejercicios que puedan poner a prueba distintos escenarios y obtener lecciones a incorporarse en las propuestas regulatorias o institucionales.

En la regulación europea, por ejemplo, primero se estableció la creación obligatoria de un equipo de respuesta a incidente nacional por cada país (Directiva NIS1), para luego establecer una red de confianza entre estos equipos y varias otras directivas para el fortalecimiento de ciberseguridad (NIS2).

Recién aquí es posible establecer una definición y obligaciones para las “ciber crisis” o más precisamente para incidentes de ciberseguridad a gran escala. En esta materia también sería conveniente que en una Estrategia Nacional de Ciberseguridad se incorpore un rol para el análisis y el establecimiento de criterios, umbrales y mecanismos para definir una crisis de esta naturaleza, así como los protocolos a seguir de acuerdo a las capacidades existentes con la planificación de mejoras sistemáticas y medibles. Los protocolos deberán abordar simulacros, la planificación, la detección, la respuesta y la recuperación ante ciberincidentes relevantes, con umbrales para que la detección pueda ser efectiva. Como así también contener las acciones para incorporar las lecciones aprendidas en un ciclo de mejora continua.



### CICLO DE VIDA DE UN INCIDENTE

#### INCIDENTE

Evento que compromete la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o de los servicios ofrecidos o accesibles a través de la red y sistemas de información.

#### INCIDENTE SIGNIFICATIVO

Incidente que ha causado o es capaz de causar una perturbación operativa grave de los servicios, o una pérdida financiera para la entidad de que se trate; ha afectado o puede afectar a otras personas físicas o jurídicas, causando daños materiales o morales considerables.

#### INCIDENTE DE GRAN ESCALA

Incidente que causa un nivel de perturbación que supera la capacidad de respuesta de un Estado.

#### CIBERCRISIS

Incidente de ciberseguridad a gran escala que se ha convertido en una crisis que no permite el correcto funcionamiento del mercado interior, o plantea graves riesgos para la seguridad pública y la protección de ciudades o ciudadanos.

Fuente: elaboración propia en base a [infografía de ENISA](#)

Por sus características los incidentes de ciberseguridad pueden comenzar pequeños por su alcance y extenderse a través de las redes e interconexiones de manera que su impacto y daños aumenten.

La gestión de las ciber crisis se debe apoyar en marcos y estructuras coordinadas a nivel nacional y estatal, para eso se debe planificar y establecer los roles necesarios a través de planes a corto, mediano y largo plazo que contemplen el desarrollo y la coordinación de las capacidades técnicas, operativas e institucionales.

**T/07** Líneas de acción de la madurez de la respuesta a incidentes

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>MADUREZ DE LA RESPUESTA A INCIDENTES</b>				
6.1	Construir capacidades para abordar escenarios de crisis cibernéticas a nivel nacional	Identificar escenarios de ciber crisis con alto impacto y documentar partes interesadas y responsabilidades		Plan de trabajo con tres escenarios y partes interesadas por cada uno
6.2	Construir capacidades para abordar escenarios de crisis cibernéticas a nivel nacional	Planificar y ejecutar ejercicios nacionales de simulación de ciberataques y elaborar planes de mejora		Cantidad anual de ejercicios de simulación de ciberataques

Fuente: elaboración propia

### III. Priorización del desarrollo de talento y de la promoción de una cultura en ciberseguridad

#### 7 Creación de un Consejo Nacional de Talento para una oferta de formación relevante y actual

La gestión de talento y el desarrollo de una fuerza laboral capacitada en ciberseguridad debe ser una parte central en la elaboración de una Estrategia Nacional de Ciberseguridad. No hay ciberseguridad sin especialistas que la apliquen. Tal es así, que todas las Estrategias recientemente publicadas en

la región comparten este objetivo. La necesidad de abordar la brecha de talento en ciberseguridad es considerada urgente, ya que la demanda de profesionales especializados sigue creciendo y desafortunadamente más del 65% las vacantes existentes a nivel mundial no son cubiertas.

##### A. Realizar un diagnóstico de la brecha laboral

Según la OCDE, entre 2021 y 2022, el número de ofertas de empleo en línea (OJPs) en ciberseguridad en México se incrementó en un 64,6%, superando el crecimiento del 27,3% observado en otras profesiones<sup>32</sup>. Las búsquedas se concentran geográficamente, con un 62,7% de las ofertas publicadas en ciudades metropolitanas. Esta concentración está impulsada por industrias clave como la manufactura de productos electrónicos, que representa el 28% de las OJPs, además de los sectores de finanzas y tecnología. A pesar de esta fuerte demanda, México enfrenta un déficit significativo en la fuerza laboral especializada. El informe cita estimaciones

que indican una escasez de 260.000 profesionales de ciberseguridad en el país para 2022, la segunda más grande de la región.

Si bien datos recientes son más alentadores, como el informe de 2024 de la ISC2 que estima la brecha en Brasil y México en 328.397 personas, una disminución del 5,7% respecto al año anterior<sup>33</sup>, postergar la solución a este desafío supondría graves consecuencias para la estabilidad económica y la protección del país.

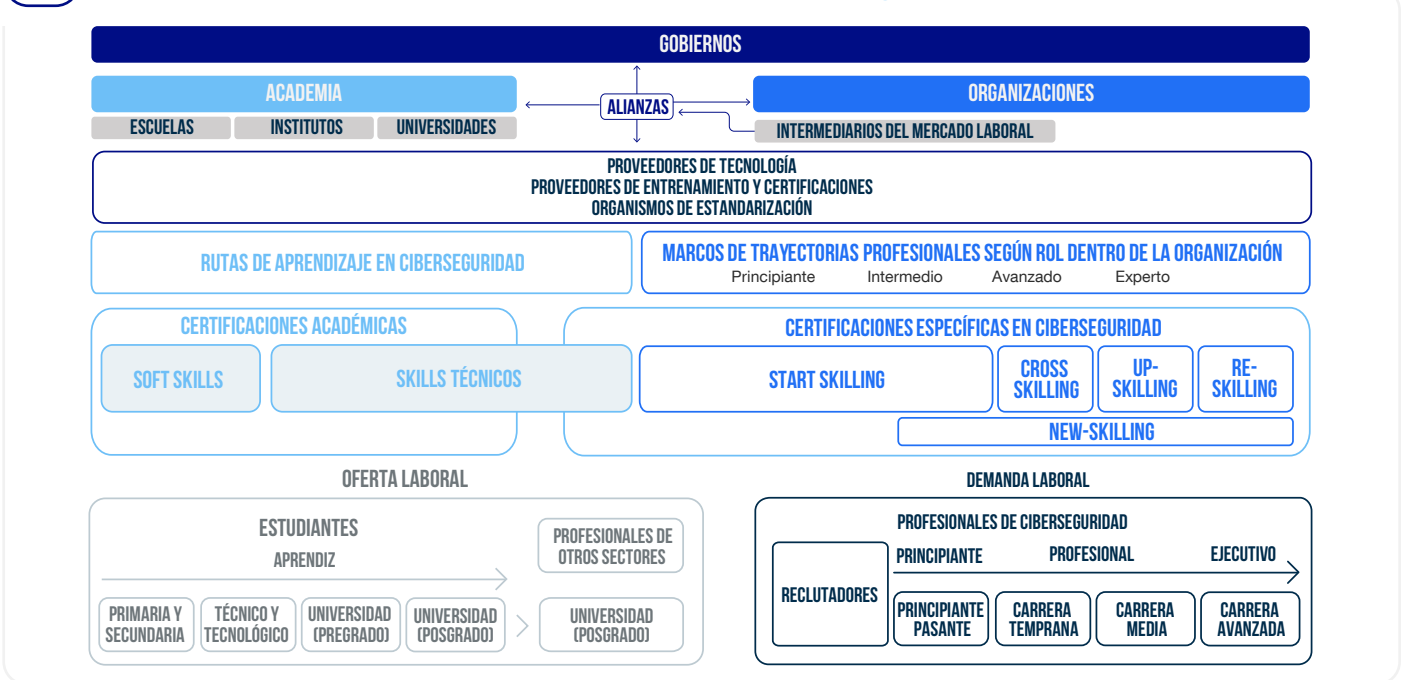
32. OECD. (2023). Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico (OECD Skills Studies). OECD Publishing.  
 33. ISC. (2024). [ISC2 Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World](#).

## Necesidad de coordinación

La plantilla de ciberseguridad es un recurso dinámico ya que sus habilidades son inherentemente adquiribles, modificables y mejorables a través de la formación. Por ello, las entidades públicas de la región tienen la responsabilidad de desarrollar y conservar este talento en evolución. Sin embargo, su desarrollo es una cuestión de política pública multifacética que debe involucrar a gobiernos, sector privado y academia. El ecosistema de demanda y oferta laboral en ciberseguridad es altamente complejo en el que interactúan actores de un lado y del otro. No se trata solo de aumentar la cantidad de certificados sino de promover una mayor coordinación entre todos los actores involucrados para el desarrollo de trayectorias de carrera claras desde educación básica hasta educación media superior.

Esta coordinación es necesaria también para que los esfuerzos estén concentrados en las sub-áreas de mayor criticidad y poder responder a las necesidades del sector con velocidad y eficacia. En este sentido, la ausencia de una gobernanza clara del talento y cultura ha llevado a una proliferación de iniciativas aisladas, muchas de ellas valiosas, pero sin articulación ni mecanismos de evaluación conjunta. Programas de becas, cursos de certificación y diplomados en ciberseguridad se multiplican, pero sin un diálogo que asegure la coherencia curricular y la alineación con las necesidades del mercado.

### 1/21 Esquematación de la oferta y demanda laborales de ciberseguridad



Fuente: elaboración propia en base a la OEA (2023)

## B. Crear el Consejo Nacional de Talento

Se propone la creación urgente de un Consejo Nacional de Talento en Ciberseguridad para articular la oferta de formación relevante y actual, tanto pública como privada. Este Consejo, compuesto por representantes del sector público, el sector privado y la academia debería estar encargado de, en primer

lugar, elaborar un diagnóstico profundo y actualizado de la situación laboral en el sector de la ciberseguridad en México. Tener una evaluación pormenorizada de la brecha actual es una necesidad para la definición de prioridades en el corto y mediano plazo.

## C. Establecer el marco de roles en ciberseguridad

El Consejo debería trabajar en la elaboración de un Marco de roles en ciberseguridad, inspirado en el NICE Framework del NIST<sup>34</sup> de Estados Unidos pero adaptado a la realidad y las necesidades mexicanas. Este marco permitiría estandarizar la terminología, las competencias y los perfiles profesionales requeridos en el ecosistema nacional de ciberseguridad,

facilitando la comunicación entre instituciones educativas, empresas, y entidades gubernamentales. Asimismo, serviría como guía para diseñar programas académicos, certificaciones, insignias y trayectorias de desarrollo profesional que respondan a los desafíos actuales del entorno digital.

34. Petersen, R., Santos, D., Smith, M. C., Wetzels, K. A., & Witte, G. (2020). [NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity \(NICE Framework\)](#). National Institute of Standards and Technology.

## Marco NICE del NIST

El Marco de Trabajo NICE para Ciberseguridad (NICE Framework) (NIST SP 800-181r1) del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST por sus siglas en inglés) establece un lenguaje común que define y categoriza las Áreas de Competencia y los Roles de Trabajo en ciberseguridad, incluyendo los Conocimientos y Habilidades necesarios para completar las tareas en esos roles.



Sirve como un recurso de referencia fundamental para describir e intercambiar información sobre el trabajo de ciberseguridad, y los conocimientos, habilidades y capacidades (CHC) necesarios para llevar a cabo las tareas que pueden fortalecer la postura de ciberseguridad de una organización.

El Marco NICE mejora la comunicación sobre la manera de identificar, contratar, formar y retener personas con talento en el campo de la ciberseguridad por medio de un léxico común y uniforme que clasifica y describe el trabajo en materia de ciberseguridad. Sirve de referencia para que las organizaciones o los sectores puedan preparar publicaciones o recursos adicionales que satisfagan sus necesidades de definir u ofrecer orientación sobre diferentes aspectos de la formación, planificación, capacitación y educación del personal de ciberseguridad.

El Marco estableció la creación de un programa de Alianzas Regionales y Asociaciones Multisectorial para Estimular la Educación en Ciberseguridad y el Desarrollo de la Fuerza Laboral (RAMPS), el cual busca establecer alianzas multisectoriales entre empleadores, escuelas e instituciones de educación superior, y otras organizaciones comunitarias. Los objetivos específicos del Programa RAMPS son alinear las necesidades de fuerza laboral de las empresas y organizaciones sin fines de lucro locales con los objetivos de aprendizaje de los proveedores de educación y capacitación que se ajustan al Marco NICE; aumentar la cantidad de estudiantes que buscan carreras en ciberseguridad; capacitar a más estadounidenses para que accedan a empleos de clase media en ciberseguridad; y apoyar el desarrollo económico local para impulsar la creación de empleo.

## D. Promover un Plan Nacional de Talento

Con estos insumos, el Consejo debería desarrollar como objetivo principal un Plan Nacional de Talento que accione las conclusiones del diagnóstico inicial en base al marco de roles desarrollado. Este Plan Nacional podría contemplar estímulos económicos para la especialización, mecanismos de certificación reconocidos y la incorporación de nuevas generaciones al sector, con énfasis en la diversidad y la inclusión. Sería recomendable que el Plan establezca una periodicidad determinada que permita ajustar las acciones estratégicas en base a las necesidades del momento, aprovechando la institucionalidad del Consejo para coordinar entre todos los actores del ecosistema. Idealmente, el Consejo

debería actuar como un espacio permanente de coordinación y evaluación, encargado de monitorear la evolución del mercado laboral, identificar tendencias tecnológicas emergentes y proponer políticas públicas que aseguren una fuerza laboral resiliente y preparada frente a las amenazas digitales del futuro.

Es importante destacar que el fortalecimiento del talento técnico debe ir acompañado del desarrollo de una cultura de ciberseguridad sostenida, que fomente hábitos seguros en todos los niveles de la sociedad.

### T/08 Líneas de acción Plan Nacional de Talento

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>PLAN NACIONAL DE TALENTO</b>				
7.1	Realizar un diagnóstico de la brecha laboral	Realizar un diagnóstico actualizado sobre la brecha laboral en ciberseguridad en México	00	Publicación del diagnóstico nacional
7.2	Crear el Consejo Nacional de Talento	Crear el Consejo Nacional de Talento en Ciberseguridad	00	Consejo institucionalizado
7.3	Establecer el marco de roles en ciberseguridad	Adaptar el Marco NICE del NIST a la realidad y necesidades mexicanas	00	Publicación del marco nacional de roles
7.4	Promover un Plan Nacional de Talento	Elaborar un plan de acciones estratégicas para la formación laboral en ciberseguridad	00	Evaluación anual de la brecha y del impacto de los planes

Fuente: elaboración propia

## Desarrollo de credenciales y habilidades en ciberseguridad

El informe mencionado de la OCDE releva que en el sector los roles más demandados fueron los de Arquitectos e Ingenieros de Ciberseguridad, responsables de diseñar soluciones de seguridad, que representan el 34% de las OJPs en el país. El rol de Analista, por su parte, experimentó el mayor crecimiento durante el período 2021-2022, aumentando un 80%.

Los empleadores otorgaron importancia a las certificaciones y estándares en ciberseguridad para señalar la experiencia de los candidatos. En México, las certificaciones más

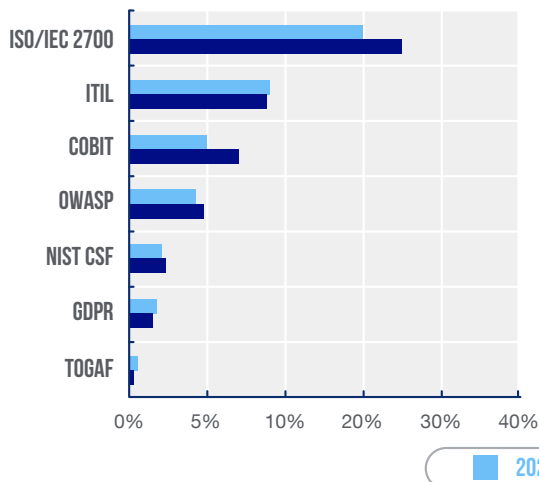
mencionadas y relevantes fueron CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager) y CEH (Certified Ethical Hacker). Sin embargo, el informe advierte sobre una desalineación significativa: las certificaciones más solicitadas, como CISSP y CISM, están diseñadas para profesionales con un mínimo de cinco años de experiencia, pero a menudo se requieren para puestos de nivel de entrada (entry-level). Esta discrepancia desanima a los candidatos y dificulta a los empleadores encontrar el talento adecuado.

1/22

### Demanda por estándares y certificaciones de ciberseguridad en México durante 2021 y 2022

#### DEMANDA POR ESTÁNDARES DE CIBERSEGURIDAD Y MARCOS

Menciones de cada elemento como porcentaje del número total de OJP sobre ciberseguridad por año.



#### DEMANDA DE CERTIFICACIONES EN CIBERSEGURIDAD

Menciones de cada elemento como porcentaje del número total de OJP sobre ciberseguridad por año.



Fuente: OCDE (2023)

El informe recomienda que los empleadores ajusten los requisitos de certificación para los puestos de nivel de entrada y adopten marcos de habilidades (como el NICE Framework) para estandarizar y alinear la demanda con la oferta educativa. Finalmente, se subraya que la competencia en inglés es una habilidad transversal de vital importancia, ya que la mayoría de los recursos de capacitación y estándares de la industria se encuentran en este idioma, un obstáculo para la fuerza laboral en América Latina, que generalmente tiene baja competencia en inglés.

Por su parte, el informe Shaping Skills<sup>35</sup> del Instituto para el Futuro de la Educación del Tecnológico de Monterrey ofrece una visión detallada de las Habilidades, Conocimientos y Capacidades (KSAs) más demandadas en el sector Infocomm (en el que incluyen el subsector de la ciberseguridad) en México, a partir de un análisis de ofertas de empleo realizado entre julio y diciembre de 2024. El estudio revela que gran parte de la demanda se centra en habilidades no técnicas.

Entre las competencias más solicitadas se encuentran la comunicación, la resolución de problemas, la gestión de riesgos, el pensamiento analítico, el dominio del inglés, la colaboración, el trabajo en equipo, la gestión de proyectos, el liderazgo y el cumplimiento normativo. Un análisis más profundo en el subsector de la ciberseguridad muestra que, para el puesto de especialista en seguridad TIC, los conocimientos técnicos y operativos son fundamentales, destacando la respuesta a incidentes, el análisis de datos, la gestión de riesgos, la evaluación de riesgos, la gestión de proyectos, el monitoreo y la gestión de incidentes, así como estándares y certificaciones como ISO 27001 y pruebas de penetración. En paralelo, las habilidades analíticas y de interacción, como colaboración, trabajo en equipo y resolución de problemas técnicos, son clave para un desempeño efectivo, mientras que capacidades como atención al detalle y adaptabilidad resultan esenciales para el rendimiento profesional.

35. Caratozzolo, P., Rueda-Castro, V., Gutierrez-Aguilar, M., Azofeifa, D., & González-Gómez, L. J. (2025). Shaping Skills Report: Discover tomorrow, shape today. Institute for the Future of Education, Tecnológico de Monterrey.

En conclusión, el estudio subraya la necesidad de que las instituciones educativas integren y fortalezcan las habilidades transversales junto con conocimientos técnicos especializados, certificaciones, estándares y dominio del inglés, considerado un factor crítico para la competitividad de la fuerza laboral de la ciberseguridad en México. Resulta

necesario destacar la importancia del involucramiento de todos los actores del ecosistema para la formación de especialistas capacitados para el mercado. No sólo las habilidades técnicas son necesarias para una trayectoria de carrera exitosa sino también las habilidades blandas.

## A. Crear un catálogo de credenciales

Las acciones propuestas deben integrar tanto a las instituciones de educación básica y superior, a las universidades y al sector privado que posee una compleja currícula de cursos y certificaciones. Por esta razón, se recomienda la elaboración de un catálogo de credenciales y micro-credenciales apilables (sumamente útiles para la

adaptación a la velocidad de los cambios tecnológicos) y de estándares de ciberseguridad mayormente demandados por el mercado. Este catálogo apunta a ser una guía para trazar trayectorias de carrera eficaces y mejorar la coordinación entre la oferta y la demanda laboral en ciberseguridad.

## B. Promover iniciativas, como el CANIETI Talent Hub

Es deseable apoyarse en la experiencia y oferta del sector privado para promover iniciativas en la materia. Desde 2023, la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) ha puesto a disposición el [CANIETI Talent Hub](#), un sitio de colaboración sin fines comerciales diseñado para poner en un

solo lugar los cursos, certificaciones, tutoriales, entre otros, que tienen las empresas para desarrollar habilidades digitales. También es un espacio donde se puede difundir la oferta laboral de las empresas y la demanda de empleabilidad de las organizaciones que se dedican a la formación de personas en temas de tecnología.



Fuente: CANIETI Talent Hub

## C. Promover programas de formación dual

Se favorece la promoción de programas de formación dual que combinen educación en las instituciones académicas con experiencia práctica en el entorno laboral. La idea central es que los estudiantes no solo adquieran conocimientos

teóricos, sino que también los apliquen en situaciones reales, colaborando con empresas, instituciones públicas o laboratorios especializados en ciberseguridad.



T/09 Líneas de acción sistema educativo nacional

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>SISTEMA EDUCATIVO NACIONAL</b>				
8.1	Crear un catálogo de credenciales	Elaborar un catálogo de credenciales, microcredenciales y estándares de ciberseguridad demandados por el mercado	000	Publicación y actualización periódica del catálogo
8.2	Promover iniciativas, como el CANIETI Talent Hub	Coordinar con el sector privado para aprovechar su experiencia y currículos en formación técnica	000	Número de iniciativas vigentes y cantidad de empresas con las que se tengan iniciativas vigentes
8.3	Promover programas de formación dual	Impulsar convenios entre instituciones educativas y empresas tecnológicas para programas de formación dual en ciberseguridad	000	Cantidad de programas de educación dual vigentes

Fuente: elaboración propia

OBJETIVO

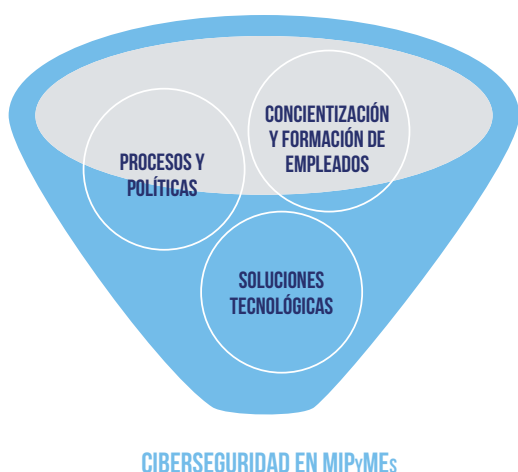
9

## Claves para atender la especificidad de las MiPyMEs

De acuerdo con datos del INEGI y la Secretaría de Economía, las MiPyMEs mexicanas representan más del 99,8% del tejido empresarial (4,7 millones de establecimientos) y son, en cuanto a la ciberseguridad, el eslabón más débil, lo que representa un riesgo sistémico para toda la economía. Su importancia radica en su impacto laboral y económico: generan el 52% de los ingresos del país y emplean a 27 millones de personas, lo que equivale al 68.4% de la fuerza laboral del sector empresarial<sup>36</sup>. El 34% son lideradas por mujeres y predominan en comercio, servicios y manufacturas,

siendo estratégicas para el Nearshoring y la democratización del comercio exterior. Enfrentan desafíos como limitada financiación, alta mortalidad (52% cierran en los primeros dos años), baja digitalización y dependencia familiar (90%). Si bien la Secretaría de Economía ha impulsado políticas de inclusión institucional, digital, financiera y comercial para fortalecerlas y mejorar su competitividad, los desafíos en ciberseguridad persisten. Por eso, una Estrategia Nacional de Ciberseguridad debe considerar acciones estratégicas para apoyar su fortalecimiento y resiliencia en materia de seguridad digital.

1/24 Tres elementos básicos para la ciberseguridad en MiPyMEs



ACCIONES ESTRATÉGICAS

- CORTO PLAZO** **GUÍAS DE CIBERSEGURIDAD PARA MIPYMEs:** elaborar y poner a disposición guías y kits que puedan utilizar las MiPyMEs para formar y concientizar a sus empleados en elementos básicos y buenas prácticas de ciberseguridad.
- MEDIANO PLAZO** **PROGRAMAS DE ASESORÍA:** desarrollar programas de asesoría para ayudar a las MiPyMEs a poner a punto la protección de su infraestructura tecnológica y digital.
- LARGO PLAZO** **LÍNEA DE ATENCIÓN DEL CERT:** poner a disposición de las MiPyMEs una línea de atención y respuesta a ciberincidentes.

Fuente: elaboración propia

36 Secretaría de Economía, Subsecretaría de Comercio Exterior. (2024). MiPyMEs mexicanas: motor de nuestra economía. Secretaría de Economía.

## A. Crear kits de concientización

Para garantizar el desarrollo económico continuo y la resiliencia de las MiPyMES, es crucial integrar la ciberseguridad en la política de impulso empresarial de México. Las MiPyMES, al carecer a menudo de equipos dedicados o evaluaciones formales de riesgos, son objetivos prioritarios para ciberataques como ransomware y phishing, los cuales pueden llevar al cierre definitivo. Por ello, se propone una estrategia integral que combine el desarrollo de capacidades no técnicas y la provisión de mecanismos de apoyo económico para fortalecer su postura digital.

Dada la baja inversión en infraestructura y transformación digital, y la limitada conciencia de seguridad, es fundamental el desarrollo de capacidades no técnicas. Inspirándose en modelos como el del INCIBE en España, se propone la creación de kits de concientización en ciberseguridad diseñados para capacitar a los empleados, complementados con guías claras para el armado de procesos y políticas de seguridad. Estos kits, disponibles a bajo costo o de forma gratuita, permitirán a las pequeñas y medianas empresas elevar su cultura de seguridad.

## B. Crear guías prácticas para la elaboración de políticas de ciberseguridad

Existen recursos que pueden servir de guía e inspiración para su desarrollo. Recientemente, el Latin America and Caribbean Cyber Competence Centre, un centro regional de capacitación en ciberseguridad respaldado y financiado por la Unión Europea, puso a disposición la Guía Práctica para Pequeñas y Medianas Empresas<sup>37</sup>, que ofrece un recorrido

para el fortalecimiento de las defensas digitales. Además, como precedente en el contexto nacional, el CERT-MX publicó en 2018 un Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa<sup>38</sup>; sin embargo, este recurso debe ser actualizado y ampliado para reflejar las tendencias actuales de amenazas.

## C. Establecer mecanismos de apoyo económico

Para permitir a las MiPyMEs realizar la inversión de capital necesaria en defensa digital, se deben implementar iniciativas fiscales y créditos que las ayuden a mejorar sus equipos de cómputo y su infraestructura de ciberseguridad. La implementación de modelos como el Paga-con-Ahorros (PAYS) con mecanismos de apoyo económico o el Crédito/ Bono Tributario a la inversión en ciberseguridad ofrecen soluciones viables. Bajo el esquema PAYS, por ejemplo, la cuota periódica para adquirir equipo seguro (como endpoints con hardening o software EDR) se diseña para ser menor al

ahorro operativo generado (menos incidentes, menos horas caídas), permitiendo a la MiPyME pagar con los ahorros y mantener un flujo positivo. Asimismo, un apoyo económico por un porcentaje del CAPEX, acreditable contra el ISR, abarataría la compra y mejoraría la liquidez, incentivando la inversión en equipos, servicios de asesoría de fabricantes y herramientas de seguridad. Estas acciones, que evitan la descapitalización, son esenciales para construir la resiliencia empresarial moderna.

### T/10 Líneas de acción ciberseguridad en MiPyMEs

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>CIBERSEGURIDAD EN MiPyMEs</b>				
9.1	Crear kits de concientización	Desarrollar kits de concientización en ciberseguridad dirigidos a las MiPyMEs		Publicación de los kits y cantidad de descargas anuales
9.2	Crear guías prácticas para la elaboración de políticas de ciberseguridad	Desarrollar guías que orienten a las MiPyMEs en el diseño de políticas internas de ciberseguridad		Publicación de las guías prácticas y cantidad de descargas anuales
9.3	Establecer mecanismos de apoyo económico	Implementar programas de créditos y exenciones fiscales para la compra y mejora de equipos tecnológicos		Número de MiPyMEs adheridas a algún programa, monto monetario de beneficios otorgados por año

Fuente: elaboración propia

37 Seeba, M., & Patiño-Villa, M. (2025). LAC4 guía para pequeñas y medianas empresas. LAC4 & EU CyberNet.

38 Guardia Nacional, Centro Nacional de Respuesta a Incidentes Cibernéticos [CERT-MX]. (2022). Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa. CERT-MX.

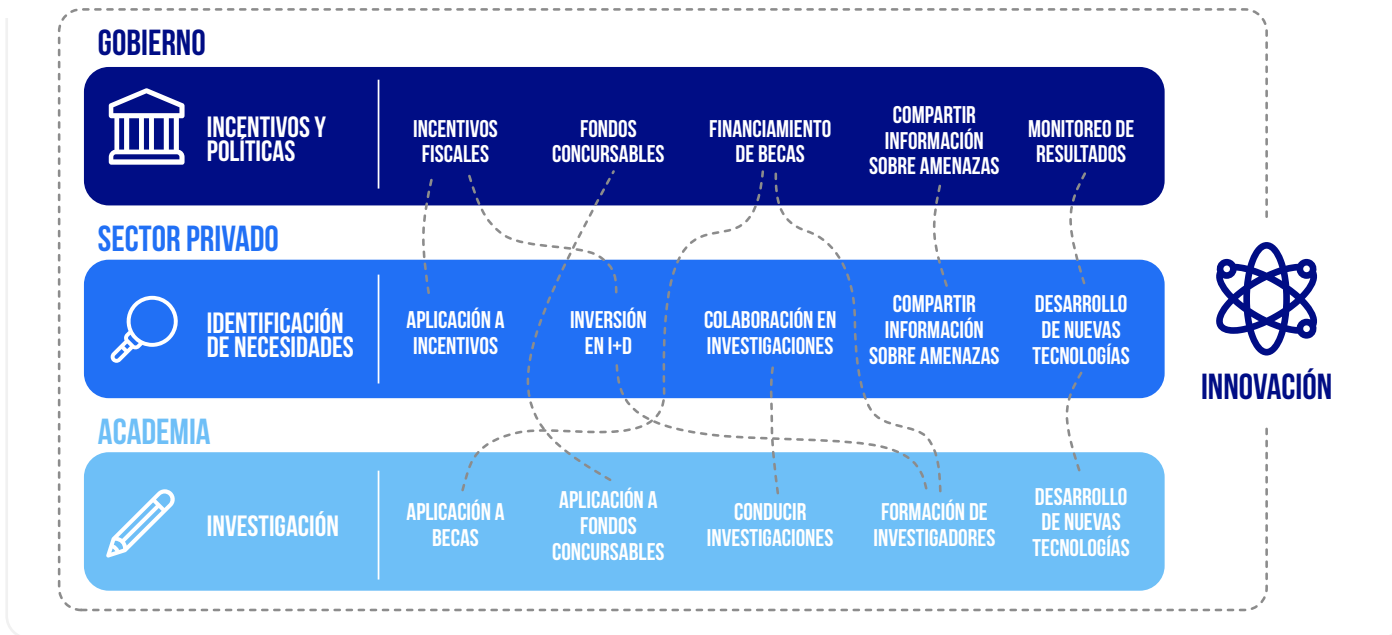
## Fomento a la Investigación y Desarrollo

La innovación en ciberseguridad es crítica para anticipar y responder a amenazas en un entorno digital cambiante de cualquier organización. Permite desarrollar soluciones más inteligentes y resilientes, fortalecer la protección de infraestructuras críticas y servicios esenciales digitales y soluciones locales que fortalezcan y complementen las

tecnologías externas. Además, impulsa la competitividad y la confianza de los usuarios, fomenta la cooperación público-privada y atrae talento especializado, consolidando un ecosistema dinámico que contribuye a la seguridad y al desarrollo económico sostenible.

1/25

### Coordinación de los actores relevantes en la innovación de ciberseguridad



Fuente: elaboración propia

Actualmente, la ciberseguridad es un sector de fructífera innovación. Soluciones como la Arquitectura Zero Trust, la detección automatizada de incidentes y amenazas impulsada por la Inteligencia Artificial, la criptografía post-cuántica, la identidad digital y el blockchain son algunos de los desarrollos

que en los últimos años han expandido la frontera de la resiliencia y protección de infraestructuras de la información. Por esta razón, es importante que una Estrategia Nacional de Ciberseguridad considere e incentive la aplicación y mejora de estas soluciones, además del desarrollo de otras nuevas.

### A. Financiar proyectos especializados en ciberseguridad

Es fundamental integrar el impulso a la Innovación, Investigación y Desarrollo (I+D) en Ciberseguridad como un eje central de una Estrategia Nacional de Ciberseguridad. Este eje estratégico debe comenzar por el establecimiento de un sistema de estímulos económicos robustos que promueva la colaboración tripartita. Esto implica ofrecer

mecanismos de apoyo económico a empresas que inviertan en o colaboren con universidades y centros de investigación; al mismo tiempo, es crucial crear becas especializadas y fondos concursables (público-privados) destinados a financiar proyectos de I+D enfocados en los desafíos de seguridad específicos del país.

### B. Impulsar la innovación y la I+D

Complementariamente, se recomienda implementar políticas de apoyo para fomentar la creación de start-ups y empresas tecnológicas dedicadas a la ciberseguridad, transformando la

investigación generada en el país en productos comerciales escalables y de alto valor estratégico.

### C. Fomentar la consolidación empresarial

Finalmente, para materializar esta innovación y reducir la dependencia, es necesario crear la infraestructura y el ecosistema empresarial adecuado. Esto se logrará mediante

el desarrollo de laboratorios de ciberseguridad que sirvan como incubadoras para la creación de software y soluciones de seguridad innovadoras y de origen doméstico. Es

crucial que estos esfuerzos de innovación se dirijan a áreas prioritarias para el desarrollo de capacidades internas y las necesidades nacionales. Se recomienda enfocar la inversión en la aplicación de la Inteligencia Artificial para la detección y respuesta automatizada de amenazas, Arquitectura Zero

Trust, el desarrollo de Criptografía Post-Cuántica (PQC), y la protección de infraestructuras críticas, prestando especial atención a la seguridad en dispositivos IoT y la protección de sistemas de control industrial (OT).

T/11 **Líneas de acción fomento I+D**

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>FOMENTO I+D</b>				
10.1	Financiar proyectos especializados en ciberseguridad	Crear becas y fondos concursables público-privados para proyectos de I+D en seguridad cibernética		Número de proyectos financiados, becarios beneficiados y monto financiado (anuales)
10.2	Impulsar la innovación y la I+D	Establecer un sistema de mecanismos de apoyo económico para promover colaboración entre empresas, universidades y centros de investigación que promuevan la innovación en soluciones de ciberseguridad		Número de empresas beneficiadas y volumen de inversión en I+D (anuales)
10.3	Fomentar la consolidación empresarial	Implementar políticas y un ecosistema de apoyo para la creación y desarrollo de start-ups tecnológicas en ciberseguridad		Número de start-ups creadas por año

Fuente: elaboración propia

## IV. Cultura, sensibilización y comunicación

### 11 La ciberseguridad como cultura

Campañas de comunicación robustas y bien dirigidas serán la piedra angular para construir una cultura de ciberseguridad nacional. Un componente prioritario será la ciberprevención

dirigida a adultos mayores y las infancias, debido a su uso intensivo y exposición a los riesgos en línea.

#### A) Fomentar la adopción de prácticas básicas de ciberhigiene

De forma general, las campañas de sensibilización deberían estructurarse en torno a una narrativa coherente, positiva y orientada a la acción. No se trata solo de alertar sobre riesgos, sino de empoderar a la población para actuar de manera segura en el entorno digital. La comunicación debe transmitir

que la ciberseguridad no es un obstáculo, sino un habilitador de confianza y desarrollo económico sostenible.

La campaña debe perseguir tres objetivos primordiales:

- Fomentar la adopción masiva de prácticas básicas de ciber higiene, convirtiendo acciones como usar contraseñas fuertes o la autenticación de doble factor en hábitos automáticos.
- Aumentar la confianza de la población en el uso de servicios digitales gubernamentales y comerciales, demostrando que la protección de datos y de los derechos fundamentales en el espacio digital es una prioridad.
- Educar a la sociedad sobre cómo identificar, evitar y reportar las ciber amenazas más comunes, como el phishing, vishing, FraudGPT, deepfakes, DarkGPT y los fraudes en línea, reduciendo así la superficie de ataque humana.

## B. Integrar materiales pedagógicos

Es importante destacar que la ciberprevención dirigida a las infancias debe ser un componente prioritario de la cultura de ciberseguridad nacional. Las niñas, niños y adolescentes son usuarios intensivos del entorno digital y, al mismo tiempo, uno de los grupos más expuestos a riesgos como el acoso en línea, la desinformación o la exposición indebida de datos

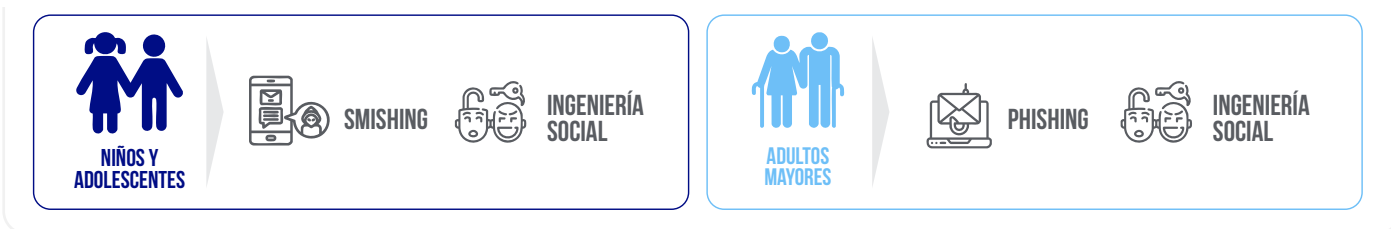
personales. Por ello, las estrategias de comunicación deben incluir programas de alfabetización digital temprana, con contenidos adaptados a la edad y la etapa educativa, que promuevan hábitos de protección, pensamiento crítico y ciudadanía digital responsable.

## C. Prevenir fraudes dirigidos a personas mayores

Para lograr mayor robustez, es esencial adaptar los mensajes y canales de comunicación a públicos específicos. La

segmentación permite maximizar su impacto y garantizar que los mensajes lleguen a la audiencia correcta de la forma correcta.

### 1/26 Principales amenazas por grupo poblacional



Fuente: elaboración propia

Esta personalización es crucial para que el contenido sea relevante y se asimile correctamente. Para la ciudadanía general, se deben usar mensajes sencillos y accionables a través de medios masivos como la televisión y la radio, enfocados en amenazas cotidianas y soluciones prácticas. En el caso de niños, adolescentes y educadores, el enfoque debe ser en el uso seguro de redes sociales, el ciberacoso y la ciudadanía digital, utilizando canales y formatos que les resulten naturales, como redes sociales de alta interacción y materiales creativos e interactivos en las escuelas. En conjunto con la Secretaría de Educación, sería recomendable elaborar guías y kits de sensibilización en ciber higiene para educadores, a fin de garantizar la correcta transmisión pedagógica de los riesgos que supone el mundo digital. A los adultos mayores, la comunicación debe ser empática

y centrada en la prevención de fraudes y estafas en línea, distribuyendo folletos y guías sencillas en bancos y oficinas de gobierno, además de spots en medios tradicionales.

Además, se recomienda la creación de un número telefónico nacional de asesoría cibernética, inspirado en el modelo de la Línea 017 del Instituto Nacional de Ciberseguridad (INCIBE) de España. Este servicio permitiría brindar orientación inmediata y confidencial a personas afectadas por incidentes cibernéticos, fraudes, acoso digital o vulneraciones de datos, así como ofrecer apoyo preventivo a empresas y familias. Su implementación fortalecería la capacidad de respuesta temprana, la educación digital y la confianza ciudadana, convirtiéndose en un canal accesible y permanente de acompañamiento técnico y psicosocial ante riesgos digitales.

### 1/27 Materiales y acciones recomendadas



Fuente: elaboración propia

## D. Medir el impacto de la estrategia

Para asegurar que la estrategia sea efectiva y se adapte a la rápida evolución de las amenazas, es crucial medir su impacto de manera continua. La evaluación debería ser dual. Por un lado, medir aspectos cualitativos a través de encuestas de percepción de la confianza pública y la interacción con plataformas y redes sociales oficiales (comentarios, descargas de guías, participación en cursos). Por otro, y con una visión orientada a resultados, monitorizar indicadores de

desempeño (KPIs) críticos de ciberseguridad. Estos incluyen la reducción del porcentaje de incidentes atribuibles a descuidos ciudadanos, el tiempo promedio que tarda un ciudadano en reportar un ataque (indicando conciencia del canal adecuado), y la identificación de las tendencias en los tipos de ataques más frecuentes. Esta medición basada en datos permitirá ajustar los mensajes y demostrar el retorno de la inversión en la estrategia de sensibilización.

## Sinergias

Es imperativo articular los esfuerzos con el ya establecido Mes de la Ciberseguridad en México. Este período debe ser explotado como el espacio de las interacciones, colaboración y cooperación para llevar a la población en general la estrategia comunicacional durante el año, concentrando el lanzamiento de campañas y eventos clave para magnificar su resonancia mediática y lograr una participación masiva. Durante este mes, se recomienda promover una coordinación activa entre instituciones públicas, sector privado, academia

y sociedad civil, con el fin de alinear mensajes y recursos bajo una identidad visual común. Asimismo, impulsar campañas temáticas anuales, actividades formativas, ferias digitales y colaboraciones con medios y plataformas tecnológicas, fortaleciendo la participación ciudadana y la visibilidad nacional. Finalmente, el Mes de la Ciberseguridad puede servir también como espacio de evaluación y retroalimentación, permitiendo medir avances, difundir resultados e incorporar aprendizajes para la mejora continua de la estrategia.

### T/12 Líneas de acción para la sensibilización

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>SENSIBILIZACIÓN</b>				
11.1	Fomentar la adopción de prácticas básicas de ciberhigiene	Desarrollar campañas masivas con mensajes sobre contraseñas seguras, doble autenticación y actualización de software		Cantidad de campañas anuales
11.2	Integrar materiales pedagógicos	Elaborar guías, kits educativos y recursos didácticos sobre ciberhigiene para docentes y escuelas		Número de escuelas que incorporan materiales de ciberseguridad
11.3	Prevenir fraudes dirigidos a personas mayores	Lanzar campañas en medios masivos, online, bancos, oficinas públicas y otros medios tradicionales		Cantidad anual denuncias de fraudes cibernéticos a personas mayores
11.4	Medir el impacto de la estrategia	Implementar encuestas, análisis de redes sociales y monitoreo de indicadores (reportes, tiempos de respuesta, incidentes)		Publicación anual de informe con métricas de impacto

Fuente: elaboración propia



## Conclusiones

Hoy en día la ciberseguridad trasciende un sector específico para convertirse en habilitadora del crecimiento económico y la transformación digital. Por eso México se encuentra en un punto de inflexión donde contar con una Estrategia Nacional de Ciberseguridad actualizada no es solo una medida operativa, sino una condición estructural para el desarrollo sostenible, la gestión soberana de los recursos digitales y el clima de confianza.

La evidencia comparada y el diagnóstico nacional muestran que la fragmentación institucional, los vacíos normativos y las brechas de talento y madurez entre sectores constituyen riesgos sistémicos que requieren coordinación superior, obligaciones transversales y prioridades comunes, articuladas bajo una visión compartida en la sociedad y centrada en las personas.

En esa línea, la presente propuesta de lineamientos para una Estrategia Nacional de Ciberseguridad de México busca aportar a la discusión y proponer opciones de acción fundamentadas en una visión clara y ambiciosa para el futuro del país, guiada por enfoques y principios que aseguran un desarrollo digital equilibrado, seguro e inclusivo.

La propuesta está estructurada en tres grandes ejes que van desde el marco institucional y de gobernanza hasta la cultura, la promoción de talento y la sensibilización. Entre sus objetivos generales, líneas de acción e indicadores de avance se apunta a crear una Coordinación Nacional de Ciberseguridad como órgano rector transicional, con mesas ejecutivas público-privadas; avanzar en una Ley General de Ciberseguridad y definiciones concretas de infraestructuras críticas y servicios esenciales digitales que sigan marcos internacionales; realizar ejercicios regulares y coordinación intersectorial para la gestión de riesgos y la respuesta a ciber crisis; establecer un Consejo Nacional de Talento en Ciberseguridad; promover programas de concientización; profundizar la cooperación internacional y el intercambio de información, alineando compromisos del T-MEC; e impulsar la investigación, desarrollo e innovación en detección y respuesta.

El marco estratégico aquí propuesto define la dirección, principios y objetivos sobre los cuales se articularán los ejes, líneas de acción y mecanismos de implementación de la Estrategia Nacional de Ciberseguridad. Más que un documento cerrado, consideramos que puede ser una base y puntapié inicial para apuntalar la discusión pública y el foco en la ciberseguridad, como catalizadora del desarrollo de México.

# Anexo: Plan de acción consolidado

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>INSTITUCIONALIDAD</b>				
1.1	Crear un órgano rector que articule la gobernanza nacional en ciberseguridad	Establecer por decreto la Coordinación Nacional de Ciberseguridad, con secretaría técnica y reglas de operación definidas		Coordinación instalada y reglas de operación publicadas
1.2	Instalar mesas de trabajo temáticas	Conformar y formalizar cinco mesas de trabajo (mejores prácticas; red de confianza CERT/CSIRT; ciber crisis nacional; vulnerabilidades e incidentes; talento y capacitación)		Actas de instalación y publicación de planes trimestrales de trabajo
1.3	Proponer un Marco Nacional de Ciberseguridad	Elaborar y presentar insumos técnicos para la Estrategia Nacional		Insumos publicados y entregados a actores políticos de alto nivel
<b>BASE LEGAL</b>				
2.1	Promover la Ley Nacional de Ciberseguridad	Generar insumos para su construcción (definiciones y principios; gobernanza y autoridades; catálogo de infraestructuras críticas y servicios esenciales digitales; enfoque basado en riesgos; derechos digitales; identidad digital; cooperación público-privada e internacional)		Insumos incorporados a un anteproyecto de ley
2.2	Revisar el marco penal existente	Conformar un grupo de expertos para revisar las normas penales y proponer actualizaciones conforme a nuevas realidades delictivas		Generación de insumos y análisis técnico-jurídico
<b>PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS, INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y SERVICIOS ESENCIALES DIGITALES</b>				
3.1	Adoptar un marco normativo para infraestructuras críticas de información	Asignar responsabilidades para la definición de normas de protección por sector		Propuesta de roles para funciones de PIC
3.2	Establecer definiciones, criterios, y catálogos de infraestructuras críticas y servicios esenciales digitales	Definir formalmente las categorías de infraestructuras críticas y servicios esenciales digitales y sus sectores y subsectores		Propuesta normativa consensuada entre sector público y privado
3.3	Establecer definiciones, criterios, y catálogos de infraestructuras críticas y servicios esenciales digitales	Definir criterios y metodología para la identificación de las ICC		Propuesta normativa consensuada para la identificación de las ICC
<b>COOPERACIÓN INTERNACIONAL</b>				
4.1	Establecer líneas de cooperación internacional	Participar activamente en foros transnacionales prioritarios en materia de ciberseguridad		Participación anual en foros transnacionales (#)
4.2	Establecer líneas de cooperación internacional	Suscribir acuerdos de asistencia mutua para el intercambio de información sobre amenazas		Convenios vigentes con entidades de confianza o proveedores de seguridad
4.3	Fortalecer las capacidades de ciberdiplomacia	Crear un foro interinstitucional para que la cancillería coordine la agenda internacional de ciberseguridad		Propuesta de mecanismos de coordinación interinstitucional sistemática

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>COORDINACIÓN DE RESPUESTA A INCIDENTES</b>				
5.1	Construir liderazgo y fortalecer la gestión de incidentes a nivel nacional	Definir y establecer un marco institucional que promueva, dirija y coordine prevención y respuesta a incidentes		Plan nacional de coordinación con responsabilidades y estrategias definidas
5.2	Construir liderazgo y fortalecer la gestión de incidentes a nivel nacional	Establecer puntos de confianza mediante un programa de adhesión voluntaria para divulgar alertas y compartir información sobre vulnerabilidades críticas		Cantidad de CERT/CSIRT adheridos a la red nacional de confianza
<b>MADUREZ DE LA RESPUESTA A INCIDENTES</b>				
6.1	Construir capacidades para abordar escenarios de crisis cibernéticas a nivel nacional	Identificar escenarios de ciber crisis con alto impacto y documentar partes interesadas y responsabilidades		Plan de trabajo con tres escenarios y partes interesadas por cada uno
6.2	Construir capacidades para abordar escenarios de crisis cibernéticas a nivel nacional	Planificar y ejecutar ejercicios nacionales de simulación de ciberataques y elaborar planes de mejora		Cantidad anual de ejercicios de simulación de ciberataques
<b>PLAN NACIONAL DE TALENTO</b>				
7.1	Realizar un diagnóstico de la brecha laboral	Realizar un diagnóstico actualizado sobre la brecha laboral en ciberseguridad en México		Publicación del diagnóstico nacional
7.2	Crear el Consejo Nacional de Talento	Crear el Consejo Nacional de Talento en Ciberseguridad		Consejo institucionalizado
7.3	Establecer el marco de roles en ciberseguridad	Adaptar el Marco NICE del NIST a la realidad y necesidades mexicanas		Publicación del marco nacional de roles
7.4	Promover un Plan Nacional de Talento	Elaborar un plan de acciones estratégicas para la formación laboral en ciberseguridad		Evaluación anual de la brecha y del impacto de los planes
<b>SISTEMA EDUCATIVO NACIONAL</b>				
8.1	Crear un catálogo de credenciales	Elaborar un catálogo de credenciales, microcredenciales y estándares de ciberseguridad demandados por el mercado		Publicación y actualización periódica del catálogo
8.2	Promover iniciativas, como el CANIETI Talent Hub	Coordinar con el sector privado para aprovechar su experiencia y currículos en formación técnica		Número de iniciativas vigentes y cantidad de empresas con las que se tengan iniciativas vigentes
8.3	Promover programas de formación dual	Impulsar convenios entre instituciones educativas y empresas tecnológicas para programas de formación dual en ciberseguridad		Cantidad de programas de educación dual vigentes
<b>CIBERSEGURIDAD EN MiPyMEs</b>				
9.1	Crear kits de concientización	Desarrollar kits de concientización en ciberseguridad dirigidos a las MiPyMEs		Publicación de los kits y cantidad de descargas anuales
9.2	Crear guías prácticas para la elaboración de políticas de ciberseguridad	Desarrollar guías que orienten a las MiPyMEs en el diseño de políticas internas de ciberseguridad		Publicación de las guías prácticas y cantidad de descargas anuales
9.3	Establecer mecanismos de apoyo económico	Implementar programas de créditos y exenciones fiscales para la compra y mejora de equipos tecnológicos		Número de MiPyMEs adheridas a algún programa, monto monetario de beneficios otorgados por año

#	OBJETIVO	ACCIÓN	HORIZONTE TEMPORAL	INDICADOR DE AVANCE
<b>FOMENTO I+D</b>				
10.1	Financiar proyectos especializados en ciberseguridad	Crear becas y fondos concursables público-privados para proyectos de I+D en seguridad cibernética		Número de proyectos financiados, becarios beneficiados y monto financiado (anuales)
10.2	Impulsar la innovación y la I+D	Establecer un sistema de mecanismos de apoyo económico para promover colaboración entre empresas, universidades y centros de investigación que promuevan la innovación en soluciones de ciberseguridad		Número de empresas beneficiadas y volumen de inversión en I+D (anuales)
10.3	Fomentar la consolidación empresarial	Implementar políticas y un ecosistema de apoyo para la creación y desarrollo de start-ups tecnológicas en ciberseguridad		Número de start-ups creadas por año
<b>SENSIBILIZACIÓN</b>				
11.1	Fomentar la adopción de prácticas básicas de ciberhigiene	Desarrollar campañas masivas con mensajes sobre contraseñas seguras, doble autenticación y actualización de software		Cantidad de campañas anuales
11.2	Integrar materiales pedagógicos	Elaborar guías, kits educativos y recursos didácticos sobre ciberhigiene para docentes y escuelas		Número de escuelas que incorporan materiales de ciberseguridad
11.3	Prevenir fraudes dirigidos a personas mayores	Lanzar campañas en medios masivos, online, bancos, oficinas públicas y otros medios tradicionales		Cantidad anual denuncias de fraudes cibernéticos a personas mayores
11.4	Medir el impacto de la estrategia	Implementar encuestas, análisis de redes sociales y monitoreo de indicadores (reportes, tiempos de respuesta, incidentes)		Publicación anual de informe con métricas de impacto

# Fuentes

Conpes 3854, 2016, (Consejo Nacional de Política Económica y Social) Documento de Política Pública de Seguridad Digital de Colombia.

Obtenido de <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Conpes 3995, 2020, (Consejo Nacional de Política Económica y Social) Documento de Política Pública de Seguridad Digital de Colombia.

Decreto 338, 2022. Política Pública de Seguridad Digital de Colombia.

Ley de ciberseguridad de Singapur Obtenido de <https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312&Provids=P11-#pr1->

Ley de ciberseguridad de Australia, 2018 <https://www.legislation.gov.au/C2018A00029/latest/text>

Ley de Infraestructuras críticas de Información de Corea del Sur, 2001 Obtenida de [https://elaw.klri.re.kr/eng\\_mobile/viewer.do?hseq=28812&type=part&key=43#:~:text=The%20purpose%20of%20this%20Act,of%20the%20life%20of%20people.](https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43#:~:text=The%20purpose%20of%20this%20Act,of%20the%20life%20of%20people.)

Recopilación de legislación sobre infraestructuras críticas UE. <https://eucyberdirect.eu/atlas/sources/act-on-the-protection-of-information-and-communications-infrastructure>

Ley de protección de Infraestructuras críticas de Estados Unidos, 2014, Obtenido de <https://www.congress.gov/bill/113th-congress/house-bill/3696/text>

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, obtenida de <https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630&tn=1&p=20220729>

Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008 , sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, obtenida de <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32008L0114>

Directiva CER y NIS2 obtenidas de <https://ec.europa.eu/newsroom/cipr/items/764849/en>

Infografía de ENISA (Agencia europea de la ciberseguridad) explicando la Ciber crisis. Obtenido en [https://www.enisa.europa.eu/sites/default/files/2025-07/ENISA\\_Cybersecurity\\_Bluprint.pdf](https://www.enisa.europa.eu/sites/default/files/2025-07/ENISA_Cybersecurity_Bluprint.pdf)

Lineamientos para la identificación de infraestructuras críticas cibernéticas en Colombia, 2025. Obtenido en [https://www.colcert.gov.co/800/articles-198657\\_ICC.pdf](https://www.colcert.gov.co/800/articles-198657_ICC.pdf)

Resolución SIP (Secretaría de Innovación Pública) 36/2020 Declara al Sistema GDE de Gestión Documental Electrónica de Argentina, 2020. Obtenida en <https://servicios.infoleg.gob.ar/infolegInternet/anexos/335000-339999/338378/norma.htm>

LAC4 <https://www.lac4.eu/es/>

