Quienes suscriben, senador Luis Donaldo Colosio Riojas del Grupo Parlamentario de Movimiento Ciudadano y senadora Lucía Trasviña Waldenrath del Grupo Parlamentario de Morena, ante la LXVI Legislatura del Honorable Congreso de la Unión, conforme a lo dispuesto en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos, así como por el artículo 8, numeral 1, fracción I, del Reglamento del Senado de la República, someto a consideración de esta honorable asamblea, la presente ***INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY DE CIBERSEGURIDAD,*** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

Vivimos en un mundo profundamente interconectado, donde el ciberespacio se ha convertido en la columna vertebral de la economía, la política, la seguridad y la vida social. México, como muchos otros países, enfrenta desafíos crecientes en materia de ciberseguridad, pero a diferencia de otros Estados, nuestro país carece aún de una estrategia, política pública o marco legal coordinado, integral y especializado que atienda eficazmente estos riesgos.

La ciberseguridad no puede seguir siendo un concepto ambiguo ni abordarse únicamente desde perspectivas parciales. Su alcance es transversal: protege la infraestructura crítica, asegura la continuidad de servicios esenciales, garantiza el respeto de los derechos humanos en el entorno digital y preserva la soberanía nacional. Esta Ley de Ciberseguridad responde a la urgencia de establecer un marco jurídico moderno, coherente y protector, conforme al mandato constitucional.

La presente Ley de Ciberseguridad se fundamenta en la necesidad de desarrollar y reglamentar de manera específica los derechos, obligaciones y principios contenidos en los artículos 1, 6 y 28 de la Constitución Política de los Estados Unidos Mexicanos, para garantizar un entorno digital seguro, resiliente y respetuoso de los derechos humanos, frente a los desafíos contemporáneos de la era digital. Nace de la necesidad impostergable de dotar al Estado mexicano de un instrumento jurídico integral que permita enfrentar los desafíos actuales del entorno digital, garantizando en todo momento el respeto irrestricto a los derechos humanos, la seguridad de las infraestructuras críticas y la soberanía digital del país. Su fundamento descansa principalmente en los artículos 1, 6 y 28 de la Constitución Política de los Estados Unidos Mexicanos, como se expone a continuación:

La ciberseguridad no es un fin en sí mismo, sino un medio para garantizar la efectividad de los derechos humanos en el entorno digital. La protección de la privacidad, la libertad de expresión, el acceso a la información, la no discriminación y el libre desarrollo de la personalidad dependen hoy, de forma ineludible, de la seguridad de los sistemas, redes y datos que usamos cotidianamente.

Siguiendo las resoluciones A/HRC/20/L.13 y A/HRC/32/L.20 del Consejo de Derechos Humanos de la ONU, el acceso a Internet y la protección en el ciberespacio se reconocen como extensiones del ejercicio de los derechos humanos. En consecuencia, reglamentar el artículo 1 constitucional implica asegurar que las acciones en materia de ciberseguridad respeten los principios de legalidad, necesidad, proporcionalidad, responsabilidad y transparencia.

El artículo 1 establece el deber del Estado de respetar, proteger, promover y garantizar los derechos humanos. En la era digital, este mandato exige que el Estado no solo defienda la dignidad, privacidad y libertad de las personas en los espacios físicos, sino también en los entornos digitales, donde los derechos pueden ser igualmente vulnerados o incluso amplificados. La ciberseguridad, definida en esta Ley como un conjunto de principios, medidas técnicas y organizativas orientadas a preservar la confidencialidad, integridad, disponibilidad, autenticación y resiliencia de sistemas y datos, se convierte así en una condición indispensable para hacer efectivo el ejercicio de los derechos humanos en el ciberespacio.

El acceso a las tecnologías de la información y comunicación, banda ancha e Internet no es solo una obligación de provisión de infraestructura; también implica garantizar su disponibilidad segura y confiable. Un acceso material, pero inseguro o plagado de vulnerabilidades, contradice la esencia del derecho reconocido en el artículo 6.

Esta Ley reglamenta dicho artículo estableciendo las bases para que los servicios digitales y de telecomunicaciones no solo sean universales, sino que estén protegidos frente a ciberamenazas, garantizando su continuidad, integridad y resiliencia. Se reconocen las nuevas amenazas derivadas del uso malicioso de tecnologías disruptivas (como la inteligencia artificial.

La libertad de acceso a las tecnologías de la información (TIC), la banda ancha e Internet no se agota en la provisión material del servicio, sino que demanda su disponibilidad segura y libre de amenazas. Reglamentar el artículo 6 implica establecer un marco que garantice que el acceso a las TIC sea asequible, de calidad, seguro y confiable, protegiendo la continuidad de los servicios esenciales y asegurando que el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información y la participación ciudadana no se vea comprometido por riesgos cibernéticos.

Finalmente, la protección de las áreas estratégicas de la Nación, prevista en el artículo 28, se vuelve urgente ante el creciente riesgo que representan las ciberamenazas para sectores como energía, telecomunicaciones, transporte, financiero y salud. México reconoce constitucionalmente áreas estratégicas cuya seguridad es vital para la estabilidad, soberanía y bienestar nacional: energía, telecomunicaciones, transporte, sistema financiero, salud, entre otros.

La creciente dependencia tecnológica ha expuesto a estas infraestructuras críticas a amenazas cibernéticas graves que pueden desestabilizar al país. Esta Ley cumple el mandato del artículo 28 al establecer:

a) La clasificación de operadores de servicios esenciales e infraestructuras críticas de información.
b) La diferenciación de obligaciones de ciberseguridad según el nivel de criticidad y riesgo.
c) La creación de mecanismos de respuesta ante incidentes (CERT nacionales y sectoriales).

Proteger estas infraestructuras significa preservar la soberanía digital, la seguridad nacional y el orden público democrático.

La Ley de Ciberseguridad, por tanto, se configura como una herramienta indispensable para articular una política pública moderna y eficaz que asegure un entorno digital libre, seguro y respetuoso de los derechos humanos, a la altura de los compromisos constitucionales y de los estándares internacionales más avanzados.

2. Justificación de la exclusión de delitos cibernéticos y su remisión al Código Penal Federal

La presente Ley opta deliberadamente por **no incorporar tipos penales** relacionados con la ciberdelincuencia, decisión que se fundamenta en:

Dado que la Ley de Ciberseguridad tiene como objeto la gestión de riesgos, resiliencia y gobernanza de la ciberseguridad y de que el derecho penal es de reserva estricta, se propone que se incorpore en el Código Penal Federal la tipificación de delitos y sanciones penales conforme al principio de legalidad penal establecido en el artículo 14 constitucional.

Más aún porque es importante que no haya riesgo de duplicidad normativa que pudiera generar antinomias y conflictos en la interpretación y la aplicación al encontrarse ya tipificados delitos cibernéticos en nuestra ley federal penal en el Título Noveno que se refiere a la Revelación de Secretos y Acceso Ilícito a Sistema y Equipo de Informática que abarca los artículos 211 bis 1 al 211 bis 7.

Es importante que en la armonización legislativa con todos los ordenamientos legales que hay que reformar, se considere la reforma a los artículos del capítulo II Acceso Ilícito a los Sistemas y Equipos de Informática, de los sistemas en lo general, en los sistemas del Estado, en los sistemas de seguridad pública y en los sistemas financieros de la legislación penal para que cualquier conducta delictiva en el entorno digital que implique la intrusión o el daño a la integridad de dichos sistemas, sea sancionada.

Así también adicionar un Capítulo III con los subsecuentes artículos 211 bis para que se incorporen los delitos que enriquezcan la capacidad del Estado de proteger a las personas y a sus instituciones en el ciberespacio a partir de esta Ley de Ciberseguridad, sobre todo considerando los delitos informáticos que no se encuentran regulados en ninguna legislación penal como el ciberacoso escolare y laboral; los ataques a los sistemas de infraestructura crítica, delitos contra la integridad de los datos; la protección de niñas, niños y personas adolescentes en entornos digitales, suplantación de identidad en los sistemas biométricos, el uso no autorizado para la minería de las criptomonedas, el secuestro de información mediante uso no autorizado del cifrado, el uso no ético de la inteligencia artificial para la elaboración de videos, imágenes, por mencionar sólo algunos

de los muchos delitos que considerarse ciberdelitos y atender a la regulación internacional en materia de ciberdelincuencia.

Nuestro país ha sido invitado a firmar el Convenio de Budapest, por ahora, se participa como observador; este documento fue emitido desde 2001 por el Consejo de Europa, en este se definen conductas delictivas que se cometen a través de redes informáticas y de Internet y las recomendaciones sobre las sanciones penales, algunas de las que ya se encuentran, como se comentó previamente, tipificadas en la legislación penal federal.

También tenemos recientemente aprobada por la Asamblea General de Naciones Unidas, diciembre de 2024, la Convención de las Naciones Unidas contra la Ciberdelincuencia, que marca una pauta de fortalecimiento de la capacidad de los países que lo firmen y de cooperación internacional que se suma a la Convención de Palermo sobre Delincuencia Organizada adoptada en el año 2000. Hemos sido de los más activos promotores de esta convención. En fecha próxima se pondrá a firma y nuestro país ha expresado la voluntad de adherirse y se habrá de cursar el proceso constitucional en nuestro Senado

3. Finalidad de la ciberseguridad según la definición normativa.

La definición de ciberseguridad establecida en esta Ley subraya que su finalidad es:

I. Garantizar la protección de los derechos humanos y las libertades fundamentales en el entorno digital, incluyendo la privacidad, la protección de datos personales y la libertad de expresión.

II. Preservar la continuidad operativa de los servicios esenciales, la seguridad pública y nacional, el bienestar social y la estabilidad económica.

III. Salvaguardar la soberanía digital del Estado mexicano, protegiendo sus infraestructuras estratégicas y recursos de información frente a amenazas internas o externas.

Esta visión integral y progresiva de la ciberseguridad justifica que la Ley se enfoque en medidas técnicas, organizativas y legales de protección, resiliencia y gestión de riesgos, sin invadir competencias del derecho penal.

Agradecemos el apoyo fundamental de la Dra. Anahiby Becerril, de la Academia Mexicana de Ciberseguridad no sólo con comentarios y observaciones, sino en la construcción de esta propuesta, así como el apoyo inicial del licenciado Ricardo Navarrete.

Por todo lo anterior, conforme a lo dispuesto en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos, así como por el artículo 8, numeral 1, fracción I, del Reglamento del Senado de la República, someto a consideración de esta honorable asamblea, la presente *INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY DE CIBERSEGURIDAD*

ARTÍCULO PRIMERO. Se expide la Ley de Ciberseguridad para quedar como sigue:

LEY DE CIBERSEGURIDAD

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO ÚNICO

Artículo 1. La presente Ley es de orden público, interés social y observancia general en todo el territorio nacional. Tiene por objeto establecer el marco jurídico para garantizar la ciberseguridad en México, mediante la protección de las personas, sus derechos humanos y libertades fundamentales, así como de las infraestructuras críticas, la soberanía, la integridad, la resiliencia y la seguridad nacional en el entorno digital; desarrolla y regula el ejercicio de los derechos reconocidos en la Constitución Política de los Estados Unidos Mexicanos

Establece el marco normativo para respetar, proteger, promover y garantizar los derechos humanos de todas las personas, reconociendo su aplicación plena también en el entorno digital, asegurando la dignidad, la privacidad, la libertad de expresión, el acceso a la información, la protección de los datos personales y la no discriminación en todos los espacios y tecnologías emergentes.

Contribuye a que el Estado garantice el acceso universal, equitativo y asequible a las tecnologías de la información y comunicación (TIC), los servicios de radiodifusión y telecomunicaciones, incluida la banda ancha e Internet, promoviendo su disponibilidad, calidad, continuidad, resiliencia y seguridad, como elementos indispensables para el ejercicio efectivo de los derechos fundamentales y el desarrollo del país en el entorno digital.

Para efectos de esta Ley, la ciberseguridad se entiende como el conjunto de políticas, acciones, medidas técnicas, organizativas, legales y sociales orientadas a preservar la confidencialidad, integridad, disponibilidad, resiliencia y autenticación de las redes, sistemas informáticos, datos e infraestructuras críticas, así como a proteger a las personas físicas, sus derechos humanos y al Estado mexicano en su conjunto, frente a amenazas, riesgos e incidentes en el ciberespacio y en entorno físico.

Tiene como finalidad la protección de las infraestructuras prioritarias, críticas, y las infraestructuras críticas de información del Estado mexicano, aquellas esenciales para la provisión de bienes y servicios públicos indispensables, cuyo funcionamiento continuo es vital para la seguridad, el bienestar social y el desarrollo económico del país, contribuyendo a preservar la soberanía digital y la estabilidad nacional.

Artículo 2. Esta ley tiene por objeto:

I. Promover, proteger y garantizar el ejercicio seguro y adecuado de los derechos digitales de las personas, el uso responsable de los datos sensibles de las personas, como una extensión de los derechos humanos en el entorno digital, asegurando la dignidad, la privacidad, la libertad de expresión, el acceso a la información, la protección de los datos personales, el anonimato y la no discriminación.

II. Impulsar y coordinar planes, estrategias, políticas públicas y estándares técnicos orientados a la prevención, detección temprana, respuesta, recuperación y resiliencia frente a amenazas, vulnerabilidades, incidentes y ataques cibernéticos, asegurando la continuidad operativa de servicios esenciales y la protección de las infraestructuras críticas de información, en alineación con las mejores prácticas nacionales e internacionales.

III. Garantizar la integridad de los datos y sistemas, asegurando su confidencialidad y disponibilidad;

IV. Promover y salvaguardar la confidencialidad, e integridad de la información, garantizando que los datos sensibles y personales sólo sean accesibles por personas o

sistemas debidamente autorizados, así como asegurar la disponibilidad y resiliencia de los sistemas, servicios y datos para los usuarios autorizados cuando estos lo requieran, conforme a los principios de seguridad informática y ciberseguridad por diseño y por defecto, adoptando estándares reconocidos internacionalmente;

V. Fomentar, fortalecer y consolidar la cultura de la ciberseguridad en la ciudadanía, en los sectores público y privado, y en la sociedad en general, mediante acciones de formación, sensibilización, investigación, innovación y cooperación internacional, promoviendo un ecosistema digital seguro, resiliente e inclusivo;

VI. Establecer la organización, integración y funcionamiento de la Agencia Nacional de Ciberseguridad, como organismo descentralizado, especializado, con autonomía técnica y operativa, encargado de coordinar las actividades, políticas, estándares y medidas en materia de ciberseguridad a nivel nacional, velando por la protección de los derechos de las personas, la soberanía digital y la continuidad de los servicios esenciales. La Agencia ejercerá sus funciones sin interferir en las competencias exclusivas de las Fuerzas Armadas en materia de seguridad nacional y ciberdefensa, conforme al marco constitucional y a la legislación aplicable, manteniendo mecanismos de coordinación y cooperación cuando así lo requiera la protección de las infraestructuras críticas, sin invadir la esfera de la defensa militar;

VII. Determinar los mecanismos de coordinación, cooperación y colaboración interinstitucional e intersectorial entre los distintos órdenes de gobierno, autoridades sectoriales, órganos autónomos, sociedad civil, academia, sector privado e instancias internacionales, para garantizar un enfoque integral y coherente en la protección del ciberespacio y las infraestructuras críticas de información, conforme a los principios de armonización;

VIII. Definir, implementar, evaluar y actualizar periódicamente la Estrategia Nacional de Ciberseguridad, estableciendo los principios rectores, objetivos, líneas de acción, mecanismos de gobernanza, estándares mínimos y procedimientos para su eficaz funcionamiento, asegurando su alineación con los derechos humanos, la protección de infraestructuras críticas, la soberanía digital, gobernanza y las mejores prácticas internacionales en ciberseguridad que resulten aplicables;

IX. Fomentar la coordinación efectiva con las autoridades competentes en la prevención, detección, gestión y comunicación de incidentes que pudieran constituir delitos informáticos o cibernéticos, asegurando el respeto a los derechos humanos, el debido proceso y la protección de datos personales, conforme al Código Penal Federal, la legislación aplicable y los tratados internacionales en la materia.

Las acciones penales relativas a la ciberdelincuencia serán competencia exclusiva de las autoridades judiciales y ministeriales, conforme al marco jurídico vigente, manteniendo su separación funcional respecto de las medidas de ciberseguridad reguladas por esta Ley, sin perjuicio de los mecanismos de coordinación y cooperación interinstitucional que aseguren una respuesta integral ante incidentes cibernéticos.

Artículo 3. Para los efectos de la Presente Ley se entenderá por:

I. Activo crítico de información: Todo recurso digital, sistema, red, base de datos o proceso que es esencial para la continuidad de un servicio esencial, la protección de derechos humanos, la seguridad nacional o la soberanía digital del Estado.

II. Agencia: La Agencia Nacional de Ciberseguridad;

III. Amenaza cibernética: Cualquier potencial causa de un incidente de ciberseguridad, que puede ser de origen humano, técnico, accidental o natural, con capacidad de afectar la seguridad, funcionamiento o resiliencia de redes, sistemas o servicios;

IV. Archivo informático: Conjunto de datos o información digital estructurada o no estructurada, representada electrónicamente, almacenada y gestionada en soportes o medios digitales, que puede ser procesada, transmitida, interpretada o recuperada por sistemas informáticos para la gestión y manipulación de la información;

V. Base de datos: Conjunto estructurado de datos organizados interrelacionados electrónicamente, diseñado para ser almacenado, gestionado, procesado y recuperado de forma eficiente, mediante sistemas de gestión automatizados o manuales;

VI. CERT: Centro de Respuesta a Incidentes de Seguridad Informática;

VII. Ciberamenaza: Cualquier evento, situación o acción que tiene el potencial de causar daño a un sistema o a los datos que contiene, ya sea a través del acceso no autorizado, la destrucción, la modificación o la divulgación de la información.;

VIII. Ciberataque: Acto deliberado, realizado mediante el uso no autorizado de tecnologías de la información o comunicación (TIC), tecnologías de operación (TO) u otras técnicas cibernéticas, cuyo propósito sea interrumpir, degradar, manipular, acceder sin autorización, exfiltrar, alterar o destruir redes, sistemas, servicios, procesos o datos, afectando la seguridad de la información o la continuidad de los servicios;

IX. Ciberdefensa: Conjunto de acciones y medidas de protección de la información, los sistemas y los dispositivos de posibles amenazas cibernéticas, incluyendo la prevención, detección y respuesta a ataques;

X. Ciberdelincuencia: Conjunto de conductas tipificadas como delitos por las leyes penales nacionales o internacionales, cometidas mediante, o contra, sistemas informáticos, redes, datos o servicios digitales;

XI. Ciberespacio: el dominio global dentro del entorno de la información, formado por redes interdependientes de infraestructuras de sistemas de información;

XII. Ciberseguridad: el proceso de proteger la información y los sistemas computacionales de amenazas, tanto internas como externas, que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, así como en las redes sociales que atente contra los derechos digitales de las personas;

XIII. Datos informáticos: Representación digital de hechos, conceptos, instrucciones o información expresada mediante códigos o cualquier otro formato electrónico, que puede ser procesada, almacenada o transmitida por sistemas informáticos.

XIV. Datos personales: Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

XV. Gobernanza de ciberseguridad: Conjunto de principios, estructuras, procesos, roles y responsabilidades que aseguran la planificación, dirección, control, supervisión y coordinación efectiva de las políticas, acciones y medidas en materia de ciberseguridad, orientadas a garantizar la protección de derechos humanos, la continuidad de los servicios esenciales, la resiliencia de las infraestructuras críticas y la soberanía digital del Estado;

XVI. Estrategia Nacional: Documento marco aprobado por el Ejecutivo Federal, que establece la visión, misión, objetivos estratégicos, líneas de acción, roles y responsabilidades interinstitucionales para garantizar la ciberseguridad nacional, en armonía con los derechos humanos, la protección de infraestructuras críticas y las mejores prácticas internacionales;

XVII. Incidente de ciberseguridad: Evento que afecta o tiene la potencialidad de afectar la confidencialidad, integridad, disponibilidad, autenticación o resiliencia de las redes, sistemas, servicios o datos, originado por causas maliciosas, accidentales o técnicas, que puede interrumpir o comprometer parcial o totalmente su funcionamiento;

XVIII. Información: Conjunto de datos procesados, organizados y estructurados, que poseen significado y utilidad para los usuarios, sistemas o procesos, y cuya confidencialidad, integridad, disponibilidad, autenticación o resiliencia puede ser objeto de protección;

XIX. Información relevante o crítica: Conjunto de datos, procesos o registros digitales cuya alteración, interrupción, pérdida o acceso no autorizado podría generar un impacto significativo en la continuidad operativa de los servicios esenciales, la seguridad pública, la economía, el bienestar social o los derechos humanos;

XX. Infraestructura crítica de información (ICI): Conjunto de activos, sistemas, redes o servicios digitales o interconectados, cuya alteración, interrupción o destrucción pueda generar consecuencias graves para la seguridad pública, la salud, la economía, la defensa nacional o el bienestar social;

XXI. Internet: Red global, descentralizada e interconectada de dispositivos, servidores, sistemas de comunicación y aplicaciones, que permite la transmisión, acceso e intercambio de datos mediante protocolos estándar, facilitando servicios digitales y comunicación global;

XXII. Ley: Ley de Ciberseguridad;

XXIII. Medidas de prevención en ciberseguridad: Conjunto de acciones técnicas, organizativas, educativas y legales destinadas a identificar, gestionar y mitigar riesgos, garantizar la confidencial, resiliencia, integridad, disponibilidad y autenticación de sistemas, servicios y datos, antes de la ocurrencia de un incidente;

XXIV. Medidas de detección en ciberseguridad: Conjunto de herramientas, procesos y procedimientos destinados a monitorear, identificar y registrar actividades, eventos o comportamientos anómalos o no autorizados en redes, sistemas o servicios, que puedan indicar la ocurrencia o potencialidad de un incidente de ciberseguridad;

XXV. Medidas de recuperación en ciberseguridad: Conjunto de estrategias, planes, herramientas y procedimientos destinados a restablecer la operación normal de sistemas, servicios o infraestructuras críticas tras la ocurrencia de un incidente, garantizando la recuperación de datos, procesos y servicios esenciales en el menor tiempo posible;

XXVI. Operadores: Entidades públicas o privadas que operan las redes públicas de Telecomunicaciones a que se refiere el Título Quinto, Capítulo I de la Ley Federal de

Telecomunicaciones y Radiodifusión, proporcionan servicios esenciales, administran infraestructuras críticas, infraestructura crítica de información o servicios digitales relevantes. Son responsables de garantizar la seguridad, resiliencia y continuidad de dichos servicios;

XXVII. Política Nacional de Ciberseguridad: Conjunto de principios, directrices y acciones de política pública desarrolladas por el Estado para implementar la Estrategia Nacional de Ciberseguridad, asegurando la protección de derechos, infraestructuras críticas y soberanía digital;

XXVIII. Programa informático (software): Conjunto de instrucciones o código ejecutable, diseñado para controlar, operar o gestionar el funcionamiento de sistemas informáticos, dispositivos electrónicos o redes, permitiendo la automatización de procesos o la realización de tareas específicas;

XXIX. Red social: Plataforma digital que permite la conexión, interacción, creación, intercambio y difusión de información, contenidos y datos entre personas, grupos u organizaciones, mediante tecnologías de comunicación en línea;

XXX. Resiliencia: Capacidad de redes, sistemas, servicios e infraestructuras para mantener sus funciones esenciales durante un incidente de ciberseguridad, operar en estado degradado si es necesario, y recuperar su funcionamiento pleno en el menor tiempo posible;

XXXI. RICI (Registro de Infraestructuras Críticas de la Información): Base de datos administrada por la Agencia Nacional de Ciberseguridad, que contiene la identificación, clasificación y estado de las infraestructuras críticas y las infraestructuras críticas de información, necesarias para la prestación de servicios esenciales y la seguridad nacional;

XXXII. Riesgo cibernético: Probabilidad de que una amenaza cibernética explote una vulnerabilidad en redes, sistemas, servicios o infraestructuras, causando un impacto negativo en su funcionamiento, en los derechos de las personas o en los intereses estratégicos del Estado.

XXXIII. Secretaría: Secretaría de Seguridad y Protección Ciudadana;

XXXIV. Seguridad informática: Conjunto de principios, políticas, medidas técnicas y organizativas destinadas a proteger los sistemas informáticos, redes, dispositivos digitales, procesos y datos frente a accesos no autorizados, ciberataques, filtraciones,

alteraciones o destrucciones, garantizando su confidencialidad, integridad, disponibilidad, autenticación y resiliencia.

XXXV. SICT: Secretaría de Infraestructura, Comunicaciones y Transportes;

XXXVI. Sistema informático: Conjunto de componentes físicos (hardware), lógicos (software), redes y procesos organizacionales, interrelacionados, que permiten recibir, procesar, almacenar, transmitir y presentar información de manera automatizada.

XXXVII. Sistema de telecomunicaciones: Conjunto de medios técnicos, dispositivos, protocolos y métodos que permiten realizar el transporte, transmisión, recepción e intercambio de información a distancia, mediante señales, cables, radiofrecuencia o tecnologías ópticas.

XXXVIII. Soberanía digital: Capacidad del Estado para proteger, controlar y gestionar sus infraestructuras digitales, datos e información estratégica, garantizando la autonomía en el ciberespacio;

XXXIX. Sujetos Obligados al cumplimiento de la presente Ley:

a) Operadores de Servicios Esenciales: Las personas físicas o morales, públicas o privadas, cuya actividad resulte indispensable para el mantenimiento de funciones sociales, económicas, sanitarias, financieras o de seguridad pública, y cuya interrupción o afectación pueda generar un impacto significativo en la seguridad nacional, la salud pública, la estabilidad económica, el orden público o el bienestar social;

b) Administradores de Infraestructuras Críticas de Información: Aquellas entidades, públicas o privadas, que operen, administren o controlen sistemas, redes o servicios estratégicos cuya vulneración pudiera comprometer la estabilidad, la seguridad nacional, el orden público, la protección del medio ambiente o el bienestar de la sociedad.;

c) Proveedores de Servicios Digitales Relevantes: Las plataformas tecnológicas, servicios en la nube, motores de búsqueda, redes sociales, servicios de alojamiento de datos o intermediación digital, cuya actividad impacte de manera significativa en el acceso a derechos fundamentales, la estabilidad informativa, la economía o la seguridad pública.;

d) Dependencias, entidades y organismos de los tres órdenes de gobierno: Las instituciones públicas que operen, administren o custodien sistemas de información, bases de datos, redes de comunicación o servicios digitales esenciales para la prestación de servicios públicos, la protección de derechos humanos o el resguardo de información estratégica, y

e) Entidades privadas que procesen, almacenen o administren información estratégica o datos personales sensibles en volúmenes o niveles de riesgo relevantes: Aun sin ser operadores esenciales, aquellas entidades cuyo nivel de exposición de riesgo tecnológico pueda comprometer la protección de derechos fundamentales, la seguridad pública o la continuidad de servicios críticos,

XL. Tecnologías de la Información y Comunicación (TIC): Conjunto de herramientas, recursos, sistemas, dispositivos y aplicaciones que permiten la gestión, almacenamiento, procesamiento, transmisión y comunicación de información y datos en formato digital, incluyendo computadoras, dispositivos móviles, redes, software, servicios en la nube, entre otros, y

XLI. Vulnerabilidad informática: Debilidad, falla o deficiencia en el diseño, implementación, configuración o gestión de sistemas, redes, aplicaciones o procesos, que puede ser explotada por amenazas internas o externas para comprometer la seguridad, integridad, disponibilidad, autenticación o resiliencia de la información o los sistemas.

Artículo 4. Para alcanzar los objetivos de esta ley se deberán observar los siguientes principios:

I. Autenticidad: Toda acción en materia de ciberseguridad deberá garantizar que los usuarios, dispositivos, sistemas o datos sean verificables como genuinos y legítimos, mediante mecanismos confiables que aseguren la identidad y origen de los mismos;

II. Confidencialidad: La información debe ser accesible únicamente por personas, entidades o sistemas autorizados, asegurando su protección frente a accesos no autorizados;

III. Control de daños: Ante un incidente de ciberseguridad, los sujetos obligados y autoridades deberán actuar de forma diligente, coordinada y proporcionada, adoptando las medidas necesarias para contener, mitigar y prevenir la escalada o propagación del incidente;

IV. Cooperación: Los sujetos obligados, autoridades y sectores involucrados deberán colaborar activamente con la autoridad competente y entre sí, considerando la interdependencia de los sistemas, para la gestión integral y eficiente de incidentes de ciberseguridad;

V. Coordinación: Las autoridades competentes deberán armonizar sus acciones y competencias, evitando duplicidades o interferencias, propiciando la unidad de acción en la gestión de ciberseguridad;

VI. Disponibilidad: Garantizar que los sistemas, servicios e información estén accesibles y utilizables por los usuarios autorizados cuando estos lo requieran;

VII. Gobernanza de ciberseguridad: Las políticas, acciones, medidas y decisiones en materia de ciberseguridad deberán ser adoptadas y ejecutadas conforme a un modelo de gobernanza estructurado, transparente y participativo, que garantice:

a) Distribución clara de responsabilidades entre las autoridades competentes, los sujetos obligados, los sectores críticos y la sociedad civil;

b) La coordinación interinstitucional e intersectorial, evitando duplicidades e interferencias;

c) La rendición de cuentas y la transparencia en la toma de decisiones y en la supervisión de las políticas de ciberseguridad, y

d) La armonización con estándares internacionales y la promoción de la cooperación internacional;

VIII. Integridad: Asegurar que la información, sistemas o procesos no sean alterados, manipulados o destruidos de manera no autorizada, preservando su exactitud y confiabilidad;

IX. Interoperabilidad: Garantizar que sistemas, organizaciones y procesos, distintos y diversos, puedan interactuar, compartir información y colaborar eficazmente, mediante estándares comunes y mecanismos seguros de intercambio de datos;

X. Innovación: La política de ciberseguridad deberá fomentar el desarrollo, adopción y mejora continua de tecnologías, procesos y capacidades innovadoras, orientadas a proteger los derechos humanos, la resiliencia de los sistemas y la soberanía digital, promoviendo la investigación y colaboración público-privada;

XI. Legalidad: Toda acción, medida o política en materia de ciberseguridad deberá estar fundada y motivada en las disposiciones constitucionales, legales y reglamentarias aplicables, respetando los principios de jerarquía normativa y control de convencionalidad;

XII. Protección de datos personales: Toda acción en materia de ciberseguridad deberá garantizar la confidencialidad, integridad, disponibilidad, autenticación y resiliencia de los datos personales, asegurando su tratamiento adecuado, legítimo, informado y proporcional, conforme a la legislación nacional y los tratados internacionales;

XIII. Racionalidad: Las medidas de ciberseguridad y las acciones de la autoridad deberán ser necesarias, proporcionales y basadas en un análisis de riesgos, considerando el impacto social, económico y en los derechos humanos;

XIV. Resiliencia: Toda acción en ciberseguridad debe garantizar la capacidad de los sistemas y servicios de resistir, adaptarse y recuperarse ante incidentes, asegurando la continuidad operativa;

XV. Respeto y promoción de los derechos humanos: Las políticas, medidas y acciones en materia de ciberseguridad deberán proteger, respetar, promover y garantizar los derechos humanos y libertades fundamentales, tanto en el entorno digital como fuera de él, asegurando su ejercicio efectivo;

XVI. Respuesta mesurada y no ofensiva: Las medidas de respuesta ante incidentes de ciberseguridad deberán ser proporcionadas y orientadas a la contención, mitigación y recuperación, sin incluir acciones ofensivas, represalias o intervenciones ilícitas en sistemas ajenos;

XVII. Seguridad en el ciberespacio: El Estado deberá garantizar un ciberespacio seguro, abierto, resiliente y accesible para todas las personas, promoviendo y garantizando el ejercicio de los derechos humanos y la protección de los sistemas esenciales;

XVIII. Seguridad informática: Toda persona tiene derecho a proteger sus sistemas, dispositivos y datos mediante medidas técnicas de seguridad, incluyendo el uso de cifrado, autenticación y anonimato, sin ser objeto de restricciones arbitrarias;

XIX. Seguridad y privacidad desde el diseño y por defecto: Los sistemas, servicios y procesos deberán ser diseñados e implementados incorporando medidas técnicas y organizativas adecuadas que garanticen la seguridad y privacidad, desde el inicio y en todo su ciclo de vida, y

XX. Transparencia y rendición de cuentas: Las autoridades y operadores deberán actuar con transparencia y responsabilidad, documentando y comunicando sus acciones en materia de ciberseguridad, garantizando e derecho a la información y la supervisión democrática.

TÍTULO II
DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD

CAPÍTULO PRIMERO
ATRIBUCIONES DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD

Artículo 5. La Agencia Nacional de Ciberseguridad, en coordinación con el Gobierno Federal, los gobiernos de las entidades federativas, los municipios y las Alcaldías de la Ciudad de México, será responsable de la implementación, supervisión y coordinación integral de las políticas, acciones y medidas en materia de ciberseguridad, conforme a las atribuciones establecidas en esta Ley y la normativa secundaria que de ella emane.

Corresponde a la Agencia Nacional de Ciberseguridad garantizar la gobernanza de la ciberseguridad, promoviendo la unidad de acción, cooperación interinstitucional e intersectorial, y la armonización con estándares internacionales, sin perjuicio de las competencias exclusivas en materia de seguridad nacional y defensa, que corresponden a las Fuerzas Armadas.

Artículo 6. La Agencia Nacional de Ciberseguridad es un organismo público descentralizado, con personalidad jurídica y patrimonio propios, dotado de autonomía técnica, operativa, administrativa y de gestión, encargado de la coordinación, supervisión y promoción de la ciberseguridad nacional, en el ámbito civil, sin interferir en las competencias de la seguridad nacional ni la ciberdefensa militar.

La Agencia tiene como objetivo garantizar la protección de los derechos humanos en el entorno digital, la continuidad operativa de los servicios esenciales, la resiliencia de las infraestructuras críticas de información y la soberanía digital del Estado mexicano, mediante la gestión integral de riesgos cibernéticos y la coordinación de actores públicos, privados, académicos y sociales.

La instancia normativa y de gobernanza de la Agencia será el Consejo Nacional de Ciberseguridad, órgano colegiado consultivo, que emitirá directrices estratégicas y políticas públicas en materia de ciberseguridad. Estará presidido por la Secretaría de Seguridad y Protección Ciudadana e integrado por representantes de:

a) Secretaria de Gobernación;

b) Secretaría de Infraestructura, Comunicaciones y Transportes;

c) Secretaría de Anticorrupción y Buen Gobierno

d) Secretaría de la Defensa Nacional;

e) Secretaría de Marina;

f) Secretaría de Relaciones Exteriores;

g) Fiscalía General de la República;

h) Agencia de Transformación Digital y Telecomunicaciones, y

i) Representantes de la sociedad civil, sector privado y academia, con voz pero sin voto.

El Consejo deberá sesionar al menos dos veces al año y contará con una Secretaría Técnica, responsable del seguimiento y ejecución de sus acuerdos.

Artículo 7. A la Agencia Nacional de Ciberseguridad le corresponden las siguientes atribuciones:

I. Asesorar al Ejecutivo Federal, en la elaboración, implementación, evaluación y actualización de la Estrategia Nacional de Ciberseguridad y de los planes y programas sectoriales;

II. Coordinar y supervisar la gobernanza de la ciberseguridad, promoviendo la cooperación interinstitucional, intersectorial e internacional, para garantizar la unidad de acción y evitar duplicidades o interferencias, respetando las competencias de las autoridades sectoriales, órganos autónomos y las Fuerzas Armadas en materia de seguridad nacional y defensa;

III. Establecer, mantener y actualizar el Registro de Infraestructuras Críticas de Información (RICI), clasificando activos, sistemas y servicios esenciales para la seguridad y continuidad operativa del país;

IV. Gestionar incidentes de ciberseguridad mediante la recepción, análisis, coordinación y respuesta a incidentes de impacto significativo, en coordinación con los CERT sectoriales y las autoridades competentes, sin perjuicio de las competencias de las autoridades penales y ministeriales en materia de ciberdelincuencia:

V. Notificar a las entidades afectadas por incidentes de ciberseguridad la obligación de informar oportuna y verazmente a los potenciales afectados, respetando los derechos humanos y la protección de datos personales;

VI. Promover la cultura de ciberseguridad, desarrollando programas de sensibilización, formación, civismo digital, capacitación, innovación tecnológica y difusión de mejores prácticas, en colaboración con la sociedad civil, el sector privado y la academia;

VII. Solicitar información específica a los operadores de servicios esenciales y los sujetos obligados, cuando sea necesario para prevenir, gestionar o responder a incidentes de ciberseguridad, asegurando que dichas solicitudes sean fundadas, motivadas y proporcionales, y que, en caso de incluir datos personales, estos se anonimicen, salvo que sea indispensable su tratamiento bajo el marco jurídico aplicable, garantizando en todo momento el respeto a los derechos humanos, la confidencialidad de la información y la legislación en materia de protección de datos personales;

VIII. Solicitar acceso a redes y sistemas informáticos en casos de incidentes de ciberseguridad de impacto significativo, mediante resolución fundada y motivada por el Director General de la Agencia, debiendo notificarse de manera inmediata a la entidad requerida. En caso de oposición o controversia, se atenderá lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y en las leyes aplicables en materia de protección de datos personales, exclusivamente respecto a las infraestructuras críticas de información y operadores de servicios esenciales, respetando los derechos humanos y las competencias de las autoridades judiciales y de procuración de justicia, y

IX. Supervisar el cumplimiento de las obligaciones de ciberseguridad, incluyendo la aplicación de medidas correctivas y la propuesta de sanciones administrativas, sin perjuicio de las competencias de las autoridades penales o sectoriales.

X. Establecerá mecanismos de cooperación técnica con el Ministerio Público para:

a) Apoyar técnicamente en la preservación de evidencia digital;

b) Asistir en la investigación de delitos cibernéticos, y

c) Garantizar el respeto al debido proceso en la gestión de información técnica.

CAPÍTULO SEGUNDO
DIRECCIÓN, ORGANIZACIÓN Y PATRIMONIO

DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD

Artículo 8. La dirección y la conducción administrativa de la Agencia corresponderá a una persona titular designada para la Dirección General de la Agencia Nacional de Ciberseguridad, quien ejercerá la máxima autoridad operativa y contará con la representación legal e institucional de la entidad y será nombrado a propuesta de la persona Presidente de México, mediante ratificación del Senado de la República.

Artículo 9. Los requisitos mínimos para ocupar la titularidad de la Dirección General serán:

I. Ser persona mexicana por nacimiento, en pleno ejercicio de sus derechos civiles y políticos.

II. Tener entre 35 y 70 años de edad.

III. Contar con experiencia mínima de diez años en ciberseguridad, gestión de riesgos tecnológicos, protección de infraestructuras críticas de información, gobernanza digital o normativas internacionales en la materia, en ámbitos técnicos, regulatorios, académicos o de servicio público;

IV. Acreditar conocimientos especializados en estándares internacionales de ciberseguridad, en derechos humanos y en gobernanza de ciberseguridad, y

V. No haber sido sancionado por faltas administrativas graves, delitos dolosos o violaciones a derechos humanos, y estar sujeto a un régimen de conflicto de intereses, conforme a la legislación en la materia;

La persona titular de la Dirección General de la Agencia Nacional de Ciberseguridad se abstendrá de desempeñar cualquier otro empleo, trabajo o comisión públicos o privados, con excepción de los cargos docentes. Asimismo, estará impedido para conocer asuntos en que tenga interés directo o indirecto, en cuyo caso avisará a la instancia normativa correspondiente.

Artículo 10. Corresponde a la persona titular de la Dirección General de la Agencia Nacional de Ciberseguridad el ejercicio de las siguientes atribuciones:

I. Ejecutar, coordinar y supervisar el funcionamiento operativo y administrativo de la Agencia, conforme a las directrices y políticas aprobadas por el Consejo Nacional de Ciberseguridad;

II. Proponer al Consejo Nacional de Ciberseguridad la creación de unidades regionales o estatales, justificando su pertinencia operativa o estratégica;

III. Emitir acuerdos, resoluciones y actos administrativos internos para el buen funcionamiento de la Agencia, sin invadir las competencias del órgano colegiado;

IV. Expedir lineamientos operativos internos dentro de las atribuciones conferidas por la ley, respetando las decisiones del Consejo;

V. Celebrar convenios y ejecutar actos jurídicos necesarios para el cumplimiento de los objetivos de la Agencia, previa información al Consejo Nacional de Ciberseguridad, especialmente en materia de cooperación internacional o cuando afecten infraestructuras críticas;

VI. Delegar funciones y atribuciones específicas al personal de la Agencia conforme a la normativa aplicable, asegurando el cumplimiento de principios de rendición de cuentas;

VII. Representar legalmente a la Agencia en actos jurídicos y procedimientos administrativos;

VIII. Presentar informes anuales al Consejo Nacional de Ciberseguridad, incluyendo la evaluación de resultados, la gestión de riesgos cibernéticos y la cooperación interinstitucional e internacional, y

IX. Las demás que determine la presente Ley y normatividad aplicable.

Artículo 11. El patrimonio de la Agencia estará integrado por:

I. Los recursos asignados en el Presupuesto de Egresos de la Federación para el ejercicio fiscal correspondiente;

II. Los recursos que reciba con base en leyes u otras disposiciones normativas;

III. Bienes muebles e inmuebles, tangibles e intangibles, que le sean transferidos o que adquiera por cualquier medio legal;

IV. Los productos financieros, rendimientos o ingresos derivados del uso o administración de sus bienes o servicios;

V. Aportaciones de organismos de cooperación internacional, recibidas en coordinación con la Secretaría de Relaciones Exteriores; y

VI. Los demás ingresos que obtenga conforme a la legislación vigente.

Artículo 12. Profesionalización y contratación de personal directivo de la Agencia Nacional de Ciberseguridad. Para la contratación del personal directivo y especializado dentro de la Agencia Nacional de Ciberseguridad, se procurará dar prioridad a las personas integrantes del Sistema de Servicio Profesional de Carrera, que acrediten competencias técnicas, experiencia y conocimientos especializados en ciberseguridad, gestión de riesgos tecnológicos, protección de infraestructuras críticas de información, gobernanza digital o normativas internacionales aplicables.

La selección de personal directivo deberá realizarse mediante procesos públicos, transparentes, basados en méritos y competencias, garantizando la independencia técnica y operativa de la Agencia y el cumplimiento de los principios de profesionalización, inclusión, equidad de género y diversidad.

Artículo 13. Régimen laboral y responsabilidades del personal de la Agencia Nacional de Ciberseguridad. El personal de la Agencia Nacional de Ciberseguridad se regirá por la Ley Federal de los Trabajadores al Servicio del Estado, Reglamentaria del Apartado B del Artículo 123 Constitucional, así como por la Ley General de Responsabilidades Administrativas, la Ley General de Transparencia y Acceso a la Información Pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Además, le serán aplicables las normas de ética pública, los principios de gobernanza de ciberseguridad, las disposiciones sobre conflicto de intereses y las responsabilidades administrativas, conforme al marco normativo vigente.

Las personas servidoras públicas estarán sujetas a responsabilidades administrativas, civiles y penales, derivadas de actos u omisiones cometidas en el ejercicio de sus funciones, sin perjuicio de las sanciones que correspondan por la inobservancia de las disposiciones de ciberseguridad o por violaciones a los derechos humanos.

En caso de cese de funciones, se reconocerán las indemnizaciones y prestaciones laborales previstas en las leyes aplicables a servidores públicos, garantizando los principios de equidad y justicia laboral.

La Dirección General de la Agencia Nacional de Ciberseguridad tendrá la facultad de aplicar comisiones de servicio, adscripciones temporales y reasignaciones, conforme a la legislación administrativa aplicable, garantizando el cumplimiento de los principios de especialización, integridad y rendición de cuentas.

La estructura orgánica y plantilla de personal de la Agencia será determinada mediante reglamento interno aprobado por el Consejo Nacional de Ciberseguridad, garantizando la autonomía técnica y de gestión de la Agencia, sin perjuicio de la coordinación con la Secretaría de Seguridad y Protección Ciudadana y el marco general de la Administración Pública Federal.

Artículo 14. Régimen de incompatibilidades y conflictos de interés del personal de la Agencia Nacional de Ciberseguridad. El personal directivo y especializado de la Agencia deberá actuar con plena independencia, integridad y transparencia, evitando conflictos de interés que puedan comprometer la objetividad y autonomía técnica de la Agencia. El régimen de incompatibilidades y conflictos de interés se aplicará bajo el principio de inclusión laboral, equidad de género y diversidad, asegurando la participación de personas expertas provenientes de distintos sectores, regiones y contextos, respetando en todo momento los derechos laborales y las libertades profesionales, sin perjuicio de las salvaguardas de integridad y autonomía técnica

No podrán prestar servicios personales, de consultoría o asesoría, ya sea directamente o a través de terceros, a individuos o entidades sujetas a supervisión o fiscalización por la Agencia, incluyendo a sus directivos, representantes o empleados, durante su permanencia en la Agencia y hasta por un año posterior al término de sus funciones.

Asimismo, deberán abstenerse de intervenir en asuntos institucionales en los que exista un interés personal, familiar o de terceros vinculados, ya sea propio o de su cónyuge, concubina o concubinario, o de parientes hasta el cuarto grado por consanguinidad o segundo por afinidad.

Queda prohibido que el personal directivo o especializado actúe como cabildero o representante de intereses privados ante entidades sujetas a la supervisión de la Agencia, incluso a través de personas morales o sociedades en las que participen.

El desempeño de funciones dentro de la Agencia será de dedicación exclusiva, incompatible con cualquier otra función o empleo que pueda comprometer la imparcialidad, independencia o dedicación operativa de la Agencia, respetando en todo momento los derechos laborales, las libertades profesionales y el derecho al desarrollo personal y profesional, así como con la participación en órganos de dirección o representación de instituciones públicas o privadas, nacionales o extranjeras, salvo:

a) Aquellas participaciones honoríficas, sin fines de lucro o en foros internacionales reconocidos, relacionadas con la promoción de la ciberseguridad, derechos digitales o cooperación internacional, siempre que no exista conflicto de interés, y previa notificación y autorización del Consejo Nacional de Ciberseguridad;

b) Actividades docentes o académicas, en instituciones reconocidas por el Estado, que no excedan doce horas semanales, y

c) Colaboración no remunerada en organizaciones de beneficencia o de carácter social sin fines de lucro, previa autorización de la Dirección General, garantizando que no existan conflictos de interés.

Asimismo, se permitirá la colaboración no remunerada en instituciones de beneficencia o de carácter social sin fines de lucro, siempre que exista autorización previa y expresa por parte de la persona titular de la Dirección General de la Agencia Nacional de Ciberseguridad. Además, al personal le serán aplicables las prohibiciones y obligaciones establecidas en la legislación en materia de responsabilidad administrativa de los servidores públicos.

Quedan excluidos de la aplicación del presente artículo todo personal que realice funciones mayormente operativas no profesionales o especializadas y las personas físicas contratadas bajo el régimen de prestación de servicios profesionales por honorarios.

TÍTULO III
DE LA PROMOCIÓN DE LA CIBERSEGURIDAD

CAPÍTULO ÚNICO
ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Artículo 15. La Estrategia Nacional de Ciberseguridad, elaborada por la Agencia en coordinación con el Consejo Nacional de Ciberseguridad, establecerá los planes, programas, políticas y acciones para garantizar la protección de infraestructuras críticas,

servicios esenciales, derechos humanos en el entorno digital y la soberanía digital del Estado.

La Estrategia deberá contemplar, como mínimo lo siguiente:

a) La promoción de los derechos digitales, garantizando la libertad de expresión, privacidad y protección de datos personales;

b) El fomento de la autenticidad, integridad, confidencialidad, disponibilidad y resiliencia de los sistemas, servicios y datos;

c) La prevención, detección temprana, respuesta, recuperación y resiliencia ante amenazas, vulnerabilidades e incidentes cibernéticos;

d) La participación multisectorial con el sector público, privado, sociedad civil y academia, asegurando gobernanza inclusiva y transparencia.

Artículo 16. La Agencia establecerá protocolos operativos, claros y seguros, para facilitar el intercambio de información relevante o crítica entre las entidades bajo su coordinación, garantizando la protección de los derechos humanos, la confidencialidad de los datos y la resiliencia operativa y protocolos específicos para la recolección, análisis y custodia de evidencia digital, respetando los principios de legalidad y proporcionalidad.

Artículo 17. La Agencia determinará el tipo y clasificación de la información considerada como relevante o crítica para la ciberseguridad nacional, bajo criterios públicos, objetivos y transparentes, previamente establecidos y publicados.

Estos criterios deberán considerar el impacto potencial en la continuidad operativa, la seguridad pública, la economía, la salud, la soberanía digital y los derechos humanos.

Artículo 18. Todas las instancias sujetas a la aplicación de esta Ley deberán designar un enlace especializado en ciberseguridad, responsable de la gestión, flujo e intercambio de información crítica, así como de la identificación, recolección, análisis y transmisión de dicha información, conforme a las funciones que les correspondan y respetando las disposiciones sobre protección de datos personales y derechos humanos.

Artículo 19. La Agencia establecerá principios, estándares, guías y lineamientos técnicos seguros y estandarizados para la transmisión de información crítica, que incluyan el uso de formatos interoperables, medios de comunicación protegidos, sistemas de cifrado robusto y métodos confiables de autenticación.

Artículo 20. Los métodos de respuesta y los plazos para el intercambio de información crítica se fijarán conforme a la urgencia del riesgo y la gravedad del incidente, priorizando la inmediatez y eficiencia en la comunicación, y respetando los principios de proporcionalidad, protección de datos y derechos humanos.

Artículo 21. Toda transmisión o intercambio de información crítica para la atención de amenazas o incidentes de ciberseguridad deberá respetar los motivos de seguridad pública o nacional, protección de derechos humanos, protección de datos personales y confidencialidad, conforme al marco jurídico aplicable.

Artículo 22. La Agencia Nacional de Ciberseguridad realizará auditorías técnicas y organizativas periódicas, conforme a un enfoque basado en riesgos:

a) Sus propios procesos internos, incluyendo la gestión de incidentes, protección de datos personales, intercambio de información crítica y cumplimiento de estándares de ciberseguridad, y

b) Los entes públicos y privados incluidos en el Registro de Infraestructuras Críticas de Información (RICI), evaluando el cumplimiento de las obligaciones en materia de ciberseguridad, resiliencia y protección de derechos humanos.

Las auditorías deberán realizarse conforme a estándares internacionales reconocidos y respetando los principios de proporcionalidad, confidencialidad, debido proceso y protección de datos personales.

Artículo 23. La Agencia Nacional de Ciberseguridad, en coordinación con las entidades sujetas a la aplicación de esta Ley, establecerá protocolos de respuesta claros, efectivos y proporcionales ante cualquier incidente o afectación a la información relevante o crítica, incluyendo:

a) Mecanismos de notificación inmediata a las autoridades competentes y a las personas potencialmente afectadas;

b) Planes de recuperación y resiliencia, conforme a estándares internacionales, y

c) Garantías para la protección de derechos humanos, la soberanía digital y los datos personales durante todo el proceso de respuesta.

Los protocolos deberán ser públicos en sus principios rectores, aunque se reservará su contenido operativo específico cuando sea necesario por razones de seguridad pública o nacional o protección de las infraestructuras críticas.

TÍTULO IV
DERECHOS DIGITALES Y PROTECCIÓN EN EL ENTORNO DE CIBERSEGURIDAD

CAPÍTULO PRIMERO
DE LOS DERECHOS DE LAS PERSONAS EN EL ENTORNO DIGITAL

Artículo 24. En el marco de la ciberseguridad, el Estado mexicano tiene como objetivo fundamental proteger, respetar, promover y garantizar los derechos digitales de las personas en el entorno digital, incluyendo el ciberespacio y los sistemas digitales interconectados, conforme a los principios de universalidad, interdependencia, indivisibilidad y progresividad de los derechos humanos, pro persona, así como los tratados internacionales de los que el Estado Mexicano forme parte y las mejores prácticas internacionales.

Los derechos digitales comprenden una extensión de los derechos humanos en el entorno digital y se articulan para:

a) Garantizar el acceso universal, asequible, seguro y de calidad a las tecnologías de la información y la comunicación, incluyendo Internet, con el fin de cerrar las brechas digitales y fomentar la inclusión digital;

b) Promover un modelo de transformación digital centrado en las personas, asegurando que las tecnologías digitales respeten y garanticen los derechos humanos, la equidad, la diversidad y la justicia social, y

c) Fomentar un entorno digital seguro, resiliente y respetuoso de los derechos, promoviendo el uso ético y responsable de las tecnologías digitales como bienes comunes globales.

Artículo 25. Todas las personas, sin distinción alguna, gozarán de los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales de los que el Estado mexicano sea parte, en esta Ley, y en las disposiciones aplicables en materia de derechos humanos, ciberseguridad, protección de datos personales y entorno digital.

Los derechos digitales son una extensión y adaptación de los derechos humanos en el entorno digital y de ciberseguridad, reconocidos conforme a los principios de universalidad, interdependencia, indivisibilidad y progresividad, y se garantizan en la medida necesaria para respetar, proteger, promover y garantizar el pleno ejercicio de los derechos humanos en el entorno digital.

Derechos humanos y digitales de las personas:

I. Toda persona tiene derecho a la privacidad; a la confidencialidad, integridad y protección de sus datos personales, sobre todo los biométricos, en el entorno digital, conforme a los tratados internacionales en la materia de los que México sea parte, a las leyes nacionales de protección de datos personales y los estándares internacionales;

II. Las niñas, niños y adolescentes tienen derecho a acceder, participar y utilizar el entorno digital, incluyendo Internet, redes y servicios digitales, de manera segura, inclusiva, accesible y adaptada a su edad y desarrollo evolutivo, como medio efectivo para ejercer sus derechos a la información, comunicación, educación, salud, esparcimiento, participación, privacidad y no discriminación, de conformidad con:

a) El principio de interés superior de la infancia reconocido en el Artículo 4º de la Constitución Política de los Estados Unidos Mexicanos;

b) Los principios de interdependencia, progresividad, participación y no discriminación; y

c) La Ley General de los Derechos de Niñas, Niños y Adolescentes y los tratados internacionales de los que México es parte.

El Estado garantizará:

i. Que el acceso seguro y libre de riesgos se proporcione mediante la implementación de medidas de ciberseguridad, privacidad por diseño y por defecto, alfabetización digital adaptada a la infancia y mecanismos de prevención de riesgos digitales (como violencia en línea, ciberacoso, explotación o abuso), y

ii. Que todas las medidas adoptadas sean adecuadas, necesarias, proporcionales y respetuosas del interés superior de la infancia, evitando restricciones arbitrarias o desproporcionadas al ejercicio de los derechos de libertad de expresión, privacidad, protección de datos y participación de niñas, niños y adolescentes en el entorno digital.

III. Las personas tienen derecho a expresarse libremente, a buscar, recibir y difundir información, así como a un Internet libre y abierto, sin restricciones arbitrarias, garantizando el principio de neutralidad de la red, transparencia algorítmica.

El ejercicio de la libertad de expresión en el entorno digital se regirá por la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales de los que el Estado mexicano forme parte, y las leyes aplicables en materia de derechos humanos, libertad de expresión y derecho a la información. Las disposiciones de esta Ley en ningún caso podrán interpretarse como una limitación a dicho ejercicio;

IV. Las personas tienen derecho a que sus dispositivos, redes y servicios digitales cuenten con medidas de ciberseguridad adecuadas, alineadas a estándares internacionales, garantizando la resiliencia y continuidad operativa;

V. Derecho al acceso universal, asequible y de calidad a Internet y tecnologías digitales: Toda persona tiene derecho a acceder a Internet y tecnologías digitales sin discriminación por motivo alguno, asegurando igualdad de condiciones, conforme al párrafo Tercero del Artículo 6º constitucional;

VI. A resguardar la Propiedad Intelectual, garantizando el reconocimiento de los autores sobre su obra artística o literaria y el derecho a ser remunerados por su uso, garantizando al mismo tiempo el libre acceso a las obras que ya sean de dominio público;

VII. Toda persona tiene derecho a proteger sus comunicaciones, datos e identidad mediante herramientas de cifrado y anonimato, sin ser objeto de restricciones arbitrarias o vigilancia masiva, garantizando la privacidad por diseño y por defecto en los sistemas y servicios digitales. Los gobiernos o empresas no pueden negar el cifrado de la información;

VIII. Las personas tienen derecho a participar en la divulgación responsable de vulnerabilidades en ciberseguridad, asegurando la confidencialidad de las personas notificantes y la adopción de medidas oportunas para mitigar los riesgos, conforme al marco jurídico aplicable;

IX. Las personas tienen derecho a la resiliencia y acceso a mecanismos de denuncia en caso de incidentes de ciberseguridad y a ser informadas clara, certera y oportunamente sobre estos incidentes de ciberseguridad que puedan afectar sus derechos o servicios esenciales, así como a acceder a mecanismos de reparación, bonificación o compensación y a mecanismos de denuncia y protección efectiva en caso de violaciones;

X. Toda persona tiene derecho a estar protegida frente a vigilancia arbitraria o masiva y el uso de tecnologías intrusivas, como el reconocimiento facial o la recopilación masiva de datos, asegurando que toda intervención esté fundada, motivada, proporcionada y supervisada judicialmente, conforme a los principios internacionales de derechos humanos, así como de las leyes y tratados internacionales especializados en la materia;

XI. Las personas tienen derecho a que las decisiones automatizadas y sistemas algorítmicos que afecten sus derechos sean equitativos, transparentes, explicables, supervisables y no discriminatorios, conforme a las buenas prácticas internacionales, y

XII. A contar con derecho al olvido para que la información privada de una persona se elimine de las búsquedas de Internet, de bases de datos y de directorios.

Las personas usuarias, al decidir la utilización de determinados servicios de telecomunicaciones y/o aplicaciones digitales, lo que incluye la elección de proveedores, la contratación y las condiciones comerciales, lo harán de conformidad con lo que se dispone en la Ley Federal de Telecomunicaciones y Radiodifusión, la Ley Federal de Protección al Consumidor, así como las disposiciones aplicables la PROFECO y la Agencia de Transformación Digital y Telecomunicaciones.

CAPÍTULO SEGUNDO
OBLIGACIONES DIGITALES

Artículo 26. Los operadores de servicios esenciales, las infraestructuras críticas de información y las entidades obligadas conforme a esta Ley deberán notificar a la Agencia Nacional de Ciberseguridad, de forma oportuna y proporcionada, cualquier incidente de ciberseguridad o actividad irregular que pueda comprometer la seguridad, resiliencia o

continuidad de los servicios o sistemas críticos bajo su responsabilidad, conforme a los protocolos y lineamientos que emita la Agencia.

Las personas usuarias del entorno digital podrán, de manera voluntaria y confidencial, notificar a la Agencia o al proveedor de servicios cualquier riesgo o incidente de ciberseguridad, garantizando en todo momento el respeto a los derechos humanos y la protección de datos personales.

TÍTULO V
DE LA PREVENCIÓN EN EL ÁMBITO DIGITAL

CAPÍTULO PRIMERO
CLASIFICACIÓN DE OPERADORES Y GESTIÓN DIFERENCIADA DE RIESGOS

Artículo 27. Los operadores sujetos a esta Ley se clasificarán en:

I. Operadores de servicios esenciales: Son aquellas entidades, públicas o privadas, cuya prestación de servicios resulta fundamental para el mantenimiento de las funciones sociales, económicas, de salud pública, seguridad pública o de bienestar general de la población, cuya interrupción tendría un impacto significativo;

II. Infraestructuras críticas de información: Son sistemas, redes, plataformas o servicios tecnológicos asociados a las áreas estratégicas a que se refiere el artículo 28 constitucional, cuya afectación pudiera poner en peligro la seguridad nacional, el orden público, la salud pública, el suministro de servicios esenciales o la estabilidad económica del país, y

III. Servicios digitales relevantes: Son las plataformas digitales, servicios en la nube, redes sociales, motores de búsqueda, servicios de alojamiento o intermediación digital cuya operación tiene un impacto significativo en el ejercicio de derechos humanos, la seguridad económica, la integridad informativa o la continuidad de los servicios públicos esenciales.

Artículo 28. La Agencia Nacional de Ciberseguridad emitirá lineamientos para la clasificación y actualización periódica de los operadores, considerando:

I. El volumen y la importancia de los servicios o sistemas proporcionados;

II. El grado de interdependencia con otros sectores críticos;

III. El potencial impacto económico, social, de salud o de seguridad pública en caso de interrupción o afectación;

IV. La sensibilidad de los datos o información gestionada;

V. La posición en el mercado y el nivel de dependencia de la población respecto al servicio, y

VI. Las áreas estratégicas definidas en el artículo 28 constitucional.

Artículo 29. La Agencia Nacional de Ciberseguridad garantizará la confidencialidad de las personas notificantes de vulnerabilidades de ciberseguridad, cuando estas hayan sido reportadas conforme a derecho. La identidad de la persona notificante sólo podrá ser revelada con su consentimiento expreso, o en cumplimiento de orden judicial debidamente fundada y motivada.

Artículo 30. Obligaciones diferenciadas por nivel de riesgo y criticidad:

I. Alta criticidad y riesgo: Operadores de infraestructuras críticas de información y servicios esenciales estratégicos deberán cumplir con obligaciones reforzadas en materia de:

a) Evaluación continua de riesgos;

b) Auditorías de ciberseguridad anuales;

c) Implementación de planes de contingencia y recuperación ante incidentes, y

d) Notificación inmediata de incidentes a la Agencia.

II. Criticidad media: Operadores de servicios esenciales no estratégicos y grandes servicios digitales relevantes deberán cumplir con:

a) Políticas internas de ciberseguridad;

b) Evaluación periódica de riesgos, y

c) Notificación de incidentes significativos en plazos razonables.

III. Baja criticidad: Otros servicios digitales relevantes de menor escala o impacto deberán cumplir con:

a) Medidas básicas de ciberseguridad, y

b) Protocolos de notificación simplificados.

Artículo 31. La clasificación de operadores será revisada al menos cada dos años o cuando existan cambios significativos en la prestación de los servicios, en el nivel de riesgos asociados, o en el contexto nacional o internacional de ciberseguridad.

CAPÍTULO SEGUNDO
MEDIDAS DE CIBERSEGURIDAD PARA LOS OPERADORES

Artículo 32. Los operadores de servicios esenciales, las infraestructuras críticas de información y las entidades digitales relevantes en el ámbito de esta Ley deberán implementar medidas mínimas de ciberseguridad, conforme a los principios de proporcionalidad, gestión de riesgos y estándares internacionales reconocidos.

La Agencia Nacional de Ciberseguridad, en coordinación con las autoridades sectoriales competentes, establecerá los criterios técnicos y organizativos diferenciados para la implementación, supervisión y actualización de dichas medidas, tomando en cuenta:

a) El nivel de riesgo y criticidad de los servicios y sistemas;

b) La capacidad técnica y organizativa del operador; y

c) El potencial impacto en los derechos humanos, la soberanía digital y la seguridad pública.

Artículo 33. Las medidas mínimas de ciberseguridad deberán incluir, de manera proporcional al nivel de riesgo y criticidad de los servicios, al menos los siguientes elementos, sin que sean limitativos:

I. Salvaguardar la confidencialidad, integridad, disponibilidad, autenticación y resiliencia de los datos personales y la información, conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y estándares internacionales de ciberseguridad;

II. Diseñar e implementar políticas internas de ciberseguridad, incluyendo:

a) La capacitación continua del personal.

b) La gestión de incidentes de ciberseguridad.

c) La evaluación y actualización periódica de riesgos y controles.

III. Cooperar con la Agencia Nacional de Ciberseguridad y las autoridades competentes en la gestión y mitigación de incidentes de ciberseguridad, respetando el Estado de Derecho, el debido proceso y los derechos humanos;

IV. Apegarse a las disposiciones nacionales e internacionales aplicables en materia de ciberseguridad, protección de datos personales y gobernanza digital;

V. Cumplir con las obligaciones derivadas de los protocolos de notificación, respuesta y recuperación ante incidentes, conforme a los lineamientos emitidos por la Agencia Nacional de Ciberseguridad, y

VI. Atender cualquier otra obligación que derive de las leyes aplicables y del objeto de esta Ley.

Artículo 34. Los operadores de servicios esenciales, las infraestructuras críticas de información y las entidades digitales relevantes en el ámbito de esta Ley deberán implementar medidas mínimas de ciberseguridad, conforme a los principios de proporcionalidad, gestión de riesgos y estándares internacionales reconocidos.

La Agencia Nacional de Ciberseguridad, en coordinación con las autoridades sectoriales competentes, establecerá los criterios técnicos y organizativos diferenciados para la implementación, supervisión y actualización de dichas medidas, tomando en cuenta:

I. El nivel de riesgo y criticidad de los servicios y sistemas;

II. La capacidad técnica y organizativa del operador, y

III. El potencial impacto en los derechos humanos, la soberanía digital y la seguridad pública.

Artículo 35. Las medidas mínimas de ciberseguridad deberán incluir, de manera proporcional al nivel de riesgo y criticidad de los servicios, los siguientes elementos, sin que sean limitativos:

I. Salvaguardar la confidencialidad, integridad, disponibilidad, autenticación y resiliencia de los datos personales y la información, conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y estándares internacionales de ciberseguridad;

II. Diseñar e implementar políticas internas de ciberseguridad, incluyendo:

a) La capacitación continua del personal;

b) La gestión de incidentes de ciberseguridad, y

c) La evaluación y actualización periódica de riesgos y controles;

III. Cooperar con la Agencia Nacional de Ciberseguridad y las autoridades competentes en la gestión y mitigación de incidentes de ciberseguridad, respetando el Estado de Derecho, el debido proceso y los derechos humanos;

IV. Apegarse a las disposiciones nacionales e internacionales aplicables en materia de ciberseguridad, protección de datos personales y gobernanza digital, y

V. Cumplir con las obligaciones derivadas de los protocolos de notificación, respuesta y recuperación ante incidentes, conforme a los lineamientos emitidos por la Agencia Nacional de Ciberseguridad.

Artículo 36. Los operadores deberán contar con medidas de prevención y respuesta ante incidentes y al menos:

I. Desarrollar e implementar planes de respuesta a incidentes, integrando procedimientos de notificación y recuperación;

II. Establecer canales seguros de comunicación para la notificación de incidentes;

III. Designar una persona responsable de ciberseguridad encargado de coordinar las acciones de respuesta y comunicación con la Agencia, y

IV. Realizar análisis post-incidente para identificar causas, evaluar daños y mejorar medidas preventivas.

Artículo 37. Para la evaluación de riesgo y auditorias, los operadores de alta y media criticidad deberán realizar evaluaciones de riesgos anuales y someterse a auditorías de ciberseguridad externas al menos cada dos años.

Los operadores de baja criticidad deberán realizar autoevaluaciones anuales de riesgos. Las auditorías deberán realizarse conforme a los estándares internacionales reconocidos y ser remitidas a la Agencia Nacional de Ciberseguridad.

Artículo 38. Los operadores deberán desarrollar programas de formación continua en para su personal con el objetivo de generar capacidades y fomentar una cultura de ciberseguridad que incluya buenas prácticas, ética digital y gestión de riesgos en todos los niveles de la organización.

Artículo 39. Los operadores de servicios esenciales e infraestructuras críticas deberán garantizar la interoperabilidad segura de sus sistemas y cooperar con otros operadores, CERTs sectoriales y el CERT Nacional en acciones de prevención, mitigación y recuperación de incidentes.

CAPÍTULO TERCERO
DE LA PREVENCIÓN DE CIBERAMENAZAS

Artículo 40. La Agencia Nacional de Ciberseguridad deberá elaborar y publicar informes periódicos sobre alertas de ciberamenazas, vulnerabilidades y tendencias cibernéticas, conforme a las siguientes directrices:

I. Reportes trimestrales, dirigidos a las autoridades competentes, incluyendo la Secretaría de Seguridad y Protección Ciudadana (SSPC), las entidades del Consejo Nacional de Ciberseguridad, y las instancias sectoriales relevantes, sobre las ciberamenazas,

vulnerabilidades e incidentes identificados, sin comprometer la confidencialidad operativa o la seguridad pública o nacional, y

II. Alertas extraordinarias o informes especiales, cuando la urgencia o gravedad de la amenaza lo requiera, con el fin de prevenir, contener o mitigar la propagación de ciberamenazas o ciberataques, respetando en todo momento los derechos humanos, la confidencialidad y el debido proceso.

Además, deberá presentar un informe anual público sobre el estado de la ciberseguridad nacional, incluyendo recomendaciones de política pública, medidas adoptadas y tendencias relevantes, al Consejo Nacional de Ciberseguridad, al Senado de la República y a la sociedad en general, con las reservas que sean necesarias por razones de seguridad operativa o nacional, de conformidad con lo que señale en Reglamento de esta Ley.

Artículo 41. La Agencia Nacional de Ciberseguridad deberá notificar en un plazo máximo de 24 horas a las autoridades de los tres órdenes de gobierno sobre la existencia de ciberamenazas o incidentes de ciberseguridad que puedan afectar la continuidad operativa de servicios esenciales, infraestructuras críticas o el ejercicio de derechos humanos.

La notificación deberá realizarse conforme a los protocolos, lineamientos y tiempos de respuesta diferenciados que emita la Agencia, basados en:

I. El nivel de riesgo y criticidad de los sistemas y servicios afectados;

II. La gravedad potencial de la amenaza o incidente.

III. El impacto en los derechos humanos, la seguridad pública y la soberanía digital.

Dichos protocolos deberán garantizar la confidencialidad, integridad y seguridad de la información compartida, así como el respeto al debido proceso.

Artículo 42. La persecución, investigación, sanción y ejecución de las penas de los delitos cibernéticos que se produzcan por los ciberataques mencionados en el artículo anterior, se regirá por el Código Penal Federal, los tratados internacionales en materia de ciberseguridad y ciberdelincuencia suscritos por México y las leyes aplicables en materia penal y de procuración de justicia.

La Agencia Nacional de Ciberseguridad deberá cooperar, coordinar y compartir información técnica pertinente con las autoridades competentes en materia penal, respetando el debido proceso, la confidencialidad de los datos y los derechos humanos, para la prevención, investigación y persecución de los delitos cibernéticos.

TITULO VI
CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CERT)

CAPÍTULO ÚNICO

Artículo 43. Se crea el CERT Nacional, bajo la coordinación de la Agencia Nacional de ciberseguridad, como entidad responsable de la detección, análisis, coordinación y mitigación de incidentes de ciberseguridad a nivel nacional.

Los sectores considerados de alta y media criticidad deberán establecer CERT sectoriales, coordinados con el CERT Nacional.

Artículo 44. Son funciones de los CERT:

I. Monitoreo y detección de amenazas;

II. Análisis y clasificación de incidentes;

III. Coordinación de la respuesta ante incidentes;

IV. Mitigación y recuperación de incidentes;

V. Emisión de alertas, boletines y recomendaciones técnicas;

VI. Capacitar a los operadores en gestión de incidentes, y

VII. Colaborar en ejercicios de simulación

Artículo 45. Los CERT Nacional y sectoriales establecerán protocolos estandarizados para:

I. Notificar incidentes de ciberseguridad de manera oportuna y proporcionada al nivel de riesgo;

II. Intercambiar información técnica relevante bajo criterios de confidencialidad, integridad y protección de datos;

III. Coordinar la respuesta frente a incidentes de forma efectiva, asegurando respeto a los derechos humanos;

IV. Establecer tiempos de respuesta diferenciados según el tipo de incidente y su impacto, y.

V. Promover la cooperación con redes internacionales de CERT, como FIRST y CSIRT Américas.

Artículo 46. El CERT Nacional y los CERT sectoriales deberán:

I. Realizar evaluaciones anuales de su desempeño operativo y tiempos de respuesta;

II. Participar en auditorías técnicas externas de ciberseguridad, al menos cada dos años;

III. Actualizar sus procedimientos y protocolos conforme a las mejores prácticas internacionales y a los resultados de las evaluaciones, y

IV. Reportar los resultados de las evaluaciones al Consejo Nacional de Ciberseguridad para el fortalecimiento de capacidades nacionales.

TÍTULO VII
SISTEMA NACIONAL DE CIBERSEGURIDAD

CAPÍTULO ÚNICO
SISTEMA NACIONAL

Artículo 47. Se crea el Sistema Nacional de Ciberseguridad como un mecanismo de coordinación entre los tres órdenes de gobierno, sector privado, academia y sociedad civil para fortalecer la protección del ciberespacio nacional.

Artículo 48. Los objetivos del Sistema Nacional de Ciberseguridad:

I. Coordinar esfuerzos nacionales de prevención, protección, detección y respuesta ante amenazas cibernéticas;

II. Articular la implementación de políticas públicas en materia de ciberseguridad;

III. Fortalecer capacidades nacionales y regionales, y

IV. Promover la cooperación internacional.

Artículo 49. El Sistema estará integrado por:

I. La Agencia Nacional de Ciberseguridad;

II. Representante del Consejo Nacional de Ciberseguridad;

III. CERT Nacional y CERT Sectoriales;

IV. Representantes de operadores de servicios esenciales y de infraestructuras críticas, y

V. Representantes de la sociedad civil, academia y sector privado.

TÍTULO VIII
COOPERACIÓN INTERNACIONAL Y CIBERDIPLOMACIA

CAPÍTULO ÚNICO

Artículo 50. La cooperación internacional en materia de ciberseguridad se regirá por los principios de respeto a los derechos humanos, soberanía digital, reciprocidad, legalidad y debido proceso.

Artículo 51. La Agencia Nacional de Ciberseguridad representará al Estado mexicano en:

I. Redes internacionales de ciberseguridad como y foros multilaterales;

II. Procesos de negociación de instrumentos internacionales de ciberseguridad, y

II. Iniciativas de cooperación técnica y de fortalecimiento de capacidades.

Artículo 52. La Agencia coordinará mecanismos de cooperación transfronteriza para:

I. Intercambio seguro de información sobre incidentes de ciberseguridad;

II. Solicitudes de asistencia técnica en gestión de incidentes y vulnerabilidades, y.

III. Participación en ejercicios conjuntos de respuesta a incidentes.

Artículo 53. La Agencia presentará un informe anual sobre cooperación internacional y ciberdiplomacia al Consejo Nacional de Ciberseguridad que incluirá:

I. Actividades de cooperación internacional realizada;

II. Resultados obtenidos, y

III. Propuestas para fortalecer la posición de México en el ámbito de la gobernanza global de la ciberseguridad.

TÍTULO IX
ALFABETIZACIÓN DIGITAL Y FORTALECIMIENTO DE CAPACIDADES NACIONALES

CAPÍTULO ÚNICO

Artículo 54. Las autoridades de todos los órdenes de gobierno y entes públicos implementarán políticas públicas para fomentar la alfabetización digital, con énfasis en:

I. Cierre de la brecha digital en poblaciones en situación de vulnerabilidad;

II. Promoción del acceso seguro, inclusivo y asequible a las tecnologías de la información. y

III. Difusión de buenas prácticas de ciberseguridad a nivel ciudadano.

Artículo 55. La Agencia Nacional de Ciberseguridad, en coordinación con instituciones educativas, centros públicos de investigación, y organismos del sector privado, impulsará:

I. Programas de formación técnica en ciberseguridad;

II. Cursos de actualización para operadores de servicios esenciales y críticos, y

III. Programas de certificación y profesionalización de personal especializado en gestión de riesgos digitales.

Artículo 56. Las acciones de alfabetización digital encaminadas a la inclusión digital deberán garantizar:

I. Igualdad de género, inclusión de personas con discapacidad y de comunidades indígenas;

II. Acceso equitativo a la educación digital y a la protección en el entorno digital, y

III. Promoción del civismo digital, el uso ético y seguro de Internet.

Artículo 57. Se promoverá la participación activa de la sociedad civil, el sector académico y el sector privado en:

I. El diseño e implementación de políticas públicas de fortalecimiento de capacidades;

II. La generación de materiales educativos abiertos sobre ciberseguridad, y

III. La colaboración en campañas de sensibilización y prevención de riesgos cibernéticos.

Artículo 58. La Agencia deberá presentar al Consejo Nacional de Ciberseguridad un informe anual que incluya:

I. Programas implementados y metas alcanzadas;

II. Evaluación de impacto en poblaciones beneficiadas y

III. Propuestas de mejora para el fortalecimiento de capacidades nacionales.

TÍTULO X
SUPERVISIÓN Y SANCIONES

Artículo 59. La Agencia Nacional de Ciberseguridad supervisará el cumplimiento de las obligaciones establecidas en esta Ley mediante:

I. Auditorías técnicas y organizativas;

II. Requerimientos de información a los operadores clasificado, y

III. Inspecciones de cumplimiento.

Artículo 60. La Agencia deberá respetar en todo momento los principios de legalidad, debido proceso, confidencialidad de la información y respeto a los derechos humanos durante las labores de supervisión.

Artículo 61. Constituyen infracciones administrativas:

I. Incumplir con las obligaciones de ciberseguridad previstas en esta Ley;

II. Omitir la notificación de incidentes de ciberseguridad en los términos y plazos establecidos;

III. Obstaculizar las labores de supervisión de la Agencia, y

IV. No implementar las medidas de seguridad requeridas.

Artículo 62. Las infracciones podrán ser sancionadas con:

I. Amonestación pública o privada;

II. Multa económica proporcional al daño o riesgo generado;

III. Suspensión temporal de operaciones relativas a servicios críticos, y

IV. Inhabilitación para prestar servicios esenciales en caso de reincidencia grave.

Artículo 63. Las sanciones se impondrán atendiendo a:

I. La gravedad de la infracción;

II. El nivel de riesgo y daño generado para la infraestructura crítica, ICI o para los derechos fundamentales;

III. La reincidencia, y

IV. El grado de colaboración con las autoridades.

Artículo 64. Las resoluciones de la Agencia podrán ser impugnadas mediante los medios de defensa previstos en la legislación administrativa aplicable.

ARTÍCULOS TRANSITORIOS

PRIMERO. El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación:

SEGUNDO. La persona titular del Ejecutivo federal deberá enviar las propuestas para designar a la persona titular de la Dirección General de la Agencia Nacional de Ciberseguridad al Senado de la República en un plazo que no exceda 90 días naturales.

TERCERO. El Senado de la República deberá evaluar y aprobar según sea el caso a la persona titular de la Dirección General de la Agencia Nacional de Ciberseguridad en un plazo que no exceda 90 días naturales.

CUARTO. A partir de la designación de la persona titular de la Dirección General de la Agencia Nacional de Ciberseguridad, se contará con 90 días naturales para la elaboración

del Registro de Infraestructuras Críticas, de la Información, dicho Registro se deberá apegar a criterios claros, concisos y transparentes.

QUINTO. A partir de la designación de la persona titular de la Dirección General de la Agencia Nacional de Ciberseguridad, contará con 180, para la publicación del programa de implementación gradual de las obligaciones para los operadores clasificados, atendiendo a su nivel de criticidad y riesgo.

SEXTO. El Ejecutivo Federal, a través de la Secretaría de Hacienda y Crédito Público, garantizará la asignación de recursos suficientes para el establecimiento y operación inicial de la Agencia Nacional de Ciberseguridad.

SÉPTIMO. La Agencia, en coordinación con el Consejo Nacional de Ciberseguridad, evaluará el impacto de la Ley y propondrá, en su caso, actualizaciones legislativas cada cuatro años.

OCTAVO. Vigencia de disposiciones complementarias. Las disposiciones reglamentarias, lineamientos y protocolos derivados de esta Ley deberán emitirse en un plazo máximo de 12 meses a partir de su entrada en vigor.

NOVENO. A partir de la entrada en vigor de la presente Ley, se deberá llevar a cabo la armonización normativa correspondiente en un plazo máximo de 180 días naturales, realizando las reformas y adecuaciones necesarias en los siguientes ordenamientos:

Código Penal Federal, para reforzar los tipos penales en materia de ciberdelincuencia, garantizando el respeto al principio de legalidad y especialización.

Ley Federal de Telecomunicaciones y Radiodifusión para asegurar la inclusión de medidas de ciberseguridad en la prestación de servicios de telecomunicaciones y radiodifusión.

Ley Federal de Protección al Consumidor para proteger los derechos de las personas usuarias en el entorno digital, especialmente en materia de seguridad de servicios y productos digitales.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para reforzar medidas de seguridad, notificación de incidentes y salvaguardas de protección de datos.

Ley General de los Derechos de Niñas, Niños y Adolescentes para garantizar el uso seguro, accesible y protegido de Internet y servicios digitales para niñas, niños y adolescentes.

La Agencia Nacional de Ciberseguridad, en coordinación con las autoridades competentes, deberá emitir las propuestas de reforma correspondientes y presentarlas a las instancias legislativas pertinentes.

Dado en el Salón de Sesiones del Senado de la República a los treinta días del mes de abril de veinte veinticinco.

Senador Luis Donaldo
Colosio Riojas
Grupo Parlamentario
Movimiento Ciudadano

Senadora Jesús Lucía
Trasviña Waldenrath
Grupo Parlamentario
MORENA