INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL EN MATERIA DE CIBERSEGURIDAD.

El que suscribe, senador Mauricio Vila Dosal del Grupo Parlamentario del Partido Acción Nacional, integrante de la LXVI Legislatura del Senado de la República del Congreso de la Unión, y con fundamento en lo dispuesto por la fracción II del artículo 71 de la Constitución Política de los Estados Unidos Mexicanos; por la fracción I, del numeral 1 del artículo 8; y por el artículo 164 del Reglamento de Senado de la República, someto a consideración de esta Soberanía, la siguiente Iniciativa con proyecto de decreto por el que se expide la Ley General en materia de Ciberseguridad, al tenor de la siguiente:

Exposición de Motivos

Planteamiento del problema

La necesidad de contar con una ley en materia de ciberseguridad se ha vuelto urgente en un mundo cada vez más interconectado y digitalizado. Contar con una ley en materia de ciberseguridad es fundamental para garantizar la protección de los derechos de los ciudadanos en entornos digitales, especialmente en lo que respecta a la protección de datos personales y la seguridad en las interacciones en línea que realizamos en nuestra vida cotidiana y en nuestra vida profesional.

En un contexto donde la tecnología avanza rápidamente, el resguardo de la información sensible y la privacidad de los individuos debe estar garantizado por la ley y por las instituciones.

Además, una legislación específica en ciberseguridad es necesaria para proteger la infraestructura tecnológica del Estado mexicano. Esto incluye garantizar la continuidad de servicios, como los financieros, de salud, comunicaciones y transportes, frente a la creciente amenaza de ataques cibernéticos. La vulnerabilidad de estas infraestructuras no solo compromete la seguridad nacional, sino que también puede interrumpir servicios para

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

la población, lo que resalta la urgencia de una regulación robusta que establezca acciones de prevención, respuesta y resiliencia.

La preocupación de los ciudadanos y las empresas ante el incremento de fraudes cibernéticos que afectan sus finanzas y patrimonio es una realidad que exige atención inmediata. La implementación de una Ley General en materia de Ciberseguridad brindaría un marco legal que proteja a los usuarios de estafas y fraudes, además de fomentar la confianza en el uso de tecnologías digitales y en el comercio electrónico.

Propuesta legislativa

Esta iniciativa propone la creación de una Ley General en materia de Ciberseguridad que establezca el marco jurídico necesario para la creación de instituciones y regulación en la materia.

De esta forma, la expedición de esta Ley General está supeditada a la reforma a la Constitución que faculta al Congreso de la Unión para legislar en la materia. Iniciativa que se presenta de forma paralela al presente proyecto. Lo anterior, permitirá que México cuente con una regulación coordinada y efectiva, donde se establezcan claramente las competencias de cada orden de gobierno en materia de ciberseguridad.

De esta forma, tendremos una legislación integral, que abarque desde la prevención hasta la respuesta ante incidentes, fomentando una mayor colaboración entre los diferentes órdenes de gobierno y el sector privado para proteger efectivamente la seguridad digital en México.

Además, contar con una Ley General en materia de Ciberseguridad permitirá crear una cultura de seguridad digital en la sociedad. Todo ello es necesario para asegurar un entorno digital seguro y confiable, donde los ciudadanos y las organizaciones puedan interactuar en un ciberespacio más seguro.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Antecedentes y panorama de la ciberseguridad

El entorno digital se ha vuelto cada vez más vulnerable a ataques cibernéticos que afectan a las instituciones y los derechos humanos de las personas. Esto ha obligado a los países y organizaciones internacionales a desarrollar legislación, estrategias y recomendaciones para prevenir, generar respuestas y resarcir los daños de los ataques cibernéticos.

En enero de 2025, el Foro Económico Mundial presentó el informe Global Cybersecurity Outlook 2025[1], que examina las tendencias en ciberseguridad que impactarán a economías y sociedades.

Este informe destaca la creciente complejidad del panorama de la ciberseguridad debido a varios factores: las tensiones geopolíticas están generando un ambiente más incierto; la rápida adopción de tecnologías emergentes crea vulnerabilidades que los ciberdelincuentes aprovechan para aumentar la sofisticación y escala de sus ataques; la creciente regulación a nivel mundial impone cargas significativas de cumplimiento e inversión para las organizaciones; una falta de competencias digitales dificulta la gestión eficaz de los riesgos cibernéticos; y la complejidad del ciberespacio alimenta la inequidad cibernética, ampliando la brecha entre grandes y pequeñas organizaciones, profundizando la división entre economías desarrolladas y emergentes.

El informe resalta que la resiliencia cibernética varía considerablemente según la región. Mientras solo el 15% de los encuestados en este estudio en Europa y América del Norte expresa desconfianza en la capacidad de su país para responder a incidentes que afecten la infraestructura crítica, esa proporción se eleva al 36% en África y al 42% en América Latina.

Además, el sector público enfrenta problemas más severos, ya que el 38% de los encuestados percibe una resiliencia insuficiente, en contraste con solo el 10% en organizaciones medianas y grandes del sector privado.

---

[1] *Foro Económico Mundial. Perspectivas* de ciberseguridad global 2025. https://es.weforum.org/publications/global-cybersecurity-outlook-2025/

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

El 49% de las organizaciones del sector público indicó que existe una falta de talento para cumplir con sus objetivos en materia de ciberseguridad. Esta cifra se incrementó un 33% respecto de 2024.

En cuanto a las nuevas tecnologías, aunque el 66% de las organizaciones anticipa que la inteligencia artificial (IA) será el principal elemento de riesgo en la ciberseguridad el próximo año, solo el 37% indica que tiene procesos para evaluar la seguridad de las herramientas de IA antes de su implementación.

En México la ciberseguridad se ha convertido en una de las principales preocupaciones de las personas, las empresas y de muchas instituciones de gobierno. Lo anterior, ha originado la creación de una cantidad importante de asociaciones dedicadas a la atención de la ciberseguridad desde la perspectiva académica, gubernamental y del sector privado.

De acuerdo con el "3er Estudio de ciberseguridad en México 2023" realizado por la Asociación del Internet de México (AIMX), Amazon y el Consejo de Datos y Tecnologías Emergentes (CDETECH)[2], entre otras organizaciones, existe una percepción de riesgos y preocupaciones relevantes en materia de ciberseguridad entre los mexicanos. Los datos de este estudio concluyen lo siguiente:

- El 69% de los usuarios de Internet expresa una gran preocupación por convertirse en víctimas de problemas de seguridad en línea; en contraste, el 21% muestra una preocupación neutral y el 10% considera el tema como un problema menor.
- El 73% de los encuestados identifica los ataques financieros como su principal motivo de preocupación, seguido por un 66% que teme a la suplantación de identidad.
- En los últimos doce meses, los encuestados han señalado que el principal riesgo al navegar por Internet es la exposición a noticias falsas (32.6%).
- Un 14.1% afirma haber sido víctima de algún tipo de fraude financiero; además, el 57.6% indica que ha sido víctimas de alguna manera, aunque no especifican cómo.
- El 26% de los encuestados afirma que en el último año ha tenido cargos no reconocidos en sus tarjetas bancarias.

---

[2] *3er Estudio de ciberseguridad en México 2023 realizado por la Asociación del Internet de México (AIMX) y el Consejo de Datos y Tecnologías Emergentes (CDETECH). https://irp.cdn-website.com/81280eda/files/uploaded/VC%20Estudio%20de%20CIberseguridad%20en%20mexico%202023%20(7)-6339c715.pdf*

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

- El 43% de los encuestados señala que sus hijos reciben en la escuela orientación sobre los riesgos asociados a Internet, aunque un número considerable, el 57%, reconoce que no sabe o no recibe este tipo de información. Esto es significativo dado que el 35% de los padres no ha recibido información sobre los riesgos de Internet y un 22% tiene información desactualizada.

En cuanto a las empresas, según estimaciones de International Data Corporation (IDC), México enfrenta un número de 85 mil millones de intentos de ataques anuales a la ciberseguridad. En ese sentido, la ciberseguridad se ha convertido en una de las principales preocupaciones de las empresas, por lo que se refiere a la continuidad y la expansión de sus operaciones en el país.

El "3er Estudio de ciberseguridad en México 2023", en relación a las empresas con operaciones en el país, da a conocer lo siguiente:

Percepción de preparación en ciberseguridad

- Un 44% de los encuestados considera que su nivel de preparación en ciberseguridad es razonable.
- Solo un 4% se siente extremadamente preparado, mientras que el 18% se siente muy preparado.
- Por otro lado, un 25% se considera poco preparado y el 9% admite no estar preparado en absoluto.

Frecuencia de campañas de concientización

- El 43% de las organizaciones realiza campañas de concientización en seguridad de la información y ciberseguridad al menos cada seis meses.
- Un 10% lo hace al menos una vez al año, mientras que el 29% solo realiza estas campañas tras un incidente.
- Un 18% afirma no llevar a cabo nunca este tipo de actividades.

Capacitación del personal técnico

- Un 46% de las empresas capacitó a su equipo técnico en ciberseguridad en los últimos seis meses.
- El 28% lo hizo entre seis meses y un año, un 8% entre uno y tres años, y otro 8% hace más de tres años.
- Por último, el 10% no ha proporcionado capacitación en temas de ciberseguridad.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Presupuesto en Ciberseguridad

- Un 64% de las empresas encuestadas no tiene un presupuesto específico destinado a proyectos de ciberseguridad.

Amenazas enfrentadas

- La suplantación de identidad (phishing) es la amenaza más común, con un 40% de incidencia en las empresas encuestadas.
- Otras amenazas significativas como ransomware, fraude financiero, modalidades de suplantación de identidad y pérdida de información están en el rango del 20%, mientras que la fuga de información sensible afecta al 13%. En todos estos casos, las empresas han logrado detectar y detener los ataques.

Costos de incidentes de ciberseguridad

- La mayoría de las empresas perdió menos de $50,000 pesos debido a incidentes de ciberseguridad (25%), seguidas por un 8% que perdió entre $50,000 y $100,000 pesos.
- Un 19% de las empresas reporta haber sufrido un incidente que afectó sus cuentas bancarias en los últimos 18 meses, lo que significa que casi una de cada cinco empresas ha tenido problemas de seguridad cibernética con repercusiones financieras.

Acciones recomendadas para el gobierno

Los encuestados consideran que las acciones más importantes que el gobierno debe implementar en ciberseguridad empresarial son las siguientes:

- Crear un organismo de coordinación nacional en ciberseguridad (64%).
- Fortalecer el marco normativo vigente (58%).
- Generar programas de capacitación (56%).
- Fomentar la colaboración entre el sector privado y el gobierno para compartir información sobre amenazas (56%).

Asimismo, se considera necesario que el gobierno:

- Promueva la investigación en ciberseguridad (35%).
- Ofrezca certificaciones e incentivos fiscales a empresas que mantengan buenos estándares e inviertan en ciberseguridad (34% cada uno).
- Desarrolle protocolos de respuesta y recuperación ante ciberataques (29%).

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Antecedentes normativos en materia de Ciberseguridad

En este contexto, el Convenio de Budapest (2001)[3], elaborado por el Consejo de Europa y conocido como el Convenio sobre Ciberdelincuencia, representó el primer esfuerzo internacional para abordar la delincuencia en el ciberespacio. Su objetivo es facilitar la cooperación entre países en la lucha contra los delitos informáticos. A partir de este convenio, los estados se comprometen a incorporar en su legislación nacional las disposiciones necesarias para investigar y perseguir penalmente los delitos cometidos contra sistemas o medios informáticos, así como aquellos que se cometen mediante el uso de estos.

De manera posterior, se han emitido diversos documentos y resoluciones internacionales, de entre los que destacan los siguientes:

- El 4 de julio de 2018, la Asamblea General de las Naciones Unidas[4] aprobó una resolución sobre los derechos humanos en Internet, subrayando que las nuevas tecnologías de información y comunicación son fundamentales para promover, proteger y disfrutar de estos derechos. La resolución destaca la importancia de:

  - Fomentar la seguridad y confianza en Internet, especialmente en lo que respecta a la libertad de opinión y expresión, la privacidad y otros derechos humanos, así como aprovechar el potencial de Internet como facilitador del desarrollo y la innovación. Esto requiere una colaboración efectiva entre gobiernos, sociedad civil, sector privado, comunidad técnica y medios académicos.
  - Se insta a los Estados a abordar los desafíos de seguridad en Internet, cumpliendo con sus obligaciones internacionales en materia de derechos humanos, para garantizar la protección en línea de derechos fundamentales, como la libertad de opinión y expresión, la libertad de asociación y la privacidad. Esto debe realizarse a través de instituciones nacionales que sean democráticas y transparentes, basándose en el estado de derecho, y asegurando la libertad y la seguridad en el entorno digital, de modo que Internet continúe siendo una fuerza dinámica para el desarrollo económico, social y cultural.

[3] Consejo de Europa. Convenio de Budapest. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
[4] Asamblea General de las Naciones Unidas. Resolución sobre la Promoción, protección y disfrute de los derechos humanos en Internet. https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

- En 2021, el Consejo de la Unión Europea (UE) adoptó medidas en el marco de la Estrategia de Ciberseguridad para la Década Digital[5], con el objetivo de proteger a ciudadanos y empresas de ciberamenazas, promover sistemas de información seguros y asegurar un ciberespacio global abierto y seguro. Los puntos principales de esta estrategia incluyen:

  - La creación de una red de centros de operaciones de seguridad en toda la UE para monitorear y anticipar ataques a las redes.
  - La adopción de normativas para Internet, que son clave para mejorar la seguridad y la competitividad de las empresas europeas.
  - El fomento del desarrollo de un cifrado robusto para proteger los derechos fundamentales y la seguridad digital.
  - La mejora de la eficacia de las herramientas de ciberdiplomacia, enfocándose en prevenir ciberataques que amenazan cadenas de suministro, infraestructuras críticas y servicios esenciales.
  - El reforzamiento de la colaboración con organizaciones internacionales y países socios para compartir una visión común sobre las ciberamenazas.

- En 2023, en el marco de la Conferencia Global de la UNESCO en febrero de 2023[6], se desarrollaron directrices para regular las plataformas digitales. Con los siguientes objetivos:

  - Enriquecer y apoyar un espacio compartido por múltiples partes interesadas a nivel mundial para debatir y compartir buenas prácticas sobre la regulación de las plataforma digitales a fin de proteger la libertad de expresión y el acceso a la información, a la vez de tratar contenidos ilegales conforme a la normativa internacional de derechos humanos y contenidos que podrían poner en riesgo significativo la democracia y el disfrute de los derechos humanos, reuniendo diferentes visiones y un amplio espectro de perspectivas.
  - Servir como una herramienta para que todas las partes interesadas relevantes aboguen por una regulación que respete los derechos humanos y que logre que las plataformas gubernamentales y digitales asuman su responsabilidad.

- En agosto de 2024, los Estados miembros de la Organización de las Naciones Unidas (ONU), con representación de una delegación de México, aprobaron de manera consensuada el texto de la Convención contra el Ciberdelito. Este pacto se convertirá

---

[5] Consejo de la Unión Europea. Ciberseguridad: el Consejo adopta unas Conclusiones sobre la Estrategia de Ciberseguridad de la UE. https://www.consilium.europa.eu/es/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

[6] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). Directrices para regular las plataformas digitales: Un enfoque de múltiples partes interesadas para salvaguardar la libertad de expresión y el acceso a la información. https://www.unesco.org/sites/default/files/medias/fichiers/2023/05/draft2_guidelines_for_regulating_digital_platforms_es.pdf

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

en el primer instrumento jurídicamente vinculante a nivel mundial en el ámbito de la ciberdelincuencia[7][8].

- La Convención establecerá las bases para una cooperación internacional y proporcionará herramientas para abordar la ciberdelincuencia de manera colectiva y eficiente. Además, ayudará a cerrar las lagunas legislativas existentes y a establecer estándares que faciliten la armonización normativa a nivel internacional.
- En este sentido, México deberá ajustar su legislación local para alinearse con estos estándares internacionales.

Ejemplos de leyes en materia de Ciberseguridad en el mundo

De acuerdo con el último informe del Foro Económico Mundial, titulado "Panorama Global de Ciberseguridad del 2024", nuevas leyes de ciberseguridad entraron en vigor en las principales economías de todo el mundo, transformando el entorno normativo mundial. A continuación, se describen los principales sistemas normativos:

1. Directiva SRI 2: nuevas normas sobre ciberseguridad de las redes y sistemas de información de la Unión Europea[9][10]

- La Directiva SRI 2 establece un marco legal unificado en la Unión Europea (UE) para fortalecer la ciberseguridad en dieciocho sectores críticos. Además, exige a los Estados miembros que formulen estrategias nacionales de ciberseguridad y cooperen con la UE

[7] Asamblea General de las Naciones Unidas. La Asamblea General de las Naciones Unidas adopta una convención histórica contra la ciberdelincuencia. https://www.unodc.org/lpomex/es/noticias/diciembre-2024/la-asamblea-general-de-las-naciones-unidas-adopta-una-convencion-historica-contra-la-ciberdelincuencia.html

[8]Secretaría de Relaciones Exteriores. El Gobierno de México celebra la adopción de la Convención contra el Ciberdelito en la ONU. https://www.gob.mx/sre/prensa/el-gobierno-de-mexico-celebra-la-adopcion-de-la-convencion-contra-el-ciberdelito-en-la-onu?idiom=es#:~:text=Los%20Estados%20miembros%20de%20la,vinculante%20en%20materia%20de%20ciberdelincuencia.

[9] Comisión Europea. Directiva SRI 2: nuevas normas sobre ciberseguridad de las redes y sistemas de información. https://digital-strategy.ec.europa.eu/es/policies/nis2-directive

[10] Comisión Europea. Ciberseguridad de las redes y sistemas de información. https://eur-lex.europa.eu/ES/legal-content/summary/cybersecurity-of-network-and-information-systems-2022.html?fromSummary=23

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

en la respuesta y el cumplimiento transfronterizo. Cada Estado miembro deberá adoptar su propia Estrategia nacional de ciberseguridad, que incluirá:

- Un marco de gobernanza que defina claramente los roles y responsabilidades de las partes interesadas a nivel nacional.
- Políticas que aborden la seguridad en las cadenas de suministro.
- Estrategias para la gestión de vulnerabilidades.
- Iniciativas para promover y desarrollar la educación y formación en ciberseguridad.
- Medidas para aumentar la concienciación de los ciudadanos sobre ciberseguridad.

- La regulación de sectores críticos se aplica principalmente a entidades medianas y grandes que operan en áreas de alta relevancia, tales como:

- Energía y electricidad: esto incluye sistemas de producción, distribución y transporte, así como puntos de recarga, calefacción y refrigeración urbanas.
- Petróleo: abarca la producción, almacenamiento y oleoductos de transporte.
- Gas: incluye sistemas de suministro, distribución, transporte y almacenamiento, así como el hidrógeno.
- Transporte: comprende el transporte aéreo, ferroviario, marítimo, fluvial y por carretera.
- Banca e infraestructuras de mercados financieros: esto incluye entidades de crédito, gestores de centros de negociación y entidades de contrapartida central.
- Sector sanitario: incluye proveedores de atención médica, fabricantes de productos farmacéuticos y dispositivos médicos esenciales, así como laboratorios de referencia de la UE.
- Agua potable y aguas residuales.
- Gestión de servicios de tecnologías de la información y comunicaciones (TIC) (de empresa a empresa).
- Administración pública a niveles central y regional, excluyendo el poder judicial, los parlamentos y los bancos centrales; sin embargo, no se aplica a entidades que trabajan en asuntos de seguridad nacional, seguridad pública, defensa o aplicación de la ley.

Además, la regulación se extiende a otros sectores críticos, tales como:

- Servicios postales y de mensajería.
- Gestión de residuos.
- Fabricación, producción y distribución de sustancias químicas y mezclas.
- Producción, transformación y distribución de alimentos.
- Fabricación de productos sanitarios, equipos informáticos, electrónicos y ópticos, ciertos tipos de materiales eléctricos, maquinaria, vehículos de motor y otros medios de transporte.
- Proveedores de servicios digitales, incluidos mercados en línea, motores de búsqueda y redes sociales.
- Organismos de investigación.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

- También incluye disposiciones sobre supervisión, aplicación y revisiones voluntarias por pares para mejorar la confianza mutua y las capacidades de ciberseguridad en toda la UE.

- Se crea una red de equipos de respuesta a incidentes de seguridad informática (CSIRT) para intercambiar información sobre amenazas cibernéticas y gestionar incidentes. Estas entidades ofrecen asistencia técnica a diversas organizaciones a través de las siguientes actividades:

  - Monitoreo y análisis de ciberamenazas, vulnerabilidades e incidentes a nivel nacional.
  - Difusión de alertas tempranas, avisos e información relevante sobre ciberamenazas y vulnerabilidades a las entidades afectadas y otras partes interesadas, en la medida de lo posible en tiempo casi real.
  - Respuesta a incidentes y provisión de asistencia cuando sea necesario.
  - Recopilación y análisis de datos forenses, así como la realización de análisis dinámicos de riesgos e incidentes para mejorar el conocimiento general de la situación de ciberseguridad.
  - Provisión, bajo solicitud, de una evaluación proactiva de sistemas de redes e información para identificar vulnerabilidades que podrían tener un impacto significativo.

- Se establece la Red Europea de Organizaciones de Enlace para Cibercrisis (EU-CyCLONe), con el objetivo de facilitar una gestión coordinada y asegurar el intercambio regular de información entre los Estados miembros y las instituciones de la UE en situaciones de incidentes y crisis a gran escala. Esta red se encargará de:
  - Coordinar la gestión de incidentes y crisis de ciberseguridad de gran envergadura, así como apoyar la toma de decisiones a nivel político.
  - Mejorar la preparación ante posibles ciberamenazas.
  - Evaluar las consecuencias y repercusiones de los incidentes y crisis de ciberseguridad a gran escala, además de proponer medidas correctivas adecuadas.

- Las entidades están obligadas a informar a la autoridad correspondiente sobre cualquier incidente que:

  - Genere o pudiera generar perturbaciones operativas significativas o pérdidas económicas para la entidad.
  - Haya afectado o pueda afectar a terceros, ocasionando daños materiales o inmateriales sustanciales.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Ley Europea de Ciberresiliencia y su reglamento

En 2024, la Ley de Ciberresiliencia de la UE entró en vigor[11], estableciendo nuevas responsabilidades para reforzar la ciberseguridad en una amplia gama de productos de hardware y software de uso cotidiano. Sus objetivos principales incluyen[12],:

- Establecer requisitos de ciberseguridad para el diseño, desarrollo y producción de productos con componentes digitales, asegurando que los fabricantes mantienen la seguridad a lo largo del ciclo de vida del producto.
- Desarrollar estándares para la comercialización de productos con elementos digitales, garantizando así su ciberseguridad y promoviendo un mercado seguro.
- Obligar a los fabricantes a implementar procesos robustos de gestión de vulnerabilidades, informando sobre las vulnerabilidades e incidentes explotados y brindando apoyo durante todo el ciclo de vida del software, o al menos por cinco años de forma efectiva.
- Fomentar que los consumidores tengan en cuenta la ciberseguridad en su elección y uso de productos digitales, mejorando la transparencia respecto al período de soporte de estos productos.
- Proveer guías y directrices a las pequeñas y medianas empresas para facilitar su cumplimiento con la ley.

Estrategia Nacional de Ciberseguridad de Estados Unidos[13]

- Lanzada por primera vez a comienzos de 2023, la Estrategia Nacional de Ciberseguridad de Estados Unidos busca "asegurar que todos los estadounidenses se beneficien de un ecosistema digital seguro" y reforzar la colaboración entre los sectores público y privado para crear un entorno cibernético protegido, según lo establece el gobierno de EE. UU[14].

Esta estrategia se fundamenta en tres principios clave:

---

[11] Comisión Europea. Entra en vigor la Ley de Ciberresiliencia para hacer que el ciberespacio europeo sea más seguro y protegido. https://digital-strategy.ec.europa.eu/es/news/cyber-resilience-act-enters-force-make-europes-cyberspace-safer-and-more-secure#:~:text=La%20Ley%20de%20Ciberresiliencia%20(CRA,productos%20de%20hardware%20y%20software.

[12] Instituto Nacional de Ciberseguridad de España. La Ley de Ciberresiliencia. https://www.incibe.es/empresas/blog/la-comision-europea-presenta-una-nueva-propuesta-de-resiliencia-cibernetica

[13] Departamento de Estado de los Estados Unidos. United States International Cyberspace & Digital Policy Strategy. https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

[14] Departamento de Estado de los Estados Unidos. Presentación de la Estrategia Internacional de Estados Unidos sobre Política Digital y Ciberespacio. https://cl.usembassy.gov/es/presentacion-de-la-estrategia-internacional-de-estados-unidos-sobre-politica-digital-y-ciberespacio/

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

1. Una visión optimista de un ciberespacio seguro e inclusivo, respaldada por el derecho internacional, incluyendo el respeto por los derechos humanos.
2. La integración de la ciberseguridad con el desarrollo sostenible y la innovación tecnológica.
3. Un enfoque integral en la política que utilice herramientas diplomáticas y de orden internacional adecuadas dentro del ecosistema digital.

Asimismo, se identifican cuatro áreas de acción:

1. Promover, construir y mantener un ecosistema digital que sea abierto, inclusivo, seguro y resiliente.
2. Armonizar enfoques con socios internacionales en gobernanza digital y de datos que respeten los derechos fundamentales.
3. Impulsar un comportamiento responsable entre los estados en el ciberespacio y contrarrestar amenazas a la infraestructura crítica mediante la formación de coaliciones y la colaboración con aliados.
4. Fortalecer y desarrollar la capacidad digital y cibernética de los socios internacionales, incluyendo habilidades para combatir la ciberdelincuencia.

Ley Marco de Ciberseguridad de Chile

El lunes 8 de abril de 2024, se publicó la Ley Marco de Ciberseguridad de Chile, que tiene como propósito fundamental establecer la institucionalidad, los principios y la normativa general necesarios para estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y su relación con el sector privado.

La ley establece requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad, así como:

1. Requisitos y atribuciones:
   - Define los requisitos mínimos para enfrentar incidentes de ciberseguridad.
   - Establece las atribuciones y obligaciones de los organismos estatales.
   - Determina los deberes de las instituciones designadas en la ley y los mecanismos de control, supervisión y responsabilidad por infracciones.
2. Definiciones claves:
   - Proporciona definiciones de conceptos como activo informático, auditorías de seguridad, ciberataque, ciberseguridad e incidente de ciberseguridad.
3. Principios rectores:

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

- Establece principios fundamentales como el control de daños, cooperación con las autoridades, coordinación y seguridad en el ciberespacio.

4. Creación de la Agencia Nacional de Ciberseguridad:
   - Se crea un organismo descentralizado con personalidad jurídica y patrimonio propio, encargado de asesorar al Presidente de la República en temas de ciberseguridad.
   - La Agencia tiene atribuciones para dictar protocolos y estándares, aplicar disposiciones legales y reglamentarias, coordinar el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y administrar un Registro Nacional de Incidentes de Ciberseguridad.
5. Ámbito de aplicación:
   - La ley se aplica a instituciones que ofrecen servicios esenciales, incluyendo organismos del Estado y concesionarios de servicios públicos, así como a instituciones privadas que realicen actividades designadas en la norma.
6. Deberes para operadores críticos:
   - Se establecen obligaciones específicas para los operadores vitales, como la implementación de un sistema continuo de gestión de información, el desarrollo de planes de continuidad operacional y ciberseguridad, y la ejecución de revisiones y medidas para mitigar el impacto de incidentes de ciberseguridad.
7. Consejos y equipos de respuesta:
   - Se crea el Consejo Multisectorial sobre Ciberseguridad para asesorar y formular recomendaciones sobre la situación de ciberseguridad en el país y las amenazas existentes.
   - Se establece el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional) para responder a ciberataques significativos y supervisar incidentes a nivel nacional, así como para llevar a cabo capacitación en ciberseguridad.
   - Se forma el CSIRT de la Defensa Nacional para supervisar las redes y sistemas del Ministerio de Defensa y de servicios esenciales relacionados.
   - Finalmente, se instituyen el Comité Interministerial sobre Ciberseguridad y la Red de Conectividad Segura del Estado (RCSE) que tiene por objeto asesorar al Presidente de la Republica en materias de ciberseguridad relevantes para el funcionamiento del país y la Red de Conectividad Segura del Estado (RCSE) encargada de proveer servicios de interconexión y conectividad a internet a los organismos de la Administración del Estado.

¿Qué debería incluir una Ley de Ciberseguridad en México?

Con base en lo anterior, de la revisión de la legislación a nivel nacional, acuerdos internacionales y buenas prácticas, se concluye que una ley de ciberseguridad en nuestro país debería incluir y favorecer lo siguiente:

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

- **Definir "ciberseguridad"**: precisar el concepto de ciberseguridad en México, incluyendo la protección de datos, la disponibilidad de servicios digitales y la protección de derechos digitales.
- **Fortalecer la seguridad nacional**: proteger la infraestructura crítica del país, incluyendo los servicios de salud, financieros, así como de comunicaciones y transporte, frente a ciberataques que pongan en riesgo la seguridad, la economía y servicios esenciales como la atención sanitaria.
- **Garantizar la seguridad digital de las personas**: proteger información personal, privacidad y libertad de expresión en el entorno digital.
- **Promover la confianza digital**: fomentar el uso seguro y responsable de tecnologías digitales y construir una cultura de ciberseguridad. Las medidas de ciberseguridad deben enfocarse en proteger los derechos de la sociedad, en lugar de ser meramente punitivas.
- **No vulnerar al acceso a Internet:** evitar la inclusión de disposiciones que puedan violar el derecho a Internet o que otorguen facultades a las autoridades para intervenir en la red.
- **Crear una regulación enfocada en prevenir riesgos en materia de ciberseguridad: Priorizar las acciones preventivas para evitar incidentes de ciberseguridad.**
- **Fomentar la innovación tecnológica**: apoyar el desarrollo de tecnologías y herramientas que mejoren la ciberseguridad.
- **Armonizar el marco legal**: unificar y coordinar las leyes en materia de ciberseguridad para evitar lagunas legales y garantizar coherencia en todos los órdenes de gobierno.
- **Darle a la legislación en materia de ciberseguridad un sustento constitucional: Facultar al Congreso para legislar en la materia.**
- **Establecer un Sistema Nacional de Ciberseguridad**: crear un sistema de coordinación entre gobierno, empresas y sociedad civil para una respuesta efectiva a incidentes cibernéticos.
- Definición de competencias: establecer claramente las competencias de los diferentes órdenes de gobierno, es decir, de la Federación, las entidades federativas y municipios.
- **Crear un organismo de ciberseguridad**: crear un organismo encargado de supervisar las acciones del gobierno en ciberseguridad.
- **Desarrollar la Estrategia Nacional de Ciberseguridad**: definir políticas y acciones concretas para fortalecer la ciberseguridad en el país.
- **Crear una Comisión Consultiva de Ciberseguridad**: integrar a expertos, funcionarios y empresas para ofrecer recomendaciones en materia de ciberseguridad.
- **Sistema de Alerta Temprana**: implementar un sistema que informe a la población, las empresas y a las instituciones sobre amenazas cibernéticas inminentes.
- **Detección de ciberataques**: establecer mecanismos efectivos para monitorear y detectar ciberataques, garantizando respuestas oportunas.
- No militarizar el ciberespacio: garantizar que las políticas de ciberseguridad se diseñen e implementen desde organizaciones de carácter civil.
- **Programas de capacitación**: desarrollar programas de ciberseguridad para diversos sectores, incluyendo niños, niñas y adolescentes.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

- **Impulsar la industria de ciberseguridad**: fomentar el crecimiento de la industria de ciberseguridad en México para crear un ecosistema robusto ante amenazas cibernéticas.
- Fomentar la oferta educativa: abrir espacios desde las universidades públicas para ofrecer a las y los jóvenes la posibilidad de estudiar especialidades, licenciaturas y posgrados sobre ciberseguridad.
- Promover de infraestructura educativa: promover la infraestructura adecuada en las universidades para preparar a las y los jóvenes ante las nuevas oportunidades laborales relacionadas a la ciberseguridad, así como brindar las herramientas tecnológicas necesarias para el desarrollo educativo.
- Establecer mecanismos prevención de delitos:
- Reforzamiento o creación de unidades especializadas en ciberseguridad en las instituciones de seguridad pública.
- La capacitación en materia de ciberseguridad.
- La promoción de la cooperación internacional para combatir el cibercrimen.

Diagnóstico de la legislación en materia de ciberseguridad en México

Actualmente, en México no existe facultad específica que permita al Congreso de la Unión expedir la ley general de ciberseguridad, lo que ha llevado a que la mayoría de las propuestas se limiten a leyes federales o a la modificación de leyes actuales. Por esta razón, se considera necesario reformar la Constitución para otorgar al Congreso la facultad de expedir una ley general.

En ese sentido, la presente iniciativa está supeditada a la reforma a la Constitución que faculta al Congreso de la Unión para legislar en la materia. Iniciativa que se presenta de forma paralela al presente proyecto. Lo anterior, en virtud de lo siguiente:

a) Al establecer una ley general de ciberseguridad a través de una reforma constitucional, se creará un marco legal sólido y coherente que abarque todas las jurisdicciones: federal, estatal y municipal.

b) Esta reforma permitirá a los gobiernos locales desarrollar y adaptar leyes de ciberseguridad de acuerdo con sus particularidades y necesidades específicas. De lo contrario, en caso de no existir una ley general, cada entidad federativa podría expedir sus propias leyes en la materia con criterios diferenciados o contradictorios.

c) Una ley general de ciberseguridad facilitará la distribución adecuada de competencias entre la federación y los gobiernos locales, asegurando que cada nivel de gobierno tenga responsabilidades claras en la materia.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

d) La ciberseguridad no solo es una cuestión de seguridad nacional, sino que también debe abordarse en el ámbito local. La reforma asegurará que todos los gobiernos cuenten con herramientas y directrices normativas para proteger adecuadamente a ciudadanos y organizaciones.

En ese sentido, la referida iniciativa en materia de reforma constitucional establece que la Ley General en materia de Ciberseguridad deberá incluir lo siguiente:

a) Las reglas para fortalecer la capacidad del Estado para prevenir, detectar, mitigar y responder efectivamente a las amenazas de ciberseguridad que puedan afectar la seguridad nacional, la infraestructura tecnológica del país, la economía y los derechos humanos de las personas.
b) El marco normativo que promueva la transparencia, la responsabilidad en el manejo de la información y los datos digitales, y el combate al robo de información, en estricto apego a los derechos humanos.
c) La coordinación entre la Federación, las entidades federativas, los municipios y las alcaldías de la Ciudad de México en materia de ciberseguridad, fomentando la colaboración con el sector privado, el sector académico y otros organismos nacionales e internacionales;
d) La creación y funcionamiento del Sistema Nacional de Ciberseguridad, que garantice una respuesta integral y coordinada ante incidentes en materia de ciberseguridad.
e) La Estrategia Nacional de Ciberseguridad, que defina las políticas, objetivos y acciones para enfrentar adecuadamente las amenazas de ciberseguridad en el país.

Descripción de la Ley General en materia de Ciberseguridad

Principios

- Para alcanzar los objetivos de esta Ley se deberán observar los siguientes principios:

  - Cooperación multisectorial
  - Control de daños
  - Fomento de la cultura digital responsable
  - Innovación
  - Interoperabilidad
  - Libre circulación de datos
  - Prevención de riesgos

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

- Proporcionalidad
- Resiliencia
- Respeto a los Derechos Humanos
- Seguridad e integridad de los datos
- Seguridad en el ciberespacio
- Transparencia

Sistema Nacional de Ciberseguridad

El Sistema Nacional de Ciberseguridad será responsable de coordinar y gestionar políticas en ciberseguridad en México. Su objetivo será fortalecer, prevenir, detectar, mitigar y responder a amenazas cibernéticas que puedan afectar la seguridad nacional, la infraestructura crítica, la economía y los derechos fundamentales.

Estará integrado por representantes de diversas instituciones, incluyendo:

1. Secretaría de Seguridad y Protección Ciudadana (presidida por ella).
2. Secretaría de Hacienda y Crédito Público.
3. Secretaría de Ciencia, Humanidades, Tecnología e Innovación.
4. Secretaría de la Defensa Nacional.
5. Secretaría de Marina.
6. Secretaría de Relaciones Exteriores.
7. Secretaría de Infraestructura, Comunicaciones y Transportes.
8. Agencia de Transformación Digital y Telecomunicaciones.
9. Centro Nacional de Ciberseguridad.
10. Guardia Nacional.
11. Unidad de Inteligencia Financiera.
12. Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública.
13. Comisión Nacional de Mejora Regulatoria.
14. Un representante designado por cada gobernador (preferiblemente el Secretario de Seguridad).
15. Otros que se determinen.

El sistema podrá invitar a autoridades estatales, legisladores, miembros del Poder Judicial, representantes de organismos internacionales y expertos en ciberseguridad, quienes participarán con derecho a voz, pero sin voto.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

El Sistema Nacional de Ciberseguridad tendrá, entre otras, las siguientes atribuciones:

- Mejorar la capacidad del Estado para prevenir, detectar, mitigar y responder a amenazas cibernéticas que afecten la seguridad nacional, la infraestructura crítica, la economía y los derechos de las personas.
- Coordinar esfuerzos entre la federación, entidades federativas, municipios y las alcaldías de la Ciudad de México, promoviendo la cooperación con el sector privado.
- Contribuir a la creación e implementación de la Estrategia Nacional de Ciberseguridad.
- Implementar mecanismos de cooperación internacional y participar en organismos para gestionar amenazas cibernéticas.
- Fomentar acuerdos y colaboraciones con otros países para combatir el cibercrimen.
- Facilitar la colaboración del sector privado y académico en el desarrollo de estrategias de ciberseguridad.

Distribución de competencias en materia de ciberseguridad

Se establece la distribución de competencias en materia de ciberseguridad entre la Federación, las entidades federativas, los municipios y las alcaldías de la Ciudad de México.

Competencias de la Federación (a través del Centro Nacional de Ciberseguridad y autoridades competentes):

1. Establecer políticas y estrategias nacionales de ciberseguridad para proteger la infraestructura crítica y la información sensible.
2. Coordinar áreas de ciberseguridad en la Administración Pública Federal y órganos autónomos.
3. Coordinar acciones de ciberseguridad con instituciones de seguridad en entidades federativas y municipios.
4. Colaborar con autoridades extranjeras y organismos internacionales.
5. Proteger y vigilar infraestructuras críticas de información.
6. Contribuir a las políticas y programas de la Estrategia Nacional en su ámbito de competencia.
7. Participar en el Sistema Nacional de Ciberseguridad en el ámbito de su competencia.
8. Realizar acciones de prevención de delitos cibernéticos.
9. Participar en programas de capacitación en ciberseguridad.
10. Otras acciones establecidas por la ley y su reglamento.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Competencias de las entidades federativas:

1. Colaborar en políticas de coordinación del Centro Nacional de Ciberseguridad.
2. Participar en políticas y programas de la Estrategia Nacional en el ámbito de su competencia.
3. Participar en programas de capacitación.
4. Llevar a cabo acciones de prevención de delitos cibernéticos.
5. Otras acciones estipuladas por la ley y su reglamento.

Competencias de los municipios y alcaldías de la Ciudad de México:

1. Colaborar en políticas de coordinación del Centro Nacional de Ciberseguridad.
2. Contribuir a las políticas y programas de la Estrategia Nacional en su ámbito de competencia.
3. Participar en el Sistema Nacional de Ciberseguridad en el ámbito de su competencia.
4. Otras acciones definidas por la ley y su reglamento.

Centro Nacional de Ciberseguridad

Se plantea que el Centro Nacional de Ciberseguridad sea un organismo desconcentrado de la Secretaría de Seguridad y Protección Ciudadana, encargado de implementar acciones relacionadas con la ciberseguridad. Sus atribuciones incluirían:

1. Establecer lineamientos para políticas que fortalezcan la prevención y respuesta ante amenazas cibernéticas.
2. Diseñar y evaluar periódicamente la Estrategia Nacional de Ciberseguridad para asegurar su efectividad.
3. Integrar y coordinar esfuerzos gubernamentales para respetar los derechos humanos en el ciberespacio y promover la educación digital.
4. Proteger la infraestructura digital y los sistemas de información, mejorando la resiliencia a nivel nacional.
5. Coordinar la colaboración en ciberseguridad entre el gobierno, sector privado, academia y sociedad civil.
6. Promover la innovación y el desarrollo de tecnologías que fortalezcan la seguridad cibernética.
7. Fomentar la industria de ciberseguridad en México para enfrentar amenazas.
8. Elaborar anualmente el Programa Nacional de Riesgos Cibernéticos y el Catálogo Nacional de Infraestructuras Críticas.
9. Evaluar y monitorear la ciberseguridad en el país, implementando medidas para mejorar la respuesta ante incidentes.
10. Establecer mecanismos de monitoreo y detección de ciberataques para asegurar respuestas oportunas.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

11. Crear un sistema coordinado de respuesta rápida ante incidentes cibernéticos.
12. Promover medidas proactivas para evitar ciberataques, incluyendo educación y capacitación.
13. Proporcionar asesoramiento técnico en ciberseguridad a empresas, administraciones públicas y ciudadanos.
14. Interactuar con proveedores de servicios digitales sobre sus obligaciones de ciberseguridad.
15. Contribuir a la protección de datos personales en el ciberespacio.
16. Desarrollar estándares de seguridad cibernética para la Administración Pública Federal.
17. Informar sobre acciones necesarias para la seguridad nacional.
18. Elaborar bases y convocatorias para seleccionar a los miembros de la Comisión Consultiva de Ciberseguridad.

El Centro será dirigido por un director general, nombrado por el titular de la Secretaría de Seguridad y Protección Ciudadana, quien también supervisará su funcionamiento.

Comisión Consultiva de Ciberseguridad

La propuesta plantea la creación una Comisión Consultiva de Ciberseguridad, como órgano de consulta no remunerado, encargado de proporcionar orientación técnica y estratégica al Centro Nacional de Ciberseguridad en México. Estararía conformada por servidores públicos, profesionales, especialistas y representantes de la sociedad civil y el sector privado con experiencia técnica. Sus integrantes serían seleccionados por un periodo de cuatro años, de acuerdo con las bases emitidas por el Centro Nacional de Ciberseguridad.

Sus principales tareas incluirían:

1. Proporcionar asesoramiento experto a autoridades gubernamentales en ciberseguridad.
2. Emitir recomendaciones sobre políticas, normativas y estrategias al Centro Nacional de Ciberseguridad.
3. Analizar tendencias y mejores prácticas en ciberseguridad, evaluando su aplicación en México.
4. Promover la adopción de estándares internacionales de ciberseguridad.
5. Evaluar el impacto y efectividad de las políticas públicas de ciberseguridad.
6. Identificar y evaluar riesgos relacionados con la ciberseguridad.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

7. Evaluar el impacto de nuevas tecnologías emergentes en la ciberseguridad.
8. Fomentar la investigación y la colaboración entre academia, industria y gobierno para innovaciones en ciberseguridad.
9. Brindar sugerencias programas educativos sobre la importancia de la ciberseguridad para la ciudadanía.
10. Facilitar la colaboración entre el gobierno y la sociedad civil en ciberseguridad.
11. Recomendar indicadores para medir la eficacia de políticas y estrategias de ciberseguridad.
12. Contribuir al desarrollo de programas de gestión de crisis cibernéticas.
13. Apoyar la protección de infraestructuras críticas mediante directrices y protocolos de seguridad.
14. Promover la ciberseguridad en diferentes niveles de gobierno y en la sociedad.
15. Integrar expertos en diversas áreas para enriquecer el enfoque consultivo del Centro Nacional de Ciberseguridad.
16. Cumplir con otras funciones que le sean asignadas por el Centro, conforme al marco legal vigente.

Estrategia Nacional de Ciberseguridad

Esta iniciativa platea la creación de una Estrategia Nacional de Ciberseguridad, misma que será desarrollada por el Centro Nacional de Ciberseguridad, con apoyo de la Comisión Consultiva de Ciberseguridad. Su vigencia será de seis años y deberá evaluarse y actualizarse al menos cada dos años, conforme al sistema de planeación establecido en la Constitución y la Ley de Planeación.

La estrategia incluiría:

1. Medidas proactivas para identificar, prevenir y mitigar amenazas cibernéticas, con capacidades avanzadas de detección y protocolos claros de respuesta coordinada.
2. Protección de sectores estratégicos como energía, salud, finanzas y transporte.
3. Fomento de la colaboración público-privada y el intercambio de información.
4. Mecanismos de cooperación internacional mediante acuerdos y participación en organismos globales.
5. Programas de formación y capacitación en ciberseguridad para profesionales desde etapas tempranas.
6. Fomentar el desarrollo de profesionales cualificados en ciberseguridad.
7. Fomento de la investigación y desarrollo tecnológico en el área.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

8. Promoción de la industria de ciberseguridad en México a través de incentivos fiscales y programas de apoyo.
9. Campañas de sensibilización para mejorar la conciencia pública sobre ciberseguridad.
10. Implementación de un sistema de alerta temprana para informar sobre amenazas cibernéticas.
11. Establecimiento de centros de operaciones de seguridad cibernética para monitoreo en tiempo real.
12. Desarrollo de lineamientos para elaborar indicadores de seguridad cibernética.
13. Medios de difusión periódica sobre riesgos y eventos cibernéticos.
14. Acciones para gestionar emergencias sanitarias que afecten la ciberseguridad, incluyendo protocolos de protección de infraestructuras críticas.
15. Generación de estadísticas oficiales sobre riesgos cibernéticos, incluyendo ubicación e incidencia de ataques.
16. Promoción de un entorno regulatorio que fomente la innovación tecnológica en ciberseguridad.
17. Implementación de incentivos fiscales para empresas que inviertan en ciberseguridad.
18. Desarrollo de un sistema de alerta temprana con orientación para la protección contra ataques cibernéticos.
19. Programas de gestión de crisis cibernéticas, con protocolos de respuesta y recuperación ante incidentes.

Protección de Infraestructuras críticas

Se considerarán infraestructuras críticas aquellas redes, servicios, equipos e instalaciones relacionadas con activos de Tecnologías de Información y Comunicaciones, cuya afectación, interrupción o destrucción podría impactar significativamente la provisión de bienes y servicios esenciales.

Estos servicios esenciales incluirán:

- Seguridad y Defensa: sistemas de seguridad nacional, pública y protección civil.
- Servicios Financieros: instituciones como bancos, bolsas de valores y sistemas de pago.
- Salud: hospitales, clínicas y sistemas de gestión de datos de salud.
- Telecomunicaciones: redes de telefonía fija, móvil e internet.
- Energía: sistemas de generación y distribución de electricidad, petróleo y gas.
- Agua y Saneamiento: infraestructuras para la distribución de agua potable y gestión de aguas residuales.
- Transporte: aeropuertos, puertos y sistemas ferroviarios.
- Alimentación y Agricultura: Infraestructuras para la producción y distribución de alimentos.
- Entre otras.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Para la protección de estas infraestructuras, se reconocerán como riesgos e incidentes cibernéticos de seguridad nacional los siguientes:

- Incidentes que afectan sistemas de energía, comunicaciones, transporte, salud o finanzas, causando interrupciones significativas en los servicios esenciales.
- Actividades de inteligencia cibernética destinadas a obtener información clasificada o sensible para la seguridad nacional.
- Ataques dirigidos a sistemas de defensa, fuerzas armadas o entidades públicas responsables de la seguridad nacional.

El objetivo de esta ley es dotar a México de una legislación de vanguardia que proteja los derechos digitales de cada persona en el ciberespacio y garantice la seguridad de la infraestructura tecnológica del país.

La Ley General en materia de Ciberseguridad abarcará desde la prevención hasta la respuesta ante incidentes, promoviendo una mayor colaboración entre el gobierno y el sector privado, lo que fortalecerá la seguridad digital del país. Además, esta legislación fomentará una cultura de seguridad digital en la sociedad, creando un entorno digital seguro y confiable en el que tanto ciudadanos como organizaciones puedan interactuar con confianza en el ciberespacio.

Decreto.

Artículo Único. Se expide la Ley General en materia de Ciberseguridad.

Disposiciones Generales

Artículo 1. Las disposiciones de la presente Ley son de orden público, interés social y observancia en todo el territorio nacional en materia de ciberseguridad.

Artículo 2. Esta Ley tiene por objeto:

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

I. Fortalecer la capacidad del Estado para prevenir, detectar, mitigar y responder efectivamente a las amenazas cibernéticas que puedan afectar la seguridad nacional, la infraestructura tecnológica, la economía y los derechos fundamentales de las personas;

II. Establecer un marco normativo que promueva la transparencia, la responsabilidad y la ética en el manejo de la información y los datos digitales, a fin de combatir la desinformación, el robo de información y fortalecer la ciberseguridad con un enfoque basado en riesgos;

III. Promover el derecho a la protección de los datos personales, la privacidad e intimidad en las interacciones realizadas en el ámbito digital, en términos de las leyes en la materia;

IV. Coordinar la colaboración entre la Federación, las entidades federativas, los municipios y las alcaldías de la Ciudad de México en materia de ciberseguridad, fomentando la colaboración con el sector privado y otros organismos;

V. Desarrollar y establecer el Sistema Nacional de Ciberseguridad, que garantice una respuesta integral y coordinada ante incidentes cibernéticos en todos los órdenes de gobierno y la sociedad;

VI. Asegurar que las medidas de ciberseguridad respeten los derechos humanos y se ejecuten con consideraciones éticas, garantizando que no se infrinjan los derechos fundamentales de las personas;

VII. Establecer derechos y obligaciones digitales para los usuarios en el ciberespacio, promoviendo su protección y el ejercicio efectivo de su privacidad, libertad de expresión y seguridad digital;

VIII. Desarrollar la resiliencia en las infraestructuras críticas contra incidentes cibernéticos, garantizando la continuidad y recuperación efectiva de los servicios esenciales en situaciones adversas;

IX. Impulsar la innovación y la investigación tecnológica en ciberseguridad, en colaboración con entidades académicas y el sector privado;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

X. Promover el desarrollo y la adopción de estándares nacionales e internacionales de ciberseguridad, así como esquemas de certificación para productos, servicios y procesos de tecnologías de la información y la comunicación, en términos de la Ley de Infraestructura de la Calidad;

XI. Fomentar la educación y la concientización pública en ciberseguridad dirigidas a todos los niveles de la sociedad, fortaleciendo el conocimiento general sobre los riesgos y las mejores prácticas en el ciberespacio;

XII. Desarrollar la Estrategia Nacional de Ciberseguridad, que defina políticas, objetivos y medidas para enfrentar adecuadamente las amenazas cibernéticas en el país;

XIII. Fomentar la cooperación internacional en materia de ciberseguridad, promoviendo acuerdos y colaboraciones con otros países y organismos internacionales para fortalecer las capacidades y recursos para combatir el cibercrimen;

XIV. Fomentar el desarrollo de la industria de ciberseguridad en México, apoyando la investigación y la innovación tecnológica en este ámbito, con el objetivo de fortalecer las capacidades nacionales para enfrentar las amenazas cibernéticas y promover la creación de soluciones y servicios que contribuyan a la ciberseguridad;

XV. Promover una cultura de ciberseguridad a través de campañas permanentes que concienticen a la población sobre la importancia de la seguridad en el uso de tecnologías digitales;

XVI. Establecer programas de capacitación en ciberseguridad para distintos sectores de la sociedad, incluyendo la educación en ciberseguridad para niños, niñas y adolescentes, así como para profesionales, funcionarios públicos y pequeñas y medianas empresas, y

XVII. Fomentar la creación de soluciones de ciberseguridad accesibles para pequeñas y medianas empresas.

Artículo 3. Para alcanzar los objetivos de esta Ley se deberán observar los siguientes principios:

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

I. Cooperación multisectorial: promover la colaboración y coordinación entre el gobierno, el sector privado, la sociedad civil, la academia y otros actores relevantes para desarrollar estrategias y efectivas en ciberseguridad, así como su constante actualización cuando se requiera;

II. Control de daños: actuar de manera coordinada y diligente ante ciberataques o incidentes de ciberseguridad, adoptando las medidas necesarias para evitar la escalada de estos incidentes y su posible propagación a otros sistemas informáticos;

III. Fomento de la cultura digital responsable: promover la educación y sensibilización sobre el uso responsable y seguro de las tecnologías digitales, fomentando una cultura que valore la protección de la intimidad y el respeto a la libertad de expresión;

IV. Innovación: fomentar la innovación y el desarrollo tecnológico en ciberseguridad, incentivando la creación de soluciones y herramientas que contribuyan a proteger la intimidad y promover la confianza digital;

V. Interoperabilidad: procurar que los sistemas, políticas y normas de ciberseguridad sean compatibles y funcionen de manera coherente entre diferentes plataformas, organizaciones y países, promoviendo un enfoque global y coordinado;

VI. Libre circulación de datos: garantizar la libre circulación de datos en el ciberespacio, respetando la protección de la privacidad y de los datos personales;

VII. Prevención de riesgos: identificar y mitigar amenazas antes de que ocurran, mediante auditorías de seguridad, capacitaciones al personal y actualización constante de sistemas. Se debe fomentar una cultura de sensibilización sobre ciberseguridad y realizar evaluaciones periódicas de vulnerabilidades, protegiendo así la infraestructura crítica y los datos sensibles, y minimizando el impacto de posibles ataques.

VIII. Proporcionalidad: las medidas de ciberseguridad deberán ser proporcionales al nivel de riesgo y a la gravedad del impacto en la intimidad, la libertad de expresión y la confianza digital, procurando que sean mínimamente invasivas y evitando restricciones innecesarias;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

IX. Resiliencia: fomentar la prevención y detección temprana de amenazas, así como la implementación de mecanismos que permitan una rápida recuperación de los servicios tras un incidente, minimizando el impacto negativo sobre la sociedad y la economía;

X. Respeto a los Derechos Humanos: todas las acciones y políticas relacionadas con la ciberseguridad deben respetar y proteger los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales de los que México sea parte, incluyendo el derecho a la privacidad, la libertad de expresión, el acceso a la información y derecho a Internet;

XI. Seguridad e integridad de los datos: establecer medidas efectivas para garantizar la seguridad y la integridad de los datos personales y de otra información sensible, protegiéndolos contra accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas;

XII. Seguridad en el ciberespacio: es deber del Estado procurar la seguridad en el ciberespacio en términos de lo dispuesto por la presente ley, para que todas las personas puedan participar de él con seguridad, protegiendo especialmente a los grupos vulnerables, y

XIII. Transparencia: las autoridades responsables de la ciberseguridad deberán operar de manera transparente, proporcionando información clara y accesible sobre sus políticas, acciones y prácticas en relación con la protección de derechos, en términos de la ley en la materia.

Definiciones

Artículo 4. Para los efectos de la presente Ley se entenderá por:

I. Ciberataque: cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, denegar, degradar, obtener un acceso no autorizado o destruir los recursos de un sistema de información tecnológica, infraestructura crítica o la información en sí misma;

II. Ciberdelito: cualquier actividad ilícita que se comete utilizando medios electrónicos, sistemas informáticos, redes de comunicación o tecnologías digitales, con el

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

objetivo de obtener beneficios económicos, causar daño o vulnerar derechos en el ciberespacio;

III. Ciberespacio: se refiere al entorno virtual o digital en el que interactúan redes de computadoras, sistemas de información y las personas que hacen uso de ellos. Es un espacio no físico compuesto por la interconexión global de infraestructura tecnológica de información, internet, servicios de telecomunicaciones y sistemas informáticos;

IV. Ciberamenaza: cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones de una organización, los activos de la organización, los individuos, otras organizaciones o la acción a través de un sistema mediante el acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio;

V. Ciberseguridad: se refiere al conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de organizaciones o usuarios en el ciberentorno, tales como dispositivos informáticos conectados, servicios/aplicaciones, sistemas de comunicaciones, comunicaciones multimedios e información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan propiedades de seguridad de los activos de la organización y los usuarios contra riesgos de seguridad en el ciberentorno, que incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad.

VI. Centro: Centro Nacional de Ciberseguridad;

VII. Comisión: Comisión Consultiva de Ciberseguridad;

VIII. Estrategia: Estrategia Nacional de Ciberseguridad, plan integral que define políticas y acciones para mejorar la seguridad cibernética en el país;

IX. Incidente de Ciberseguridad: un evento que resulta en un riesgo real o potencial para la confidencialidad, integridad o disponibilidad de un sistema de información o de la información que el sistema procesa, almacena o transmite, o que constituye una violación o una amenaza inminente de violación de las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

X. Infraestructuras Críticas: son redes, servicios, equipos e instalaciones vinculados a activos de Tecnologías de Información y Comunicaciones, cuya afectación, interrupción o destrucción podría tener un impacto significativo en la provisión de bienes y servicios esenciales. Estos servicios esenciales incluyen la seguridad y defensa, que abarcan sistemas de seguridad nacional, seguridad pública y protección civil; los servicios financieros, como bancos, bolsas de valores y sistemas de pago; la salud, que incluye hospitales, clínicas y sistemas de gestión de datos de salud; las telecomunicaciones, como redes de telefonía fija y móvil e internet; la energía, involucrando la generación y distribución de electricidad, petróleo y gas; el agua y saneamiento, que comprende la distribución de agua potable y gestión de aguas residuales; el transporte, incluyendo aeropuertos, puertos y ferrocarriles; la alimentación y agricultura, que aseguran la producción y distribución de alimentos, y los demás que se consideren. Para efectos de la aplicación de esta ley, se deberá diferenciar entre el proveedor responsable y el proveedor de soporte de infraestructuras críticas, en función del nivel de responsabilidad compartida respecto al servicio prestado, estableciendo derechos y obligaciones proporcionales y razonables.

XI. Ley: Ley Federal de Ciberseguridad;

XII. Seguridad Informática: conjunto de tecnologías, procesos y prácticas diseñadas para proteger el procesamiento de información a través de redes, dispositivos y programas, contra amenazas o ataques cibernéticos;

XIII. Seguridad de la Información: conjunto de procedimientos, políticas y herramientas que protegen la información confidencial de usos indebidos, accesos no autorizados, interrupciones o destrucción;

XIV. Sistema Nacional: Sistema Nacional de Ciberseguridad, instancia de coordinación, investigación y concertación en materia de ciberseguridad, y

XV. Tecnologías de la Información y Comunicación (TIC): tecnologías que integran la informática, microelectrónica y telecomunicaciones para facilitar nuevas formas de comunicación a través de herramientas tecnológicas, promoviendo la emisión, acceso y tratamiento de información.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Sistema Nacional de Ciberseguridad

Artículo 5. El Sistema Nacional de Ciberseguridad es una instancia de coordinación, concertación, deliberación y evaluación, responsable de organizar y gestionar la política en materia de ciberseguridad.

El Sistema Nacional de Ciberseguridad tiene como objeto fortalecer, prevenir, detectar, mitigar y responder efectivamente a las amenazas a la ciberseguridad que puedan afectar la seguridad nacional, la infraestructura crítica, la economía y los derechos fundamentales de las personas.

Artículo 6. El Sistema Nacional de Ciberseguridad, se integra por el titular de las siguientes instituciones:

I. La Secretaría de Seguridad y Protección Ciudadana, quien lo presidirá;

II. La Secretaría de Hacienda y Crédito Público;

III. La Secretaría de Ciencia, Humanidades, Tecnología e Innovación;

IV. La Secretaría de la Defensa Nacional;

V. La Secretaría de Marina;

VI. La Secretaría de Relaciones Exteriores;

VII. La Secretaría de Infraestructura, Comunicaciones y Transportes;

VIII. La Agencia de Transformación Digital y Telecomunicaciones;

IX. El Centro Nacional de Ciberseguridad;

X. La Guardia Nacional;

XI. La Unidad de Inteligencia Financiera;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

XII. El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública;

XIII. La Comisión Nacional de Mejora Regulatoria;

XIV. Un representante designado por cada uno de los gobernadores de las entidades federativas, preferentemente el Secretario de Seguridad o su equivalente, y

XV. Los demás que se consideren en el Reglamento de la presente Ley para apoyar su funcionamiento.

El titular de las instituciones anteriormente señaladas podrá ser suplido en ausencia de conformidad con lo que establezca el Reglamento de la presente Ley.

Artículo 7. El Sistema Nacional de Ciberseguridad podrá invitar a sus sesiones a las siguientes personas, a propuesta de cualquiera de sus integrantes:

I. Autoridades de gobiernos estatales y municipales, así como de la Ciudad de México;

II. Integrantes de Comisiones Legislativas del Congreso de la Unión;

III. Ministros, magistrados o jueces del Poder Judicial, tanto a nivel federal como estatal;

IV. Autoridades de la Fiscalía General de la República;

V. Integrantes de la Comisión Consultiva de Ciberseguridad;

VI. Representantes de organismos internacionales;

VII. Expertos en ciberseguridad de la sociedad, academia y sector privado, y

VIII. Servidores públicos del ámbito federal, estatal o municipal, o particulares responsables de infraestructuras críticas o sistemas de ciberseguridad con repercusión nacional.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Todos los invitados participarán con derecho a voz, pero sin voto.

El titular de la Secretaría de Seguridad y Protección Ciudadana podrá invitar al sus organismos desconcentrados y sectorizados al Sistema Nacional de Ciberseguridad, para que participen con derecho a voz, pero sin voto.

Artículo 8. El Sistema Nacional de Ciberseguridad tendrá las siguientes atribuciones:

I. Fortalecer la capacidad del Estado para prevenir, detectar, mitigar y responder efectivamente a las amenazas cibernéticas que puedan afectar la seguridad nacional, la infraestructura crítica, la economía y los derechos fundamentales de las personas.

II. Definir las funciones y responsabilidades de las instituciones federales en materia de ciberseguridad;

III. Actuar como el ente principal de coordinación en la implementación de políticas y estrategias de ciberseguridad, asegurando una respuesta integrada y efectiva ante incidentes cibernéticos en todos los órdenes de gobierno;

IV. Coordinar la colaboración entre la Federación, las entidades federativas, los municipios y las alcaldías de la Ciudad de México en materia de ciberseguridad, fomentando la cooperación con el sector privado;

V. Contribuir en el desarrollo e implementación de la Estrategia Nacional de Ciberseguridad, que defina políticas, objetivos y medidas para enfrentar adecuadamente las amenazas cibernéticas en el país;

VI. Establecer políticas integrales que promuevan la transparencia, la responsabilidad y la ética en el manejo seguro de la información y los datos digitales, a fin de combatir el robo de información y fortalecer la ciberseguridad;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

VII. Desarrollar la resiliencia en las infraestructuras críticas contra incidentes cibernéticos, garantizando la continuidad y recuperación efectiva de los servicios esenciales en situaciones adversas;

VIII. Impulsar la innovación y la investigación tecnológica en ciberseguridad, en colaboración con entidades académicas y el sector privado, fomentando el desarrollo de tecnologías y herramientas que mejoren la protección en el ciberespacio, en particular los sistemas de Inteligencia Artificial;

IX. Promover el desarrollo y la adopción de estándares nacionales e internacionales de ciberseguridad, así como esquemas de certificación en la materia para productos, servicios y procesos de tecnologías de la información y comunicación en términos de la Ley de Infraestructura de la Calidad;

X. Fomentar la educación y sensibilización en materia de ciberseguridad a todos los niveles educativos, en empresas y en la sociedad en general, para crear conciencia sobre la importancia de la ciberseguridad y las mejores prácticas para prevenir riesgos;

XI. Desarrollar e implementar programas de capacitación en ciberseguridad dirigidos a diferentes sectores y grupos de población, incluyendo niños, niñas y adolescentes, así como funcionarios públicos y profesionales de las tecnologías de la información y comunicación;

XII. Fomentar una cultura de ciberseguridad a través de campañas permanentes que concienticen a la población sobre la importancia de la seguridad en el uso de tecnologías digitales, incluyendo las redes sociales;

XIII. Desarrollar e implementar mecanismos de cooperación internacional en materia de ciberseguridad, que incluyan la participación en organismos internacionales, y el intercambio de información relevante para la gestión de amenazas cibernéticas;

XIV. Fomentar la cooperación internacional en materia de ciberseguridad, promoviendo acuerdos y colaboraciones con otros países y organismos internacionales para fortalecer las capacidades y recursos para combatir el cibercrimen, y

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

XV. Promover y facilitar la participación activa del sector privado y académico en el desarrollo de estrategias y políticas de ciberseguridad, mediante la creación de plataformas de colaboración que incentiven el intercambio de conocimientos, tecnologías y mejores prácticas.

Distribución de competencias

Artículo 9. La Federación, las entidades federativas, los municipios y las alcaldías de la Ciudad de México se coordinarán y colaborarán en materia de ciberseguridad en el ámbito de su competencia, en los términos de esta Ley, de su Reglamento y de la legislación aplicable.

A. Corresponde a la Federación, por conducto del Centro Nacional de Ciberseguridad, la Secretaría de Seguridad y Protección Ciudadana y las autoridades competentes:

I. Establecer las políticas y estrategias nacionales en materia de ciberseguridad, procurando la protección de la infraestructura crítica y la información sensible del Estado, así como un ciberespacio seguro. Esto incluirá la coordinación con las entidades federativas, los municipios y las alcaldías de la Ciudad de México, así como con organismos internacionales, para prevenir, detectar y responder a ciberamenazas y ataques cibernéticos que pongan en riesgo la seguridad nacional, la integridad de la nación y el bienestar de la población;

II. Coordinar el funcionamiento de las áreas encargadas de la ciberseguridad en la Administración Pública Federal y los Órganos Constitucionales Autónomos;

III. Coordinar las acciones en materia de ciberseguridad con las áreas especializadas de las instituciones de seguridad pública en las entidades federativas y los municipios;

IV. Colaborar con las autoridades extranjeras y organismos internacionales en materia de ciberseguridad;

V. Efectuar las acciones de protección y vigilancia de las infraestructuras críticas de la información del país, en los términos de las leyes en materia de protección de datos, propiedad industrial y sus reglamentos;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

VI. Ejecutar la Estrategia Nacional de Ciberseguridad;

VII. Realizar acciones en materia de prevención de delitos cibernéticos;

VIII. Participar en los programas de capacitación en materia de ciberseguridad, y

IX. Las demás que establezcan esta Ley, su Reglamento y otras disposiciones legales.

B. Corresponde a las entidades federativas, por conducto de las autoridades competentes:

I. Colaborar en el ámbito de su competencia en las políticas de coordinación elaboradas por el Centro Nacional de Ciberseguridad;

II. Participar en el ámbito de su competencia en las políticas y programas de la Estrategia Nacional;

III. Participar en el Sistema Nacional de Ciberseguridad en el ámbito de su competencia;

IV. Participar en los programas de capacitación en materia;
V. Realizar acciones en materia de prevención de delitos cibernéticos, y

VI. Las demás que establezcan esta Ley, su Reglamento y otras disposiciones legales.

C. Corresponde a los municipios y a las alcaldías de la Ciudad de México, por conducto de las autoridades competentes:

I. Colaborar en el ámbito de su competencia en las políticas de coordinación elaboradas por el Centro Nacional de Ciberseguridad;

II. Contribuir en el ámbito de su competencia en las políticas y programas de la Estrategia Nacional;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

III. Participar en el Sistema Nacional de Ciberseguridad en el ámbito de su competencia;

IV. Realizar acciones en materia de prevención de delitos cibernéticos, y

V. Las demás que establezcan esta Ley, su Reglamento y otras disposiciones legales.

Del Centro Nacional de Ciberseguridad

Artículo 10. El Centro Nacional de Ciberseguridad es un organismo desconcentrado de la Secretaría de Seguridad y Protección Ciudadana, que tiene como finalidad establecer e implementar las acciones de la presente ley en materia de ciberseguridad.

Artículo 11. El Centro Nacional de Ciberseguridad tendrá las siguientes atribuciones:

I. Establecer lineamientos para políticas generales que fortalezcan la prevención y respuesta ante amenazas cibernéticas que puedan impactar la seguridad nacional, infraestructura crítica, economía y derechos fundamentales;

II. Diseñar y evaluar periódicamente los resultados de la Estrategia Nacional de Ciberseguridad, asegurando su efectividad y adecuación a las amenazas y desafíos emergentes;

III. Integrar y coordinar los esfuerzos del gobierno federal para asegurar el respeto y ejercicio de los derechos humanos en el ciberespacio, promoviendo la seguridad, gestión de riesgos, educación y cultura digital en todo el país.

IV. Coordinar y promover acciones para proteger la infraestructura digital y los sistemas de información, fortaleciendo la resiliencia cibernética a nivel nacional con un enfoque basado en riesgos;

V. Coordinar la colaboración en ciberseguridad entre entidades gubernamentales, sector privado, academia y sociedad civil;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO.
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

VI. Promover la innovación en ciberseguridad, apoyando el desarrollo de tecnologías y herramientas que fortalezcan la seguridad del ciberespacio;

VII. Fomentar el desarrollo de la industria de la ciberseguridad en México, fortaleciendo la capacidad nacional para enfrentar amenazas cibernéticas;

VIII. Gestionar programas de cooperación internacional y representar al país en foros internacionales sobre ciberseguridad;

IX. Elaborar anualmente el Programa Nacional de Riesgos Cibernéticos y el Catálogo Nacional de Infraestructuras Críticas, identificando y priorizando los riesgos y activos más críticos;

X. Evaluar y monitorear el estado de la ciberseguridad en el país, implementando medidas para fortalecer la respuesta ante incidentes cibernéticos;

XI. Implementar un sistema de alerta temprana para informar a la población y a las instituciones sobre amenazas cibernéticas;

XII. Establecer mecanismos para el monitoreo y detección de ciberataques, asegurando una respuesta oportuna y eficaz;

XIII. Crear un sistema de respuesta rápida y coordinada ante incidentes cibernéticos para fortalecer la colaboración entre instituciones;

XIV. Promover la implementación de medidas proactivas para evitar ciberataques, como la educación, capacitación, concientización y protocolos de seguridad;

XV. Proporcionar asesoramiento técnico en materia de ciberseguridad a empresas, administraciones públicas y ciudadanos, ayudándoles a mejorar su protección ante amenazas digitales;

XVI. Interactuar con los proveedores de servicios digitales, empresas que manejan datos personales, e instituciones públicas, en relación con sus obligaciones en materia de ciberseguridad en los términos de la presente ley y demás disposiciones aplicables;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

XVII. Coadyuvar a la protección de datos personales en el ciberespacio en los términos de la legislación aplicable;

XVIII. Desarrollar y promover estándares de seguridad cibernética aplicables para la Administración Pública Federal con un enfoque basado en riesgos, alineado a estándares internacionales;

XIX. Informar a las autoridades competentes de las acciones necesarias para la seguridad nacional en el marco de las atribuciones legales;

XX. Definir lineamientos y protocolos para la colaboración de la policía y ministerios públicos en materia de ciberseguridad, y

XXI. Elaborar las bases y convocatorias para seleccionar integrantes de la Comisión Consultiva de Ciberseguridad.

Artículo 12. Al frente del Centro Nacional de Ciberseguridad estará un director general, quien será nombrado por la persona titular de la Secretaría de Seguridad y Protección Ciudadana. La supervisión de este órgano desconcentrado corresponderá a dicha secretaría.

El Centro Nacional de Ciberseguridad contará con los recursos, el personal y estructura administrativa que se establezcan en el Presupuesto de Egresos de la Federación de manera anual y en su reglamento.

Artículo 13. El Centro Nacional de Ciberseguridad deberá sesionar cuando menos una vez al trimestre e informar de sus acuerdos a la Comisión Bicamaral de Seguridad Nacional del Congreso de la Unión de manera semestral.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Comisión Consultiva de Ciberseguridad

Artículo 14. La Comisión Consultiva de Ciberseguridad será un órgano de consulta no remunerado, encargado de proporcionar orientación técnica y estratégica al Centro Nacional de Ciberseguridad. Su objetivo principal es asesorar en el desarrollo y mejora de políticas y acciones relacionadas con la ciberseguridad en México.

La Comisión Consultiva de Ciberseguridad estará conformada por servidores públicos, profesionales, especialistas, y representantes de la sociedad civil y el sector privado, con reconocida capacidad técnica y experiencia. Los integrantes desempeñarán su cargo por un periodo de cuatro años y serán seleccionados de conformidad con las bases y convocatoria que emita el Centro Nacional de Ciberseguridad para este fin.

Artículo 15. La Comisión Consultiva de Ciberseguridad tendrá las siguientes tareas:

I. Proporcionar asesoramiento experto a las autoridades gubernamentales en cuestiones de ciberseguridad, ofreciendo perspectivas y recomendaciones técnicas;

II. Emitir recomendaciones sobre políticas, normativas y estrategias relacionadas con la ciberseguridad al Centro Nacional de Ciberseguridad;

III. Analizar tendencias y mejores prácticas en ciberseguridad a nivel nacional e internacional para evaluar su posible aplicación en México;

IV. Promover la adopción de estándares internacionales de ciberseguridad, asegurando que las prácticas de ciberseguridad en México se alineen con las mejores prácticas y estándares internacionales para mejorar la cooperación global;

V. Analizar el impacto y eficacia de las políticas públicas existentes en materia de ciberseguridad, proponiendo ajustes y mejoras al Centro Nacional de Ciberseguridad;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

VI. Coadyuvar en la identificación y evaluación de riesgos relacionados con la ciberseguridad;

VII. Evaluar el impacto de nuevas tecnologías emergentes, analizando cómo las tecnologías emergentes impactan la ciberseguridad y asesorando sobre cómo integrarlas de manera segura;

VIII. Fomentar la investigación y promover la colaboración entre el sector académico, la industria y el gobierno para el desarrollo de tecnologías y prácticas innovadoras en ciberseguridad;

IX. Coadyuvar en el desarrollo de programas educativos y de concienciación, dirigidos a la ciudadanía y diferentes sectores de la sociedad, sobre la importancia de la ciberseguridad;

X. Facilitar la colaboración entre el gobierno y la sociedad civil, representando los intereses y preocupaciones de los ciudadanos y actores académicos en torno a la ciberseguridad;

XI. Sugerir indicadores para medir la eficacia de las políticas y estrategias de ciberseguridad implementadas, asegurando que los objetivos se cumplan de manera eficiente;

XII. Coadyuvar en el desarrollo de programas de gestión de crisis cibernéticas, con protocolos de respuesta y recuperación ante incidentes cibernéticos;

XIII. Apoyar la protección de infraestructuras críticas colaborando estrechamente con sectores clave para desarrollar directrices y protocolos de seguridad específicos, asegurando la resiliencia frente a ciberataques;

XIV. Coadyuvar en actividades de fomento y promoción de la ciberseguridad en distintos niveles de gobierno, instituciones académicas, el sector privado y con la ciudadanía en general;

XV. Integrar a expertos en diferentes áreas relacionadas con la ciberseguridad, incluyendo aspectos técnicos, legales, educativos y de investigación, para enriquecer el enfoque consultivo y estratégico del Centro Nacional de Ciberseguridad, y

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

XVI. Cumplir con otras funciones que le sean asignadas por el Centro Nacional de Ciberseguridad, acorde con el marco legal vigente.

Estrategia Nacional de Ciberseguridad

Artículo 16. La Estrategia Nacional de Ciberseguridad será desarrollada por el Centro Nacional de Ciberseguridad con el apoyo de la Comisión Consultiva de Ciberseguridad, misma que deberá ser desarrollada, ejecutada y supervisada conforme al sistema nacional de planeación previsto en la Constitución Política de los Estados Unidos Mexicanos y la correspondiente Ley de Planeación. Su vigencia será sexenal y deberá ser evaluada y actualizada al menos cada 2 años.

Artículo 17. La Estrategia Nacional de Ciberseguridad deberá sujetarse a los siguientes principios:

I. Adaptabilidad y resiliencia: asegurarse de que las políticas y prácticas de ciberseguridad sean flexibles y capaces de adaptarse rápidamente a las nuevas amenazas y tecnologías emergentes;

II. Colaboración y cooperación: fomentar una estrecha colaboración interna y externa, tanto nacional como internacional, para compartir información y mejores prácticas;

III. Confidencialidad, integridad y disponibilidad: garantizar que la información esté protegida contra accesos no autorizados o alteraciones, y que los servicios de ciberseguridad estén disponibles cuando se necesiten;

IV. Educación y concienciación: enfocar esfuerzos en educar y sensibilizar a todos los niveles de la sociedad sobre la importancia de la ciberseguridad y las buenas prácticas en el ámbito digital;

V. Evaluación y mejora continua: implementar mecanismos regulares de evaluación y mejora continua para asegurar que las políticas y prácticas de ciberseguridad estén siempre optimizadas;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

VI. Innovación: promover el desarrollo y la implementación de nuevas tecnologías y enfoques que fortalezcan la ciberseguridad nacional;

VII. Interoperabilidad tecnológica: asegurar que las tecnologías utilizadas para ciberseguridad interoperen eficientemente en los sistemas existentes y sean fácilmente actualizables;

VIII. Control de Daños: frente a un ciberataque o incidente de ciberseguridad, se deberá actuar de manera coordinada y diligente, adoptando medidas necesarias para prevenir la escalada del incidente y evitando su posible propagación a otros sistemas informáticos;

IX. Racionalidad: las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de las autoridades competentes deberán ser necesarias y proporcionales al grado de riesgo, y al eventual impacto social y económico;

X. Seguridad en el Ciberespacio: es deber del Estado proteger la seguridad en el ciberespacio, asegurando que todas las personas puedan participar en un entorno digital seguro. El Estado otorgará especial atención a las redes y sistemas informáticos que contienen información de grupos y personas que son especialmente vulnerables a ciberataques;

XI. Seguridad Informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el uso de cifrado, para proteger su información personal y comunicaciones digitales;

XII. Prevención de Riesgos: identificar y mitigar amenazas antes de que ocurran, mediante auditorías de seguridad, capacitaciones al personal y actualización constante de sistemas. Se debe fomentar una cultura de sensibilización sobre ciberseguridad y realizar evaluaciones periódicas de vulnerabilidades, protegiendo así la infraestructura crítica y los datos sensibles, y minimizando el impacto de posibles ataques.

XIII. Proporcionalidad y equidad: asegurar que las medidas de seguridad sean proporcionales a los riesgos y se implementen de manera justa, respetando los derechos y libertades individuales;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

XIV. Protección de los derechos humanos: garantizar que las políticas de ciberseguridad respeten los derechos humanos, incluidos la privacidad, la libertad de expresión y la información;

XV. Responsabilidad compartida: reconocer que la ciberseguridad es una responsabilidad conjunta entre el gobierno, el sector privado, la academia y la sociedad civil;

XVI. Inversión sostenida, proporcional y adecuada en ciberseguridad: asegurar que las medidas de ciberseguridad sean implementadas bajo criterios de inversión sostenida, proporcional y adecuada, de tal forma que su operación sea constante y no representen una carga excesiva sobre las empresas o el gobierno, y

XVII. Transparencia: para mantener una comunicación clara y abierta sobre las políticas, prácticas y problemas de ciberseguridad, para construir confianza entre todas las partes interesadas.

Artículo 18. La Estrategia Nacional de Ciberseguridad deberá incluir lo siguiente:

I. Implementar medidas proactivas para identificar, prevenir y mitigar amenazas cibernéticas; desarrollar capacidades avanzadas de detección de amenazas, incluyendo monitoreo continuo y detección temprana de intrusiones con un enfoque basado en riesgos; establecer protocolos claros y eficaces de respuesta ante incidentes, con coordinación entre autoridades, sector privado y actores relevantes;

II. Implementar medidas de protección para garantizar la seguridad de sectores estratégicos como energía, salud, finanzas y transporte;

III. Fomentar la colaboración público privada y el intercambio de información entre gobierno, empresas, academia y sociedad civil;

IV. Establecer mecanismos de cooperación internacional mediante acuerdos y participación en organismos globales;

V. Promover programas de formación y capacitación en ciberseguridad para profesionales, y la educación desde etapas tempranas;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

VI. Fomentar el desarrollo y la disponibilidad de profesionales cualificados en el ámbito de la ciberseguridad;

VII. Fomentar la investigación y desarrollo tecnológico en ciberseguridad, incentivando la innovación y creación de soluciones avanzadas;

VIII. Promover el desarrollo de la industria de ciberseguridad en México mediante incentivos fiscales y programas de apoyo;

IX. Mejorar la conciencia pública sobre ciberseguridad a través de campañas de sensibilización y educación, promoviendo el uso seguro y responsable de tecnología digital;

X. Fomentar el desarrollo de la industria de la ciberseguridad en México, con el fin de fortalecer la capacidad nacional para enfrentar las amenazas cibernéticas;

XI. Implementar un sistema de alerta temprana para informar a la población y a las instituciones públicas y privadas sobre las amenazas cibernéticas;

XII. Establecer centros de operaciones de seguridad cibernética para el monitoreo y respuesta a amenazas en tiempo real;

XIII. Desarrollar lineamientos para la elaboración de indicadores de seguridad cibernética, dirigidos a entidades públicas y privadas para identificar vulnerabilidades y evaluar riesgos;

XIV. Contemplar medios de difusión periódica sobre riesgos y eventos cibernéticos, de conformidad con la ley en materia de protección de datos, con el objetivo de fortalecer la estrategia de prevención e informar a la población sobre las amenazas cibernéticas;

XV. Establecer acciones específicas para la gestión de emergencias sanitarias y catástrofes que afecten la ciberseguridad, que incluyan protocolos de respuesta que incluyan la protección de infraestructuras críticas, la continuidad operativa de los servicios digitales esenciales; además de incluir procedimientos de comunicación claros para informar al público sobre medidas a seguir durante situaciones de crisis;

XVI. Generar estadísticas oficiales que recopilen datos de instituciones públicas y privadas acerca de los tipos de riesgos cibernéticos. Esta información incluirá detalles sobre la ubicación, periodicidad e incidencia de los ataques, y

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

XVII. Promover un entorno que evite requisitos restrictivos que puedan inhibir la innovación en el ámbito de la ciberseguridad, garantizando que las regulaciones fomenten, en lugar de limitar, el desarrollo y la adopción de innovaciones tecnológicas.

XVIII. Establecer recomendaciones para implementar incentivos fiscales o facilidades regulatorias destinadas a las empresas que inviertan en ciberseguridad;

XIX. Implementar programas de gestión de crisis cibernéticas, con protocolos de respuesta y recuperación ante incidentes mayores.

Artículo 19. La Estrategia Nacional de Ciberseguridad establecerá protocolos mínimos que deberán ser considerados por los actores involucrados en el ámbito de la ciberseguridad en México. Dichos protocolos comprenderán al menos:

I. Atlas de Riesgo de Ciberseguridad: para identificar nuevas amenazas y ajustar la estrategia nacional acorde a riesgos emergentes;

II. Continuidad de Operaciones: que desarrolle planes de continuidad de operaciones y recuperación ante desastres para asegurar la disponibilidad y operatividad de sistemas y servicios digitales frente a posibles interrupciones causadas por eventos cibernéticos adversos;

III. Normas de Seguridad Informática: que establezca estándares y buenas prácticas en seguridad informática para proteger sistemas, redes y datos de amenazas cibernéticas. Esto incluye la implementación de medidas como el control de acceso, la encriptación de datos y la gestión de parches y actualizaciones;

IV. Gestión de Incidentes: que defina procedimientos y protocolos para una gestión eficaz de incidentes cibernéticos. Esto abarca la detección, notificación, respuesta y recuperación ante ataques o violaciones de seguridad, con el objetivo de minimizar el impacto y mitigar los riesgos asociados;

V. Progresividad: que establezca protocolos mínimos incluirán medidas específicas de seguridad cibernética que deberán ser implementadas de manera gradual y proporcional al nivel de riesgo y al impacto potencial de las operaciones de cada organización en el entorno digital;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

VI. Protección de la Privacidad: que desarrolle directrices y políticas para garantizar la protección de la privacidad y los datos personales en el ciberespacio. Estas medidas aseguran el cumplimiento de la legislación vigente en materia de protección de datos y el respeto a los derechos individuales de los usuarios, y

VII. Sensibilización y Capacitación: que implemente programas de sensibilización y capacitación en ciberseguridad dirigidos a todos los niveles de la organización. Estos programas buscan promover una cultura de seguridad digital y concienciar a los empleados sobre las amenazas y riesgos cibernéticos.

Derechos Digitales en el Ciberespacio.

Artículo 20. Las acciones que desarrolle el Estado en materia de ciberseguridad tendrán por objeto garantizar los derechos digitales de las personas en el ciberespacio, incluyendo, pero no limitándose a, el derecho a la privacidad, la libertad de expresión, la seguridad digital, el acceso a la información, y el respeto a la dignidad humana. El Estado promoverá políticas y estrategias que protejan estos derechos, asegurando un ambiente digital seguro y accesible para todos los ciudadanos, y fomentando la educación y concientización sobre la importancia de la ciberseguridad.

Obligaciones de implementación de medidas de ciberseguridad

Artículo 21. Los proveedores de servicios digitales, las organizaciones que manejan datos personales, ya sean públicas o privadas, y los prestadores de servicios públicos, tendrán las siguientes obligaciones en materia de ciberseguridad:

I. Implementar y mantener medidas de ciberseguridad adecuadas para proteger los datos personales y la información de los usuarios contra acceso no autorizado, alteraciones, divulgaciones o destrucción, con un enfoque basado en riesgos;

II. Desarrollar e implementar políticas de ciberseguridad que incluyan la capacitación constante del personal en la prevención y respuesta ante incidentes de seguridad;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

III. Colaborar con las autoridades competentes en la prevención de delitos cibernéticos y en la notificación de incidentes de seguridad, en términos de la normatividad aplicable;

IV. Informar a los usuarios sobre los riesgos asociados con el uso de sus servicios y sobre las medidas que se están tomando para proteger su seguridad, en términos de la legislación aplicable;

V. Cumplir con la legislación vigente en materia de protección de datos personales y ciberseguridad en terminos de las leyes respectivas, y

VI. Las demás que se establezcan en la legislación aplicable y en esta Ley.

El Centro Nacional de Ciberseguridad deberá diseñar medidas de ciberseguridad diferenciadas según el tipo de organización de que se trate, teniendo especialmente en consideración las características y posibilidades de las pequeñas y medianas empresas.

Protección de Datos Personales en el Ciberespacio.

Artículo 22. En términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, se considerará lo siguiente en cuanto la protección de datos personales en el ciberespacio:

I. Las instituciones públicas y los particulares deberán implementar medidas de seguridad adecuadas y proporcionales al tipo de datos manejados y a los riesgos asociados para garantizar la confidencialidad, integridad y disponibilidad de los datos personales;

II. Se garantizará la confidencialidad de la información de las víctimas de ciberataques, prohibiendo la divulgación no autorizada de datos que puedan afectar su reputación;

III. Los entes públicos deberán garantizar la transparencia en el manejo de los datos personales, informando a los usuarios sobre la recopilación, uso, almacenamiento y eliminación de sus datos, así como sobre sus derechos en relación con dicha información, conforme a los términos ya previstos al respecto en la legislación especial aplicable, y

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

IV. Se deberá promover la adopción de buenas prácticas en el manejo y tratamiento de datos personales, así como la actualización continua de las políticas de protección de datos, de acuerdo con los avances tecnológicos y la evolución de las amenazas cibernéticas.

Protección de las Infraestructuras Críticas

Artículo 23. Se consideran infraestructuras críticas aquellas redes, servicios, equipos e instalaciones vinculados a activos de Tecnologías de Información y Comunicaciones, cuya afectación, interrupción o destrucción podría tener un impacto significativo en la provisión de bienes y servicios esenciales. Estos servicios esenciales incluyen, entre otros:

I. Seguridad y Defensa: sistemas de seguridad nacional, seguridad pública y protección civil;

II. Servicios Financieros: instituciones, como bancos, bolsas de valores y sistemas de pago;

III. Salud: Hospitales, clínicas y sistemas de gestión de datos de salud;

IV. Telecomunicaciones: redes de telefonía fija, móvil e internet;

V. Energía: sistemas de generación y distribución de electricidad, así como petróleo y gas;

VI. Agua y Saneamiento: infraestructuras dedicadas a la distribución de agua potable y la gestión de aguas residuales;

VII. Transporte: Aeropuertos, puertos y sistemas ferroviarios;

VIII. Alimentación y Agricultura: infraestructuras que aseguran la producción y distribución de alimentos, y

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

IX. Otros: aquellas que se consideren críticas para el funcionamiento del país.

Para la protección de las infraestructuras críticas, se considerarán como riesgos e incidentes cibernéticos de seguridad nacional los siguientes:

I. Ataques Cibernéticos contra Infraestructuras Críticas: tales como los de sistemas de energía, comunicaciones, transporte, salud o finanzas, que puedan causar interrupciones significativas en los servicios esenciales para la población y la economía del país;

II. Ciberespionaje y Actividades de Inteligencia Cibernética: aquellos realizados con el objetivo de obtener información clasificada, estratégica o sensible para la seguridad nacional, y

III. Ciberataques Dirigidos a Instituciones Gubernamentales: aquellos ataques que se enfocan en sistemas de defensa, fuerzas armadas o entidades públicas encargadas de la seguridad nacional.

Para efectos de la aplicación de esta ley, se deberá diferenciar entre el proveedor responsable y el proveedor de soporte de infraestructuras críticas, en función del nivel de responsabilidad compartida respecto al servicio prestado, estableciendo derechos y obligaciones proporcionales y razonables.

Artículo 24. El Estado, a través del Centro Nacional de Ciberseguridad y en coordinación con las autoridades federales y locales competentes, así como los propietarios y operadores de infraestructuras críticas, tendrán las siguientes responsabilidades:

I. Implementar medidas de ciberseguridad que refuercen la resiliencia de las infraestructuras críticas ante los riesgos identificados;

II. Llevar a cabo evaluaciones periódicas de riesgos para detectar vulnerabilidades y establecer un marco efectivo de respuesta ante incidentes;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

III. Fomentar la capacitación y concientización del personal en ciberseguridad y en la protección de infraestructuras críticas, asegurando que estén debidamente preparados para reaccionar ante incidentes, y

IV. Colaborar con las autoridades competentes para garantizar la integridad y continuidad de los servicios esenciales, así como facilitar el intercambio de información sobre amenazas y mejores prácticas en ciberseguridad.

V. Diseñar medidas de ciberseguridad específicas según el tipo de organización, estableciendo derechos y obligaciones proporcionales y razonables. Se deberá diferenciar entre el proveedor responsable y el proveedor de soporte, en función del nivel de responsabilidad compartida respecto al servicio prestado.

Educación y Capacitación en materia de Ciberseguridad

Artículo 25. El Centro Nacional de Ciberseguridad tendrá la obligación de promover la educación y la sensibilización en materia de ciberseguridad en las instituciones públicas, en todos los niveles educativos, así como en las empresas y en la sociedad en general. Para lograr este objetivo, se establecerán las siguientes acciones:

I. Desarrollar programas de capacitación en ciberseguridad dirigidos a diferentes sectores y grupos de población, incluyendo, pero no limitándose a:

a) Niños, niñas y adolescentes, con el fin de fomentar una cultura de seguridad en el uso de tecnologías digitales desde temprana edad;
b) Funcionarios públicos, asegurando que comprendan la importancia de la ciberseguridad en la protección de datos y en la integridad de la información del gobierno, y
c) Profesionales de las Tecnologías de la Información y Comunicaciones, para que mantengan actualizados sus conocimientos y habilidades en un entorno tecnológico en constante evolución.

II. Implementar programas de sensibilización que se difundan a través de campañas informativas y educativas, abordando temas como el uso seguro de Internet, la prevención del ciberacoso, y la importancia de proteger la información personal;

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

III. Colaborar con instituciones educativas y empresas para integrar la ciberseguridad como un componente en los currículos académicos y en la formación profesional, garantizando que el conocimiento en esta área sea parte esencial de la educación contemporánea;

IV. Fomentar la creación de redes de cooperación entre diferentes entidades, incluyendo organismos gubernamentales, instituciones educativas, y el sector privado, para asegurar un enfoque conjunto y eficaz en la promoción de la ciberseguridad en toda la sociedad, y

V. Evaluar y actualizar periódicamente los programas de educación y capacitación en ciberseguridad, asegurando que se adapten a los nuevos desafíos y amenazas que emergen en el ciberespacio.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx

Transitorios

Primero. El presente decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Segundo. Las entidades federativas deberán expedir sus leyes en materia de ciberseguridad, con base en esta ley general, en los 180 días posteriores a su publicación en el Diario Oficial de la Federación.

Tercero. El Centro Nacional de Ciberseguridad deberá quedar integrado en los 30 días posteriores a la publicación del presente decreto.

Cuarto. El Centro Nacional de Ciberseguridad deberá elaborar las bases y convocatoria para seleccionar a los integrantes de la Comisión Consultiva de Ciberseguridad en los 30 días posteriores a su integración.

Quinto. El Centro Nacional de Ciberseguridad deberá expedir la Estrategia Nacional de Ciberseguridad en los 180 días posteriores a su integración.

Sexto. El Sistema Nacional de Ciberseguridad deberá constituirse y tener su primera sesión dentro de los 180 días posteriores a la publicación del presente decreto.

ATENTAMENTE,

SEN. MAURICIO VILA DOSAL.

Dado en la sede del Senado de la República a los 26 días del mes de febrero de 2025.

AV. PASEO DE LA REFORMA No. 135, HEMICICLO, NIVEL 06, OFICINA 12, COL. TABACALERA, ALCALDÍA CUAUHTÉMOC, C.P. 06030, CIUDAD DE MÉXICO
TEL./ DIR.: 55 5345 3806 CONM. 55 5345 3000, EXTS. 3806 / 3459, mauricio.vila@senado.gob.mx