INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD Y SE DEROGAN LOS ARTÍCULOS 211 BIS 1, 211 BIS 2, 211 BIS 3, 211 BIS 4, 211 BIS 5, 211 BIS 6 Y 211 BIS 7 DEL CÓDIGO PENAL FEDERAL

Sen. Ana Lilia Rivera Rivera
Presidenta de la Mesa Directiva
de la H. Cámara de Senadores
Presente.

Los suscritos Senadores **Checo Pérez Flores** y **Rafael Espino de la Peña**, pertenecientes a la LXV Legislatura del H. Senado de la República, ejerciendo la facultad consagrada en el artículo 71 fracción II de la Constitución Política de los Estados Unidos Mexicanos, así como por los artículos 8 numeral 1, fracción I, 164 numeral 1 y 169 del Reglamento del Senado de la República, sometemos a la consideración de esta H. Asamblea la siguiente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD Y SE DEROGAN LOS ARTÍCULOS 211 BIS 1, 211 BIS 2, 211 BIS 3, 211 BIS 4, 211 BIS 5, 211 BIS 6 Y 211 BIS 7 DEL CÓDIGO PENAL FEDERAL**, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

La ciberseguridad es la aplicación de un sistema de medidas organizativas, normativas, técnicas, educativas y políticas, destinado a garantizar la protección y el uso legal del ciberespacio.

De acuerdo a los expertos de Information Systems Audit and Control Association (ISACA)[1], la ciberseguridad se define como "*una capa de protección para los archivos de información"*. También, para referirse a la ciberseguridad, se utiliza el término seguridad informática o seguridad de la información electrónica.

Uno de los objetivos de la ciberseguridad es generar confianza entre clientes, proveedores y el mercado en general. En un mundo hiperconectado, donde la mayoría de nuestras actividades las hacemos a través de la red y dispositivos

[1] https://www.isaca.org/

electrónicos, garantizar la seguridad de las operaciones es una necesidad imperante.

Los empresarios y líderes mundiales consideran a los ataques cibernéticos como uno de los principales riesgos a los que se enfrentan en la actualidad y a la ciberseguridad como su mayor reto.

Ante este panorama, las empresas, además de desarrollar una fuerte cultura organizacional de seguridad cibernética, han pedido leyes que garanticen la ciberseguridad en América Latina. Al respecto, Gianncarlo Gómez, profesor del curso Gestión de la Ciberseguridad del PEE de ESAN[2], menciona:

> Los marcos legales en América Latina van a permitir fomentar la regulación y la implementación de buenas prácticas en busca de garantizar la confidencialidad y la integridad de la información, tanto de entidades públicas como privadas.

En relación con lo anterior, en el siguiente cuadro se muestra la legislación en materia de ciberseguridad en los países de América Latina y el Caribe, que registran avances importantes en esta materia.

LEGISLACIÓN EN MATERIA DE CIBERSEGURIDAD AMÉRICA LATINA Y EL CARIBE	
LEGISLACIÓN	**DISPOSICIONES**
Argentina[3] (**Ley núm. 26.388**, de Delito Informático)	Esta ley especial introduce la tipificación de nuevos delitos a distintos artículos del Código Penal de la Nación. En esta ley se incorporan sanciones para las siguientes conductas: • Posesión de pornografía infantil con la finalidad de distribuirla por Internet o a través de otros medios electrónicos.

[2] https://www.esan.edu.pe/conexion-esan/la-necesidad-de-leyes-para-la-ciberseguridad-en-america-latina
[3] https://ciberseguridad.com/normativa/latinoamerica/

	• La apropiación, violación y difusión de comunicaciones electrónicas. • Interceptar cualquier tipo de comunicaciones electrónicas. • Suspensión de las comunicaciones electrónicas. • Acceder ilícitamente a sistemas informáticos. • Acceder a bases de datos personales. • Comunicar información almacenada en bases de datos personales. • Causar daños informáticos y propagar virus. • Introducir datos falsos en un archivo de datos personales. • Cometer fraude informático. • Causar daño o sabotaje informático.
Brasil[4] (**Ley núm. 12737**, sobre Delitos cibernéticos) (**Ley N° 12.965**) Marco de Derechos Civiles de Brasil para proteger la privacidad en Internet.	Esta ley modifica el Código penal y tipifica los delitos cibernéticos. Según esta norma, las personas que violen las contraseñas u obtengan datos privados y comerciales sin el consentimiento del titular de la cuenta, serán condenadas a penas de entre tres meses y dos años de cárcel, además de abonar una multa. Los delitos que contempla esta ley son los siguientes: • Invasión de dispositivo electrónico. • Interrupción o perturbación del servicio telegráfico, telefónico, informático, telemático o de información de utilidad pública. • Falsificación de documento particular. Esta normatividad se desarrolló a través de un proceso de consulta de múltiples partes interesadas para regular el uso de Internet en Brasil mediante el

[4] https://ciberseguridad.com/normativa/latinoamerica/#Brasil

	establecimiento de principios, garantías, derechos y deberes para los usuarios de Internet.
Perú[5] (**Ley núm. 30999,** de Ciberdefensa)	Disposiciones generales de esta ley. **Objeto.** Establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley. **Finalidad.** Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional. **Ámbito de aplicación.** Se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional. **Definición.** Por ciberdefensa se entiende la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio, cuando estos afecten la Seguridad Nacional.
(**Ley núm. 300096,** de Delitos informáticos)	Esta ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. Entre otros, esta ley prevé los siguientes delitos: • Acceso ilícito a un sistema informático.

[5] https://ceeep.mil.pe/2021/11/18/politica-sectorial-de-ciberdefensa-una-necesidad-impostergable/#:~:text=En%20el%20Per%C3%BA%2C%20la%20Ley,estos%20afecten%20la%20Seguridad%20Nacional

	• Atentado a la integridad de datos informáticos. • Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. • Tráfico ilegal de datos. • Fraude informático. • Suplantación de identidad.
República Dominicana (**Ley No. 53-07**, sobre Crímenes y Delitos de Alta Tecnología)	Esta ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o morales, en los términos previstos en esta ley. Destacan las siguientes conductas punibles previstas en esta ley: • Clonación de Dispositivos de Acceso. • Uso de Datos por Acceso Ilícito. • Dispositivos Fraudulentos. • Daño o Alteración de Datos. • Sabotaje. • Atentado contra la Vida de la Persona. • Obtención Ilícita de Fondos. • Robo de Identidad. • Uso de Equipos para Invasión de Privacidad. • Difamación. • Atentado Sexual.

	• Pornografía Infantil. • Crímenes y Delitos contra la Nación.
Venezuela[6] (Ley Especial contra los Delitos Informáticos)	Esta ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías. Entre los delitos más importantes que contempla esta ley, tenemos los siguientes: • Acceso indebido a un sistema que utilice tecnologías de información. • Sabotaje o daño a sistemas. • Acceso indebido o sabotaje a sistemas protegidos. • Posesión de equipos o prestación de servicios de sabotaje. • Espionaje informático. • Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. • Violación de la privacidad de las comunicaciones. • Exhibición pornográfica de niños o adolescentes. • Apropiación de propiedad intelectual.

De las legislaciones mencionadas en materia de ciberseguridad, me permito hacer énfasis en las siguientes conductas y tipos penales:

1. **Bien jurídico tutelado:** En contra de la libertad, integridad y formación sexuales de niñas, niños y adolescentes:

[6] https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

a. Posesión de pornografía infantil con la finalidad de distribuirla por Internet o a través de otros medios electrónicos.
b. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.
c. Exhibición pornográfica de niños o adolescentes.

2. **Bien jurídico tutelado:** En contra de las comunicaciones y dispositivos electrónicos; de los sistemas y datos informáticos:
   a. Apropiación, intercepción, violación, suspensión y difusión de comunicaciones electrónicas.
   b. Invasión y clonación de dispositivos electrónicos.
   c. Atentado a la integridad y tráfico ilegal de datos informáticos.
   d. Acceso indebido o propagación de virus a sistemas informáticos o de tecnologías de la información.
   e. Introducción de datos falsos en archivos de datos personales.

3. **Bien jurídico tutelado:** En contra del Estado y sus instituciones.
   a. Crímenes y delitos contra la Nación.
   b. Interrupción o perturbación del servicio telegráfico, telefónico, informático, telemático o de información de utilidad pública.
   c. Acceso indebido, sabotaje o daño a sistemas protegidos.
   d. Espionaje informático.

4. **Bien jurídico tutelado:** En contra del patrimonio de las personas:
   a. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.
   b. Obtención Ilícita de Fondos.
   c. Fraude informático.
   d. Daño a los sistemas informáticos.

5. **Bien jurídico tutelado:** En contra de la privacidad de las personas.
   a. Violación de la privacidad de las comunicaciones.
   b. Apropiación de propiedad intelectual.
   c. Suplantación de identidad.

En el caso de México, en el 2017 se presentó la estrategia nacional de seguridad cibernética con el objetivo principal de identificar y establecer las acciones de seguridad cibernética aplicables a las áreas social, económica y política para permitirles a la población y las organizaciones públicas y privadas el uso de las

Tecnologías de la Información y la Comunicación (TIC), de manera responsable para el desarrollo sostenible del Estado Mexicano.[7]

De acuerdo con el reporte *"Ciberseguridad, Riesgos, Avances y el Camino a seguir en América Latina y el Caribe 2020"*, publicado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA)[8], con el cibercrimen como una preocupación creciente, las organizaciones mexicanas que conducen proyectos de transformación digital han observado que grupos de interés con responsabilidades en la toma de decisiones (tales como ejecutivos) han incluido personal de seguridad y privacidad en el 96% de los casos (91% a nivel mundial) y el 44% de los casos (53% a nivel mundial), respectivamente. También, por diseño, contempla la gestión proactiva de los riesgos cibernéticos y de la privacidad en su planificación y presupuesto de proyectos como una consideración clave.

Actualmente México no cuenta con una ley dedicada a la ciberseguridad, pero en el Código Penal Federal se prevén los delitos informáticos.[9] Incluso, no existe una definición de "cibercrimen" y "ciberseguridad" en la legislación mexicana, y nuestro país aún no ha adoptado normas internacionales aplicables a los delitos cibernéticos.

No obstante, el 14 de abril de 2015 se publicaron en el Diario Oficial de la Federación las siguientes normas mexicanas oficiales:

NMX-I-25021-NYCE-2015	**Tecnologías de la Información Sistemas e Ingeniería de software-requisitos de calidad y evaluación de sistemas y software (square)-elementos de medición de la calidad.**
NMX-I-27001-NYCE-2015	Tecnologías de la Información-Técnicas de Seguridad-Sistemas de gestión de seguridad de la información-requisitos (cancela a la nmx-i-27001-nyce-2009).

[7] file:///C:/Users/HP%20MORENA/Downloads/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
[8] Ídem.
[9] Título Noveno, Capítulo II, "Acceso ilícito a sistemas y equipos de informática"; artículos 211 bis 1 al 211 bis 7".

NMX-I-27002-NYCE-2015	Tecnologías de la Información-Técnicas de Seguridad-Código de buenas prácticas para el control de la seguridad de la información (cancela a la nmx-i-27002-nyce-2009).

Dichas normas oficiales especifican, entre otros, los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, así como la valoración y tratamiento de riesgos de seguridad de la información de usuarios privados y públicos, relacionados con las TIC.

Con los avances tecnológicos, se han introducido en el mundo de los derechos humanos diversas formas de vulnerarlos que obligan a la ampliación de la protección de los mismos. Esta transición de la humanidad desde la revolución industrial hasta nuestros tiempos ha generado cambios en el plano jurídico, social y político que exigen nuevas formas de protección.

Respecto de lo anterior y para entender la evolución que ha tenido la protección de los derechos humanos, vale la pena hacer una breve reseña histórica. Los derechos civiles y políticos, también llamados derechos humanos de primera generación, son aquellos que recaen sobre la libertad de los individuos; estos derechos están comprendidos en la *Declaración Universal de los Derechos Humanos* de 1948 y los Pactos Internacionales de 1966, a saber, el de los *Derechos Civiles y Políticos*, y el de los *Derechos Económicos, Sociales y Culturales*. El derecho a la dignidad de la persona, y a su autonomía y libertad frente al estado, su integridad física, las garantías procesales, son derechos que tienen como soporte la filosofía de la ilustración y las teorías del contrato social.[10]

Los derechos humanos de segunda, tercera y cuarta generación se incorporan a partir de pensamiento humanista y socialista; son de naturaleza económica y social, e inciden sobre la expresión de igualdad de los individuos. Los derechos de primera generación defendían a los ciudadanos frente al poder del estado, en cambio, actualmente se exige al estado su intervención activa para garantizar un acceso igualitario a los derechos citados, compensando las desigualdades naturales creadas por las ventajas y desventajas de clases, etnia y religión que caracterizan las diferencias sociales de los individuos. El movimiento obrero y las ideologías de corte internacionalista impulsaron definitivamente la consciencia de la necesidad de

[10] file:///C:/Users/HP%20MORENA/Downloads/CESOP-IL-72-14-DerHumaCuartaGeneracion-310817.pdf

extender a todos los ciudadanos, y de forma progresiva, el derecho de educación, al trabajo y a la salud garantizados por el Estado.[11]

Esto posibilitó nuevas condiciones para ir materializando nuevos derechos. Se reivindica el derecho a la paz y a la intervención desde un poder legítimo internacional en los conflictos armados; el derecho a crear un Tribunal Internacional que actúe en crímenes contra la humanidad; el derecho a un desarrollo sostenible; preservar el medio ambiente natural y el patrimonio cultural de la humanidad; el derecho a un mundo multicultural; el derecho a la libre circulación de las personas y no sólo de capitales y bienes, que permita condiciones de vida dignas a los trabajadores inmigrantes. Este conjunto de derechos ha ido tomando forma en las últimas décadas, y abre el camino para un gran reto añadido en el siglo XXI: las nuevas formas que cobran los derechos de primera, segunda y tercera generación en el entorno del ciberespacio, es decir, la cuarta generación de los derechos humanos.[12]

Así, los derechos humanos de cuarta generación se encuentran sustentados en la necesidad de asegurar el acceso a las TIC a todos los individuos. La tecnología surge por una necesidad y su fin es hacer más eficientes los recursos y facilitar nuestra vida cotidiana. Hablar de derechos humanos es considerar la calidad de vida y de acceso a mejores condiciones reconociendo en ellas algo mucho más que la existencia biológica. Al hablar de calidad de vida debe entenderse también a la tecnología que, como ya dijimos, es el sustento de los derechos humanos de cuarta generación.

En el ámbito internacional de los Derechos Humanos, en junio del 2012 el Consejo de Derechos Humanos de la ONU aprobó la resolución A/HRC/20/L.13 *Promoción, protección y disfrute de los derechos humanos en Internet*[13] que, en esencia, dice lo siguiente:

> *Observando* que el ejercicio de los derechos humanos, en particular del derecho a la libertad de expresión, en Internet es una cuestión que reviste cada vez más interés e importancia debido a que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones,
>
> *Tomando nota* de los informes del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, presentados al

[11] *Ídem.*
[12] *Ibidem.*
[13] https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

Consejo de Derechos Humanos en su 17º período de sesiones y a la Asamblea General en su 66º período de sesiones, relativos a la libertad de expresión en Internet,

1. *Afirma* que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;

2. *Reconoce* la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas;

3. *Exhorta* a los Estados a que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países;

4. *Alienta* a los procedimientos especiales a que tengan estas cuestiones en cuenta en sus mandatos actuales, según proceda;

5. *Decide* seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos, de conformidad con su programa de trabajo.

De esta resolución se observa, que el Consejo de Derechos Humanos de la ONU consideró, entre otras cosas, lo siguiente:

a) Que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión.

b) Reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas.

c) Exhorta a los Estados a que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países.

Por otra parte, el aumento de la conectividad a Internet hace que un número cada vez mayor de personas estén conectadas en un espacio en gran parte público y transnacional, y proporciona una plataforma dinámica y de crecimiento que permite que avance la comunicación, la colaboración y la innovación en maneras en que nunca hubiéramos podido imaginar hace muy poco tiempo.

Esto es particularmente cierto en América Latina y el Caribe, donde más de la mitad de nuestra población ya está en línea y la tasa de crecimiento de usuarios de Internet se encuentra entre las más altas del mundo.

Se está utilizando Internet para compartir ideas y cultura; para mejorar el gobierno y los servicios sociales; para colaborar en la educación, las ciencias y las artes; y para hacer negocios, todo con una mayor accesibilidad y eficiencia.

No se puede ignorar, sin embargo, que la creciente conectividad y dependencia de las plataformas y servicios basados en Internet han aumentado considerablemente la exposición al riesgo a una gran cantidad de actividades y actores relacionados con la delincuencia y seguridad.

Los incidentes y ataques cibernéticos, en particular los que se realizan con intención criminal, están aumentando en frecuencia y sofisticación. Las agencias gubernamentales y las empresas han llegado a reconocer la necesidad de tener fuertes marcos, medidas y capacidades de seguridad cibernética, así como contar imperiosamente con cooperación e intercambio de información.

En la actualidad se entiende que el delito cibernético no reconoce fronteras nacionales y que se requiere un esfuerzo multilateral y multidimensional para abordar la cantidad de amenazas informáticas.

En relación con lo anterior, en el documento titulado *Riesgo Cibernético y Ciberseguridad*, publicado por la Comisión Nacional de Seguros y Fianzas, de la Secretaría de Hacienda y Crédito Público (2019)[14], en relación con los conceptos de Riesgo Cibernético y Ciberseguridad, se menciona lo siguiente:

[14] https://www.gob.mx/cms/uploads/attachment/file/478193/181.-_Riesgo_Cibern_tico_y_Ciberseguridad_2019.pdf

Concepto de Riesgo Cibernético

De acuerdo con el Instituto Nacional de Estándares y Tecnología de los Estados Unidos de Norteamérica1 (NIST por sus siglas en inglés), se define el riesgo cibernético como el riesgo de pérdida financiera, interrupción operativa o daño, debido a la falla de las tecnologías digitales empleadas para funciones informativas y/o operativas introducidas a un sistema por medios electrónicos sin acceso autorizado, para el uso, divulgación, interrupción, modificación o destrucción de los sistemas.

El término riesgo cibernético o ciber riesgo, se encuentra íntimamente vinculado a los conceptos de ciber amenaza y ciber ataque.

De acuerdo con el Instituto Nacional de Estándares y Tecnología de los Estados Unidos de Norteamérica (NIST por sus siglas en inglés), se define el riesgo cibernético como el riesgo de pérdida financiera, interrupción operativa o daño, debido a la falla de las tecnologías digitales empleadas para funciones informativas y/o operativas introducidas a un sistema por medios electrónicos sin acceso autorizado, para el uso, divulgación, interrupción, modificación o destrucción de los sistemas.

Asimismo, el organismo refiere el término ciber amenaza como una circunstancia, evento, acción, ocurrencia o persona con el potencial de explotar vulnerabilidades basadas en la tecnología e impactar adversamente en las operaciones, activos de la organización (incluyendo la información y sistemas de información), individuos, otras organizaciones o en la sociedad.

Derivado de lo anterior, podemos decir que un ciber ataque corresponde a la materialización de una o varias ciber amenazas, de esta forma el ciber riesgo o riesgo cibernético, constituye la probabilidad de ocurrencia de un ciber ataque con la severidad o daño que dicho ciber ataque pueda ocasionar; o bien, dicho de otra forma, la pérdida potencial por la materialización de uno o varios ciber ataques.

Los ciber ataques pueden ocasionar una multiplicidad de daños, esto es, podrían generar en su caso un efecto de contagio en cadena hacia distintas entidades o eslabones de la cadena productiva.

Concepto de Ciber seguridad

Por otra parte, la Organización Internacional de Estandarización (ISO por sus siglas en inglés), en la norma ISO/IEC 270323 define la ciber seguridad como la preservación de la confidencialidad, integridad y disponibilidad de la

información en el ciber espacio, el que a su vez se define como el entorno complejo que resulta de la interacción de personas, software y servicios en internet mediante dispositivos tecnológicos y redes conectadas a él, que no existen en cualquier forma física.

Asimismo, la Iniciativa Nacional para la profesionalización y estudios en materia de Ciberseguridad (NICCS por sus siglas en inglés) del Departamento de Seguridad Nacional de los Estados Unidos de Norteamérica, define la ciber seguridad como la actividad o proceso, habilidad o capacidad, o estado por el cual los sistemas de información y comunicación, así como la información contenida en ellos, se encuentran protegidos y/o son defendidos contra daños, uso o modificación no autorizados, o su explotación.

De lo anterior, podemos deducir que la ciber seguridad se refiere al proceso de proteger la información o sistemas de información, mediante la prevención, detección y respuesta a uno o varios ciber ataques.

En el mismo documento, se señalan los principales tipos de ciber ataques de acuerdo con el glosario de términos utilizados por el NIST[15]; a saber:

1. **Malware:** Es el término simplificado para denotar "malicious code" y consiste en aquel software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema de información. Dentro de esta categoría se encuentran principalmente los siguientes tipos:

a) **Virus:** Sección oculta y auto replicante de software informático, que se propaga al infectar (es decir, al insertar una copia de sí mismo en otro programa y convertirse en parte de él). Un virus no puede correr solo; requiere que su programa huésped se ejecute para activarlo.

b) **Spyware:** Software que se instala de forma secreta o subrepticia en un sistema de información para recopilar información sobre individuos u organizaciones sin su conocimiento.

c) **Adware:** Software que reproduce, muestra o descarga automáticamente material publicitario a una computadora después de instalar el software o mientras se utiliza la aplicación. El programa malicioso está diseñado para mostrar publicidades no deseadas en la computadora de la víctima sin su permiso, los pop-ups o anuncios son incontrolables y tienden a comportarse

[15] National Institute of Standards and Technology (NIST), glosario de términos, disponible en https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary
En este documento se respetarán los nombres en inglés de los tipos de ciber ataques, debido a que la terminología utilizada es de uso común.

de forma errática, por lo general aparecen muchas veces en la pantalla y resulta tedioso cerrarlos.

d) **Trojan Horse:** Programa de computadora que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad que invoca el programa.

e) **Ransomware:** Es un virus que impide que el usuario acceda a los archivos o programas y para su eliminación se exige pagar un “rescate” a través de ciertos métodos de pago en línea. Una vez pagada la cantidad, el usuario puede reanudar el uso de su sistema.

2. **Phishing:** Una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta en un correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por un negocio legítimo o una persona con reputación.

3. **Man-in-the-middle attack (MitM):** Un ataque MitM es cuando un atacante altera la comunicación entre dos usuarios, haciéndose pasar por ambas víctimas para manipularlos y obtener acceso a sus datos. Los usuarios no son conscientes de que realmente se están comunicando con un atacante y no entre ellos.

4. **Distributed denial-of-service attack (DDoS):** Un ataque de denegación de servicio inunda sistemas, servidores o redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede cumplir con solicitudes legítimas. Los atacantes también pueden usar múltiples dispositivos comprometidos para lanzar este ataque. Esto se conoce como un ataque de denegación de servicio distribuido.

5. **SQL injection:** Ocurre cuando un atacante inserta código malicioso en un servidor que utiliza SQL (Structured Query Language). Sólo tienen éxito cuando existe una vulnerabilidad de seguridad en el software de una aplicación. Los ataques de SQL exitosos obligan a un servidor a proporcionar acceso o modificar datos.

6. **Zero-day attack:** Un ataque que explota una vulnerabilidad de hardware, o software desconocida anteriormente. El uso de software obsoleto (no parcheado), abre oportunidades para que los piratas informáticos criminales aprovechen las vulnerabilidades. Una vulnerabilidad de día cero puede ocurrir cuando una vulnerabilidad se hace pública antes de que el desarrollador haya implementado un parche o una solución.

Para los fines que persigue esta iniciativa, es muy importante conocer los conceptos de ciberseguridad, ciberamenaza y ciberataque, así como identificar los diferentes tipos que existen de ciberataques en todo el mundo; a partir de ello, estar al tanto de la problemática en Latinoamérica, particularmente en México, en materia de ataques cibernéticos y ciber delincuencia.

De acuerdo con un estudio elaborado en 2018 por el Centro de Estudios Estratégicos e Internacionales (CSIS por sus siglas en inglés)[16], en asociación con McAfee, después de Brasil, México es el país que presenta el mayor número de ataques cibernéticos en América Latina. Asimismo, se estima que los delitos cibernéticos costaron al país alrededor de 3 billones de dólares.

En relación con lo anterior, la Asociación Mexicana de Ciberseguridad (AMECI), sostiene: *"el riesgo de ciberataques suscita preocupación en varios ámbitos, entre ellos: pérdida de datos, costos, daños a la organización y la reputación ante la visión de sus clientes y socios"*[17]. Por lo que esos hackeos muestran las vulnerabilidades de diferentes sistemas de almacenamientos de datos, al tiempo de generar diferentes tipos de ilícitos, en perjuicio de personas, dependencias públicas, empresas, universidades, asociaciones, entre otras organizaciones.

De acuerdo con el *Índice de Ciberseguridad Global* (ICG), publicado por la Unión Internacional de Telecomunicaciones (UIT)[18], los países mejor posicionados frente a los desafíos de la ciberseguridad son: Estados Unidos de América (100); Reino Unido (99.54); Arabia Saudita (99.54); Estonia (99.48); Corea del Sur (98.52); Singapur (98.52); y España (98.52) son los mejores posicionados. En contraste, los países peor calificados para el tema de ciberseguridad a escala mundial son: Guinea Ecuatorial (1.46); Corea del Norte (1.35); Micronesia (0); el Vaticano (0); y Yemen (0). A escala continental, los países mejor posicionados en materia de seguridad de acuerdo con el índice de la UIT son: Estados Unidos (100); Canadá (97.67); Brasil (96.6); **México (81.68)**; Uruguay (75.15); y República Dominicana (75.07). Esta medición es útil para encontrar áreas de oportunidad y mejora para el tema de seguridad cibernética, y evitar riesgos para la población, la administración pública, y las empresas.

[16] https://www.csis.org/

[17] https://www.ameci.org/

[18] https://www.itmastersmag.com/noticias-analisis/mexico-sube-11-lugares-en-el-indice-global-de-ciberseguridad-es-cuarto-en-america/#:~:text=Noticias%20%26%20An%C3%A1lisis-,M%C3%A9xico%20sube%2011%20lugares%20en%20el%20%C3%8Dndice,Ciberseguridad%3A%20Es%20cuarto%20en%20Am%C3%A9rica&text=M%C3%A9xico%20alcanz%C3%B3%20la%20posici%C3%B3n%2052,y%20comunicaci%C3%B3n%20de%20Naciones%20Unidas.

No obstante, los ciberataques en diferentes partes del mundo aumentaron en frecuencia en los últimos meses, al coincidir con un mayor uso de ordenadores debido a los estragos por la pandemia de Covid-19. Al respecto, la compañía Kaspersky dio a conocer que, de enero a agosto de 2020 se incrementó en 24% el número de este tipo de incidentes en América Latina. Con ello, se realizan docenas de ataques por segundo en todo el continente, al referir que "Brasil lidera la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto); Perú (96 por minuto), Ecuador (89 por minuto) y Colombia (87 por minuto)". Lo cual es una muestra de la magnitud del riesgo actual por esta amenaza en esta región.[19]

Respecto a la situación de la Ciberseguridad en México, el Banco Interamericano de Desarrollo (BID) refiere que:

> México no cuenta con una ley dedicada de delito cibernético, pero el artículo N° 211 del Código Penal prevé el delito informático. Sin embargo, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen (BID, 2020: 125).[20]

Entre los impactos ocasionados por la falta de leyes armoniosas con el tema de ciberseguridad en México, Héctor Cueto puntualiza: "*79% de los ataques de ciberseguridad que sucedieron el año pasado fueron a Pymes; hubo más de 4,000 millones de intentos por atacarlas"*[21]. Es decir, la falta de precauciones adecuadas en el rubro de ciberseguridad daña el desarrollo económico y la cadena productiva de gran parte de las empresas mexicanas.

De acuerdo con American Chamber México[22], los problemas más comunes que enfrentan los usuarios de internet en nuestro país, son:

Problemática	***Número de personas que sufren este problema***	***Porcentaje del universo total de usuarios de internet den México***
Exceso de información no deseada	***20.5 millones***	***25.5%***

[19] Véase: Aguirre Quezada, Juan Pablo "Ciberseguridad, desafío para México y trabajo legislativo", *Cuaderno de Investigación* N° 87, Instituto Belisario Domínguez, Senado de la República, Ciudad de México, 2022.
[20] Ídem.
[21] https://businessinsider.mx/importancia-marco-regulatorio-ciberseguridad-mexico/
[22]https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%CC%81xico%20(1).pdf

Mensajes de personas desconocidas	***16.4 millones***	***20.3%***
Infección por virus	***10.6 millones***	***13.1%***
Fraudes con información financiera personal	***3.2 millones***	***4.0%***
Violación a la privacidad	***2.5 millones***	***3.1%***

De acuerdo con el Estudio de hábitos de los usuarios en ciberseguridad en México 2019, elaborado por la Secretaría de Comunicaciones y Transportes (SCT)[23], el 34% de los participantes ha sufrido algún tipo de acoso, de los cuales dos terceras partes son menores de edad; el 27% de los participantes han sufrido robo de identidad en medios digitales, de los cuales sólo una tercera parte son adultos; asimismo, el 21% de los adultos encuestados ha sufrido fraudes financieros por medios digitales.

Este estudio confirma la alta vulnerabilidad de la población mexicana a sufrir algún tipo de ataque cibernético, particularmente de las niñas, niños y adolescentes. Incluso, de las encuestas se infiere que existe un exceso de confianza por parte de los usuarios al conectarse a cualquier red pública, sin considerar que a través de dicha red su información podría ser robada, ingresar sin autorización al equipo móvil o realizar alguna actividad ilícita.

Para dimensionar las actividades de los usuarios de internet y de teléfonos celulares en México, en la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020, publicada por el INEGI y la Secretaría de Infraestructura, Comunicaciones y Transportes (SCT)[24], se menciona que en nuestro país existen 84.1 millones de usuarios de internet (72.0% de la población de seis años o más), y 88.2 millones de usuarios de teléfonos celulares (75.5% de la población de seis años o más).

Nueve de cada diez usuarios de teléfono celular disponen de un celular inteligente (Smartphone). Entre 2019 y 2020 los usuarios que sólo dispusieron de celular inteligente registraron un crecimiento de 3.5 puntos porcentuales (88.1% a 91.6%). La encuesta estima que, en 2020, de los usuarios que se conectan a internet

[23] https://ciberseguridad.ift.org.mx/files/guias_y_estudios/estudio_habitos_en_ciberseguridad.pdf
[24] https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

mediante su celular, inteligente (Smartphone), se observa un aumento de quienes se conectan sólo por Wi Fi, que pasaron de 9.4% en 2019 a 13.7% en 2020.

En el caso de los usuarios de computadoras, la ENDUTIH reflejó que en el 2020 se estimaron 44.4 millones de usuarios de estos equipos, lo que representa un 38.0% del total de la población de seis años o más. Las principales actividades de los usuarios de computadora en el hogar son: labores escolares (54.9%) -casi diez puntos porcentuales más que en 2019-; actividades laborales (42.8%) y como medio de capacitación (30.6%).

Entre las principales actividades que realizan los usuarios de internet en 2020 están para comunicarse (93.8%), buscar información (91.0%) y acceder a redes sociales (89.0%). Cabe resaltar que la compra de productos o servicios presenta un crecimiento significativo de 5.6 puntos porcentuales en 2020 (27.7%) comparando con 2019 (22.1%).

Por otro lado, las actividades que menos realizan los usuarios de internet, pero que presentan un cambio considerable en comparación a 2019 son: ventas en internet con un crecimiento de 2 puntos porcentuales (11.3% en 2020), utilizar servicios en la nube con un crecimiento de 2 puntos porcentuales (19.4% en 2019 y 21.4% en 2020) y operaciones bancarias en línea con un crecimiento de 4.9 puntos porcentuales (16.8% en 2019 y 21.7% en 2020).

La finalidad de la presente iniciativa es regular las acciones que protejan el patrimonio y las funciones de las instituciones del Estado Mexicano de cualquier ataque cibernético, así como tipificar conductas que tutelen el patrimonio de los usuarios de los sistemas informáticos, electrónicos y telemáticos, así como la libertad, integridad y formación sexuales de niñas, niños y adolescentes, entre otros bienes jurídicos, a través de una ley, cuyo objeto sea:

A. Regular la integración, organización y funcionamiento de la instancia encargada de las actividades de ciberseguridad a nivel nacional, estableciendo las bases de coordinación y colaboración entre los tres órdenes de gobierno.
B. Implementar y revisar la Estrategia Nacional de Ciberseguridad, definiendo los requisitos fundamentales y los objetivos principales para garantizar la seguridad cibernética.
C. Salvaguardar el uso seguro y responsable de las redes, los sistemas de información y comunicaciones, a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, y contribuir a la promoción de un ciberespacio seguro.

D. Contribuir a la prevención especial y general de los delitos federales y locales cometidos en el ciberespacio, así como a la investigación y la persecución de dichos delitos por parte de instituciones especializadas en la materia, en los términos de esta Ley y de la legislación aplicable.

E. Prever un catálogo amplio de ciberdelitos del orden federal, agrupándolos por el bien jurídico tutelado, a saber: la confidencialidad, integridad y seguridad de tecnologías de la información y comunicación; las instituciones del Estado; la provisión de bienes y prestación de servicios públicos esenciales para el país; la seguridad nacional; el patrimonio, libertad y privacidad de las personas; la libertad, integridad y formación sexuales de niñas, niños y adolescentes, entre los más importantes.

Se propone la creación de la Comisión Nacional de Ciberseguridad, como instancia para la consecución del objeto de esta ley en el territorio nacional, destacando las siguientes facultades:

a) Formular políticas públicas, programas y estrategias en materia de ciberseguridad;
b) Proponer, ejecutar y evaluar la Estrategia Nacional, que deberá alinearse al Sistema Nacional de Planeación Democrática, previsto en la Ley de la materia;
c) Formular propuestas para los programas nacionales de ciberseguridad;
d) Promover políticas de coordinación con la Fiscalía General de la República y las fiscalías generales de las entidades federativas;
e) Promover políticas de coordinación con el Poder Judicial de la Federación y los poderes judiciales de las entidades federativas;
f) Promover políticas de coordinación con las instancias de seguridad pública locales, municipales y de las demarcaciones territoriales de la Ciudad de México;
g) Impulsar programas de capacitación en materia de ciberseguridad con instituciones educativas, centros de investigación y entidades públicas y privadas;
h) Aprobar los lineamientos de ciberseguridad y administración de riesgos, así como los programas de prevención de los delitos en contra de las infraestructuras críticas de la información.

Por otra parte, se propone la derogación de aquellos artículos del Código Penal Federal, en los que se regulan actualmente algunos delitos cuyo bien jurídico tutelado es el acceso ilegal a los sistemas y equipos de informática, no obstante, dichos delitos no abarcan la totalidad de las conductas que hoy en día utilizan las tecnologías de la información y comunicación en perjuicio de las instituciones del

Estado; de la provisión de bienes y prestación de servicios públicos esenciales para el país; de la seguridad nacional; del patrimonio, libertad y privacidad de las personas, así como de la libertad, integridad y formación sexuales de niñas, niños y adolescentes, entre los bienes jurídicos más importantes que deben protegerse cuando se utilizan sistemas informáticos con fines ilícitos. Delitos que se propone establecer de manera especial en la Ley propuesta.

Para mejor ilustración, enseguida se muestra un cuadro en el que se observan los artículos del Código Penal que se propone derogar:

CÓDIGO PENAL FEDERAL TEXTO VIGENTE	**CÓDIGO PENAL FEDERAL TEXTO PROPUESTO**
Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.	**Artículo 211 bis 1.- DEROGADO**
Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o	**Artículo 211 bis 2.- DEROGADO**

equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.	
Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.	**Artículo 211 bis 3.- DEROGADO**

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.	
Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún	**Artículo 211 bis 4.- DEROGADO**

mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa	
Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero	**Artículo 211 bis 5.- DEROGADO**
Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.	**Artículo 211 bis 6.- DEROGADO**
Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información	**Artículo 211 bis 7.- DEROGADO**

obtenida se utilice en provecho propio o ajeno.	

Por lo anteriormente expuesto, se presenta ante esta soberanía la iniciativa con proyecto de Decreto por el que se expide la Ley Federal de Ciberseguridad y se derogan diversos artículos del Código Penal Federal, para quedar como sigue:

PROYECTO DE DECRETO

Artículo Primero. - Se expide la Ley Federal de Ciberseguridad.

LEY FEDERAL DE CIBERSEGURIDAD

LIBRO PRIMERO

TÍTULO PRIMERO
Disposiciones Generales

Artículo 1. Las disposiciones de esta Ley son de orden público y de aplicación en todo el territorio nacional.

Artículo 2. Esta Ley tiene por objeto:

I. Regular la integración, organización y funcionamiento de la instancia encargada de las actividades de ciberseguridad a nivel nacional;

II. Establecer las bases de coordinación y colaboración entre la Federación, las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México en esta materia;

III. Implementar y revisar periódicamente la Estrategia Nacional de Ciberseguridad, definiendo los requisitos fundamentales y los objetivos principales para garantizar la seguridad cibernética;

IV. Salvaguardar el uso seguro y responsable de las redes, los sistemas de información y comunicaciones, a través del fortalecimiento de las

capacidades de prevención, detección y respuesta a los ciberataques, adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro;

V. Establecer el catálogo de delitos cibernéticos de competencia federal y contribuir a la prevención especial y general de dichos delitos; y

VI. Contribuir a la investigación y la persecución de los delitos cibernéticos por parte de instituciones especializadas en la materia, en los términos de esta Ley y de la legislación aplicable.

Artículo 3. Corresponde al Gobierno Federal, por conducto de la Secretaría de Seguridad y Protección Ciudadana, de las entidades federativas, de los municipios y de las demarcaciones territoriales de la Ciudad de México, el control y la regulación de los actos derivados de esta Ley, de su Reglamento y de la normatividad secundaria en la materia, en el ámbito de su competencia.

El Reglamento definirá, entre otros aspectos, las competencias de la Comisión Nacional de Ciberseguridad, los procesos de coordinación, los protocolos de actuación, y los criterios para la implementación de medidas de ciberseguridad.

Además, la normatividad secundaria en la materia determinará aspectos adicionales, como los estándares técnicos, los mecanismos y los procedimientos sancionatorios, así como los demás aspectos necesarios para la implementación de esta Ley.

Artículo 4. Para los efectos de esta Ley, se entenderá por:

I. **Archivo Informático:** Conjunto organizado de unidades de información (bytes) almacenados en un dispositivo electrónico.

II. **Área de Inteligencia:** Área de inteligencia en materia de ciberseguridad dependiente de la Comisión Nacional de Ciberseguridad.

III. **Base de Datos:** Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

IV. **Ciberamenaza:** Es la posibilidad de comisión de daños a personas u organismos mediante el uso de Internet.

V. **Ciberataque:** Conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas.

VI. **Ciberdefensa:** Conjunto de acciones de tipo activo, pasivo, proactivo, preventivo y reactivo que se aplican para asegurar el uso propio del

ciberespacio nacional, en virtud de los incidentes cibernéticos que provengan o sean promovidos por otros Estados sujetos de derecho internacional.

VII. **Ciberdelincuencia:** Actividades delictivas que tienen como objetivo principal un ordenador, una red asociada a éste o cualquier dispositivo electrónico.

VIII. **Ciberespacio:** Es el espacio virtual constituido por redes informáticas y de telecomunicaciones, en donde interactúan las personas, el *software* y los servicios de Internet.

IX. **Ciberseguridad:** Aplicación de un sistema de medidas organizativas, normativas, técnicas, educativas y políticas, destinado a garantizar la protección y el uso legal del ciberespacio.

X. **Comisión:** Comisión Nacional de Ciberseguridad.

XI. **Datos Informáticos:** Representación simbólica, numérica o alfabética, cuyo valor está listo para ser procesado por un ordenador y mostrarlo a un usuario en modo de información.

XII. **Datos Personales:** Toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables.

XIII. **Delito cibernético o ciberdelito:** Todo aquel acto que, estando tipificado como delito, se desarrolla en internet o requiere del uso de medios informáticos para ser realizado.

XIV. **Estrategia Nacional:** Estrategia Nacional de Ciberseguridad, que es el documento que establece la misión, visión y objetivos del Estado Mexicano en materia de ciberseguridad.

XV. **Información:** Conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado.

XVI. **Infraestructuras críticas de la información:** Son las infraestructuras de información consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la seguridad nacional.

XVII. **Internet:** Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios.

XVIII. **Ley:** Ley Federal de Ciberseguridad.

XIX. **Medidas de prevención:** Son estrategias y controles diseñados para evitar que ocurran incidentes cibernéticos. Esto incluye la implementación de políticas de seguridad, la segmentación de redes, la autenticación y la educación en materia de ciberseguridad para minimizar vulnerabilidades.

XX. **Medidas de detección:** Se refieren a las acciones para identificar y alertar sobre actividades anómalas o posibles amenazas cibernéticas, tales como la monitorización constante de la red,
sistemas de detección de intrusiones y análisis de riesgos en materia de seguridad cibernética.

XXI. **Medidas de recuperación:** Son medidas que se centran en restaurar la operatividad y la integridad de sistemas y datos, después de que ha ocurrido un incidente cibernético, tales como la restauración de copias de seguridad, análisis forense, implementación de cambios para evitar futuros ataques, entre otras.

XXII. **Operadores:** Operadores de las Redes Públicas de Telecomunicaciones a que se refiere el Título Quinto, Capítulo I, de la Ley Federal de Telecomunicaciones y Radiodifusión.

XXIII. **Ordenador:** Es una máquina electrónica que recibe y procesa datos con la misión de transformarlos en información útil.

XXIV. **Programa informático:** Conjunto de aplicaciones y recursos que permiten desarrollar diferentes tareas en un ordenador, un teléfono u otros equipos tecnológicos.

XXV. **Red social:** Estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. A través de ellas, se crean relaciones entre individuos o empresas de forma rápida, sin jerarquía o límites físicos.

XXVI. **Reglamento:** Reglamento de la Ley Federal de Seguridad.

XXVII. **RICI:** Registro de Infraestructuras Críticas de la Información.

XXVIII. **RNDC:** Registro Nacional de Delitos Cibernéticos.

XXIX. **Secretaría:** Secretaría de Seguridad y Protección Ciudadana.

XXX. **Seguridad informática:** Conjunto de medidas que impiden la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software.

XXXI. **Sistema informático:** Conjunto de técnicas que nos permiten guardar y garantizar la seguridad de información mediante sistemas informatizados.

XXXII. **Sistema de telecomunicaciones:** Infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones.

XXXIII. **Tecnologías de la Información y Comunicación (TIC):** Son tecnologías que utilizan la informática, la microelectrónica y las telecomunicaciones para crear nuevas formas de comunicación a través de herramientas de carácter tecnológico y comunicacional, esto con el fin de facilitar la emisión, acceso y tratamiento de la información.

XXXIV. **Vulnerabilidad informática:** Debilidad que puede ser explotada por un ataque cibernético para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático.

TÍTULO SEGUNDO

Capítulo Único
Coordinación y colaboración entre la Federación, las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México

Artículo 5. La Federación, las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México, se coordinarán y colaborarán 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 de las autoridades competentes:

I. Coordinar las acciones en materia de Ciberseguridad con las áreas especializadas de las instituciones de Seguridad Pública en las entidades federativas y los municipios;
II. Ejecutar las estrategias y mecanismos para la ciberdefensa del país;
III. Colaborar con las autoridades extranjeras en materia de ciberdefensa y operaciones militares conjuntas en el ciberespacio mexicano;
IV. Integrar y operar la Comisión Nacional de Ciberseguridad;
V. Efectuar las acciones de protección y vigilancia de las Infraestructuras críticas de la información del país, en los términos de la Ley y su Reglamento;
VI. Ejecutar la Estrategia Nacional de Ciberseguridad;
VII. Desempeñar las políticas de coordinación y colaboración elaboradas por la Comisión en materia de ciberseguridad con la Federación, las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México;
VIII. Realizar acciones y políticas en materia de prevención, investigación y persecución de delitos cibernéticos del fuero federal;
IX. Participar en los programas de capacitación en materia de ciberseguridad que impulse la Comisión;
X. Administrar y coordinar el RNDC; y
XI. Las demás que establezcan esta Ley, su Reglamento y otras disposiciones legales.

En las acciones de protección y vigilancia de las Infraestructuras críticas de la información del país a que se refiere la fracción V de este apartado, se solicitará la colaboración de las autoridades estatales y municipales, así como de los órganos constitucionalmente autónomos, cuando así se requiera.

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 la Comisión en materia de ciberseguridad;
II. Participar en el ámbito de su competencia, en las políticas y programas de la Estrategia Nacional;
III. Colaborar con la Federación reportando mensualmente al RNDC el informe homologado de carpetas de investigación y procesos penales, relacionados con los delitos cibernéticos del fuero común;
IV. Participar en la Comisión Nacional de Ciberseguridad, por conducto de un representante de los gobernadores de las entidades federativas, que será designado en términos del Reglamento;
V. Participar en los programas de capacitación en materia de ciberseguridad que impulse la Comisión;
VI. Implementar acciones y políticas en materia de prevención, investigación y persecución de delitos cibernéticos del fuero común;
VII. Colaborar con la Federación en la investigación de los delitos cibernéticos del fuero federal; y
VIII. Las demás que establezcan esta Ley, su Reglamento y otras disposiciones legales.

Se sugiere a las entidades federativas implementar el modelo homologado de Policía Cibernética que defina la Federación a través de la Secretaría, en el marco de la Ley General del Sistema Nacional de Seguridad Pública.

C. Corresponde a los municipios y a las demarcaciones territoriales 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 la Comisión en materia de ciberseguridad;
II. Contribuir en el ámbito de su competencia, en las políticas y programas de la Estrategia Nacional;

III. Participar en la Comisión Nacional de Ciberseguridad, por conducto de un representante de los municipios y de las demarcaciones territoriales de la Ciudad de México, que será designado en términos del Reglamento;

IV. Implementar campañas y acciones de prevención de delitos cibernéticos del fuero común, en el ámbito de la entidad federativa a la que pertenezcan; y

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

TÍTULO TERCERO
Instancia Nacional de Ciberseguridad

Capítulo I
De la Comisión Nacional de Ciberseguridad

Artículo 6. La Comisión Nacional de Ciberseguridad estará integrada por:

I. La persona titular de la Secretaría de Seguridad y Protección Ciudadana, quien la presidirá;

II. Un Secretario Técnico, quien será designado por la persona titular de la Secretaría de Seguridad y Protección Ciudadana;

III. La persona titular de la Secretaría de la Defensa Nacional;

IV. La persona titular de la Secretaría de Marina;

V. La persona titular de la Fiscalía General de la República;

VI. La persona titular de la Secretaría de Relaciones Exteriores;

VII. La persona titular de la Secretaría de Infraestructura, Comunicaciones y Transportes; y

VIII. La persona titular de la Secretaría de Hacienda y Crédito Público.

En la Comisión podrán participar una persona representante de los gobernadores de las entidades federativas y una persona representante de los municipios y de las demarcaciones territoriales de la Ciudad de México.

Las personas titulares de las Secretarías de Estado podrán designar a un servidor público para que los represente en las sesiones de la Comisión, el cual deberá tener la categoría, cuando menos, de Director General.

A las sesiones de la Comisión se podrá invitar, con carácter honorífico y de acuerdo a la naturaleza de los asuntos a tratar, a las personas físicas o morales, instituciones educativas y representantes de la sociedad civil que tengan experiencia y conocimientos en materia de ciberseguridad.

La Comisión será parte integrante tanto del Consejo de Seguridad Nacional como del Consejo Nacional de Seguridad Pública, en los términos que establezca la legislación en la materia.

Artículo 7. La Comisión tendrá las siguientes atribuciones:

I. Formular políticas públicas, programas y estrategias en materia de ciberseguridad;

II. Emitir acuerdos y resoluciones generales para el funcionamiento de la Comisión;

III. Proponer la Estrategia Nacional, la cual deberá alinearse al Sistema Nacional de Planeación Democrática;

IV. Elaborar criterios uniformes de homologación para la organización, operación y modernización tecnológica de las instituciones especializadas en materia de ciberseguridad;

V. Formular propuestas para los programas nacionales de ciberseguridad en los términos de la normatividad en la materia;

VI. Establecer medidas para vincular a la Comisión con otros organismos internacionales, nacionales, regionales o locales en materia de ciberseguridad;

VII. Elaborar estrategias y mecanismos para la ciberdefensa del país, así como esquemas de colaboración internacional en materia de ciberdefensa;

VIII. Promover políticas de coordinación con la Fiscalía General de la República y las fiscalías generales de las entidades federativas, con la finalidad de recabar información estadística sobre las investigaciones relacionadas con los delitos cibernéticos;

IX. Promover políticas de coordinación con el Poder Judicial de la Federación y los poderes judiciales de las entidades federativas, con la finalidad de recabar información estadística sobre los procesos penales relacionadas con los delitos cibernéticos;

X. Promover políticas de coordinación en las que participen la Secretaría y las instancias de seguridad pública en las entidades federativas y los municipios, con la finalidad de llevar a cabo acciones de prevención de los delitos cibernéticos;

XI. Fomentar la armonización legislativa nacional de ciberseguridad, tomando en cuenta los instrumentos internacionales en la materia;

XII. Impulsar programas de capacitación en materia de ciberseguridad con instituciones educativas, centros de investigación y entidades públicas y privadas, tanto nacionales como internacionales;

XIII. Aprobar los lineamientos de ciberseguridad y administración de riesgos, así como los programas de prevención de los delitos en contra de las infraestructuras críticas de la información; y

XIV. Las demás que establezcan esta Ley, su Reglamento y otras disposiciones normativas para el buen funcionamiento de la Comisión.

En la elaboración de la Estrategia Nacional de Ciberseguridad a que se refiere la fracción III de este artículo, la Comisión tomará en cuenta las opiniones de la iniciativa privada, de expertos en la materia y de la sociedad en general, conforme a la convocatoria que se emita para tal efecto.

Artículo 8. La Comisión funcionará en Pleno y estará compuesta por las siguientes comisiones y grupos de trabajo, encargados de abordar aspectos específicos de la ciberseguridad:

I. **Comisión de políticas y estrategias en ciberseguridad:** Será responsable de la elaboración y revisión de políticas y estrategias nacionales en ciberseguridad, identificando amenazas, tendencias y medidas preventivas y correctivas.

II. **Comisión de normatividad en ciberseguridad:** Se encargará de la creación y revisión de la normatividad relacionada con la ciberseguridad, asegurando su adecuación a estándares nacionales e internacionales.

III. **Comisión de incidentes y respuesta en ciberseguridad:** Supervisará y coordinará las respuestas a incidentes de ciberseguridad, estableciendo protocolos de actuación y colaboración con entidades relacionadas.

IV. **Comisión de capacitación y concienciación en ciberseguridad:** Promoverá la capacitación, concienciación y educación en ciberseguridad, tanto a nivel público como privado.

V. **Grupo de trabajo en protección de infraestructuras críticas de la información:** Se enfocará en identificar, proteger y garantizar la resiliencia de las infraestructuras críticas de la información, evaluando sus vulnerabilidades y riesgos.

VI. **Grupo de trabajo en seguridad de la información y gestión de riesgos:** Se concentrará en la gestión de riesgos y seguridad de la

información en todas las entidades sujetas a la Ley Federal de Ciberseguridad.

VII. **Grupo de trabajo en cooperación internacional en ciberseguridad:** Facilitará la colaboración y cooperación con organismos e instituciones internacionales en temas de ciberseguridad.

Artículo 9. Corresponde a la Secretaría de la Defensa Nacional y a la Secretaría de Marina desarrollar y ejecutar estrategias y mecanismos para la ciberdefensa del país, así como la colaboración internacional en materia de ciberdefensa y operaciones militares conjuntas en el ciberespacio mexicano.

Artículo 10. La Comisión contará con un Área de Inteligencia en materia de Ciberseguridad que se coordinará con el Secretariado Ejecutivo del Sistema Nacional de Seguridad, en términos de la Ley General del Sistema Nacional de Seguridad Pública y la normatividad reglamentaria aplicable.

El Área de Inteligencia en materia de Ciberseguridad tendrá el propósito de recopilar, analizar y proporcionar información estratégica y táctica relacionada con la ciberseguridad, con el fin de fortalecer la capacidad de prevención, detección, respuesta y recuperación ante incidentes cibernéticos. Sus atribuciones serán las siguientes:

I. Recopilar información de fuentes abiertas y cerradas relacionada con amenazas, vulnerabilidades y eventos cibernéticos de interés;

II. Analizar las amenazas cibernéticas, identificando tendencias, actores y métodos utilizados en el ciberespacio;

III. Supervisar las infraestructuras críticas de la información para identificar posibles vulnerabilidades y riesgos;

IV. Colaborar con entidades gubernamentales, instituciones privadas y organismos internacionales para compartir información relevante y coordinar acciones;

V. Generar informes de inteligencia cibernética que contengan evaluaciones de riesgos, indicadores de compromiso y recomendaciones para la protección de activos digitales;

VI. Emitir alertas y advertencias en tiempo real sobre amenazas cibernéticas inminentes que puedan afectar la seguridad nacional o la infraestructura crítica;

VII. Mantener un seguimiento constante de incidentes cibernéticos en curso, proporcionando apoyo a las entidades responsables de la respuesta;

VIII. Evaluar los riesgos relacionados con la ciberseguridad y colaborar en la elaboración de estrategias de mitigación;

IX. Participar en iniciativas de capacitación y concienciación sobre ciberseguridad, compartiendo conocimientos y mejores prácticas; y,

X. Garantizar la protección y clasificación adecuada de la información sensible relacionada con la ciberseguridad.

Artículo 11. El Área de Inteligencia tendrá bajo su responsabilidad el RICI, en los términos que determine esta Ley, su Reglamento y la normatividad aplicable.

Capítulo II

Principios rectores de la Comisión Nacional de Ciberseguridad

Artículo 12. La Comisión, en el ejercicio de sus funciones y en su relación con las instancias coadyuvantes, se regirá por los principios de cooperación y coordinación, confidencialidad, integralidad y veracidad, respeto a los derechos humanos, proporcionalidad y legalidad, rendición de cuentas y seguridad de la información.

Artículo 13. La Comisión promoverá la cooperación y la coordinación activa entre las instancias coadyuvantes, con el fin de garantizar una respuesta efectiva ante incidentes y amenazas cibernéticas y fomentará la comunicación constante y la colaboración en la gestión de la ciberseguridad nacional.

Artículo 14. La Comisión y las instancias coadyuvantes preservarán la confidencialidad de la información intercambiada en el marco de la ciberseguridad, respetando las disposiciones aplicables en materia de protección de datos y privacidad. Sólo se compartirá la información necesaria y pertinente para el cumplimiento de sus responsabilidades a otras autoridades.

Artículo 15. La Comisión promoverá la integridad y veracidad de la información compartida entre las instancias coadyuvantes, asegurando que sea precisa y completa. La información proporcionada será verificada para evitar la diseminación de datos erróneos o desinformación.

Artículo 16. La Comisión y las instancias coadyuvantes respetarán en todo momento los derechos humanos de las personas, incluyendo el derecho a la privacidad y la no discriminación, al recopilar, procesar o compartir información en el ámbito de la ciberseguridad.

Artículo 17. La recopilación y el uso de información por parte de la Comisión y las instancias coadyuvantes se ajustarán a los principios de legalidad y proporcionalidad. La obtención y el tratamiento de datos personales se realizarán de acuerdo con la normativa aplicable.

Artículo 18. La Comisión mantendrá mecanismos de rendición de cuentas efectivos y transparentes en relación con el uso de la información compartida entre las instancias coadyuvantes. Se promoverá la revisión y evaluación periódica de las acciones emprendidas en el ámbito de la ciberseguridad.

Artículo 19. La Comisión y las instancias coadyuvantes adoptarán medidas de seguridad apropiadas para proteger la información intercambiada y prevenir accesos no autorizados, pérdidas, alteraciones o divulgaciones no autorizadas.

Capítulo III

Reglas generales para el intercambio de información estratégica

Artículo 20. La Comisión establecerá los procedimientos de actuación necesarios para el intercambio de información estratégica entre las instancias sujetas a sus lineamientos, con el objetivo de fortalecer la ciberseguridad nacional.

Artículo 21. La Comisión definirá los tipos de información que se considerarán estratégicos para la ciberseguridad nacional. Esta información comprenderá datos críticos, amenazas cibernéticas significativas y otros elementos relevantes para la protección de infraestructura y activos críticos.

Artículo 22. Las instancias sujetas a los lineamientos de la Comisión deberán designar personas responsables de la gestión y compartición de información estratégica. Estas serán las encargadas de identificar, recopilar, procesar y transmitir la información en cumplimiento de sus funciones.

Artículo 23. La Comisión establecerá procedimientos claros y seguros para la transmisión de información estratégica entre las instancias coadyuvantes. Estos procedimientos incluirán aspectos como formatos, canales de comunicación, cifrado y autenticación de datos.

Artículo 24. Los plazos y términos de respuesta para el intercambio de información estratégica se definirán considerando la naturaleza y la gravedad de la amenaza o el incidente cibernético, priorizando la agilidad en la comunicación para una respuesta efectiva.

Artículo 25. Los procedimientos garantizarán la protección de los datos personales y la privacidad de las personas, de conformidad con la legislación en la materia. La información compartida será la exclusivamente necesaria para la gestión de la ciberseguridad.

Artículo 26. La Comisión establecerá mecanismos de acceso restringido a la información estratégica, limitando su divulgación únicamente a personas autorizadas y con interés jurídico en el asunto de que se trate.

Artículo 27. La Comisión llevará a cabo una evaluación continua de los procedimientos de actuación para garantizar su eficacia y adecuación a la evolución de las amenazas cibernéticas.

Artículo 28. La Comisión establecerá protocolos de respuesta a incidentes cibernéticos que contemplen la participación de las instancias coadyuvantes. Estos protocolos definirán roles y responsabilidades, plazos de actuación y la forma de compartir información durante la gestión de incidentes cibernéticos.

Artículo 29. La Comisión, en aras de permitir una gestión más eficiente y segura de la información compartida, establecerá categorías de clasificación de la información estratégica, de acuerdo con su nivel de sensibilidad y su relevancia para la ciberseguridad nacional.

Capítulo IV

Autoridades responsables

Artículo 30. La ejecución de la Estrategia Nacional será responsabilidad de las siguientes autoridades en sus respectivos ámbitos de competencia:

I. En el orden federal, la Secretaría de Seguridad y Protección Ciudadana coordinará la ejecución de la Estrategia y supervisará su implementación.

II. En los órdenes estatal, municipal y de las demarcaciones territoriales de la Ciudad de México, las autoridades de seguridad pública de estos órdenes de gobierno colaborarán con la Estrategia Nacional en sus respectivas jurisdicciones.

Las autoridades ejecutoras llevarán a cabo las acciones necesarias para cumplir con los objetivos y directrices de la Estrategia Nacional, incluyendo la promoción de buenas prácticas en ciberseguridad, la gestión de incidentes y la protección de infraestructura crítica.

Artículo 31. La evaluación de la Estrategia Nacional será competencia de las siguientes autoridades en sus respectivos ámbitos de competencia:

I. En el orden federal, la Comisión será la entidad encargada de evaluar la implementación y efectividad de la Estrategia Nacional, presentando informes periódicos al Ejecutivo federal.

II. En el orden estatal, municipal y de las demarcaciones territoriales de la Ciudad de México, las autoridades de seguridad pública de estos órdenes de gobierno colaborarán en la aplicación de la Estrategia Nacional en sus respectivos ámbitos de competencia, y reportarán sus hallazgos a la Comisión.

Las autoridades evaluadoras realizarán revisiones periódicas de los avances, logros y desafíos en la implementación de la Estrategia Nacional, proponiendo ajustes y mejoras cuando sea necesario.

Artículo 32. Las autoridades ejecutoras y evaluadoras colaborarán estrechamente para garantizar la adecuada implementación y revisión de la Estrategia Nacional.

Artículo 33. La Comisión facilitará la coordinación y el intercambio de información entre las distintas autoridades responsables para promover la gestión integral de la ciberseguridad a nivel nacional.

TÍTULO CUARTO

Ciberamenazas, Ciberataques y Seguridad Informática

Capítulo I

De las Ciberamenazas

Artículo 34. El Área de Inteligencia publicará periódicamente un reporte de ciberamenazas y ciberataques para la población en general y generar un informe anual sobre el estado que guarda la ciberseguridad nacional.

Artículo 35. El Área de Inteligencia tendrá la obligación de informar a las autoridades de los tres órdenes de gobierno de las ciberamenazas y los ciberataques que enfrenten en el ejercicio de sus funciones.

Capítulo II

De la Seguridad Informática

Artículo 36. Los operadores deberán contar con estándares mínimos de protección que garanticen la seguridad informática de los usuarios de las redes públicas de telecomunicaciones.

La Comisión implementará un mecanismo para que los proveedores de servicios de internet que cuenten con usuarios en nuestro país, tengan al menos una representación legal en el territorio nacional.

Artículo 37. Las personas físicas y morales serán las responsables de sus sitios de Internet, por lo que en ningún caso podrán realizar actividades ilícitas a través de las redes públicas de telecomunicaciones, por sí o a través de grupos que se constituyan exprofeso.

Artículo 38. Una vez que los operadores conozcan de actividades ilícitas que se cometan a través de las redes públicas de telecomunicaciones, deberán detener de manera inmediata la transmisión y difusión de la información producto de dichas actividades ilícitas; debiendo guardar los registros respectivos e informar a la brevedad a las autoridades competentes.

La contravención a los artículos 36, 37 y 38 de la Ley por parte de los operadores y de los proveedores de los servicios de internet, será sancionada en términos de lo que disponga el Reglamento.

LIBRO SEGUNDO

DE LOS DELITOS CIBERNÉTICOS

TÍTULO PRIMERO

Delitos contra la confidencialidad, integridad y seguridad de tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos, y contra la intimidad sexual

Capítulo I

Acceso ilícito a tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos

Artículo 39. Al que sin autorización de la persona que legalmente pueda otorgarla, vulnere, modifique, dañe, borre, deteriore, destruya o provoque pérdida de información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de quinientas a mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 40. Al que sin autorización de la persona que legalmente pueda otorgarla, conozca o copie información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de doscientas cincuenta a quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 41. Al que sin autorización de la persona que legalmente pueda otorgarla, modifique, destruya o provoque pérdida de información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de dos a seis años de prisión y de mil a dos mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 42. Al que sin autorización de la persona que legalmente pueda otorgarla, conozca o copie información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a tres años de prisión y de quinientas a mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 43. Al que sin autorización de la persona que legalmente pueda otorgarla, conozca, obtenga, copie o utilice información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad de las instituciones de seguridad pública, protegido por algún medio de seguridad, se le impondrán pena de cuatro a ocho años de prisión y de quinientas a mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta descrita en el párrafo anterior sea o haya sido servidor público en una institución de seguridad pública, se le impondrán, además de las sanciones previstas para dicha conducta, las que establezca la legislación en materia de responsabilidades administrativas.

Cuando la conducta descrita en el primer párrafo de este artículo obstruya, entorpezca, obstaculice, limite o imposibilite las actividades de las instituciones encargadas de la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes, las sanciones previstas en el primer párrafo de este artículo se duplicarán, sin perjuicio de las que establezca la legislación en materia de responsabilidades administrativas.

Artículo 44. Al que con la autorización de la persona que legalmente pueda otorgarla, indebidamente modifique, destruya o provoque pérdida de información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad del Estado, se le impondrán de uno a cuatro años de prisión y de quinientas a mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta descrita en el párrafo anterior sea o haya sido servidor público en una dependencia o entidad de la Administración Pública federal, se le impondrán, además de las sanciones previstas para dicha conducta, las que establezca la legislación en materia de responsabilidades administrativas.

Capítulo II

Delitos contra las instituciones del Sistema Financiero Mexicano

Artículo 45. Al que sin autorización de la persona que legalmente pueda otorgarla, modifique, destruya o provoque pérdida de información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad de las instituciones que integran el Sistema Financiero Mexicano, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de quinientas a mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 46. Al que sin autorización de la persona que legalmente pueda otorgarla, conozca o copie información contenida en tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad de las instituciones que integran el Sistema Financiero Mexicano, protegidos por algún mecanismo de seguridad, se le impondrán de dos meses a un año de prisión y de doscientas cincuenta a quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 47. Al que, teniendo autorización para acceder a tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad de las instituciones que integran el Sistema Financiero Mexicano, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de tres meses a dos años de prisión y de quinientas a mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta descrita en el párrafo anterior sea servidor público o empleado de las instituciones que integran el Sistema Financiero Mexicano, se aumentarán las sanciones hasta en una mitad.

Artículo 48. Al que, teniendo autorización para acceder a tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos propiedad de las instituciones que integran el Sistema Financiero Mexicano, indebidamente copie información que contengan dichas tecnologías o sistemas, se le impondrán de dos meses a un año de prisión y de doscientas cincuenta a quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta descrita en el párrafo anterior sea servidor público o empleado de las instituciones que integran el sistema financiero mexicano, se aumentarán las sanciones hasta en una mitad.

Capítulo III

Falsificación informática

Artículo 49. Al que sin autorización de la persona que legalmente pueda otorgarla, por cualquier medio altere, modifique o imite datos informáticos, electrónicos o telemáticos previamente almacenados en un sistema de redes de computadoras, bases de datos o programas, con la intención de que dichos datos sean utilizados como auténticos, se le impondrán de dos a ocho años de prisión y multa de quinientas a cinco mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Capítulo IV

Delitos contra la intimidad sexual

Artículo 50. Al que, a través de tecnologías de la información y comunicación, sistemas informáticos, electrónicos o telemáticos, distribuya, comercialice, exhiba, reproduzca, transmita, intercambie o difunda fotografías, audios o videos reales o simulados de contenido sexual íntimo de una persona, sin su consentimiento o mediante engaño, se le impondrán de cinco a diez años de prisión y multa de dos mil a cuatro mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Las sanciones a que se refiere el párrafo anterior se aumentarán hasta una mitad, cuando el sujeto activo sea el cónyuge, concubino o concubinario, o que mantenga o haya mantenido una relación sentimental, afectiva o de confianza con la víctima.

TÍTULO SEGUNDO

Delitos contra el patrimonio

Capítulo I

Hurto informático

Artículo 51. Al que, a través de tecnologías de la información y comunicación sistemas informáticos, electrónicos o telemáticos, acceda, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial, sin consentimiento de la persona que legalmente puede disponer de esos bienes o valores, se le impondrán de cuatro a ocho años de prisión y multa de quinientas a cinco mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la víctima de la conducta descrita en el párrafo anterior sea una institución del Estado y el sujeto activo tenga el carácter de servidor público, se aumentarán las sanciones hasta en una mitad.

Capítulo II

Fraude informático

Artículo 52. Al que engañe o se aproveche del error en que otro se halle mediante cualquier medio o método informático, electrónico o telemático, para obtener cualquier bien o derecho patrimonial en perjuicio de un tercero o del Estado, se le impondrán de cuatro a doce años de prisión y multa de quinientas a cinco mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la víctima de la conducta descrita en el párrafo anterior sea una institución del Estado y el sujeto activo tenga el carácter de servidor público, se aumentarán las sanciones hasta en una mitad.

TÍTULO TERCERO

Delitos contra la privacidad y la libertad, integridad y formación sexuales

Capítulo I

Violación de la información de carácter personal

Artículo 53. Al que acceda de manera ilegítima a cualquier sistema informático, electrónico o telemático, para copiar información de carácter personal considerada datos personales, se le impondrán de dos a cuatro años de prisión y multa de cien a quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 54. Al que a través de cualquier sistema informático, electrónico o telemático acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de información de carácter personal de un tercero, se le impondrán de dos a cuatro años de prisión y multa de cien a quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 55. Al que revele, difunda o transmita, todo o en parte, hechos, imágenes, audio o, en general, datos o información de carácter personal obtenidos por cualquier sistema informático, electrónico o telemático, con fines de lucro o para causar perjuicio a otro, se le impondrán de dos a cuatro años de prisión y multa de cien a quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Capítulo II

Suplantación de identidad

Artículo 56. Al que, a través de cualquier sistema informático, electrónico o telemático, suplante la identidad de otra persona para realizar actos con consecuencias jurídicas de cualquier índole, se le impondrán de tres a seis años de prisión y multa de quinientas a mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Para la configuración de este delito, se tomarán en consideración los datos personales que puedan ser utilizados para la identificación de una persona, ya sea directa o indirectamente, por medios físicos o digitales.

Capítulo III

Pornografía de niñas, niños y adolescentes o de personas que no tienen la capacidad de comprender el hecho o de resistir la conducta

Artículo 57. Al que, por medio de cualquier sistema informático, electrónico o telemático, solicite, procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a niñas, niños y adolescentes o de personas que no tienen la capacidad de comprender el hecho o de resistir la conducta, a realizar actos sexuales o de exhibición corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, audio grabarlos, fotografiarlos, filmarlos, transmitirlos, exhibirlos o describirlos, se le impondrán de seis a doce años de prisión y multa de mil a ocho mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales que se hubieren utilizado.

Si se hiciere uso de violencia física o moral, o se aproveche de la ignorancia, extrema pobreza o cualquier otra circunstancia que disminuya o elimine la voluntad de la víctima para resistirse, las sanciones previstas en el párrafo anterior se aumentarán hasta en una mitad.

Artículo 58. Al que, por medio de cualquier sistema informático, electrónico o telemático, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niñas, niños y adolescentes o de personas que no tienen la capacidad de comprender el hecho o de resistir la conducta, se le impondrán de cuatro a ocho años de prisión y multa de mil a cinco mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales que se hubieren utilizado.

Artículo 59. Al que, por medio de cualquier sistema informático, electrónico o telemático, financie, elabore, reproduzca, distribuya, comercialice, difunda, adquiera o intercambie el material a que se refieren las conductas establecidas en los artículos 42 y 43 de esta Ley, se le impondrán de cuatro a ocho años de prisión y

multa de mil a cinco mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 60. Al que, por medio de cualquier sistema informático, electrónico o telemático, contacte, incite, facilite, induzca u obligue a niñas, niños y adolescentes o de personas que no tienen la capacidad de comprender el hecho o de resistir la conducta, a realizar transmisión en vivo o video llamadas en tiempo real, o reciba archivos electrónicos de imagen, audio o video, en los que aparezca la víctima realizando actividades sexuales explícitas, actos de exhibición corporal con fines lascivos o sexuales, o le solicite un encuentro con propósitos sexuales, se le impondrán de seis a doce años de prisión y multa de mil a ocho mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Capítulo IV

Turismo sexual de niñas, niños y adolescentes o de personas que no tienen la capacidad de comprender el hecho o de resistir la conducta

Artículo 61. Al que, por medio de cualquier sistema informático, electrónico o telemático, promueva, publique, divulgue, publicite, invite o gestione que una o más personas viajen al interior o exterior del territorio nacional con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados, con niñas, niños y adolescentes o de personas que no tienen la capacidad de comprender el hecho o de resistir la conducta, se le impondrán de seis a doce años de prisión y multa de mil a ocho mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

TÍTULO CUARTO

Delitos contra el Estado Mexicano y la Seguridad Nacional

TÍTULO PRIMERO

Capítulo I

Delitos contra las Infraestructuras Críticas de la Información

Artículo 62. A quien realice actos tendientes a vulnerar, inhabilitar, robar, destruir o afectar permanente o temporalmente las infraestructuras críticas de la información, se le impondrán de cinco a quince años de prisión y de quinientas a dos mil quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta descrita en el párrafo anterior sea servidor público, se aumentarán las sanciones hasta en una mitad.

Artículo 63. Al que auxilie en la planeación o ejecución del delito establecido en el artículo anterior, se le impondrán de dos a ocho años de prisión y de doscientas cincuenta a mil quinientas veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta descrita en el párrafo anterior sea servidor público, se aumentarán las sanciones hasta en una mitad.

Capítulo II

Delitos contra las instituciones del Estado Mexicano

Artículo 64. Al que lleve a cabo modificaciones no autorizadas en los sistemas informáticos que tengan como consecuencia la generación de una vulnerabilidad informática en las instituciones del Estado Mexicano, se le impondrán de seis a doce años de prisión y multa de mil a cinco mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta descrita en el párrafo anterior sea servidor público, se aumentarán las sanciones hasta en una mitad.

Artículo 65. Al que sin autorización acceda, copie, extraiga, altere, modifique, destruya o elimine dolosamente la información contenida en cualquier sistema informático, electrónico o telemático, con la intención de afectar los procesos de protección de las infraestructuras críticas de la información o de las instituciones del Estado Mexicano, protegidos o no por un mecanismo de seguridad, se le impondrán de cinco a quince años de prisión y multa de dos mil a ocho mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Capítulo III

Delitos contra la Seguridad Nacional

Artículo 66. Al que de manera individual o en grupo, mediante cualquier sistema informático, electrónico o telemático y de manera dolosa, promueva o favorezca de forma sistemática las amenazas a la seguridad nacional referidas en el artículo 5 de la Ley de Seguridad Nacional, se le impondrá pena de ocho a quince años de prisión y multa de dos mil a diez mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta.

Artículo 67. Al que siendo o habiendo sido servidor público de las instituciones de seguridad pública de la Federación, las entidades federativas, los municipios o las demarcaciones territoriales de la Ciudad de México, o de las instituciones de Seguridad Nacional, de manera dolosa y mediante cualquier sistema informático, electrónico o telemático, ponga en peligro o afecte la funcionalidad de las infraestructuras críticas de la información, o realice la conducta prevista en el artículo 44 de la Ley, se le impondrá una pena de diez a veinte años de prisión y multa de cinco mil a quince mil veces la unidad de medida y actualización, vigente al momento de la realización de la conducta, lo anterior, sin perjuicio de las sanciones que establezca la legislación en materia de responsabilidades administrativas.

Artículo Segundo. - Se derogan los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7, todos del Código Penal Federal, para quedar como sigue:

CÓDIGO PENAL FEDERAL

Artículo 211 bis 1.- Derogado.

Artículo 211 bis 2.- Derogado.

Artículo 211 bis 3.- Derogado.

Artículo 211 bis 4.- Derogado.

Artículo 211 bis 5.- Derogado.

Artículo 211 bis 6.- Derogado.

Artículo 211 bis 7.- Derogado.

ARTÍCULOS TRANSITORIOS

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

SEGUNDO. El titular del Poder Ejecutivo Federal, en un plazo que no excederá de 180 días naturales, contados a partir de la entrada en vigor del presente Decreto, deberá expedir el Reglamento de Ley Federal de Ciberseguridad.

TERCERO. El Congreso de la Unión, en un plazo que no excederá de 180 días naturales, contados a partir de la entrada en vigor del presente Decreto, realizará las reformas a la legislación secundaria que lo requiera para armonizarla a la Ley Federal de Ciberseguridad.

CUARTO. La Secretaría de Seguridad y Protección Ciudadana, en un plazo que no excederá de 180 días naturales, contados a partir de la entrada en vigor del presente Decreto, realizará las adecuaciones reglamentarias correspondientes para armonizarlas con el texto de la Ley Federal de Ciberseguridad.

QUINTO. Los recursos para llevar a cabo los programas y estrategias que se deriven de la Ley Federal de Ciberseguridad, así como los recursos humanos, materiales y financieros que requiera la Comisión Nacional de Ciberseguridad y el Área de Inteligencia en materia de Ciberseguridad, se cubrirán con cargo al presupuesto autorizado a la Secretaría de Seguridad y Protección Ciudadana, para el presente ejercicio fiscal y los subsecuentes; por lo que la implementación de Ley Federal de Ciberseguridad no representará un impacto presupuestal.

SEXTO. Para dar cumplimiento a las políticas y acciones de coordinación y colaboración entre las instancias federales, estatales y municipales que se prevén en la Ley Federal de Ciberseguridad, se aprovecharán las estructuras y capacidades del Consejo Nacional de Seguridad Pública, del Consejo de Seguridad Nacional, de la Comisión Intersecretarial de Tecnologías de la Información y Comunicación y de la Seguridad de la Información, y de la Coordinación de Estrategia Digital Nacional.

Dado en el Salón de Sesiones del Senado de la República a los 14 días del mes de febrero del 2024.

Suscriben

Sen. Checo Pérez Flores. **Sen. Rafael Espino de la Peña.**