005603

CÁMARA DE SENADORES
SECRETARÍA GENERAL
SERVICIOS PARLAMENTARIOS

VERDE

**Ciudad de México, a 15 de agosto de 2024**
**LXV/GPPVEM-OD/228/24**

2024 AGO 15 PM 1 59

**Sen. Ana Lilia Rivera Rivera**
Presidenta de la Mesa Directiva
de la Comisión Permanente
Presente.

AT'N RECIBIDO
Lic. Michael Rolla Negrete Cárdenas
Secretario Técnico

En alcance al oficio núm. **LXV/GPPVEM-OD/227/24** y por instrucción del Senador Raúl Bolaños Cacho Cué, Coordinador del Grupo Parlamentario del Partido Verde Ecologista de México, y a petición de la Sen. Alejandra Lagunes Soto Ruíz, remito el siguiente asunto para que se sustituya del Orden del Día de la sesión del Pleno de la Comisión Permanente del miercoles 14 de agosto del año en curso, por sufrir cambios y ajustes de fondo:

- **De la Sen. Alejandra Lagunes Soto Ruíz**, Integrante del Grupo Parlamentario del Partido Verde Ecologista de México. – Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Ciberseguridad y Confianza Digital y se reforman y adicionan diversas disposiciones en materia de ciberdelitos. ***(turno directo a comisiones)***

Asimismo, le solicito que la presente versión sustituya a la anterior en todos los registros parlamentarios y órganos de difusión de este Senado de la República.

Anexo a la presente la versión impresa y electrónica del documento en comento.

Sin más por el momento, reciba un cordial saludo.

**Atentamente**

**Mtro. Javier Carreón Valencia**
Coordinador de Asesores PVEM

JVC/rrs

CÁMARA DE SENADORES
SECRETARÍA GENERAL DE SERVICIOS PARLAMENTARIOS
Oficialía de Partes
2024 AGO 15 PM 1 37
017450

**COMISIÓN PERMANENTE**
**DEL H. CONGRESO DE LA UNIÓN**
**LXV LEGISLATURA**

De la **Senadora Alejandra Lagunes Soto Ruíz** integrante del Grupo Parlamentario del Partido Verde Ecologista de México, en la LXV Legislatura del H. Congreso de la Unión, de conformidad con lo establecido en los artículos 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos; 55, fracción II, y 179 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos; 8, numeral 1, fracción I, 164 y 169 del Reglamento del Senado de la República, se somete a consideración de esta Honorable Asamblea la siguiente: **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD Y CONFIANZA DIGITAL Y SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES EN MATERIA DE CIBERDELITOS** con base en la siguiente:

## EXPOSICIÓN DE MOTIVOS

### I. Antecedentes

El desarrollo de las tecnologías de la información y la comunicación (TIC) ha transformado la forma en que entendemos el mundo y cómo nos vinculamos unos con otros, expandiendo de manera considerable el crecimiento y oportunidades económicas y sociales, la mejora en la prestación y capacidad de servicios. Además, se han generado enormes oportunidades para construir instituciones públicas más abiertas, transparentes y eficientes; para el desarrollo de la economía digital y la construcción de sociedades más justas, democráticas e informadas. Por otro lado, también se debe reconocer que han surgido nuevos retos en materia de riesgos y amenazas a los derechos y libertades, a la protección de la privacidad y los datos personales, el patrimonio de las personas y organizaciones públicas y privadas, las infraestructuras críticas e incluso peligros latentes para la seguridad nacional del país.

La incorporación de las TIC en las economías globales ha tenido un crecimiento considerable, en los últimos años se han duplicado los usuarios de Internet en todo el mundo, que en 2014 alcanzaron el 50.1% de la población[1]. México no ha sido ajeno a este crecimiento, de acuerdo con el 15° Estudio sobre los Hábitos de los

[1] INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), 2024.
https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/ENDUTIH/ENDUTIH_23.pdf

Usuarios de Internet en México (2019), nuestro país alcanzó un 71% de penetración entre la población de personas de 6 años en adelante, con 82.7 millones de usuarios conectados[2]. Por su parte, según el 20° Estudio sobre los hábitos de usuarios de internet en México 2024, el número de usuarios de Internet en México, representó un crecimiento de 5.2%, pasando de los 96.9 millones de internautas a 101.9 millones, que representa el 84% de la población mayor a 6 años.

La expansión tan rápida de internet y de las tecnologías de la información, ha multiplicado el número de ciudadanos digitales. El internauta mexicano pasa conectado a internet diariamente en promedio 8 horas con 20 minutos; desgraciadamente, esta expansión no se ha visto acompañada por un aumento proporcional en los protocolos y políticas públicas para proteger la seguridad de las personas en línea.

De acuerdo con datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH 2024) señala que, en 2023, 97.0 millones de personas usaban internet, es decir, 81.2 % de la población de 6 años o más. En el mismo periodo, 97.2 millones de personas usaban un teléfono celular, lo que equivale a 81.4 % de la población de 6 años o más. Y qué 43.8 % de los hogares disponía de computadora (laptop, tablet o de escritorio), lo que correspondió a 16.9 millones de hogares.

A partir de las reformas constitucionales publicadas en el DOF del 11 de junio del año 2013 en materia de telecomunicaciones y radiodifusión, el apartado B) del artículo 6º consagró tres cuestiones relevantes: i) Que el Estado garantizará el derecho de acceso a las TIC, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet; ii) Que el Estado garantizará a la población su integración a la Sociedad de la Información y el Conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales; y iii) Que el acceso digital debe otorgarse en condiciones de competencia, neutralidad, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias (que comprende la seguridad y la libertad de expresión en el entorno digital).

El derecho internacional de los derechos humanos es aplicable a las nuevas tecnologías de la comunicación, tal y como es reconocido en la Declaración de Principios de Ginebra con motivo de la Cumbre Mundial sobre la Sociedad de la Información[3].

Asimismo, como parte de las conclusiones del Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, presentado en Asamblea General de las

2 Asociación Mexicana de Internet. "Estudio sobre los Hábitos de los Usuarios de Internet en México 2022, 2024 respectivamente".

3 https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html

Naciones Unidas en 2013,[4] se establece que el derecho internacional, y en particular la Carta de las Naciones Unidas, son aplicables y esenciales para mantener la paz y la estabilidad, y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones. También se refieren a la adopción de medidas voluntarias para incrementar la confianza, la transparencia, y la cooperación internacional para construir capacidades en la esfera de la seguridad de las tecnologías de la información y las comunicaciones.

En el entorno nacional, la Suprema Corte de Justicia de la Nación, mediante la tesis emitida por la Segunda Sala bajo el rubro "Flujo de información en red electrónica (Internet). Principio de restricción mínima posible."[5] determinó que el marco del derecho internacional de los derechos humanos sigue siendo pertinente y aplicable a las nuevas tecnologías de la comunicación; afirmando que Internet se ha convertido en un medio fundamental para que las personas ejerzan su derecho a la libertad de opinión y de expresión, atento a sus características singulares, como su velocidad, alcance mundial y relativo anonimato. Por tanto, en atención a ese derecho humano, se reconoce que en el orden jurídico nacional y en el derecho internacional de los derechos humanos, existe el principio relativo a que el flujo de información por Internet debe restringirse lo mínimo posible, esto es, en circunstancias excepcionales y limitadas, previstas en la ley, para proteger otros derechos humanos.

En los próximos años el uso de las TIC se intensificará en todos los ámbitos de la vida pública y privada de las personas y comunidades. Con ello, también incrementará las amenazas digitales, y el número y naturaleza de los ciberdelitos. Ante este escenario, resulta necesario actualizar el marco legal de México en la materia, así como implementar programas permanentes de capacitación para las autoridades encargadas de la impartición y procuración de la justicia.

Por un lado, conforme a lo previsto en el artículo 6° de nuestra Constitución, el Estado mexicano tiene la obligación de garantizar el acceso a las tecnologías de la información y comunicación, a los servicios de internet y de banda ancha, a la manifestación de ideas, así como el acceso a la información. Por otro lado, las cifras de ciberdelitos e incidencia informática que se cometen en nuestro país crecen día con día. Por lo anterior, resulta necesaria la implementación de medidas legislativas para la tipificación de delitos que sancionen severamente el uso indebido de las tecnologías de la información y comunicaciones.

En México, como resultado de las acciones y programas impulsados por la reforma constitucional en materia de telecomunicaciones, entre 2012 y 2017 el número de

[4] http://undocs.org/es/A/68/98

[5] https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=FLUJO%2520DE%2520INFORMACI%25C3%2593N%2520EN%2520RED%2520ELECTR%25C3%2593NICA%2520(INTERNET).%2520PRINCIPIO%2520DE%2520RESTRICCI%25C3%2593N%2520M%25C3%258DNIMA%2520POSIBLE&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=1&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2014515&Hit=1&IDs=2014515&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema=

usuarios de Internet aumentó en más de 30 millones, pasando de 40.9 a 71.3 millones de usuarios.[6] El enfoque de conectividad, penetración y acceso a Internet que ha premiado en el diseño programático y legislativo del país necesita acompañarse de la creación y articulación de definiciones sobre las prácticas y conductas maliciosas y delictivas en Internet.

La Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC) en su *"Estudio Exhaustivo Sobre el Delito Cibernético, 2013"*[7] señala que las definiciones de delito cibernético dependen en gran medida del propósito para el que se use el término. Un número limitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos representan el núcleo del delito cibernético; los actos informáticos realizados para beneficio, daño personal o financiero, que incluyen formas delincuenciales relacionadas con la identidad y actos relacionados con contenidos informáticos, no se prestan fácilmente para los esfuerzos de generar definiciones legales del término compuesto. Asimismo, el término delito cibernético debe ser considerado como un conjunto de actos o conductas que pueden organizarse en categorías basadas en el objeto del delito material y el *modus operandi*.

La *National Crime Agency* (Agencia Nacional Criminal de Reino Unido) divide al delito cibernético en dos categorías amplias:

- Los delitos ciber-dependientes o crímenes cibernéticos "puros", definidos como delitos que sólo pueden cometerse utilizando una computadora, redes de computadoras u otras formas de tecnologías de la información y comunicación.
- Los delitos ciber-habilitados (como el fraude, la compra de drogas ilegales o la explotación sexual infantil) que pueden llevarse a cabo en línea o fuera de línea, pero al utilizar Internet llegan a tener una escala y velocidad sin precedentes.[8]

De acuerdo con las definiciones antes valoradas, se pueden identificar distintas tipologías que engloban a las conductas criminales que se realizan con el empleo de tecnologías de la información y digitales, como medio, fin o habilitadores. Mientras que un delito informático, tiene como común denominador el ataque a activos de información, es decir la disponibilidad, confidencialidad e integridad de la información, los ciberdelitos o cibercrímenes se definen por su relación, ataque y/o utilización de medios tecnológicos.

La revolución digital ha traído consigo problemas y retos parcialmente nuevos, a los que el derecho penal y su sistema no pueden ser ajenos. La caracterización, tanto

[6] Sexto informe de Gobierno. 1 de septiembre de 2018. http://cdn.presidencia.gob.mx/sextoinforme/informe/6_IG_INFORME_COMPLETO.pdf p. 504
[7] https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf
[8] http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved

criminológica como dogmática, de los ciberdelitos no es sencilla y plantea problemas jurídico-penales de diversa índole. Las variadas denominaciones que se han utilizado (en primer lugar, "delitos informáticos", y posteriormente "ciberdelitos" o "cibercrímenes", entre otras) reflejan una evolución en el conjunto de figuras delictivas agrupadas en diversas clasificaciones pero que, en realidad, no se han traducido en un concepto dogmático de ciberdelito.

La delincuencia organizada ha aprovechado rápidamente las oportunidades que ofrece Internet, en particular el crecimiento del comercio electrónico y la banca en línea. Los grupos delictivos especializados se dirigen a individuos, pequeñas empresas y grandes redes corporativas para sustraer información personal de forma masiva a fin de aprovechar los datos sensibles que tienen a su disposición.

Por lo que se refiere a la legislación en materia de delitos cibernéticos, ésta debe articularse de forma que sea tecnológicamente neutral y flexible para responder a la evolución constante del crimen y la tecnología, para garantizar el estado de derecho y los derechos humanos, y estar armonizada con las leyes de otros países con miras a una cooperación internacional.

El Informe 2016 del Observador de la Ciberseguridad en América Latina y el Caribe, desarrolla el Modelo de Madurez de Capacidad de Seguridad Cibernética como punto de referencia para encontrar soluciones que contribuyan en la prevención y mitigación de riesgos de la actividad delictiva o maliciosa en el ciberespacio, a través de cinco dimensiones de capacidad de seguridad cibernética (no necesariamente independientes unas de otras):1) políticas y estrategia nacional de seguridad cibernética; 2) cultura cibernética y sociedad; 3) educación, formación y competencias en seguridad cibernética; 4) marco jurídico y reglamentario; y 5) normas, organización y tecnologías.

El Índice Global de Ciberseguridad (IGC) de la Unión Internacional de Telecomunicaciones (UIT), coloca a México en el lugar 52 del ranking global y en cuarto lugar del continente americano, debajo de Estados Unidos de América, Canadá y Brasil. El IGC se compone de 5 dimensiones, que sirven de indicador para evaluar el grado de madurez de los países. Estas dimensiones son: 1) Medidas legales, 2) Medidas técnicas, 3) Medidas organizativas, 4) Desarrollo de capacidades y 5) Medidas de cooperación. México muestra áreas críticas que son necesarias atender, como contar con una agencia nacional de ciberseguridad, responsable de coordinar y supervisar la implementación de una Estrategia Nacional de Ciberseguridad; establecer acuerdos bilaterales y multilaterales; fomentar una industria doméstica; y firmar acuerdos público - privados en la materia[9].

El objetivo principal de la Estrategia Nacional de Ciberseguridad, publicada en conjunto por la Organización de Estados Americanos (OEA) y la Presidencia de la

[9] Índice Global de Ciberseguridad 2017. Unión Internacional de Telecomunicaciones. 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

República en 2017 a recomendación internacional, consiste en propiciar que individuos, empresas y entes públicos -de los diferentes poderes y órdenes de gobierno, realicen sus actividades con el uso de tecnologías de información y comunicación de manera libre, confiable, segura y resiliente, y con ello impulsar el desarrollo económico, social y político de México.[10]

Este documento establece la visión del Estado mexicano en la materia y reconoce lo siguiente:

- La importancia de las Tecnologías de la Información y Comunicación (TIC) como un factor de desarrollo político, social y económico de México, en el entendido de que cada vez más individuos están conectados a internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.
- Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.
- La necesidad de una cultura general de ciberseguridad.

De acuerdo con el *National Cyber Security Index* (indice Nacional de Ciberseguridad) preparado por la e-*Governance Academy Foundation* de Estonia, con datos al 7 de abril de 2018[11], nuestro país ocupa la posición 64 de 126. Una de sus referencias en materia de seguridad cibernética a nivel global mide la preparación de los países para prevenir amenazas de ciberseguridad y la gestión de incidentes, centrándose en cuatro aspectos medibles de la ciberseguridad implementados por los gobiernos:

I. Legislación vigente;
II. Unidades establecidas;
III. Formatos de cooperación; y
IV. Políticas

El Foro Económico Mundial, en su Informe Mundial de Riesgos 2018[12], reconoce que: a nivel tecnológico los ciberataques y el fraude o robo masivo de datos constituyen uno de cinco principales riesgos mundiales percibido por los países. Esto se traduce en el crecimiento de los riesgos en materia de ciberseguridad tanto en términos de su prevalencia, como de su potencial disruptivo y en el crecimiento de casi al doble de los ataques en contra de empresas. Otra de las tendencias que refiere el Informe es el crecimiento de los ciberataques a infraestructura esencial y a sectores industriales estratégicos, lo cual podría provocar el colapso de sistemas que mantienen en funcionamiento a sociedades enteras.

---

[10] https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS%20(1).pdf

[11] https://ncsi.ega.ee/country/mx/

[12] http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

La ciberdelincuencia es uno de los delitos transnacionales de mayor riesgo y de más rápido crecimiento a los que se enfrentan los países, personas, instituciones financieras y corporaciones. La naturaleza sin fronteras de estos delitos, así como la inmediatez, asimetría en capacidades técnicas y humanas para prevenirlos, investigarlos, mitigar su impacto, perseguirlos y sancionarlos han representado serios obstáculos para responder eficazmente a estas amenazas.

El empleo de términos como delincuencia informática, cibercriminalidad, delitos informáticos, entre otros, se ha convertido en una constante en nuestra sociedad. El nacimiento y la rápida difusión de las redes informáticas están propiciando que la cibercriminalidad sea uno de los ámbitos delictivos con más rápido crecimiento. La rapidez, el anonimato, la comodidad y la amplitud de alcance que facilitan las nuevas tecnologías, hacen que los delincuentes aprovechen las mismas para llevar a cabo diversas actividades delictivas, tanto tradicionales aprovechando los nuevos medios, como otras nuevas modalidades nacidas dentro de este ámbito.

Ataques contra sistemas informáticos, robo y manipulación de datos, usurpación de identidad, actividades pedófilas, estafas comerciales y bancarias mediante distintas técnicas como la suplantación de identidad, difusión de software malicioso, creación de redes de *bots* para distintos fines, entre otros, constituyen parte de estas actividades delictivas cometidas utilizando medios informáticos. El alcance mundial y la rápida difusión de este tipo de actividades han causado que gobiernos de todo el mundo empiecen a implementar en sus legislaciones medidas para combatirlas y tratar de evitar y prevenir los efectos nocivos que puedan causar en sus ciudadanos.[13]

En México, se ha calculado, que la ciberdelincuencia genera pérdidas anuales por 5 mil millones de dólares, sin embargo, también se señala que cerca del 80% de los delitos cibernéticos se pueden prevenir.[14]

Los ciberdelitos se han convertido en una epidemia digital, mundial y silenciosa. La mayoría de los usuarios de Internet en el mundo ha sufrido y sido víctima de actividades delictivas en la red, quedándose indefensos al intentar hacer frente a los ciberdelincuentes cobijados por el anonimato de la Internet.

Por otra parte, la empresa de seguridad en sistemas Norton, ha reportado una cifra mayor, afirmando que en 2017 los ciberdelincuentes robaron a clientes de servicios financieros, bancarios y empresas en México 7 mil 700 millones de dólares. En el mismo año, de acuerdo a esta empresa, México fue el segundo país en el mundo con mayor número de víctimas de fraude cibernético, con poco más de 33 millones de afectados.[15]

---

[13] http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815
[14] El Economista. Ciberdelincuencia deja pérdidas anuales de 5,000 mdd. 13 de noviembre de 2017
https://www.eleconomista.com.mx/tecnologia/Ciberdelincuencia-deja-perdidas-anuales-de-5000-mdd-20171113-0070.html
[15] Televisa News. México es el segundo país con el mayor número de fraudes cibernéticos. 23 de enero de 2018
https://noticieros.televisa.com/ultimas-noticias/mexico-es-segundo-pais-mayor-numero-fraudes-ciberneticos/

Para el primer trimestre de 2018, de acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), los fraudes cibernéticos crecieron 63% respecto del mismo periodo de 2017 y representan cada año una mayor proporción, pasando del 13% en 2013 al 61% en 2018.

El monto de los fraudes cibernéticos ascendió a $2,340 millones de pesos; se bonificó el 60% del monto reclamado y 89 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario.[16] Asimismo, de acuerdo con los últimos datos generados por dicho organismo, al cierre del primer semestre de 2018 se han disparado los fraudes cibernéticos con un promedio mensual de 333 mil casos, destacando el crecimiento en fraudes cibernéticos realizados en operaciones de comercio electrónico y las operaciones con banca móvil[17].

De acuerdo con el Banco de México, de acuerdo con entre los principales incidentes cibernéticos relevantes ocurridos en 2023, en el sistema financiero nacional, que han sido reportados al Banco de México; se encuentran el secuestro de datos o información (conocido como ransomware) y la venta de información de tarjetas bancarias (card seller). El monto aproximado por estos incidentes ha sido de cerca de 88 MDP.

Estas cifras revelan que los ciberdelitos se encuentran al alza, por lo que se requieren mayores esfuerzos para combatirlos efectivamente.

La tendencia internacional de cibercrimen indica que los incidentes y ataques cibernéticos están en aumento tanto en frecuencia, como en grado de afectación y sofisticación. Es urgente fortalecer las medidas de seguridad y las capacidades de la infraestructura digital de nuestro país, así como el marco jurídico que lo regula, para que contribuyan a gestionar y mitigar los riesgos a los nuevos requerimientos, riesgos y amenazas en el ciberespacio, así como a que atiendan la prevención y atención de delitos.

La lucha efectiva contra la ciberdelincuencia requiere de una cooperación internacional reforzada, rápida y eficaz en materia penal, los Estados miembros del Consejo de Europa impulsaron en 2001 la firma del Convenio de Budapest sobre la Ciberdelincuencia, tanto para los Estados Miembros del Consejo de Europa como los Estados no miembros mediante la adhesión a dicho Convenio por invitación del Comité de Ministros del Consejo de Europa. Por lo que se refiere a México, es imperativa la adhesión a este Convenio, y es que de poco sirve tener una legislación penal actualizada como se busca con esta iniciativa, si no existe un marco de coadyuvancia internacional para combatir una forma de delincuencia que no reconoce fronteras físicas.

[16] CONDUSEF. Estadísticas (consultado en septiembre de 2018) https://www.condusef.gob.mx/gbmx/?p=estadisticas
[17] https://www.eluniversal.com.mx/cartera/negocios/cada-hora-se-cometen-463-fraudes-ciberneticos-en-mexico-condusef

Los antecedentes de esta iniciativa se remontan a una serie de reformas al Código Penal Federal que se han realizado a partir de 1999 con el objetivo de brindar herramientas necesarias para la procuración e impartición de justicia frente al desarrollo de las TIC.

a) Decreto de Reformas publicado en el Diario Oficial de la Federación del 17 de mayo de 1999 del entonces Código Penal Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, en el que entre otros rubros, se adiciona el artículo 168 Bis y el Capítulo II al Título Noveno del Libro Segundo denominado acceso ilícito a sistemas y equipos de informática, y con ello los artículos 211 Bis 1; 211 Bis 2; 211 Bis 3; 211 Bis 4; 211 Bis 5; 211 Bis 6; 211 Bis 7; asimismo, se agregaron los artículo 424 Bis y Ter.

A continuación se presentan las reformas aprobadas en ese entonces - resaltando los cambios para su fácil identificación:

> **"Artículo 167.-** Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:
>
> **VI.** Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de **fibra óptica**, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;
>
> **Artículo 168 bis.-** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:
>
> **I.** Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o
>
> **II.** Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas.
>
> **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 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 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.

**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.

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.

**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 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 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 7.-** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

**Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

**I.** A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

**II.** A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

**Artículo 424 ter.-** Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, videogramas o libros, a que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código."

b) Posteriormente, mediante Decreto publicado en el Diario Oficial de la Federación, el 24 de junio de 2009, se modificaron los artículos 211 bis 2 y bis 3 para quedar de la siguiente forma:

**Artículo 211 bis 2.-** ... ...

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.

**Artículo 211 bis 3.-** ... ...

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.

c) Finalmente, y de manera más reciente, se publicaron reformas en Diario Oficial de la Federación el 17 de junio de 2016 al artículo 211 Bis 2, para quedar como sigue:

**Artículo 211 Bis 2.-** ... ... ...

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.

## II. Proceso de creación de la iniciativa

La construcción de la iniciativa de ciberseguridad y confianza digital se llevó a cabo de manera colaborativa, multisectorial y multidisciplinaria. A lo largo de diversas sesiones de trabajo, que sumaron más de 50 horas de diálogo, se convocaron a diversos expertos provenientes de diversos sectores, incluyendo la sociedad civil, la comunidad científica, organismos autónomos y la academia.

Durante estas discusiones, se revisó puntualmente cada detalle y modificación propuesta en la iniciativa de ley, con el objetivo de obtener un texto que contempla todas las visiones en materia de neuroderechos. En estas sesiones participaron:

- Anahiby Anyel Becerril Gil;
- Claudia Alin Escoto Velázquez;

- Elizabeth Tenorio Reyes;
- Ernesto Ibarra Sánchez;
- Gerardo Natanael Hernández Ortiz;
- Héctor Cortés;
- Israel Cedillo Lazcano;
- José Antonio López Alonso;
- José Luis Ponce López;
- Kiyoshi Tsuru Alberú;
- Nuhad Ponce Kuri;
- Omar Mendoza González;
- Orlando Pérez Gárate;
- Oscar Castillo;
- Pablo Corona Fraga;
- Velda Abigail Gámez Bustamante;
- Victor Lagunes

Este esfuerzo colectivo y detallado surge para dar contenido normativo a la iniciativa constitucional presentada el 26 de septiembre de 2023 por las senadoras Alejandra Lagunes Soto Ruiz, Nancy de la Sierra Arámburo, Xóchitl Gálvez Ruiz, Indira Kempis Martínez, Beatriz Paredes Rangel, María Graciela Gaitán Díaz y Marcela Mora; y de los senadores Oscar Eduardo Ramírez Aguilar, Jorge Carlos Ramírez Marín, Gustavo Madero Muñoz, Miguel Ángel Mancera Espinosa, Alfredo Botello Montes, Gilberto Herrera Ruiz, Mario Zamora Gastélum, Héctor Vasconcelos, Emilio Álvarez Icaza Longoria y Damián Zepeda Vidales, de diversos grupos parlamentarios que propone reformar la fracción XVII del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, con el propósito de facultar al Congreso la emisión de una ley en materia de ciberseguridad.

Este proceso minucioso y participativo aseguró que la legislación resultante refleje un consenso amplio y una comprensión profunda de los temas involucrados, garantizando la protección y promoción de los neuroderechos en el contexto del avance tecnológico.

## III. De los contenidos de la iniciativa

La propuesta de Decreto de la Ley Federal de Ciberseguridad y Confianza Digital contempla un Título Primero que abarca las disposiciones generales, estableciendo los fundamentos, objetivos y principios clave que regirán la aplicación de la ley.

La ciberseguridad es reconocida internacionalmente como el conjunto de medidas, técnicas y procesos orientados a proteger los sistemas informáticos, redes, dispositivos y datos contra amenazas cibernéticas, garantizando la confidencialidad, integridad y disponibilidad de la información, así como la protección de los activos digitales y la privacidad de los usuarios.

Esta disciplina abarca diversas áreas y ámbitos de aplicación incluyendo entre otras: la protección contra ataques informáticos, la gestión de riesgos cibernéticos, la detección y respuesta a incidentes, la educación y concientización en seguridad digital, la regulación y cumplimiento de normativas, y la cooperación internacional en la lucha contra el ciberdelito.

De la misma forma se fundamenta en principios y prácticas establecidas internacionalmente tales como la autenticación, autorización, cifrado, monitoreo y auditoría de sistemas y redes, así como en el desarrollo de políticas y procedimientos de seguridad que promuevan una cultura de protección y responsabilidad en el uso de la tecnología.

Debido a lo anterior, y al constante cambio y evolución de las tecnologías de la información resulta necesario un marco regulatorio flexible, moderno y que pueda adaptarse a los constantes cambios, la ciberseguridad es un componente crucial para la protección de la infraestructura crítica, la seguridad nacional, la economía digital, los derechos individuales en el ciberespacio y la confianza pública en el entorno digital, por lo que su promoción y fortalecimiento son de vital importancia para el desarrollo seguro y sostenible de la sociedad digital en México.

Ante este panorama, la necesidad de una regulación integral, interdisciplinaria y actualizada en materia de ciberseguridad se vuelve cada vez más urgente.
Protección de la infraestructura crítica:

- México cuenta con infraestructura crítica en sectores como energía, telecomunicaciones y finanzas, cuya vulnerabilidad a ataques cibernéticos podría tener graves consecuencias para la seguridad nacional y la economía.

- El robo de información confidencial, la interrupción de servicios digitales y la falsificación de identidad pueden tener un impacto negativo en las empresas y la economía en general.

- La falta de confianza en la seguridad del ciberespacio puede frenar la adopción de tecnologías digitales y la economía digital.

- La seguridad del ciberespacio es un pilar fundamental para el desarrollo de la economía digital. Sin embargo, la falta de confianza en la protección de datos y la privacidad en línea puede frenar la adopción de tecnologías digitales por parte de usuarios y empresas.

- Los ciberataques, el robo de información y la suplantación de identidad son algunos ejemplos de las amenazas que generan desconfianza en el ámbito digital. Esta desconfianza puede traducirse en una menor disposición a realizar transacciones en línea, a utilizar servicios digitales o a compartir información personal.

Para fomentar la confianza en el ciberespacio, es necesario implementar medidas que fortalezcan la seguridad de los sistemas informáticos, protejan la privacidad de los datos y brinden a los usuarios herramientas para defenderse de las amenazas digitales.

México ha experimentado un aumento significativo en el número y la sofisticación de los ciberataques en los últimos años, conforme a lo que se ha expuesto con anterioridad.

La legislación actual en materia de ciberseguridad se caracteriza por ser fragmentada y no responder a las necesidades y desafíos del mundo digital actual.

Diversas leyes y normas dispersas, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o el Código Penal Federal, abordan aspectos específicos de la ciberseguridad. Sin embargo, no existe una ley general que armonice y fortalezca el marco legal en este ámbito.

Esta fragmentación genera diversos problemas:

- Falta de claridad y coordinación: Dificulta la aplicación efectiva de las normas y la identificación de responsabilidades.
- Vacíos legales: No se contemplan nuevos tipos de delitos cibernéticos ni las últimas tendencias en las amenazas digitales.
- Debilidad en la protección de la infraestructura crítica: No se establecen medidas específicas para proteger los sectores estratégicos del país.

- Falta de incentivos para la inversión en ciberseguridad: No se ofrecen mecanismos para que las empresas y organizaciones adopten medidas de protección adecuadas.

Es urgente contar con una ley general de ciberseguridad que:

- Consolide y actualice el marco legal: Integre las normas existentes y responda a las necesidades actuales.
- Defina una estrategia nacional: Establezca objetivos, prioridades y acciones para fortalecer la ciberseguridad en el país.
- Promueva la cultura de la ciberseguridad: Fomente la educación y el conocimiento sobre la seguridad digital en la sociedad.
- Fortalezca la cooperación público-privada: Involucre a todos los sectores en la construcción de un espacio digital más seguro.

La creación de una Ley Federal de Ciberseguridad y Confianza digital representa un paso fundamental para proteger a México de las amenazas digitales y garantizar el desarrollo de una economía digital segura y confiable.

**Necesidad de una estrategia nacional.**

Se requiere una estrategia nacional de ciberseguridad que articule las acciones de los diferentes sectores del gobierno, la iniciativa privada y la sociedad civil.

Ante este panorama, la necesidad de una Estrategia Nacional de Ciberseguridad (ENC) que articule las acciones de los diferentes sectores del gobierno, la iniciativa privada y la sociedad civil se vuelve cada vez más urgente.

La ENC debe ser integral y abarcar:

- Prevención: Fortalecimiento de las capacidades nacionales para identificar y prevenir ciberataques.
- Detección: Implementación de sistemas para la detección temprana de amenazas cibernéticas.
- Respuesta: Desarrollo de planes de acción para responder a incidentes de ciberseguridad.
- Recuperación: Establecimiento de mecanismos para la recuperación de los sistemas afectados por un ciberataque.
- La participación de todos los sectores es fundamental para el éxito de la ENC:

- Gobierno: Debe liderar la creación e implementación de la estrategia, así como la inversión en medidas de ciberseguridad.
- Iniciativa privada: Debe invertir en la protección de sus sistemas informáticos y colaborar con el gobierno en la implementación de la ENC.
- Sociedad civil: Debe ser partícipe en la creación de la estrategia y en la promoción de una cultura de la ciberseguridad.

La ENC es una herramienta indispensable para:

- Proteger la infraestructura crítica: La seguridad de los sistemas informáticos que controlan sectores como el energético, financiero y de telecomunicaciones es vital para la seguridad nacional.
- Promover la economía digital: La confianza en la seguridad del ciberespacio es fundamental para el desarrollo de la economía digital.
- Proteger la privacidad de los ciudadanos: La ENCS debe garantizar la protección de la información personal de los ciudadanos frente al robo y el uso indebido.

La ciberseguridad no se limita a la protección de sistemas informáticos. Es un problema complejo que involucra aspectos técnicos, legales, sociales, económicos y políticos.

En el ámbito técnico, se requiere de medidas para proteger la infraestructura crítica, los sistemas informáticos y los datos frente a ataques cibernéticos.

Desde el punto de vista legal, es necesario contar con leyes y regulaciones que establezcan marcos jurídicos claros para la protección de la información y la persecución de los delitos cibernéticos.

Las dimensiones sociales y económicas de la ciberseguridad también son fundamentales. Se necesita educar a la población sobre los riesgos y las buenas prácticas en el mundo digital, e incentivar a las empresas a invertir en medidas de seguridad. Mientras que los gobiernos deben asumir un rol activo en la creación de estrategias nacionales de ciberseguridad y en la promoción de la cooperación internacional para combatir las amenazas cibernéticas.

Durante la construcción de esta propuesta de Ley se han considerado las bases para la conformación desde la ley, de una Estrategia Nacional de Ciberseguridad, que se enfoque en:

- Identificación de riesgos: Es fundamental realizar un análisis exhaustivo de los riesgos y amenazas que enfrenta México en el ciberespacio.

- Desarrollo de capacidades: Se requiere fortalecer las capacidades del país en materia de prevención, detección, respuesta y recuperación de incidentes cibernéticos.

- Cultura de la ciberseguridad: Es necesario promover una cultura de la ciberseguridad entre la población en general.

- Cooperación internacional: La colaboración con otros países y organismos internacionales es fundamental para combatir las amenazas cibernéticas.

- Políticas Públicas para la Gestión del Riesgo y la Promoción de la Confianza Digital:

- Marco legal robusto: Se requiere una ley general de ciberseguridad que establezca los principios, objetivos y lineamientos generales en la materia.

- Esquemas de certificación: Implementar esquemas de certificación para garantizar la seguridad de los productos y servicios digitales.

- Programas de educación y concientización: Es necesario promover la educación y el conocimiento sobre la ciberseguridad en todos los niveles de la sociedad.

- Incentivos para la inversión: Se deben crear incentivos para que las empresas inviertan en medidas de ciberseguridad.

**Objetivos de la Ley.**

- Establecer un marco regulatorio integral para la seguridad y confianza en el uso de las tecnologías de la información y las comunicaciones en México.
- Proteger la infraestructura crítica, la economía y los derechos fundamentales de las personas en el ciberespacio.
- Responder a incidentes cibernéticos.

Estos objetivos serán conseguidos a través de los siguientes principios:

- Autonomía.
- Proporcionalidad.
- Transparencia.
- Monitoreo y seguimiento.
- Colaboración Multisectorial.
- Seguridad e Integridad de los Datos.
- Protección de la privacidad.
- Fomento de la Cultura Digital Responsable.
- Innovación.
- No discriminación.

Se crea un Sistema Nacional para la Ciberseguridad y Confianza Digital que será un instancia de coordinación, evaluación y deliberación. Conformado por:

- Consejo Nacional de Ciberseguridad: Define la política pública. Órgano colegiado que establece las políticas y estrategias nacionales en materia de ciberseguridad. Integrado por representantes del gobierno federal
- Comisión Consultiva de Ciberseguridad: Asesora al Consejo. Órgano de asesoramiento que proporciona orientación técnica y estratégica al Consejo Nacional de Ciberseguridad. Conformado por profesionales, especialistas y representantes de la sociedad civil. Ofrece análisis, recomendaciones y propuestas en materia de ciberseguridad.
- Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad: Ejecuta acciones operativas y técnicas. Entidad pública responsable de ejecutar las acciones operativas y técnicas para proteger la infraestructura digital del país. Brinda asistencia técnica, capacitación, investigación y desarrollo en materia de ciberseguridad. Coordina la operación de los centros de respuesta ante incidentes cibernéticos

La creación del Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad conlleva una serie de importantes razones y justificaciones que se centran en la optimización de recursos técnicos y humanos, así como en la eficiencia en el uso del presupuesto público.

A continuación, se detallan algunos puntos clave:

Su objetivo en conjunto será fortalecer, prevenir, detectar, mitigar y responder a las amenazas cibernéticas.

La transformación del INFOTEC en el nuevo Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad permitirá crear un Centro Público de Investigación del Gobierno Federal, que contribuya a la Transformación Digital de México, a través de la investigación, la innovación, la formación académica y el desarrollo de productos y servicios TIC. Sus alcances abarcan al sector público y privado, habilitando caminos que conduzcan hacia un México moderno y de inclusión digital.

Actuar como centro de referencia en ciberseguridad en México, proporcionando recursos y servicios especializados para proteger la información y los sistemas digitales del país.

Además de pertenecer a la red de Centros Públicos de Investigación (CPI) del Consejo Nacional de Humanidades, Ciencias y Tecnologías (Conahcyt).

Con esta medida, se logrará además:

- Consolidación de recursos: Al transformar el INFOTEC en el Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad, se aprovechan y consolidan los recursos técnicos y humanos ya existentes en el INFOTEC, lo que evita la duplicación de esfuerzos y recursos que podrían ocurrir si se estableciera una nueva entidad desde cero. Esto permite una transición más fluida y eficiente hacia un enfoque más especializado en ciberseguridad.

- Especialización en ciberseguridad: La creación del Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad refleja el reconocimiento de la importancia crítica de la ciberseguridad en el mundo actual, donde las amenazas cibernéticas están en constante evolución y representan riesgos significativos para la seguridad nacional, la economía y la sociedad en general. Al dedicar un instituto completo a este campo específico, se puede garantizar un enfoque más especializado y eficaz en la prevención, detección y respuesta a las amenazas cibernéticas.

- Aprovechamiento del conocimiento y experiencia existentes: El INFOTEC México ya cuenta con un personal altamente capacitado y con experiencia en áreas relacionadas con la tecnología de la información y la seguridad cibernética. Transformar esta institución en un Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad permite

aprovechar este conocimiento y experiencia acumulados a lo largo de los años, garantizando así una base sólida para abordar los desafíos en materia de ciberseguridad.

- Ahorro de presupuesto público: La transformación del INFOTEC en el Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad puede conducir a ahorros significativos en el presupuesto público al evitar la duplicación de funciones y estructuras administrativas. En lugar de financiar múltiples entidades con enfoques similares, consolidar recursos bajo un solo instituto especializado permite una asignación más eficiente de los fondos públicos, maximizando así el impacto y la efectividad de las iniciativas en ciberseguridad.

- Mejora de la coordinación y cooperación: Al centralizar las actividades relacionadas con la ciberseguridad en un único Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad, se facilita la coordinación y cooperación entre diferentes actores gubernamentales, instituciones académicas, sector privado y sociedad civil. Esto promueve una respuesta más efectiva y coordinada ante las amenazas cibernéticas, así como una colaboración más estrecha en el desarrollo de políticas, estándares y mejores prácticas en materia de ciberseguridad.

## Marco Regulatorio

En su Capítulo Cuarto, la propuesta incorpora un marco regulatorio que garanticen los siguientes derechos: a la privacidad digital, libertad de expresión, seguridad digital y acceso universal a internet.

Así como las siguientes obligaciones: como el respeto a los derechos de autor, uso responsable de internet, protección de datos personales, colaboración en la prevención de delitos cibernéticos y protección de niños, niñas y adolescentes.

Se crea un marco normativo para la prevención de amenazas y ataques cibernéticos, con distribución de competencias entre autoridades, mecanismos de monitoreo y detección de amenazas, y una Normateca de Ciberseguridad.

Lo anterior bajo una serie de mecanismos que faciliten la coordinación con medidas que den cumplimiento a:

- Compromisos internacionales: El marco regulatorio se basa en los compromisos internacionales de México en materia de ciberseguridad.
- Armonización con estándares internacionales: Se busca la coherencia y compatibilidad con los estándares y principios internacionales.
- Coordinación y cooperación: Se establecen mecanismos de coordinación entre las diferentes instituciones y actores involucrados en la ciberseguridad.
- Protección de infraestructuras críticas: Incorpora Criterios y estándares de seguridad, colaboración entre operadores y autoridades; así como ejercicios y simulacros de seguridad

**Combate al ciberdelito.**

En alineación con los derechos humanos consagrados en nuestra carta magna, este proyecto de Ley busca combatir el ciberdelito desde una perspectiva integral de prevención, reparación del daño y no ser de carácter punitiva, observando lo siguiente:

- Respeto a los derechos humanos en el ciberespacio:
- Se reconoce el derecho a la privacidad y protección de datos personales.
- Se prohíbe la difusión de información falsa, el acoso cibernético y la discriminación en línea.
- Se promueve la educación y la cultura digital responsable.
- Delimitación de delitos:
- Se define el delito cibernético y se tipifican diversas figuras delictivas.
- Se establecen penas y sanciones proporcionales a la gravedad del delito.
- Se fomenta la cooperación internacional en la investigación y persecución de los delitos cibernéticos.
- Figuras delictivas especializadas:
- Se crea la figura del perito en ciberseguridad.
- Se establece la figura del fiscal especializado en delitos cibernéticos.
- Se designan unidades especializadas dentro de las fuerzas de seguridad.
- Combate al ciberdelito:
- Se crea el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.
- Se fortalece la Guardia Cibernética para prevenir, investigar y combatir los delitos cibernéticos.

- Se establecen estrategias de prevención, investigación y persecución
- Cooperación Internacional y Estrategias de Prevención:
- Se crea el marco normativo para la coordinación de Equipos de Respuesta a Incidentes Cibernéticos (CIRT).
- Se establece el Banco de Datos de Incidentes Cibernéticos.
- Se promueve la adopción de mejores prácticas en ciberseguridad.
- Se fomenta la cooperación internacional en materia de ciberseguridad.

**Seguridad Nacional**

La propuesta legislativa garantiza la seguridad nacional y protección de la infraestructura crítica del país ante riesgos e incidentes cibernéticos. Tomando en consideración:

- Define: Riesgos e incidentes cibernéticos de seguridad nacional.
- Establece: La participación de la Secretaría de la Defensa Nacional en la protección y defensa del ciberespacio.
- Crea: Protocolos de colaboración entre autoridades civiles y militares.
- Identifica y clasifica: Infraestructura crítica del país.
- Establece: Medidas de protección y seguridad para infraestructuras críticas.
- Crea: Registro nacional de incidentes cibernéticos en infraestructuras críticas.
- Obliga: A las entidades responsables de las infraestructuras críticas a reportar incidentes cibernéticos.
- Define: El Consejo de Seguridad Nacional como responsable del registro nacional de incidentes cibernéticos.

**Fomento de la confianza digital:**

En este capítulo, la propuesta legislativa busca:

- Se garantiza el pleno respeto a los derechos humanos en el ciberespacio.
- Se prohíben la discriminación, el acoso y la violencia en línea.
- Se promueve la educación y la concientización sobre los derechos humanos en el ciberespacio.
- Se establecen mecanismos de protección y reparación para las víctimas de violaciones de derechos humanos en línea.
- Se promueve el uso seguro, responsable y ético de las tecnologías digitales.

- Se divulgan las medidas para garantizar la integridad, disponibilidad y confidencialidad de la información en línea.
- Se incentiva la colaboración entre el sector público, privado, sociedad civil y otros actores para mejorar la confianza digital.
- Se establecen mecanismos de evaluación y seguimiento para medir el nivel de confianza digital en el país.

**Prevención de campañas de desinformación:**

- Se establecen mecanismos para prevenir y contrarrestar la difusión de desinformación en línea.
- Se promueve la alfabetización mediática y digital, la verificación de datos y la promoción de fuentes de información fiables y transparentes.
- Se establecen protocolos de actuación para la detección y el seguimiento de campañas de desinformación.
- Se promueve la transparencia y la rendición de cuentas en la información en línea.
- Se fomenta la educación y el pensamiento crítico entre los usuarios de Internet.

**Uso ético de tecnologías emergentes:**

Se promueve el uso ético y responsable de tecnologías como la inteligencia artificial y el metaverso, protegiendo derechos y dignidad de las personas, y fomentando el bienestar social y desarrollo sostenible.

Establece principios éticos para el desarrollo, implementación y uso de tecnologías emergentes e incorpora un modelo de regulación sandbox para nuevos desarrollos, para:

- Fomentar la investigación y desarrollo de tecnologías emergentes que beneficien a la sociedad.
- Promover el diálogo y la colaboración entre diferentes actores para abordar los riesgos y desafíos éticos asociados a estas tecnologías.
- Incorporar principios de privacidad y seguridad por diseño en el desarrollo e implementación de sistemas y servicios digitales.
- Promover la adopción de medidas técnicas y organizativas para garantizar la privacidad y seguridad de la información.

- Establecer estándares y mejores prácticas para la protección de datos y la seguridad de la información.

**Educación, Capacitación y Cultura Digital**

En este rubro la iniciativa busca fomentar la educación y sensibilización sobre la importancia de la privacidad y seguridad de la información, promoviendo una cultura de protección de datos y seguridad digital en la sociedad.

Objetivos:

- Implementar programas de concientización y capacitación en ciberseguridad para todos los niveles de la sociedad mexicana.
- Desarrollar materiales educativos, campañas de sensibilización y actividades de formación en ciberseguridad.
- Fomentar la colaboración con instituciones educativas, organizaciones de la sociedad civil, el sector privado y otros actores relevantes.
- Establecer programas de capacitación en ciberseguridad dirigidos a diferentes poblaciones en México.
- Integrar contenidos de ciberseguridad en los programas educativos de todos los niveles.
- Establecer estrategias integrales de concientización y promoción de una cultura de ciberseguridad en México.
- Desarrollar programas de capacitación en ciberseguridad para comunidades indígenas, personas con discapacidad y otros grupos vulnerables.
- Promover la colaboración con organizaciones indígenas, asociaciones de personas con discapacidad y grupos de la sociedad civil.
- Establecer mecanismos de seguimiento y evaluación de los programas de capacitación.

El principio de progresividad garantizará que las organizaciones puedan mejorar continuamente su postura de ciberseguridad a lo largo del tiempo, mediante la implementación gradual de medidas adicionales y la actualización periódica de sus sistemas y procesos en respuesta a las nuevas amenazas y vulnerabilidades identificadas.

Integrar a expertos en diferentes áreas relacionadas con la ciberseguridad, incluyendo aspectos técnicos, legales, educativos y de investigación, para abordar de manera integral los desafíos en este campo.

Esta propuesta legislativa refleja un esfuerzo colaborativo por adaptar el marco legal a los avances tecnológicos, protegiendo los derechos humanos en la era de la neurociencia. Se establecen medidas adicionales para garantizar la confidencialidad y seguridad de los datos neuronales durante la comunicación entre autoridades y en todo el proceso judicial. En conjunto, estas modificaciones refuerzan la protección de la intimidad, la privacidad y la dignidad de las personas frente al uso de ciberseguridad en el ámbito penal.

Considerando la innegable influencia de los avances científicos y su impacto en todos los campos del conocimiento, se requiere actualizar y armonizar las normas tanto de derecho internacional como aquellas internas de los Estados que rigen los procesos de convivencia social para que el ámbito legal responda a su función reguladora y sancionadora de forma armónica, considerando para ello la aplicación conjunta de reglas, estándares, lineamientos y normas, que respondan a las recientes necesidades sociales, regulando acertada y suficientemente cada uno de los fenómenos, relaciones o actividades humanas que impactan la vida cotidiana, trazando de forma transversal el camino a seguir de las innumerables actividades donde éstas se encuentren inmersas.

Desde esta perspectiva, en algunos países, el derecho penal cuya función primordial es la protección de bienes jurídicos, debe adaptarse al avance tecnológico y en su caso seguir los avances de otras regulaciones marco para atender no solamente la exacta aplicación de la ley penal, sino contar con los elementos necesarios para describir los elementos positivos del delito, así como objetivos, normativos y subjetivos del tipo penal.

Esto implica atender a nuevos paradigmas de protección, identificar conductas indebidas o no autorizadas, reconsiderar las penas y sanciones establecidas y en su caso determinar la incorporación de nuevos tipos penales, siempre y cuando esto sea necesario.

Además, es imprescindible trabajar con una visión más amplia en cuanto a los daños que causan los diversos incidentes que México ha sufrido donde pueda dimensionar el impacto económico a corto, mediano y largo plazo, para que con ellos se puedan crear no solo las políticas públicas, sino las políticas criminales que sean suficientes, necesarias e integrales, sostenidas en visiones multifactoriales e interdisciplinarias para su aplicación.

En este orden de ideas, es necesario puntualizar que la política criminal, se encuentra sostenida en el artículo 21 Constitucional, donde se establece de forma expresa lo siguiente:

*"... La investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función...".*

Y en concordancia con lo anterior, la Ley General del Sistema Nacional de Seguridad Pública, en artículo 2, establece que:

"... La seguridad pública es una función a cargo de la Federación, las entidades federativas y municipios, que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos y comprende la prevención especial y general de los delitos, la sanción de las infracciones administrativas, así como la investigación y la persecución de los delitos y la reinserción social del sentenciado, en términos de esta Ley, en las respectivas competencias establecidas en la Constitución Política de los Estados Unidos Mexicanos...".

Por tanto, resulta primordial, que las disposiciones en materia de ciberdelitos, se ajusten a la normativa penal, pues ello refleja las realidades a las que se enfrentan los Estados.

Asimismo, resulta necesario robustecer las capacidades de las autoridades encargadas de la investigación, procuración e impartición de justicia en nuestro país.

Lo cual permita a corto y mediano plazo, contar con una mayor colaboración a nivel internacional, pues al ser conductas que trascienden el ámbito territorial, la asistencia por parte de otros países en las labores de investigación y sanción, permitirán contar con una mayor eficacia en la impartición de justicia respecto de este tipo de delitos.

A continuación, se presenta un desglose de las propuestas atendiendo las categorías (capítulos) correspondientes en el Código Penal Federal vigente.

## EN MATERIA DE DELITOS A LAS VÍAS DE COMUNICACIÓN Y CORRESPONDENCIA

En materia de ciberseguridad, cobran también relevancia aquellos ilícitos con mayor recurrencia en las redes de comunicación y telecomunicación inalámbricas en detrimento de los derechos fundamentales de las personas. Por lo anterior, esta iniciativa propone agregar tres fracciones y dos incisos al Artículo 168 Bis a efecto de integrar al Código Penal Federal tipos penales que sancionen todo tipo de conducta que propicie el uso ilícito de dispositivos que intervengan sin anuencia del o los interesados, señales de comunicaciones privadas, geolocalización o datos de navegación en internet, así como de contraseñas, códigos de acceso o datos informáticos.

De igual forma se propone sancionar aquellas conductas que posibiliten el uso indebido de dispositivos, programas de computación especializados en señales, redes y aplicativos de cualquier aparato portátil o casero que atenten contra la privacidad, confidencialidad, integridad, disponibilidad de la información y sistemas informáticos.

## EN MATERIA DE DELITOS DE VIOLACIÓN DE CORRESPONDENCIA

En materia de ciberdelitos cobran también relevancia aquellas conductas ilícitas, en las redes de comunicación y telecomunicación inalámbricas en detrimento de los derechos fundamentales de las personas.
Por lo anterior, esta iniciativa propone agregar tres fracciones y dos incisos al Artículo 168 Bis a efecto de integrar al Código Penal Federal tipos penales que sancionen todo tipo de conducta que tenga como finalidad el uso delictivo de dispositivos.

De igual forma se propone sancionar aquellas conductas que posibiliten el uso delictivo de dispositivos, programas de computación especializados en señales, redes y aplicativos de cualquier aparato portátil o casero que atenten contra la privacidad, confidencialidad, integridad, disponibilidad de la información y sistemas informáticos.

## EN MATERIA DE DELITOS DE CORRUPCIÓN Y DE PORNOGRAFÍA DE MENORES DE 18 AÑOS O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA COMPRENDER EL SIGNIFICADO DEL HECHO O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA RESISTIRLO.

El uso masificado de las TIC ha traído consigo la evolución de las prácticas de delincuencia, particularmente en ámbitos tan sensibles y graves como la pornografía infantil. La pornografía infantil es definida por la UNICEF como la representación material -por vía de película, impresión, foto, audio o video-grabación y representaciones digitales computarizadas- de niños, niñas y adolescentes

realizando actos sexuales reales o simulados para la gratificación sexual de los usuarios, incluyendo la producción.[18]

En el contexto actual, a través del uso de herramientas de edición y sobreposición de rostros, el delito de pornografía infantil ha evolucionado a tal grado que se puede manipular con herramientas de edición, ya fotografías o videos como *deep fakes* (videos pornográficos modificados utilizando tecnología de intercambio de caras a través de inteligencia artificial, por lo que el rostro del protagonista se reemplaza por el de otra persona.)

En función de lo anterior, se propone una modificación al artículo 200, para sancionar a aquellas personas que produzcan, almacenen, difundan o transmitan a menores de dieciocho años, cualquier tipo de material enunciado en el artículo 200 a través también de medios electrónicos, virtuales, digitales o dispositivos de almacenamiento de datos informáticos.

**EN MATERIA DE DELITOS DERIVADOS DEL ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**

La incidencia de ataques informáticos ha ido en aumento, subrayando con ello la necesidad de su regulación legal. EN MATERIA DE DELITOS DERIVADOS DEL ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Uno de los factores que deben superarse para contar con una adecuada política criminal en materia de tecnologías de la información y comunicación, se debe en parte a la confusión de terminologías en el ámbito de aplicación de las normativas que hoy día México cuenta, y esto ha favorecido la "incertidumbre" que se traduce en una falsa creencia de inexistencia de obligatoriedad para denunciar los hechos delictivos de esta naturaleza.

El resultado de lo anterior, ha provocado una inadecuada atención oportuna a incidentes, generando las siguientes situaciones:

a) Se considera que la atención legal de un incidente aumenta el costo (jurídico, patrimonial y reputacional) al acudir ante las autoridades para denunciar el hecho, si es que se decide iniciar esta acción.

b) Se piensa que las policías no tienen las capacidades para investigar este tipo de delitos.

c) En caso de identificar a un probable responsable del incidente, el llamado "insider", se considera también un costo el ejercicio de los actos de investigación y se prefiere llegar a algún tipo de acuerdo que no vaya a generar alguna demanda de

[18] Infancia robada, UNICEF, https://www.unicef.org/mexico/spanish/mx_resources_infancia_robada.pdf

carácter laboral y en este proceso judicial evidenciar el ataque a la organización, pues se tendría que aportar la evidencia digital correspondiente, la cual seguramente no fue generada o bien, ya no cumple con los estándares correspondientes para poder presentarla ante la autoridad.

d) Para aquellos responsables de haber sido omisos en la operación de las herramientas de seguridad, se les retira del cargo y se entrega algún tipo de "indemnización", con tal de ahorrarse un proceso judicial que consuma recursos humanos y tiempo.

e) En el caso de que se decida denunciar, no se realiza bajo una perspectiva de política criminal, debido a que se acude ante el agente del ministerio público para "evadir" la responsabilidad de un incidente, o bien, únicamente se da parte de este hecho a la autoridad con el objetivo de cubrir uno de los requisitos que se requieren para ejercer la póliza de seguro que auxiliará en el pago de los costos generados con motivo de la gestión del incidente.

f) Además de que el adecuado resguardo de la evidencia digital, se torna una carga en su correcta entrega, se inicia pensando que la existencia de una acción judicial es para señalar únicamente a un responsable, y no se prevén el resto de las consecuencias legales en otras materias como aquellas vinculadas con contratos o actividades mercantiles, hacendarias etc.

Todo ello trae como consecuencia directa un aumento en la impunidad y un fomento indirecto de la economía del cibercrimen.

Como consecuencia, se hace cada vez más necesario un perfil de usuario más atento, con más herramientas para hacer un uso responsable y consciente de la tecnología, que sepa, no solo cómo protegerse, sino además que conozca los riesgos que conlleva subir información a la nube.[19]

México se ha convertido en un referente de ciberataques a nivel mundial. Cifras recientes detallan que en 2018, México sufrió más de 21.000 intentos de descargar o difundir *ransomware* , y que ha sido el punto de origen de más del 60% de los ataques de este tipo en América Latina.[20]

En México, la usurpación de identidad aumenta día con día, según datos del Banco de México, nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos, se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria. Comúnmente, desemboca en ilícitos tales como abrir cuentas de crédito, contratar

[19] TENDENCIAS 2019: Privacidad e intrusión en la aldea global, ESET, https://www.welivesecurity.com/wp-content/uploads/2018/12/Tendencias-Ciberseguridad-2019-ESET.pdf
[20] FortiGuardLabs Research Center, https://fortiguard.com/, Marzo 2019

líneas telefónicas, seguros de vida, realizar compras e incluso, en el cobro de seguros de salud, vida y pensiones.[21]

En virtud de lo anterior, se propone sancionar a quien sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información o datos informáticos contenidos en equipos, redes, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos por algún mecanismo de seguridad físico y/o digital en los términos del primer párrafo del artículo del artículo 211 bis 1.

Adicionalmente, se propone sancionar a quien sin autorización modifique, cause daño u obstaculice por cualquier medio o método, el funcionamiento de equipos o sistemas informáticos protegidos contra el acceso no autorizado. en los términos del segundo párrafo del referido artículo.

Se propone adicionar un tercer párrafo a dicho artículo 211 bis 1 a fin de sancionar a sin autorización, por cualquier medio o método, modifique, dañe, deteriore, suprima o provoque la pérdida parcial o total de información o datos informáticos contenidos en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos contra el acceso no autorizado, imponiéndose de uno a tres años de prisión y multa de ciento cincuenta a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente.

Respecto al artículo 211 Bis 2 se propone sancionar a quien sin autorización altere, modifique, destruya o provoque por cualquier medio o método, la pérdida, inaccesibilidad, parcial, o total de información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, protegidos por algún mecanismo de seguridad.

Al que por cualquier medio o método, sin autorización o excediendo de la autorización que posea de la persona física o moral que legalmente pueda otorgarlo, dolosamente acceda, conozca, copie, extraiga, reproduzca modifique, altere, destruya o elimine la información provocando la pérdida de la confidencialidad, integridad y disponibilidad de la misma contenida en equipos, sistemas o medios informáticos, electrónicos o telemáticos, que estén protegidos por un mecanismo de seguridad físico o lógico.

Por autorización deberá entenderse el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido.

**INTERCEPTACIÓN ILÍCITA.**

[21] Robo de identidad un delito en aumento, Condusef, https://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf

la interceptación deliberada y sin derecho, por medios técnicos, de transmisiones no públicas de datos electrónicos a un sistema de tecnología de la información y las comunicaciones, desde él o dentro de él, incluidas las emisiones electromagnéticas provenientes de un sistema de tecnología de la información y las comunicaciones que transportan esos datos electrónicos

**INTERFERENCIA CON UN SISTEMA DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES.**

La obstaculización grave, deliberada y sin derecho del funcionamiento de un sistema de tecnología de la información y las comunicaciones mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos electrónicos.

Otra adición a este artículo consiste en sancionar a quien sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, infringiendo medidas de seguridad con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático en los términos señalados en dicho precepto.

Por cuanto concierne al artículo 211 Bis 3, se propone adicionar al tipo penal existente al que, estando autorizado para acceder a equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, del Estado, indebidamente, por cualquier medio o método altere, modifique, extraiga, destruya, dañe, deteriore, suprima o provoque pérdida parcial o total de información contenida en dichos equipos, sistemas o medios de almacenamiento del Estado, se hará acreedor a las sanciones señaladas en el primer párrafo. Respecto al segundo párrafo también se sancionará en los términos señalados, al que estando autorizado, indebidamente copie o reproduzca información contenida en equipos, sistemas o medios de almacenamiento, físicos o virtuales del Estado. Finalmente, en el párrafo tercero se agregan medios de almacenamiento informáticos físicos o virtuales, en donde se extraiga o facilite información indebidamente.

Respecto el Artículo 211 Bis 4 primer párrafo se agrega al que sin autorización cause daño, altere u obstaculicen, por cualquier medio o método, el funcionamiento de sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad físico y/o digital ahí señalados se hará acreedor a la sanción correspondiente. Respecto al segundo párrafo se agrega que al que sin autorización, por cualquier medio o método, modifique, altere, deteriore, suprima, destruya o provoque la pérdida parcial o total de información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema

financiero, protegidos por algún mecanismo de seguridad, se le impondrán las sanciones ahí señaladas.

Se agrega un tercer párrafo que establece que al que sin autorización acceda, conozca, copie, extraiga, reproduzca, o difunda, para beneficio propio o de un tercero, por cualquier medio o método, información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y multa de cien a seiscientos días.

En el Artículo 211 Bis 5 se agrega que al  al que estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero indebidamente altere, modifique, destruya, inhiba, bloquee o provoque pérdida parcial o total de información contenida en sistemas o equipos de informática por cualquier mecanismo o método, se le impondrán las sanciones señaladas en el párrafo primero. Respecto al segundo párrafo se agrega que al quien estando autorizado para acceder sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales de las instituciones que integran el sistema financiero, indebidamente copie, extraiga, reproduzca, o difunda información, para beneficio propio o de un tercero, se le impondrán las sanciones ahí señaladas.

Se agrega un nuevo tipo penal en el Artículo 211 Ter referido a la falsificación informática para quedar en los siguientes términos:

> *Se le impondrán de cuatro a ocho años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización introduzca, altere, borre o suprima datos informáticos que generen datos no auténticos con la intención de que sean tomados o utilizados como auténticos para efectos legales, con independencia de que los datos sean directamente legibles e inteligibles.*
>
> *Se impondrá pena de cuatro a diez años de prisión y multa de doscientos a quinientos de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente en los casos siguientes:*
>
> *a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito, lucrar; y,*
>
> *b) Cuando los actos descritos en el inciso anterior se realicen para inducir a usuarios a la provisión de datos confidenciales*, personales y/o financieros, tanto de personas físicas como de personas morales.

También se agrega el Artículo 211 Quáter, el cual es especialmente importante ya que por fin se introduce a nivel federal, luego de haber estado regulado desde hace algunos años en los Códigos Penales locales, el delito de Usurpación de Identidad con la siguiente redacción:

> *Se le impondrán de uno a cuatro años de prisión y multa de cien a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien usurpe la identidad de otra persona, a través de un sistema o medio informático, o infringiendo medidas de seguridad físicas o digitales, con la intención de causar un daño o perjuicio a una persona, u obtener un beneficio indebido, para sí mismo o para otra persona.*
>
> *Las penas señaladas en este artículo se incrementarán hasta en una mitad cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su formación, profesión o empleo para ello.*

## EN MATERIA DE DELITOS DE FRAUDE

El delito de fraude es uno de los que más se ha visto robustecido a través del uso ilícito de la informática, incrementando el número de víctimas, de beneficios económicos e impunidad de quienes los cometen. En la Iniciativa se agregan dos fracciones al artículo 387 del Código Penal Federal para quedar de esta forma: *"Las mismas penas señaladas en el artículo anterior, se impondrán:*

*I. a XXI. …*

***XXII.** Al que causare un perjuicio patrimonial a otro, mediante la introducción, alteración, borrado o supresión de datos informáticos.*

*Asimismo, a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.*

***XXIII.** A quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.*

## EN MATERIA DE DELITOS DE DERECHOS DE AUTOR

Finalmente, y considerando que de acuerdo con la Encuesta Global de Software 2018 elaborada por la Business Software Alliance (BSA) generó pérdidas anuales en 2017 en nuestro país por 760 millones de dólares y que por otro lado arrojó que

un 49% del software que se usa en nuestro país carece de licencia legal, es necesario realizar una actualización en materia de delitos autorales proponiendo una adición a la fracción II del Artículo 424 bis para quedar como sigue: "Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. ...

II. A quien fabrique con fin de lucro un dispositivo o sistema físico o digital, cuya finalidad sea desactivar, inhibir o alterar los dispositivos electrónicos de protección de un programa de computación.

## PROGRAMAS DE CAPACITACIÓN PERMANENTES

Uno de los aspectos más importantes en las acciones para hacer frente a la ciberdelincuencia es el contar con instituciones capaces de investigar, perseguir, asegurar evidencia electrónica y juzgar el cibercrimen.
En ese sentido, organismos como el Consejo de Jueces Europeos han establecido que es esencial que las y los jueces, además de realizar sus estudios en derecho, reciban capacitación detallada y diversa para que puedan realizar sus labores efectivamente.[22] Asimismo, el Índice de Ciberseguridad de la Unión Internacional de Telecomunicaciones integra a la construcción de capacidades como uno de sus 5 pilares. La construcción de capacidades incluye, entre otros elementos, el análisis de la existencia de programas de capacitación en el país[23].

Por ello, se proponen dos transitorios para establecer que:

- La Fiscalía General de la República y la Guardia Nacional, deberán implementar un programa permanente de capacitación especializada en materia de ciberseguridad y ciberdelincuencia dirigido a las autoridades y personal de las entidades gubernamentales federales responsables de la denuncia e investigación de los delitos en la materia; y que

- El Consejo de la Judicatura Federal deberá implementar un programa permanente de capacitación judicial continua y especializada en materia de ciberseguridad y ciberdelincuencia dirigido a las autoridades de los órganos jurisdiccionales federales responsables en sancionar los delitos en la materia.

A continuación se detallan los cambios propuestos al código penal federal en la iniciativa:

---

[22] "Cybercrime training for judges and prosecutors: a concept" Project on Cybercrime and Lisbon Network. Council of Europe. October 8th, 2009.
https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybercrime%20training%20for%20judges%20and%20prosecutors.pdf
[23] Global Cybersecurity Index. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

| CÓDIGO PENAL FEDERAL | |
|---|---|
| **Legislación vigente** | **Propuesta de modificación** |
| **Artículo 168 bis.-** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:<br><br>I. al II. ... | **Artículo 168 Bis.-** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien deliberada e ilegítimamente:<br><br>I. al II. ...<br><br>III. Produzca, venda, obtenga para su utilización, arriende, importe, difunda o que mediante cualquier otra forma ponga a disposición:<br><br>a) Dispositivos, incluidos programas informáticos diseñados o adaptados principalmente para la intervención de comunicaciones privadas, geolocalización o la interceptación de datos de navegación en internet sin consentimiento;<br>b) Contraseñas, códigos de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático sin consentimiento.<br><br>IV. Produzca, venda, obtenga para su utilización, arriende, difunda o que mediante cualquier otra forma ponga a disposición dispositivos electrónicos, programas informáticos o tecnologías de comunicación que permitan la obtención encubierta de datos, información confidencial o que atenten contra la privacidad.<br><br>V. Posea alguno de los elementos contemplados en la fracción anterior, con la intención de ser utilizados para cometer ilícitos relacionados con la violación de confidencialidad, integridad, privacidad y disponibilidad de la información y sistemas informáticos. |
| **Artículo 177.-** A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. | **Artículo 177.-** Se impondrán de seis a doce años de prisión y multa de trescientos a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien, sin mandato de autoridad judicial competente, |

| | |
|---|---|
| | intercepte o intervenga comunicaciones privadas o los datos transmitidos a través de las redes o servicios públicos de telecomunicaciones o por cualquier medio o método, datos informáticos en transmisiones dirigidas a un sistema o equipo informático, originadas desde otro sistema o equipo, o realizadas dentro del mismo, incluidas las emisiones electromagnéticas y radiofrecuencias provenientes de un sistema o equipo informático que transporte dichos datos informáticos.<br><br>La pena prevista en este artículo se duplicará para el caso de servidores públicos que en ejercicio de sus funciones o aprovechando su cargo, ordenen, permitan, autoricen o realicen las conductas señaladas en este artículo, además de la privación del cargo y la inhabilitación para ocupar otro hasta por cinco años. |
| **Artículo 199 Septies.-** Se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil días multa a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo y le requiera imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual. | **Artículo 199 Septies.-** Se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil días multa a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo y le requiera imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual.<br><br>**Se impondrá la misma sanción a quien haciendo uso de sistemas, software, y/o herramientas basados en inteligencia artificial, cree audios, fotografías o videos de índole sexual, en las que simulen aparecer personas que correspondan a las señaladas en el párrafo anterior.** |
| **Artículo 199 Octies.-** Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo | **Artículo 199 Octies.-** Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique |

| | |
|---|---|
| sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.<br><br>Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.<br><br>Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización. | imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.<br><br>Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.<br><br>**Se impondrá la misma sanción a quien haciendo uso de sistemas, software, y/o herramientas basados en inteligencia artificial, cree audios, fotografías o videos de índole sexual, en las que simulen aparecer personas que correspondan a las señaladas en el párrafo anterior.**<br><br>Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización. |
| **Artículo 200.-** Al que comercie, distribuya, exponga, haga circular u oferte, a menores de dieciocho años de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales o simulados, sea de manera física, o a través de cualquier medio, se le impondrá de seis meses a cinco años de prisión y de trescientos a quinientos días multa.<br><br>.... | **Artículo 200.-** Se impondrán de seis meses a cinco años de prisión y multa de trescientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, **a quien financie, comercie, distribuya, exponga, ponga en circulación, oferte, difunda o transmita a menores de edad,** libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales, simulados o creados por medios tecnológicos, sea de manera física, o a través de cualquier medio **electrónico, digital o de dispositivos de almacenamiento de datos informáticos.**<br><br>... |
| **Sin correlativo** | **Artículo 200 Bis.- Comete el delito de acoso cibernético quien utiliza la tecnología para amenazar, intimidar, acosar o humillar a alguien con la intención de dañarlo social, psicológica o físicamente. A quien cometa el delito de acoso cibernético se le impondrán de seis meses a cinco años de prisión y multa de trescientos a quinientas veces el** |

| | |
|---|---|
| | **valor diario de la Unidad de Medida y Actualización vigente.** |
| **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. | **Artículo 211 Bis 1.-** Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, **a quien** sin autorización **acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método,** información **o datos informáticos contenidos en equipos, redes, sistemas o medios de almacenamiento informáticos, físicos o virtuales**, protegidos por algún mecanismo de seguridad **físico y/o digital.** |
| 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. | Se le impondrán de tres meses a un año de prisión y multa de cincuenta a ciento cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **modifique, cause daño u obstaculice por cualquier medio o método, el funcionamiento de equipos o sistemas informáticos protegidos contra el acceso no autorizado.** |
| **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. | **Artículo 211 Bis 2.-** Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **altere,** modifique, destruya o provoque **por cualquier medio o método,** la pérdida, **inaccesibilidad, parcial, o total de** información contenida en equipos, **sistemas o medios de almacenamiento informáticos, físicos o virtuales** del Estado, protegidos por algún mecanismo de seguridad. |
| Al que sin autorización conozca o copie información contenida en sistemas o 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. | Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **acceda,** conozca, copie, **extraiga o reproduzca por cualquier medio o método,** información contenida en **equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales** del Estado, **infringiendo medidas de seguridad con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema** |

| | |
|---|---|
| | **informático conectado a otro sistema informático,** 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.<br><br>... | Se le impondrán de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización **acceda**, conozca, obtenga, copie, **extraiga** o utilice información contenida **en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales** de seguridad pública, protegidos por algún mecanismo de seguridad.Si el responsable es o hubiera sido servidor público en una institución de seguridad pública **o de justicia penal, se le destituirá** y se le impondrá una inhabilitación de cuatro a diez años para desempeñarse **en otro cargo público.**<br><br>... |
| **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.-** Se le impondrán de dos a ocho años de prisión y multa de trescientos a novecientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que, estando autorizado para acceder a equipos, sistemas **o medios de almacenamiento informáticos, físicos o virtuales,** del Estado, indebidamente, **por cualquier medio o método altere,** modifique, **extraiga,** destruya, **dañe, deteriore, suprima, encripte o** provoque pérdida **parcial o total** de información **contenida en dichos equipos, sistemas o medios de almacenamiento del Estado.** |
| 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. | Se le impondrán de uno a cuatro años de prisión y multa de ciento cincuenta a cuatrocientos cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado, **indebidamente copie o reproduzca información contenida en equipos, sistemas o medios de almacenamiento, físicos o virtuales del Estado.** |
| A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice | Se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización |

| | |
|---|---|
| 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. | vigente, a quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, **físicos o virtuales,** en materia de seguridad pública, indebidamente obtenga, **extraiga,** copie, **facilite** o utilice información que contengan. 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 establecida, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en **otro cargo público.** |
| **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.<br><br>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 mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. | **Artículo 211 Bis 4.-** Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **cause daño, altere u obstaculice, por cualquier medio o método, el funcionamiento de sistemas o equipos de informática** de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad **físico y/o digital.**<br><br>Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización, **por cualquier medio o método, modifique, altere, deteriore, suprima, encripte, destruya o provoque la pérdida parcial o total de información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales,** de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.<br><br>**Se le impondrán de tres meses a dos años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga, reproduzca, o difunda, para beneficio propio o de un tercero, por cualquier medio o método, información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que** |

| | |
|---|---|
| | **integran el sistema financiero, protegidos por algún mecanismo de seguridad.** |
| **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.<br><br>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.<br><br>... | **Artículo 211 Bis 5.-** Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder a sistemas, **equipos o medios de almacenamiento informáticos, físicos o virtuales,** de las instituciones que integran el sistema financiero indebidamente **altere,** modifique, destruya, **inhiba, bloquee** o provoque pérdida **parcial o total** de información **contenida en sistemas o equipos de informática por cualquier mecanismo o método.**<br><br>Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder sistemas, equipos **o medios de almacenamiento informáticos, físicos o virtuales** de las instituciones que integran el sistema financiero, indebidamente copie, **extraiga, reproduzca, o difunda información, para beneficio propio o de un tercero.**<br><br>... |
| Sin correlativo | **Artículo 211 Ter.- Se le impondrán de cuatro a ocho años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización introduzca, altere, borre o suprima datos informáticos que generen datos no auténticos con la intención de que sean tomados o utilizados como auténticos para efectos legales, con independencia de que los datos sean directamente legibles e inteligibles.**<br><br>**Se impondrá pena de cuatro a diez años de prisión y multa de doscientos a quinientos de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente en los casos siguientes:** |

| | |
|---|---|
| | **a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito, lucrar; y,**<br><br>**b) Cuando los actos descritos en el inciso anterior se realicen para inducir a usuarios a la provisión de datos confidenciales, personales y/o financieros, tanto de personas físicas como de personas morales.** |
| Sin correlativo | **Artículo 211 Quáter.- Se le impondrán de uno a cuatro años de prisión y multa de cien a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien usurpe la identidad de otra persona, a través de un sistema o medio informático, o infringiendo medidas de seguridad físicas o digitales, con la intención de causar un daño o perjuicio a una persona, u obtener un beneficio indebido, para sí mismo o para otra persona.**<br><br>**Las penas señaladas en este artículo se incrementarán hasta en una mitad cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su formación, profesión o empleo para ello.** |
| **Artículo 387.-** Las mismas penas señaladas en el artículo anterior, se impondrán: | **Artículo 387.-** Las mismas penas señaladas en el artículo anterior, se impondrán:<br><br>I. a XXI. ...<br><br>**XXII. Al que causare un perjuicio patrimonial a otro, mediante la introducción, alteración, borrado o supresión de datos informáticos.**<br><br>**Asimismo, a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.**<br><br>**XXIII. A quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.** |

| | |
|---|---|
| **Artículo 390.-** Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa.<br><br>... | **Artículo 390.-** Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa.<br><br>...<br><br>**Las penas previstas en este artículo se duplicarán si el constreñimiento se realiza a través de un medio de comunicación digital o electrónica.**<br><br>**Las penas previstas en este artículo se triplicarán si la extorsión es con motivo de la divulgación de contenido íntimo sexual de una persona, real o simulado.** |
| **Artículo 403.-** Se impondrán de veinte a doscientos días multa y prisión de uno a seis años, a quien:<br><br>I. a III. (...)<br><br>IV. Obstaculice o interfiera dolosamente el desarrollo normal de las votaciones, el escrutinio y cómputo, el traslado y entrega de los paquetes y documentación electoral, o el adecuado ejercicio de las tareas de los funcionarios electorales;<br><br>... | **Artículo 403.- Se impondrán de veinte a doscientos días multa y prisión de uno a seis años, a quien:**<br><br>**I. a III. (...)**<br><br>IV. Obstaculice, **impida** o interfiera dolosamente, **de manera física o virtual, la organización y** el desarrollo normal de las votaciones, el escrutinio y cómputo, el traslado y entrega de los paquetes y documentación electoral, el adecuado ejercicio de las tareas de los funcionarios electorales, **o que pretenda alterar los resultados de las elecciones;**<br><br>**...** |
| **Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:<br><br>I. ...<br><br>II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación. | **Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:<br><br>I. ...<br><br>II. A quien fabrique con fin de lucro un dispositivo o sistema **físico o digital,** cuya finalidad sea desactivar, inhibir o alterar los dispositivos electrónicos de protección de un programa de computación. |

Por lo anterior, es fundamental que la Ley cuente con instrumentos capaces de establecer las condiciones mínimas para la ciberseguridad de manera que, únicamente se empleen en aras de mejorar las condiciones de vida de las personas.

Además, busca garantizar la protección, confidencialidad y privacidad en el tratamiento de los datos personales sensibles, haciendo posible la autonomía, la identidad, y la integridad personal; y promoviendo la igualdad y acceso equitativo a la ciencia y la tecnología.

Por su parte, no cabe duda que el desarrollo de las tecnologías emergentes debe ser progresiva, por lo que, en ningún momento debe implicar una amenaza o peligro a los derechos humanos. En ese sentido, esta iniciativa provee un marco jurídico de protección a las personas ante los avances científicos y tecnológicos que inciden en su esfera más personal e íntima.

## PROYECTO DE DECRETO

**PRIMERO: SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD Y CONFIANZA DIGITAL, PARA QUEDAR COMO SIGUE:**

### LEY FEDERAL DE CIBERSEGURIDAD Y CONFIANZA DIGITAL

### Título Primero

### Disposiciones Generales

### Capítulo Único

**Artículo 1. Ley es de orden público, interés social, de observancia general en todo el territorio nacional; y tiene por objeto establecer un marco regulatorio integral en el uso y aplicación de las tecnologías de la información y las comunicaciones digitales, y tecnologías emergentes en México, con la finalidad de garantizar la ciberseguridad y promover la confianza en su utilización, de conformidad con las obligaciones establecidas en la Constitución Política de los Estados Unidos Mexicanos.**

**Este marco se centrará en proteger y fomentar la resiliencia de las infraestructuras críticas y esenciales identificadas, incluyendo los sectores de energía, salud, transporte y servicios financieros, y se fundamentará en un enfoque basado en riesgos para adaptar las medidas de seguridad a las necesidades específicas de cada sector.**

**Artículo 2. Son objetivos de esta Ley:**

I. **Establecer los principios y procedimientos a los que deberán sujetarse los entes públicos a fin de garantizar la seguridad en uso de las tecnologías de la información y comunicaciones.**

II. **Asegurar que todas las actividades que se realizan en línea y las medidas de ciberseguridad, respeten los derechos humanos y se realicen con consideraciones éticas, garantizando que las medidas implementadas no infrinjan los derechos fundamentales de las personas.**

III. **Señalar las obligaciones de los organismos que conforman la Administración Pública Federal, centralizada y paraestatal, y organismos constitucionales autónomos en materia de seguridad en el uso de las tecnologías de la información y comunicaciones;**

IV. **Establecer la competencia de las autoridades en materia de ciberseguridad, delimitando sus responsabilidades y facultades para asegurar una coordinación efectiva y una respuesta adecuada ante incidentes cibernéticos**

V. **Coordinar la colaboración de las autoridades competentes con otros organismos del Estado y la promoción de la cooperación internacional en materia de ciberseguridad;**

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

VII. **Desarrollar y establecer un marco normativo integral que promueva la transparencia, responsabilidad y ética en el manejo de la información y los datos digitales, a fin de combatir la desinformación y fortalecer la ciberseguridad, garantizando la protección de los derechos digitales y la confianza en el entorno digital.**

VIII. **Fomentar el desarrollo de la resiliencia en las infraestructuras críticas contra incidentes cibernéticos, incluidos ciberataques, garantizando la continuidad y recuperación efectiva de los servicios esenciales en situaciones adversas.**

IX. Impulsar la innovación y la investigación tecnológica en ciberseguridad, en colaboración con entidades académicas y el sector privado, para desarrollar nuevas tecnologías y métodos avanzados de protección.

X. Promover el desarrollo y la adopción de estándares nacionales e internacionales de ciberseguridad, así como esquemas de certificación para productos, servicios y procesos de Tecnologías de la Información y la Comunicación, con el fin de mejorar la calidad, confiabilidad y seguridad del ecosistema digital.

XI. Promoción de la educación y la concienciación pública en ciberseguridad dirigidos a todos los niveles de la sociedad, fortaleciendo el conocimiento general sobre los riesgos y las mejores prácticas en el ciberespacio.

Artículo 3. El objeto a que se refiere esta ley se sujetará a los siguientes principios:

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

II. Proporcionalidad. Las medidas de ciberseguridad deben ser proporcionales al nivel de riesgo y a la gravedad del impacto en la intimidad, la libertad de expresión y la confianza digital, procurando que sean mínimamente invasivas y garantizando que no se impongan restricciones innecesarias o desproporcionadas a los derechos de los usuarios;

III. Transparencia. Las autoridades responsables de la ciberseguridad deben operar de manera transparente, proporcionando información clara y accesible sobre sus políticas, acciones y prácticas en

**relación con la protección de la intimidad, la libertad de expresión y la confianza digital;**

**IV. Monitoreo y seguimiento: Se deben establecer mecanismos de monitoreo para verificar el cumplimiento de las políticas públicas en la materia y mecanismos efectivos de rendición de cuentas para garantizar su actuación conforme a la ley y a los principios establecidos;**

**V. Colaboración Multisectorial. Se debe promover la colaboración y coordinación entre el gobierno, el sector privado, la sociedad civil, la academia y otros actores relevantes, con el fin de desarrollar estrategias integrales y efectivas para proteger la intimidad, fomentar la libertad de expresión y fortalecer la confianza digital en el país;**

**VI. Seguridad e Integridad de los Datos: Se deben establecer medidas efectivas para garantizar la seguridad y la integridad de los datos personales y de cualquier otra información sensible en el ciberespacio, protegiéndolos contra accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas;**

**VII. Protección de la privacidad. Se prohíbe cualquier forma de censura y vigilancia excesiva en el ciberespacio que restrinja indebidamente la libertad de expresión y la privacidad de los usuarios, asegurando el respeto a la diversidad de opiniones y el derecho a la autodeterminación informativa;**

**VIII. Fomento de la Cultura Digital Responsable. Se promueve la educación y sensibilización de las personas sobre el uso responsable y seguro de las tecnologías digitales, fomentando una cultura digital que valore la protección de la intimidad, el respeto a la libertad de expresión y la construcción de la confianza digital en línea;**

**IX. Innovación. Se debe fomentar la innovación y el desarrollo tecnológico, incentivando la creación de soluciones y herramientas que contribuyan a proteger la intimidad, promover la libertad de expresión y fortalecer la confianza digital en el ciberespacio;**

X. **Inclusión: Se reconoce el derecho fundamental de todas las personas a la protección de su intimidad en el ciberespacio, sin discriminación alguna por motivos de origen étnico o nacional, género, edad, discapacidad, condición social, religión, orientación sexual, identidad de género, opinión política, filosófica o de cualquier otra índole;**

XI. **Resiliencia: Se fomenta no solo la prevención y detección temprana de amenazas, sino también la implementación de mecanismos que permitan una rápida recuperación de los servicios tras un incidente, minimizando el impacto negativo sobre la sociedad y la economía;**

XII. **Interoperabilidad: Se debe procurar que los sistemas, políticas y normas de ciberseguridad sean compatibles y funcionen de manera coherente entre diferentes plataformas, organizaciones y países. Este principio es esencial para facilitar la colaboración internacional y el manejo efectivo de incidentes que trasciendan fronteras, promoviendo un enfoque global y coordinado en ciberseguridad;**

XIII. **Sostenibilidad: El diseño, desarrollo e implementación de tecnologías y políticas de ciberseguridad debe incluir la adopción de prácticas que apoyen el desarrollo sostenible, asegurando que las iniciativas de ciberseguridad no contribuyan a la degradación ambiental ni generen impactos negativos a largo plazo;**

XIV. **Ética: Establecer un marco ético claro y robusto para la implementación de tecnologías y políticas de ciberseguridad, con especial énfasis en el desarrollo y uso de inteligencia artificial y otras tecnologías emergentes;**

XV. **Disponibilidad de la información: Establecer políticas de seguridad informática y de la información, con la finalidad de que exista disponibilidad o capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados o usuarios, es decir, que lo necesitan para desenvolver sus actividades;**

XVI. **Neutralidad tecnológica y de acceso al internet: Se debe garantizar el respeto a los principios de neutralidad de las redes en términos de lo**

**previsto en los artículos 145 y 146 de la Ley Federal de Telecomunicaciones y Radiodifusión;**

**XVII. Libre circulación de datos: Se debe garantizar la libre circulación de datos, sin perjuicio de la protección a privacidad y protección de datos personales.**

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

I. **CSIRT. Se define CSIRT (Computer Security Incident Response Team, por sus siglas en inglés) entidad, equipo o grupo de expertos especializados en ciberseguridad, designado para detectar, analizar, mitigar y responder a incidentes de seguridad informática en una organización, sector o país;**

II. **Ciberdelito. Cualquier actividad ilícita que se comete utilizando medios electrónicos, sistemas informáticos, redes de comunicación o tecnologías digitales, con el objetivo de obtener beneficios económicos, causar daño o vulnerar derechos en el ciberespacio;**

III. **Ciberresiliencia: Capacidad de un sistema, organización o red para anticipar, resistir, recuperarse y adaptarse a eventos adversos, ataques cibernéticos o desastres naturales que afectan a la infraestructura de información y comunicaciones. Incluye la habilidad de restaurar servicios y procesos de manera oportuna y confiable bajo diversas condiciones adversas;**

IV. **Ciberseguridad. Conjunto de medidas, técnicas y procesos orientados a proteger los sistemas informáticos, redes, dispositivos y datos contra amenazas cibernéticas, garantizando la confidencialidad, integridad y disponibilidad de la información, así como la protección de los activos digitales y la privacidad de los usuarios;**

V. **Comisión. Comisión Consultiva de Ciberseguridad;**

VI. **Consejo. Consejo Nacional de Ciberseguridad;**

VII. **Criterios de privacidad. Conjunto de principios y normas que deben cumplir las innovaciones en ciberseguridad para garantizar la protección de los datos personales;**

VIII. **Criterios de Seguridad. Conjunto de requisitos técnicos y organizativos que deben cumplir las innovaciones en ciberseguridad para ser autorizadas;**

IX. **Criterios de Uso Ético. Conjunto de principios y valores que deben cumplir las innovaciones en ciberseguridad para garantizar un uso responsable y ético de la tecnología;**

X. **Dato. Se define como cualquier representación simbólica o material de un hecho, concepto o instrucción que se encuentra almacenado, procesado o transmitido en un sistema informático o electrónico;**

XI. **ENC. Estrategia Nacional de Ciberseguridad;**

XII. **Estrategia. Estrategia Nacional de Ciberseguridad;**

**XIII. Gestión de incidentes: Proceso de identificación, análisis y respuesta a incidentes de ciberseguridad. Incluye la preparación, detección, contención, erradicación y recuperación, así como la comunicación y coordinación necesarias para manejar un incidente eficazmente;**

**XIV. Gestión de riesgos: Proceso sistemático de identificación, evaluación y control de los riesgos asociados con la seguridad de la información y las tecnologías de la información. Involucra la evaluación de la probabilidad y el impacto de los eventos adversos y la implementación de medidas adecuadas para mitigarlos;**

**XV. Incidente o ciberincidente: Cualquier evento adverso que amenace la seguridad, integridad, disponibilidad o confidencialidad de los sistemas de información y redes;**

XVI. **Instituto. Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad;**

XVII. **INFOTEC. Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad;**

XVIII. **Innovación. Cualquier desarrollo, aplicación, modelo de negocio o tecnología que represente una novedad en el ámbito de la ciberseguridad y que tenga el potencial de mejorar la protección de los sistemas informáticos y de la información;**

XIX. **Ley. Ley Federal de Ciberseguridad y Confianza Digital;**

XX. **Malware. Cualquier tipo de software malicioso diseñado para infiltrarse o dañar un sistema informático, dispositivo electrónico, red de computadoras o cualquier otro sistema digital, sin el consentimiento del usuario y con el propósito de causar daño, robar información, o comprometer la seguridad y el funcionamiento del sistema afectado.**

**XXI. Operador de servicios esenciales: Entidad pública o privada identificada por los Estados miembros bajo la Directiva NIS como crítica para mantener servicios esenciales como la salud, seguridad, económicos o sociales. Estos operadores requieren una infraestructura de redes y sistemas de información robusta porque su interrupción o fallo tendría un impacto significativo en la seguridad nacional o bienestar de los ciudadanos;**

**XXII. Proveedor de servicios digitales: Según la Directiva NIS, se refiere a las organizaciones que ofrecen servicios digitales dentro de la UE como motores de búsqueda en línea, nubes computacionales y plataformas de comercio electrónico;**

**XXIII. Redes y sistemas de información: Comprende las infraestructuras digitales, incluidas redes privadas y públicas, sistemas informáticos, y otros dispositivos de procesamiento de datos e infraestructuras que almacenan, transmiten o procesan información;**

XXIV. **Sandbox. Entorno de pruebas controlado y acotado en el que se autorizan, de manera temporal y con ciertas condiciones, el**

**desarrollo, la prueba y la implementación de nuevas tecnologías en materia de ciberseguridad;**

**XXV. Seguridad Informática: Es el conjunto de tecnologías, procesos y prácticas diseñadas para la protección del procesamiento de la información, a través de redes, dispositivos, programas y datos, contra alguna amenaza o ataque cibernético.**

**XXVI. Seguridad de la Información: Es el conjunto de procedimientos y herramientas de seguridad que protegen ampliamente el procesamiento de la información confidencial, para evitar su uso indebido, así como el acceso no autorizado, y la interrupción o destrucción de la propia información.**

XXVII. **Sistema Nacional. Sistema Nacional para la Ciberseguridad y Confianza Digital;**

XXVIII. **Software. Conjunto de programas, instrucciones y datos que permiten a un sistema informático realizar diversas tareas, operaciones y funciones de manera automatizada y controlada;**

XXIX. **TIC. Tecnologías de la Información y Comunicaciones;**

**XXX. Vulnerabilidad: Debilidad en un sistema, red o componente de software que puede ser explotada por una amenaza para realizar acciones no autorizadas. La vulnerabilidad puede deberse a errores de software, configuraciones incorrectas o deficiencias en los procesos de seguridad.**

**Artículo 5. En lo no previsto por la presente Ley, se aplicarán, conforme a su naturaleza y de forma supletoria, las disposiciones contenidas en:**

**I. La Ley General del Sistema Nacional de Seguridad Pública;**

**II. La Ley General de Transparencia y Acceso a la Información Pública;**

**III. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;**

IV. La Ley Federal de Telecomunicaciones y Radiodifusión;

V. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

VI. La Ley Federal de Transparencia y Acceso a la Información Pública;

VII. Código Penal Federal;

VIII. La Ley de Seguridad Nacional;

IX. La Ley de la Guardia Nacional;

X. Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación

## Título Segundo
## Sistema Nacional para la Ciberseguridad y Confianza Digital

### Capítulo Primero

### Del Sistema Nacional de Ciberseguridad y Confianza Digital

**Artículo 6.** El Sistema Nacional para la Ciberseguridad y Confianza Digital, es una instancia de coordinación, evaluación y deliberación, responsable de la organización de los esfuerzos de cooperación, investigación, colaboración, promoción, difusión y coordinación permanente en materia de seguridad en uso de las tecnologías de la información y comunicación, de conformidad con lo señalado en la presente Ley y demás normatividad aplicable.

**Artículo 7.** El Sistema Nacional para la Ciberseguridad y Confianza Digital tiene como objeto la construcción, desarrollo y vigilancia de una política pública integral, ordenada y articulada, con una visión nacional, que garantice el efectivo ejercicio y respeto de los derechos humanos en el ciberespacio, a través de la promoción y fomento de la seguridad, gestión de riesgos, educación y cultura digital en todo el territorio nacional.

**Artículo 8.** El Sistema Nacional para la Ciberseguridad y Confianza Digital, se integra por el conjunto orgánico y articulado del Consejo Nacional de

**Ciberseguridad, la Comisión Consultiva de Ciberseguridad y el Instituto Nacional para la Ciberseguridad, así como sus miembros, procedimientos, instrumentos y políticas, con el objeto de fortalecer, prevenir, detectar, mitigar y responder efectivamente a las amenazas cibernéticas que puedan afectar la seguridad nacional, la infraestructura crítica, la economía y los derechos fundamentales de las personas.**

**Artículo 9. El Sistema Nacional para la Ciberseguridad y Confianza Digital se conformará a partir de la coordinación que se realice entre las distintas instancias que, en razón de sus ámbitos de competencia, contribuyan a fortalecer, prevenir, detectar, mitigar y responder efectivamente a las amenazas cibernéticas e informáticas que puedan afectar la seguridad nacional, la infraestructura crítica, la economía y los derechos fundamentales de las personas en todo el territorio nacional.**

**Este esfuerzo conjunto e integral, se debe enfocar a la construcción de la Estrategia Nacional de Ciberseguridad, la generación de información de calidad, políticas públicas transversales e inclusivas, a la gestión de la información; así como al procesamiento de la misma como un medio para facilitar el conocimiento y evaluación de la gestión pública.**

## Capítulo Segundo

## Del Consejo Nacional de Ciberseguridad

**Artículo 10. El Consejo Nacional de Ciberseguridad es una instancia deliberativa, cuya finalidad es establecer y articular la política pública en materia de ciberseguridad y seguridad de la Información y datos digitales. Por tanto, conocerá los asuntos siguientes:**

I. **La integración y coordinación de los esfuerzos orientados a garantizar el efectivo ejercicio y respeto de los derechos humanos en el ciberespacio, a través de la promoción y fomento de la seguridad, gestión de riesgos, educación y cultura digital en todo el territorio nacional;**

II. **La coordinación y promoción de las acciones para proteger la infraestructura digital y los sistemas de información del país, así como para fortalecer la resiliencia cibernética a nivel nacional.**

III. **Los lineamientos que permitan el establecimiento políticas generales para fortalecer, prevenir, detectar, mitigar y responder efectivamente a las amenazas cibernéticas que puedan afectar la seguridad nacional, la infraestructura crítica, la economía y los derechos fundamentales de las personas en territorio nacional;**

IV. **Proponer a la persona Titular del Ejecutivo la Estrategia Nacional de Ciberseguridad;**

V. **La definición anual de la Agenda Nacional de Riesgos Cibernéticos, el Atlas de Riesgos Cibernéticos y su informe de actividades;**

VI. **La evaluación periódica de los resultados de la Estrategia Nacional de Ciberseguridad y el seguimiento de la Agenda Nacional de Riesgos Cibernéticos;**

VII. **La coordinación de la colaboración entre entidades gubernamentales, sector privado, academia y sociedad civil en materia de ciberseguridad;**

VIII. **La evaluación y monitoreo del estado de la ciberseguridad en el país;**

IX. **Las medidas para fortalecer la respuesta ante incidentes cibernéticos;**

X. **Los programas de cooperación internacional y la representación del país en foros internacionales sobre ciberseguridad;**

XI. **Informar las acciones necesarias para la Seguridad Nacional, dentro del marco de atribuciones previsto en la presente Ley, así como en otros ordenamientos aplicables;**

XII. **Los lineamientos, protocolos y programas para que la Guardia Cibernética preste auxilio y colaboración en materia de Seguridad Pública, procuración de justicia y en cualquier otro ramo de la Administración Pública que acuerde el Consejo;**

XIII. **Autorizar el programa anual de trabajo en materia de ciberseguridad, del Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad;**

**XIV.** **Elaborar las bases y/o convocatorias para el proceso de selección de los integrantes de la Comisión Consultiva de Ciberseguridad.**

**XV.** **Elegir por mayoría simple a los integrantes de la Comisión Consultiva de Ciberseguridad que hayan cubierto el proceso de selección.**

**XVI.** **Ratificar el nombramiento del Director Ejecutivo para la ciberseguridad, del Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad; y**

**XVII.** **Los demás que establezcan otras disposiciones o la persona titular de la Presidencia de la República.**

**Artículo 11. El Consejo Nacional de Ciberseguridad conformará un órgano colegiado encargado de establecer las políticas y estrategias nacionales en materia de ciberseguridad, integrado por:**

**I.** **Titular del Consejo Nacional de Ciberseguridad, quien la presidirá;**

**II.** **Titular de la Secretaría de Gobernación, quien ejercerá en la secretaria del consejo;**

**III.** **Titular de la Secretaria de Seguridad y Participación Ciudadana, quien ejercerá en la secretaria del consejo;**

**IV.** **Titular del Consejo de Seguridad Nacional;**

**V.** **Titular de la Coordinación de Estrategia Digital Nacional;**

**VI.** **Titulares de las Unidades de Tecnologías de la Información y Comunicación, y Seguridad de la Información o equivalentes que conforman la Administración Pública Federal, centralizada y paraestatal;**

**VII.** **Titulares de las Unidades de Tecnologías de la Información y Comunicación, y Seguridad de la Información o equivalentes de los Organismos Constitucionales Autónomos;**

**VIII. Las personas servidoras públicas que designe el Titular del Ejecutivo Federal para integrar el Consejo, participarán con derecho a voz, pero sin voto, y;**

**IX. Titular de la Comisión Consultiva de Ciberseguridad, participará con derecho a voz, pero sin voto.**

**Las personas integrantes del Consejo tendrán derecho a voz y voto.**

**En sus ausencias temporales por causas justificadas, podrán ser suplidos por la persona servidora pública con nivel inmediato inferior a quien designen como suplente.**

**En caso de ausencia de la Presidencia del Consejo, alguna de las Secretarías del Consejo presidirán la reunión.**

**Los titulares de la Secretaría de Gobernación y de la Secretaria de Seguridad y Participación Ciudadana podrán designar a un suplente en sus ausencias, los cuales deberán ejercer el cargo de Subsecretaria de Estado o equivalente.**

**Artículo 12. El Consejo Nacional podrá invitar a sus sesiones, a propuesta de cualquiera de sus integrantes, a:**

**I. Autoridades de los gobiernos de las entidades federativas y de los municipios o demarcaciones territoriales de la Ciudad de México;**

**II. Integrantes de las Comisiones Legislativas del Honorable Congreso de la Unión.**

**III. Integrantes del Poder Judicial de la Federación; y**

**IV. Autoridades de la Fiscalía General de la República;**

**Dichas representaciones participarán con derecho a voz, pero sin voto.**

**Artículo 13. El Consejo Nacional deberá sesionar cuando menos una vez al trimestre.**

**Las sesiones ordinarias deberán ser convocadas por la Presidencia del Consejo con una anticipación de 48 horas previas a llevarse a cabo la reunión, acompañando de ser posible la orden del día con los temas a tratarse en la sesión, y en su caso, con la remisión de la información digital que se encuentre relacionada a los temas.**

**Las sesiones extraordinarias podrán ser convocadas por la Presidencia del Consejo o por el Titular del Ejecutivo Federal y deberán ser convocadas con una anticipación de al menos 5 horas previas a llevarse a cabo la reunión, sin que exista necesidad de informar el orden del día, así como el envío previo de información relacionada a los rubros a tratar.**

**Artículo 14. El Titular del Consejo Nacional de Ciberseguridad será nombrado por la persona Titular del Ejecutivo Federal, contará con un equipo técnico especializado y un presupuesto asignado en el Presupuesto de Egresos de la Federación.**

**Artículo 15. El Titular del Consejo Nacional de Ciberseguridad tendrá la obligación de promover en todo tiempo la efectiva coordinación y funcionamiento del Consejo, y estará facultado para celebrar los convenios y bases de colaboración que acuerde el Consejo.**

**Artículo 16. El Consejo contará con una Secretaría Técnica, que será nombrada por el Titular del Consejo Nacional de Ciberseguridad, dependerá directamente de la Presidencia del Consejo. Ésta no será integrante del Consejo.**

**Artículo 17. La Secretaría Técnica del Consejo tendrá a su cargo las siguientes funciones:**

I. **Elaborar y certificar los acuerdos que se tomen en el Consejo, llevando su archivo y el de los instrumentos jurídicos que se generen en el seno del mismo;**

II. **Realizar las acciones necesarias para la debida ejecución y seguimientos de los acuerdos del Consejo;**

III. **Recibir y proponer al Consejo políticas, lineamientos y acciones en materia de Ciberseguridad;**

**IV.** **Proponer el contenido de la Estrategia Nacional de Ciberseguridad;**

**V.** **Presentar anualmente al Consejo la Agenda Nacional de Ciberseguridad;**

**VI.** **Elaborar los informes de actividades que ordene el Consejo;**

**VII.** **Emitir las bases y/o convocatorias para el proceso de selección de los integrantes de la Comisión Consultiva de Ciberseguridad.**

**VIII.** **Entregar a más tardar el 30 de noviembre de cada año a las Presidencias de las Cámaras de Diputados y Senadores la documentación e informes a las que se refiere el artículo 10 fracción V de la presente Ley;**

**IX.** **Administrar y sistematizar los documentos, archivos y datos electrónicos que se generen en el seno del Consejo;**

**X.** **Promover la ejecución de las acciones conjuntas que se acuerden en el Consejo, de conformidad con las bases y reglas que emita el mismo y con respeto a las atribuciones de las instancias vinculadas;**

**XI.** **Solicitar a la Comisión Consultiva y al Instituto la realización de informes, estudios especializados y estadísticas en materias relacionadas con la seguridad en uso de las tecnologías de la información y comunicaciones, previa autorización del Consejo.**

**XII.** **Actualizar y someter para su aprobación el atlas de riesgo cibernético;**

**XIII.** **Actualizar y someter para su aprobación el inventario de la infraestructura crítica del país;**

**XIV.** **Solicitar información necesaria a las dependencias federales para ciberseguridad que requiera explícitamente el Consejo;**

**XV.** **Emitir la convocatoria a las reuniones ordinarias y extraordinarias del Consejo; y**

**XVI. Las demás que señalen las leyes y reglamentos, o que sean necesarias para cumplir las anteriores.**

## Capítulo Tercero

## De la Comisión Consultiva de Ciberseguridad

**Artículo 18. La Comisión Consultiva de Ciberseguridad es un órgano de asesoramiento que proporciona orientación técnica y estratégica al Consejo Nacional de Ciberseguridad para mejorar las políticas y acciones relacionadas con la ciberseguridad en México. Por tanto ejercerá las siguientes funciones:**

**I. Proporcionar asesoramiento experto en cuestiones de ciberseguridad a las autoridades gubernamentales, ofreciendo perspectivas y recomendaciones basadas en el conocimiento y la experiencia ciudadana y académica;**

**II. Coadyuvar en la identificación y evaluación de los riesgos relacionados con la ciberseguridad, así como en la formulación de estrategias para mitigarlos y gestionarlos de manera efectiva;**

**III. Supervisar la implementación de las políticas y medidas de ciberseguridad establecidas por el gobierno, asegurando su efectividad y relevancia continua en un entorno en constante evolución tecnológica;**

**IV. Desarrollar y someter a aprobación del Consejo los programas educativos y de concientización dirigidos a la ciudadanía y a diferentes sectores de la sociedad sobre la importancia de la ciberseguridad;**

**V. Fomentar la investigación en el campo de la ciberseguridad y promover la colaboración entre el sector académico, la industria y el gobierno para el desarrollo de nuevas tecnologías y prácticas innovadoras en este ámbito;**

**VI. Llevar a cabo actividades de fomento y promoción de la ciberseguridad, en instancias de gobierno de los tres niveles, instituciones académicas, iniciativa privada y con la ciudadanía en general.**

**VII. Analizar el impacto y la eficacia de las políticas públicas existentes en materia de ciberseguridad, y proponer al Consejo los ajustes y mejoras según sea necesario para garantizar su eficacia y cumplimiento de los objetivos establecidos;**

**VIII. Analizar tendencias y mejores prácticas en ciberseguridad a nivel nacional e internacional;**

**IX. Facilitar la colaboración entre el gobierno y la sociedad civil, representando los intereses y preocupaciones de los ciudadanos y los actores académicos en relación con la ciberseguridad y las políticas públicas asociadas;**

**X. Emitir recomendaciones sobre políticas, normativas y estrategias relacionadas con la ciberseguridad; y**

**XI. Las demás que apruebe el Consejo.**

**Artículo 19. La Comisión Consultiva de Ciberseguridad será conformada por profesionales, especialistas o representantes de la sociedad civil, de reconocida capacidad o experiencia, designados por el Titular de la Presidencia de la República de conformidad, observando el principio de la paridad de género y a lo dispuesto en el artículo 21 de la Ley Orgánica de la Administración Federal y el artículo 17 de la presente Ley.**

**Artículo 20. La Comisión Consultiva estará integrada por personas expertas, representantes del sector académico, sociedad civil, cámaras empresariales, organismos constitucionales autónomos, representantes de los poderes de la unión y de los gobiernos estatales y municipales.**

**Durarán en su cargo por tres años y deberán llevar a cabo el proceso de selección que para este efecto emita el Consejo Nacional de Ciberseguridad.**

**Artículo 21. La lista de los integrantes que sea aprobada por el Consejo Nacional de Ciberseguridad, será remitida al Titular de la Presidencia de la República para su designación, quien tendrá derecho de veto.**

**Artículo 22. Al instalar los trabajos de la Comisión Consultiva, será necesario que se elija una Presidencia y dos Secretarias Ejecutivas, mediante votación secreta de la mayoría simple de los integrantes de la Comisión.**

**Artículo 23. La Comisión contará con una Secretaría Técnica, que será nombrada por el Titular del Consejo Nacional de Ciberseguridad, dependerá directamente de la Presidencia del Consejo. Ésta no será integrante del Consejo.**

**Artículo 24. La Secretaría Técnica de la Comisión tendrá a su cargo las siguientes funciones:**

I. **Elaborar y certificar los acuerdos que se tomen en la Comisión, llevando su archivo y el de los instrumentos jurídicos que se generen en el seno del mismo;**

II. **Realizar las acciones necesarias para la debida ejecución y seguimientos de los acuerdos de la Comisión;**

III. **Elaborar los informes de actividades que acuerde la Comisión;**

IV. **Administrar y sistematizar los documentos, archivos y datos electrónicos que se generen en la Comisión;**

V. **Llevar a cabo el registro de asistencia, votaciones y versiones estenográficas de las reuniones públicas de la Comisión.**

VI. **Emitir la convocatoria a las reuniones ordinarias y extraordinarias de la Comisión; y**

VII. **Las demás que señalen las leyes y reglamentos, o que sean necesarias para cumplir las anteriores.**

## Capítulo Cuarto

## Del Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad

**Artículo 25. El Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad es una entidad pública dependiente del Consejo Nacional de Humanidades, Ciencias y Tecnologías, responsable de ejecutar las acciones operativas y técnicas para proteger la infraestructura digital del país y responder ante incidentes cibernéticos. Para tal fin, ejercerá las siguientes funciones:**

I. **Actuar como centro de referencia en ciberseguridad en México, proporcionando recursos y servicios especializados para proteger la información y los sistemas digitales del país. Perteneciendo a la red de Centros Públicos de Investigación (CPI) del Consejo Nacional de Humanidades, Ciencias y Tecnologías;**

II. **Contribuir a aumentar la ciberseguridad de México, así como a reforzar su posicionamiento como referente internacional en este ámbito.**

III. **Fortalecer las capacidades técnicas y operativas en materia de ciberseguridad para prevenir, detectar, mitigar y responder eficazmente a amenazas cibernéticas;**

IV. **Llevar a cabo campañas de sensibilización y educación pública para fomentar buenas prácticas de seguridad cibernética entre ciudadanos, empresas y organizaciones;**

V. **Desarrollar y promover estándares de seguridad cibernética aplicable para la Administración Pública Federal;**

VI. **Coordinar la operación de los centros de respuesta ante incidentes cibernéticos;**

VII. **Brindar asistencia técnica y capacitación en ciberseguridad;**

VIII. **Realizar investigaciones, estudios, encuestas y análisis forenses en casos de incidentes cibernéticos;**

IX. **Coadyuvar en la coordinación de respuesta ante emergencias cibernéticas a nivel nacional y proporcionar asistencia técnica en caso de ataques informáticos;**

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

XI. Ofrecer programas de formación académica, cursos y diplomados especializados en ciberseguridad para profesionales del sector, con el objetivo de mejorar sus habilidades y conocimientos en esta área;

XII. Integrar a expertos en diferentes áreas relacionadas con la ciberseguridad, incluyendo aspectos técnicos, legales, educativos y de investigación, para abordar de manera integral los desafíos en este campo;

XIII. Realizar actividades de investigación y desarrollo en ciberseguridad, colaborando con universidades, centros de investigación y empresas para impulsar la innovación en este campo;

XIV. Implementar un programa de capacitación continua para los miembros de la Comisión en las últimas tendencias y desafíos en ciberseguridad y protección de datos personales.

XV. Colaborar con otros organismos nacionales e internacionales en la lucha contra el cibercrimen y en la promoción de la ciberseguridad a nivel global. Previa autorización del Consejo Nacional de CIberseguridad;

XVI. Las demás que apruebe el Consejo Nacional de Humanidades, Ciencias y Tecnologías.

Artículo 26. El INFOTEC en coordinación con el Instituto Federal de Telecomunicaciones establecerá una Línea Telefónica, de alcance nacional, gratuita, confidencial, accesible y con carácter permanente para proporcionar el servicio de ayuda en ciberseguridad, dirigido a la ciudadanía, empresas, instituciones públicas y a niñas, niños y adolescentes.

Este servicio centralizará, de una forma cercana y rigurosa, la asistencia en relación a las dudas y consultas sobre ciberseguridad, privacidad, confianza digital y uso seguro y responsable de Internet y de la tecnología. Sobre todo,

**las derivadas de riesgos, amenazas, conflictos e incidentes que surgen en su uso.**

**Identificar fraudes o extorsiones en línea, mantener los dispositivos protegidos frente a malware; Además, proporcionar una respuesta integral a incidentes de ciberseguridad que sean reportados que se atenderán en coordinación con el CSIRT y la Guardia Cibernética.**

## Título Tercero

## Estrategia Nacional de Ciberseguridad

### Capítulo Único

**Artículo 27. Se establece que el Consejo Nacional de Ciberseguridad como el órgano encargado de formular, coordinar y evaluar la Estrategia Nacional de Ciberseguridad de México, de conformidad a los objetivos y principios previstos en esta Ley y a lo dispuesto en la Ley de Planeación.**

**Artículo 28. La Estrategia Nacional de Ciberseguridad establecerá un marco integral y efectivo que fortalezca la ciberseguridad en México, garantizando la protección de los sistemas, de la información, datos e infraestructuras críticas del país frente a amenazas cibernéticas, promoviendo la confianza digital y asegurando el respeto a los derechos humanos en el ciberespacio.**

**Para tal fin, la Estrategia Nacional de Ciberseguridad se enfocará en los siguientes pilares fundamentales:**

I. **Prevención: Implementar medidas proactivas para identificar, prevenir y mitigar posibles amenazas cibernéticas, incluyendo la promoción de buenas prácticas de seguridad informática, la sensibilización de la ciudadanía y la promoción de la cultura de ciberseguridad.**

II. **Detección: Desarrollar capacidades avanzadas de detección de amenazas cibernéticas, incluyendo sistemas de monitoreo continuo, análisis de comportamiento de redes y detección temprana de intrusiones para identificar y responder rápidamente a posibles incidentes de seguridad.**

III. **Respuesta: Establecer protocolos claros y eficaces de respuesta ante incidentes cibernéticos, incluyendo la coordinación entre autoridades competentes, sector privado y otros actores relevantes, así como la implementación de planes de contingencia y recuperación de desastres.**

IV. **Cooperación: Fomentar la colaboración y el intercambio de información entre diferentes sectores y actores involucrados en la ciberseguridad, incluyendo el gobierno, el sector privado, la academia, la sociedad civil y la comunidad internacional, para abordar de manera integral los desafíos en este ámbito.**

V. **Capacitación y Desarrollo: Promover la formación y capacitación continua en ciberseguridad, tanto a nivel técnico como estratégico, para garantizar la disponibilidad de profesionales cualificados y el desarrollo de capacidades avanzadas en el ámbito de la ciberseguridad en México.**

**Artículo 29. La Estrategia Nacional de Ciberseguridad será desarrollada por el Consejo Nacional de Ciberseguridad con apoyo de la Comisión Consultiva de Ciberseguridad cubriendo por los menos las siguientes líneas de acción:**

**Artículo 30. La implementación de la Estrategia Nacional de Ciberseguridad se llevará a cabo de manera coordinada y gradual, con la participación activa de todas las partes interesadas, y será evaluada periódicamente para garantizar su efectividad y adecuación a las necesidades, respeto a los derechos fundamentales y desafíos cambiantes en el entorno digital.**

**Artículo 31. La Estrategia Nacional de Ciberseguridad tendrá una vigencia trianual, debiendo ser revisada y actualizada al menos una vez cada tres años para garantizar su pertinencia y efectividad en la protección de los sistemas y datos digitales del país.**

**Artículo 32. La Estrategia Nacional de Ciberseguridad promoverá un modelo de responsabilidad compartida en el ámbito de la ciberseguridad, en el que se garantice la participación activa y coordinada de diversos actores, incluyendo el gobierno, el sector privado, la academia, la sociedad civil y los ciudadanos, en la generación, implementación y cumplimiento de las disposiciones legales y normativas en materia de ciberseguridad.**

**El modelo de responsabilidad compartida será fundamentado en los siguientes principios:**

I. **Diagnóstico del estado actual que guarda el país en materia de ciberseguridad.**

II. **Fortalecimiento de la legislación y regulación en materia de ciberseguridad, promoviendo leyes actualizadas que aborden los desafíos emergentes en el ciberespacio y establezcan sanciones proporcionales para los delitos cibernéticos.**

III. **Implementación de medidas de protección y fortalecimiento de la infraestructura crítica del país, incluyendo sistemas de control y vigilancia para garantizar la seguridad de sectores estratégicos como energía, salud, finanzas y transporte.**

IV. **Promoción de la colaboración público-privada en la ciberseguridad, fomentando alianzas entre el gobierno, empresas, instituciones académicas y organizaciones de la sociedad civil para compartir información, recursos y buenas prácticas en materia de ciberseguridad.**

V. **Desarrollo de capacidades técnicas y humanas en ciberseguridad, mediante programas de formación, capacitación y certificación para profesionales del sector, así como la promoción de la educación en STEM (Ciencia, Tecnología, Ingeniería y Matemáticas) desde etapas tempranas.**

VI. **Establecimiento y coordinación de centros de operaciones de seguridad cibernética a nivel nacional, regional y sectorial para monitorear, detectar y responder a amenazas cibernéticas en tiempo real, garantizando una coordinación eficaz entre las partes involucradas.**

VII. **Mejora de la conciencia y cultura de ciberseguridad en la sociedad, mediante campañas de sensibilización, educación y difusión de buenas prácticas para promover un uso seguro y responsable de la tecnología digital.**

VIII. **Desarrollo de estrategias y planes de respuesta ante incidentes cibernéticos, incluyendo la creación de equipos de respuesta rápida, la**

**elaboración de planes de contingencia y la realización de simulacros y ejercicios de ciberseguridad a nivel nacional.**

**IX. Fortalecimiento y actualización de la legislación de protección de datos personales y privacidad en línea, mediante la promulgación y aplicación de leyes y estándares que garanticen el respeto a la intimidad de los usuarios y la seguridad de su información personal.**

**X. Fomento de la investigación y desarrollo en ciberseguridad, incentivando la innovación tecnológica y la creación de soluciones avanzadas para hacer frente a las amenazas cibernéticas emergentes, como el desarrollo de inteligencia artificial para la detección de intrusiones y el análisis de comportamiento.**

**XI. Establecimiento de mecanismos de coordinación y cooperación internacional en ciberseguridad, mediante la suscripción de acuerdos bilaterales y multilaterales, así como la participación activa en organismos y foros internacionales para intercambiar información y mejores prácticas en materia de ciberseguridad.**

**XII. Implementación de indicadores y evaluaciones periódicas de seguridad cibernética en entidades públicas y privadas, con el fin de identificar vulnerabilidades, evaluar riesgos y garantizar el cumplimiento de normativas y estándares de seguridad.**

**XIII. Fomento del desarrollo de la industria de ciberseguridad en México mediante la creación de incentivos fiscales, programas de financiamiento y apoyo a la investigación y desarrollo de tecnologías innovadoras en el sector, con el objetivo de fortalecer la capacidad nacional para enfrentar y prevenir amenazas cibernéticas.**

**XIV. Implementación de un mecanismo integral de combate, denuncia y sanción del ciberdelito que incluya la creación de unidades especializadas en las instituciones de seguridad y justicia, el fortalecimiento de capacidades de investigación forense digital, y la actualización de leyes y regulaciones que establezcan sanciones proporcionales y efectivas para los delitos cibernéticos.**

**XV.** **Establecimiento de un sistema nacional de alerta temprana en ciberseguridad para informar a la población sobre amenazas y vulnerabilidades cibernéticas, así como proporcionar orientación y recomendaciones para protegerse contra posibles ataques.**

**XVI.** **Corresponsabilidad: Reconocimiento de que la protección y defensa de la ciberseguridad es una responsabilidad compartida entre el gobierno, las empresas, las organizaciones, los profesionales de la tecnología, las instituciones académicas públicas y privadas, así como la ciudadanía en general.**

**XVII.** **Colaboración: Fomento de la cooperación y colaboración entre los diferentes actores involucrados en la ciberseguridad, mediante la compartición de información, recursos, buenas prácticas y experiencias para hacer frente a las amenazas cibernéticas de manera efectiva y coordinada.**

**XVIII.** **Transparencia: Promoción de la transparencia en las acciones y decisiones relacionadas con la ciberseguridad, garantizando la rendición de cuentas y la participación de las empresas, las organizaciones, los profesionales de la tecnología, las instituciones académicas públicas y privadas, así como la ciudadanía en general, en la elaboración y evaluación de políticas, programas y medidas de ciberseguridad.**

**XIX.** **Inclusión: Garantía de la participación equitativa y representativa de todos los sectores de la sociedad en la formulación y aplicación de la ley en materia de ciberseguridad, con especial atención a la protección de los derechos humanos, la privacidad y la libertad de expresión en el ciberespacio.**

**Artículo 33. La Estrategia Nacional de Ciberseguridad establecerá mecanismos y programas específicos para promover la adopción y aplicación efectiva del modelo de responsabilidad compartida en ciberseguridad, incluyendo la creación de espacios de diálogo y colaboración, la promoción de estándares y buenas prácticas, y el fortalecimiento de capacidades y recursos en todos los niveles y sectores de la sociedad.**

**Artículo 34. La Estrategia Nacional de Ciberseguridad establecerá protocolos mínimos de ciberseguridad que deberán ser adoptados y cumplidos por todos los sectores y actores involucrados en el ámbito de la ciberseguridad en México.**

**Dichos protocolos mínimos comprenderán, al menos, los siguientes aspectos:**

I. **Normas de Seguridad Informática: Establecimiento de estándares y buenas prácticas en seguridad informática, para la protección de sistemas, redes y datos frente a amenazas cibernéticas, incluyendo la implementación de medidas de control de acceso, encriptación de datos, gestión de parches y actualizaciones, entre otros.**

II. **Gestión de Incidentes: Definición de procedimientos y protocolos para la gestión eficaz de incidentes cibernéticos, incluyendo la detección, notificación, respuesta y recuperación ante ataques o violaciones de seguridad, con el objetivo de minimizar el impacto y mitigar los riesgos asociados.**

III. **Protección de la Privacidad: Establecimiento de directrices y políticas para garantizar la protección de la privacidad y los datos personales en el ciberespacio, asegurando el cumplimiento de la legislación vigente en materia de protección de datos y el respeto a los derechos individuales de los usuarios.**

IV. **Continuidad de operaciones: Desarrollo de planes de continuidad de operaciones y recuperación ante desastres para asegurar la disponibilidad y la operatividad de sistemas y servicios digitales frente a posibles interrupciones causadas por eventos cibernéticos adversos.**

V. **Sensibilización y Capacitación: Implementación de programas de sensibilización y capacitación en ciberseguridad dirigidos a todos los niveles de la organización, con el fin de promover una cultura de seguridad digital y concienciar sobre las amenazas y riesgos cibernéticos.**

VI. **Progresividad. Los protocolos mínimos comprenderán medidas específicas de seguridad cibernética que deberán implementarse de**

manera gradual y proporcional al nivel de riesgo y al impacto potencial de las operaciones de cada organización en el entorno digital.

VII. Actualización: Se mantendrá actualizado el Atlas de Riesgo de Ciberseguridad, de acuerdo a la aparición de amenazas cibernéticas e informáticas en el mundo, y de la misma manera, de ser necesario, se modificará o adecuará la estrategia nacional, de conformidad con dicho catálogo de riesgos, así como con las nuevas tecnologías cibernéticas dañinas y que afecten a la sociedad.

## Título Cuarto

## Marco Regulatorio

### Capítulo Primero

### Sobre el Marco Regulatorio y Competencias

**Artículo 35.** En apego a los derechos consagrados en la Constitución Política de los Estados Unidos Mexicanos, el marco regulatorio de la presente Ley, establece los siguientes derechos y obligaciones digitales

I. Derechos:
   A. Derecho a la Privacidad Digital: Toda persona tiene derecho a la privacidad y protección de sus datos personales en línea, incluyendo la confidencialidad de sus comunicaciones electrónicas y el control sobre el uso y tratamiento de su información por parte de terceros.
   B. Derecho a la Libertad de Expresión: Se garantiza el derecho de las personas a expresar sus opiniones, ideas y creencias en internet y plataformas digitales, siempre y cuando no infrinjan los derechos de terceros ni promuevan discursos de odio, violencia o discriminación.
   C. Derecho a la Seguridad Digital: Se reconoce el derecho de las personas a utilizar internet de manera segura y protegida, incluyendo la protección contra amenazas cibernéticas, el acceso

a herramientas de seguridad informática y la educación en buenas prácticas en seguridad digital.

D. Derecho al Acceso Universal a Internet: Se promueve la neutralidad tecnológica, el acceso equitativo y universal a internet para todas las personas, sin discriminación por motivos de género, edad, etnia, discapacidad, ubicación geográfica o condición socioeconómica.

II. Obligaciones:

A. Respeto a los Derechos de Autor: Se establece la obligación de respetar los derechos de propiedad intelectual y de autor en internet, incluyendo el respeto a las licencias de uso de contenido digital y la prohibición de la reproducción o distribución no autorizada de material protegido por derechos de autor, conforme a la normatividad aplicable en la materia.

B. Uso Responsable de Internet: Se exige el uso responsable de internet, incluyendo el respeto a las normas de convivencia y ética en línea, la prevención del ciberacoso, y la protección de la reputación y dignidad de las personas en el entorno digital.

C. Protección de Datos Personales: Se establece la obligación de proteger la privacidad y confidencialidad de los datos personales en línea, incluyendo la adopción de medidas de seguridad adecuadas para prevenir el acceso no autorizado, la divulgación o el uso indebido de la información personal.

D. Colaboración en la Prevención de Delitos Cibernéticos: Se insta a las personas a colaborar con las autoridades y organismos competentes en la prevención y denuncia de delitos cibernéticos, incluyendo la cooperación en investigaciones y la adopción de medidas para protegerse contra amenazas digitales.

E. Protección de niños, niñas y adolescentes: Se establecen medidas especiales para proteger a niños y adolescentes en internet, incluyendo la supervisión parental, la restricción de acceso a contenido inapropiado y la prevención del grooming y la explotación sexual infantil en línea.

**Artículo 36.** El Sistema Nacional para la Ciberseguridad y Confianza Digital, deberá proponer un marco normativo integral para la prevención de amenazas y ataques cibernéticos en México, con el objetivo de proteger los sistemas y

**datos digitales del país contra posibles vulnerabilidades y riesgos en el ciberespacio. El marco normativo deberá contener:**

I. **Distribución integral de competencias entre autoridades y dependencias de la administración pública para desarrollar políticas y programas de prevención que incluyan la identificación temprana de amenazas, la evaluación de riesgos, la implementación de medidas de seguridad proactivas y la promoción de la colaboración entre los sectores público y privado en la detección y mitigación de posibles ataques cibernéticos.**

II. **Establecer mecanismos de monitoreo y detección de amenazas cibernéticas, mediante el uso de herramientas tecnológicas avanzadas, el intercambio de información entre entidades gubernamentales y la cooperación con organismos internacionales especializados en ciberseguridad.**

III. **Establecer una Normateca de Ciberseguridad, la cual contendrá la legislación aplicable, estrategias, programas, lineamientos, guías y procedimientos en materia de ciberseguridad en México, que incluya mecanismos de actualización y revisión periódica, con el fin de garantizar su pertinencia y adecuación a los avances tecnológicos y cambios normativos en el ámbito de la ciberseguridad.**

**Artículo 37. La Normateca de Ciberseguridad será desarrollada y administrada por el Instituto, con el objetivo de proporcionar un repositorio centralizado y actualizado de información normativa y técnica relacionada con la protección de los sistemas y datos digitales del país.**

**La Normateca de Ciberseguridad incluirá, entre otros, los siguientes elementos:**

I. **Legislación aplicable en materia de ciberseguridad, incluyendo leyes, reglamentos, normas nacionales e internacionales y disposiciones normativas relacionadas con la protección de datos, la privacidad, la seguridad de la información digital, la seguridad informática y la lucha contra el ciberdelito.**

II. **Estrategias y programas nacionales de ciberseguridad, que establezcan los objetivos, prioridades y acciones a seguir para fortalecer la ciberseguridad en el país.**

III. **Lineamientos y guías técnicas en materia de ciberseguridad, que proporcionen recomendaciones y mejores prácticas para la implementación de medidas de seguridad informática y la gestión de riesgos cibernéticos.**

IV. **Procedimientos y protocolos para la prevención, detección, respuesta y recuperación ante incidentes cibernéticos, que establezcan los pasos a seguir y las responsabilidades de las partes involucradas en la gestión de crisis y emergencias en el ámbito digital.**

**La Normateca de Ciberseguridad estará disponible de forma pública y accesible en línea, con el fin de facilitar el acceso a la información y promover la transparencia y el cumplimiento normativo en materia de ciberseguridad en México.**

**Artículo 38. Los protocolos mínimos de ciberseguridad establecidos en la Estrategia Nacional de Ciberseguridad serán de aplicación obligatoria para todas las entidades públicas y privadas que operen en territorio mexicano, debiendo ser cumplidos en su totalidad y actualizados de manera periódica en función de las nuevas amenazas y desafíos en el ámbito de la ciberseguridad.**

**Los protocolos mínimos que deberán ser adoptados por todas las entidades públicas y privadas en México, se establecerán con un principio de progresividad que considere el tamaño, la complejidad y la importancia de cada entidad.**

**Las organizaciones de mayor tamaño o importancia informático y/o computacional, se encontrarán sujetas a requisitos más adecuados y de mayor alcance en materia de ciberseguridad, incluyendo la adopción de controles adicionales, la realización de auditorías periódicas y la designación de responsables específicos de seguridad de la información, quienes deberán estar certificadas por el INFOTEC, o a través de terceros acreditados por dicho Instituto.**

**Artículo 39. Se establecerán categorías o niveles de cumplimiento de acuerdo con la naturaleza y el alcance de las actividades de cada organización, permitiendo una adaptación flexible de las medidas de seguridad cibernética en función de sus capacidades y recursos disponibles.**

**El Consejo Nacional de Ciberseguridad establecerá directrices, criterios y políticas en la materia que serán claras, con la finalidad de determinar el nivel de cumplimiento de los protocolos mínimos en función de la naturaleza y el contexto de cada organización, promoviendo la transparencia y la equidad en la aplicación de las medidas de seguridad cibernética en el país.**

**Artículo 40. El Consejo establecerá los lineamientos de operación de los mecanismos de monitoreo y detección de amenazas cibernéticas, mediante el uso de herramientas tecnológicas avanzadas, el intercambio de información entre entidades gubernamentales y la cooperación con organismos internacionales especializados en ciberseguridad.**

**Artículo 41. Se adoptarán medidas específicas para la protección de las infraestructuras críticas de México, incluyendo sectores como energía, transporte, salud, finanzas, telecomunicaciones y gobierno, que son fundamentales para el funcionamiento y la seguridad del país.**

**Las autoridades de conformidad a lo señalado en el Artículo 39 de la Ley, establecerán criterios, políticas y estándares de seguridad para las infraestructuras críticas, que incluyan la implementación de controles de acceso, sistemas de detección de intrusiones, protocolos de respuesta ante incidentes, así como planes de contingencia y recuperación de desastres.**

**Artículo 42. El Consejo promoverá la colaboración entre los operadores de infraestructuras críticas y las autoridades de ciberseguridad para la identificación y mitigación de posibles vulnerabilidades, así como la realización de ejercicios y simulacros de seguridad para evaluar la preparación y capacidad de respuesta ante posibles ataques cibernéticos.**

**Así como generar convenios en la materia con las entidades federativas, para la colaboración y la cooperación en materia de ciberseguridad, mediante la participación en foros, iniciativas y programas de cooperación multilateral.**

**Artículo 43. El Consejo Nacional de Ciberseguridad propondrá al Titular del Ejecutivo, la distribución de facultades en materia de ciberseguridad en México, para ejercer las siguientes competencias:**

I. **Formular y ejecutar políticas y estrategias nacionales de ciberseguridad, en coordinación con otros órganos y entidades del gobierno.**

II. **Supervisar y regular el cumplimiento de las disposiciones normativas en materia de ciberseguridad por parte de entidades públicas y privadas.**

III. **Coordinar la respuesta y la gestión de incidentes cibernéticos, en colaboración con otros actores relevantes del sector público y privado.**

IV. **Promover la colaboración y la cooperación internacional en materia de ciberseguridad, mediante la participación en foros, iniciativas y programas de cooperación multilateral.**

**Artículo 44. El Consejo Nacional de Ciberseguridad propondrá al Titular del Ejecutivo una estructura institucional multidisciplinaria en el ámbito de la ciberseguridad, conformada por diversas entidades y organismos del gobierno, sector privado, academia y sociedad civil, con el fin de garantizar una respuesta integral y coordinada ante las amenazas cibernéticas.**

**Artículo 45. El Consejo Nacional de Ciberseguridad coordinará con la Secretaría de Hacienda y Crédito Público los planes y lineamientos para que las autoridades competentes en ciberseguridad cuenten con los recursos humanos, técnicos y financieros necesarios para cumplir con sus funciones y responsabilidades en la protección de los sistemas y datos digitales del país, incluyendo la capacitación y el desarrollo de capacidades en el ámbito de la ciberseguridad.**

## Capítulo Segundo

## De la Coordinación y Homologación

**Artículo 46. El marco regulatorio en materia de ciberseguridad y resiliencia operacional en México estará basado en los compromisos internacionales**

**asumidos por el país en este ámbito, incluyendo tratados, convenciones y acuerdos multilaterales relacionados con la protección de sistemas y datos digitales.**

**Artículo 47. El Consejo debe procurar que las disposiciones normativas nacionales en ciberseguridad sean coherentes y compatibles con los estándares y principios establecidos en los instrumentos internacionales ratificados por México, con el fin de garantizar la armonización y la interoperabilidad con las regulaciones de otros países y promover la cooperación internacional en la lucha contra las amenazas cibernéticas transnacionales.**

**Artículo 48. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital coordinarán sus acciones y esfuerzos con otras entidades y organismos del gobierno, sector privado, academia y sociedad civil, con el fin de promover una respuesta integrada y eficaz ante las amenazas cibernéticas.**

**Artículo 49. El Consejo en apego de sus facultades, promoverá la homologación y actualización de la legislación nacional en materia de ciberseguridad con los estándares y normativas internacionales establecidos en tratados, convenciones y acuerdos suscritos por México, con el fin de garantizar la coherencia y la convergencia con las regulaciones de otros países en este ámbito.**

## Título Quinto

## Combate al Ciberdelito

### Capítulo Primero

### Respeto a los derechos humanos en el ciberespacio

**Artículo 50. El Consejo deberá establecer los mecanismos de supervisión y control para garantizar el respeto a los derechos humanos en el ciberespacio, con la participación activa de autoridades competentes, organizaciones de la sociedad civil y otros actores relevantes, de acuerdo con lo establecido en la**

**legislación nacional y los tratados internacionales de los que México sea parte.**

**Artículo 51. El Consejo deberá establecer los mecanismos de supervisión y control para garantizar la prohibición de cualquier actividad que se realice a través del ciberespacio o en plataformas digitales, que atenten contra los derechos fundamentales de las personas, incluyendo la difusión de información falsa o discriminatoria, el acoso cibernético, la suplantación de identidad, la vulneración a derechos de propiedad intelectual y cualquier forma de violencia o discriminación basada en género, orientación sexual, raza, religión, nacionalidad u origen étnico, sin que dicha supervisión y control límite o transgreda los derechos humanos de los ciudadanos.**

**Artículo 52. El Consejo promoverá la educación y la concientización sobre el uso responsable y ético de las tecnologías de la información y la comunicación, así como la promoción de la cultura digital basada en el respeto a los derechos humanos, con especial interés y apoyo de las instituciones académicas públicas y privadas, así como los centros de capacitación en el país.**

## Capítulo Segundo

## Delimitación de Delitos

**Artículo 53. Se define como delito cibernético cualquier acción u omisión que viole la seguridad, la integridad, la confidencialidad y/o la disponibilidad de la información digital, los datos electrónicos, así como de los sistemas informáticos y las redes de comunicaciones o servicios en línea, con el fin de obtener un beneficio ilícito o causar un perjuicio a terceros.**

**Artículo 54. Se identifican como delitos cibernéticos, entre otros, el acceso no autorizado a sistemas informáticos, el sabotaje cibernético, el robo de información confidencial, el fraude electrónico, el espionaje cibernético, la difusión de malware, el gromming y la distribución de contenidos ilegales en línea, la suplantación de identidad, el espionaje informático, el acceso ilícito a computadoras o redes o sistemas informáticos, las estafas para obtener datos privados de los usuarios (phishing), la modificación, daño, uso, divulgación, copia o sustracción de datos o programas de computación sin autorización debida, así como aquellas conductas de acción omisión que atenten contra la**

**confidencialidad, la integridad y la disponibilidad de los datos, información y/o sistemas informáticos.**

**Artículo 55. El Consejo deberá analizar, vigilar y proponer la actualización de las penas y sanciones contenidas en el Código Penal Federal relativas a los delitos cibernéticos, las cuales deben ser proporcionales a la gravedad de la conducta, considerando el daño causado, el grado de premeditación y la intención delictiva del autor o autores.**

**Artículo 56. El consejo deberá fomentar la cooperación internacional en la investigación y persecución de delitos cibernéticos, mediante la suscripción de acuerdos de colaboración, convenios, intercambio de información y cualquier otro instrumento jurídico o administrativo adecuado, que se realice entre autoridades competentes de diferentes países.**

**De la misma forma, deberá fomentar la cooperación dentro de territorio nacional, en la investigación y persecución de delitos cibernéticos, mediante la suscripción de acuerdos de colaboración, convenios, intercambio de información y cualquier otro instrumento jurídico o administrativo adecuado, que se realice entre autoridades competentes de cada estado, así como con las instituciones académicas públicas y privadas, la sociedad civil, las organizaciones y/o empresas relacionadas con las tecnologías de información y comunicación.**

## Capítulo Tercero

## Figuras especializadas en ciberseguridad.

**Artículo 57. El Consejo deberá proponer al Titular del Ejecutivo Federal la creación de figuras jurídicas que coadyuven a los objetivos del Consejo y de la presente Ley como son:**

I. **Perito en materia ciberseguridad: Profesional especializado en la investigación y análisis de delitos cibernéticos, con conocimientos técnicos y jurídicos para recopilar pruebas digitales y brindar asesoramiento experto en procesos judiciales relacionados con la ciberseguridad.**
II. **Perito en seguridad de la información digital: Profesional especializado en mecanismos e instrumentos, y soporte informático para el resguardo**

**y protección, de la confidencialidad, integridad y disponibilidad de la información digital.**

III. **Perito en informática y cibernética forense: Profesional especializado en las formas de procesamiento de los datos y/o información digital, así como su seguridad a través del uso de tecnologías de la información y comunicación en el ciberespacio.**

IV. **Oficial de seguridad de la información digital, así como de sistemas informáticos y cibernéticos: Profesional experto en materia de ciberseguridad, seguridad de la información digital, así como de sistemas y procesos en el ámbito de la informática y cibernética.**

**Artículo 58. El Consejo deberá coordinar con la Fiscalía General de la República, el establecimiento de la figura de fiscal especializado en delitos cibernéticos, que será el funcionario encargado de investigar y perseguir los delitos cometidos en el ámbito digital, con formación y experiencia en las materias de ciberseguridad, informática, forense digital y tecnologías de la información.**

**Artículo 59. El Consejo a través de la ENC deberá evaluar que la Fiscalía General de la República, y la Secretaría de Seguridad y Participación Ciudadana, designen a unidades especializadas dentro de las fuerzas de seguridad y cuerpos policiales, con la tarea de prevenir, investigar y combatir los delitos cibernéticos, así como de brindar apoyo técnico en la protección de infraestructuras críticas y en la respuesta ante incidentes de seguridad informática, los servidores públicos que integren dichas unidades, se deberán certificar en los rubros que establezca el INFOTEC**

**Artículo 60. El instituto establecerá programas de formación y capacitación especializada en ciberseguridad para personal administrativo y académico en las instituciones de educación superior, asegurando la actualización continua.especializada en ciberseguridad para los profesionales del derecho, las fuerzas de seguridad, los peritos y otros actores involucrados en la investigación y persecución de delitos cibernéticos.**

## Capítulo cuarto

## Combate al ciberdelito

**Artículo 61. El Consejo en coordinación con la Secretaría de Seguridad y Participación Ciudadana establecerá y actualizará el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, que permita fortalecer la actuación de la Guardia Cibernética en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país, con la finalidad de alcanzar los niveles de riesgo aceptables en la materia.**

**Este protocolo deberá ser revisado y actualizado de forma bianual.**

**Artículo 62. La Secretaría de Seguridad y Participación Ciudadana, a través del Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional, brindará los servicios de apoyo en la respuesta a incidentes cibernéticos que afectan a las instituciones en el país que cuentan con infraestructura crítica de información, que incluye la identificación de amenazas y modus operandi de la ciberdelincuencia para el alertamiento a la ciudadanía, mediante la gestión de incidentes de seguridad informática, fungiendo como el único punto de contacto y coordinación dentro y fuera del territorio nacional y actuando en la investigación forense digital y el análisis técnico policial en apoyo al Ministerio Público, de conformidad a los acuerdos y protocolos emitidos por el Consejo y a lo dispuesto en la Ley de la Guardia Nacional.**

**Artículo 63. La Guardia Cibernética dependerá de la Guardia Nacional de conformidad a lo dispuesto en la Ley de la Guardia Nacional operando de acuerdo al Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos y los lineamientos establecidos por la Secretaría de Seguridad y Participación Ciudadana.**

**Artículo 64. La Estrategia Nacional de Ciberseguridad establecerá las líneas de acción que deberán ser adoptadas y cumplidas por la Guardia Cibernética.**

**Dichos protocolos mínimos comprenderán, al menos, los siguientes aspectos:**

I. **Prevención de Delitos Cibernéticos:**
   A. **Desarrollar y ejecutar estrategias para prevenir delitos cibernéticos, incluyendo campañas de concientización, capacitación y difusión de buenas prácticas en seguridad digital.**

B. Monitorear y analizar tendencias de amenazas cibernéticas para identificar potenciales riesgos y vulnerabilidades en sistemas informáticos y redes.

II. Investigación de Delitos Cibernéticos:
   A. Investigar y recopilar pruebas relacionadas con delitos cibernéticos, incluyendo intrusiones informáticas, fraudes electrónicos, extorsiones en línea y otros actos ilícitos cometidos en el entorno digital.
   B. Colaborar con otras agencias policiales, autoridades judiciales y entidades gubernamentales en la recopilación y análisis de evidencia digital en el marco de investigaciones criminales.

III. Persecución y Arresto de Delincuentes Cibernéticos:
   A. Identificar, localizar y detener a presuntos delincuentes cibernéticos responsables de cometer delitos informáticos y cibernéticos.
   B. Coordinar operativos y acciones tácticas para el arresto y la captura de individuos involucrados en actividades delictivas en el ciberespacio.

IV. Cooperación Internacional en Seguridad Cibernética:
   A. Colaborar con agencias policiales y organismos internacionales en la lucha contra el ciberdelito, facilitando el intercambio de información, la asistencia mutua y la coordinación de operaciones conjuntas.
   B. Participar en redes de cooperación internacional y tratados de asistencia legal mutua en materia de ciberseguridad para fortalecer la capacidad de respuesta y persecución de delitos cibernéticos a nivel global.

V. Desarrollo de Capacidades y Entrenamiento:
   A. Brindar capacitación y entrenamiento especializado en técnicas de investigación cibernética, análisis forense digital y gestión de incidentes cibernéticos a personal policial y otros actores involucrados en la lucha contra el ciberdelito.
   B. Fomentar el desarrollo de capacidades técnicas y tecnológicas en el ámbito de la guardia cibernética para mejorar la efectividad y

**eficiencia en la prevención, detección y persecución de delitos informáticos.**

VI. **Protección de Víctimas y Recuperación de Activos:**
   A. **Brindar apoyo y asistencia a víctimas de delitos cibernéticos, incluyendo asesoramiento legal, psicológico y técnico para mitigar el impacto del incidente y facilitar la recuperación de activos afectados.**
   B. **Colaborar con instituciones financieras, proveedores de servicios de internet y otros actores relevantes en la identificación y recuperación de activos robados o malversados en el contexto de delitos cibernéticos.**

## Capítulo Quinto

## Registro de incidentes cibernéticos

**Artículo 65. El Consejo establecerá un marco normativo para la coordinación efectiva de Equipos de Respuesta a Incidentes Cibernéticos (CSIRT) en México, con el propósito de garantizar una respuesta rápida y coordinada ante eventos cibernéticos adversos.**

**Artículo 66. El Consejo designará y regulará la operación de los CSIRT, los cuales estarán integrados por expertos en ciberseguridad y técnicos especializados en la detección, análisis y mitigación de amenazas cibernéticas.**

**Artículo 67. Los CSIRT tendrán como funciones principales:**

I. **Detectar y analizar incidentes cibernéticos;**

II. **Coordinar la respuesta y la recuperación ante incidentes;**

III. **Proporcionar asesoramiento y apoyo técnico a las organizaciones afectadas;**

IV. **Proporcionar asesoría y capacitación a particulares**

V. Colaborar con otros CSIRT nacionales e internacionales;

**Artículo 68. El INFOTEC establecerá mecanismos de comunicación y colaboración entre los CSIRT y otras entidades relevantes, como la Guardia Cibernética, Ejército Mexicano, Marina Armada de México, organismos gubernamentales, empresas, instituciones académicas y organizaciones de la sociedad civil, para facilitar el intercambio de información y la coordinación de acciones en materia de ciberseguridad.**

**Artículo 69. El INFOTEC deberá crear y administrar un Banco de Datos de Incidentes Cibernéticos con el fin de recopilar, almacenar y analizar información sobre incidentes de seguridad digital ocurridos en México.**

**El Banco de Datos de Incidentes Cibernéticos contendrá registros de incidentes reportados por organizaciones públicas y privadas, así como por ciudadanos, y proporcionará estadísticas y análisis sobre la frecuencia, el impacto y la naturaleza de los incidentes cibernéticos en el país.**

**Artículo 70. El INFOTEC garantizará que el acceso y la gestión de la información almacenada en el Banco de Datos de Incidentes se regirá por estrictas medidas de seguridad y confidencialidad, con el objetivo de proteger la privacidad y la integridad de los datos personales y sensibles.**

**Artículo 71. La información recopilada en el Banco de Datos de Incidentes Cibernéticos se utilizará para mejorar la comprensión de las amenazas cibernéticas, fortalecer las capacidades de respuesta y prevención, y orientar el desarrollo de políticas y estrategias de ciberseguridad en México.**

**Artículo 72. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital promoverán la adopción de estrategias de mejores prácticas en ciberseguridad, basadas en estándares internacionales reconocidos, con el fin de fortalecer la protección de los sistemas y datos digitales en México.**

**Salvo que exista dolo o intención de cometer algún ilícito o alguna de las conductas tipificadas o sancionadas por esta Ley, el hecho de que organizaciones públicas o privadas, o ciudadanos informen o reporten sobre incidentes cibernéticos a las autoridades responsables, no les generará, por ese simple acto, responsabilidad alguna por violaciones de esta Ley.**

**Artículo 73. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital fomentarán la cooperación internacional en materia de ciberseguridad, mediante la participación en foros, iniciativas y programas de colaboración multilateral, con el objetivo de compartir información, experiencias y recursos para hacer frente a las amenazas cibernéticas transnacionales.**

**Artículo 74. El Consejo establecerá mecanismos de coordinación y colaboración con otros países, organizaciones internacionales y agencias especializadas en ciberseguridad, con el fin de fortalecer la capacidad de respuesta y la cooperación en la lucha contra el ciberdelito y otras amenazas digitales.**

## Título sexto

## Seguridad Nacional y Protección de Infraestructura Crítica

### Capítulo Único

**Artículo 75. Se define como riesgos e incidentes cibernéticos de seguridad nacional aquellos incidentes, eventos, acciones o amenazas en la seguridad de la información digital y los sistemas informáticos, que se presentan en el ciberespacio, y que pueden comprometer la integridad, la estabilidad, la soberanía o los intereses fundamentales del Estado mexicano.**

**Se consideran riesgos e incidentes cibernéticos de seguridad nacional, entre otros, los siguientes:**

I. **Ataques cibernéticos contra infraestructuras críticas, como sistemas de energía, comunicaciones, transporte, salud o finanzas, que puedan causar interrupciones significativas en los servicios esenciales para la población y la economía del país.**

II. **Ciberespionaje y actividades de inteligencia cibernética realizadas por actores extranjeros o grupos cibernéticos hostiles con el objetivo de obtener información clasificada, estratégica o sensible para la seguridad nacional.**

III. Ciberataques dirigidos a instituciones gubernamentales, sistemas de defensa, fuerzas armadas o entidades públicas encargadas de la seguridad nacional, con el fin de perturbar o comprometer sus operaciones y capacidades de defensa.

IV. Propagación de desinformación, campañas de influencia o manipulación de la opinión pública a través de medios digitales con el propósito de desestabilizar el orden público, socavar la confianza en las instituciones democráticas o generar conflictos sociales, que provengan o sean promovidos por otros Estados sujetos de derecho internacional.

V. Ataques cibernéticos contra sistemas de información y comunicaciones del Estado mexicano, incluyendo redes gubernamentales, portales web oficiales, bases de datos gubernamentales y servicios electrónicos, con el fin de afectar su funcionamiento o comprometer su seguridad.

Ante la ocurrencia de cualquier riesgo o incidente cibernético de seguridad nacional, las autoridades que integran el Sistema Nacional para la Seguridad y Confianza Digital deberán activar los mecanismos de respuesta y coordinación establecidos en la legislación correspondiente, con el fin de mitigar los efectos, proteger los intereses del Estado y garantizar la seguridad y el bienestar de la población.

Artículo 76. La Secretaría de la Defensa Nacional participará activamente en la protección y defensa de la seguridad nacional en el ámbito cibernético, en coordinación con las autoridades que integran el Sistema Nacional para la Seguridad y Confianza Digital.

Artículo 77. La Secretaría de la Defensa Nacional estará facultada para tomar medidas preventivas y de respuesta ante amenazas cibernéticas que representen exclusivamente un riesgo para la seguridad nacional, en cumplimiento de las disposiciones legales vigentes y respetando los derechos fundamentales de las personas. Para tal efecto, la ejecución de acciones relacionadas a la protección de la ciberseguridad, en contra de amenazas cibernéticas que no representen un riesgo a la seguridad nacional, corresponderá y será responsabilidad de las demás autoridades competentes que prevé la presente Ley.

**Artículo 78. El Consejo en coordinación con el Consejo de Seguridad Nacional establecerán protocolos de colaboración y coordinación entre la Secretaría de la Defensa Nacional y las autoridades civiles responsables de la ciberseguridad, con el fin de garantizar una respuesta integral y efectiva ante incidentes cibernéticos que puedan afectar la seguridad nacional.**

**Artículo 79. El Consejo en coordinación con el Consejo de Seguridad Nacional identificará y clasificará las infraestructuras críticas del país, considerando su importancia para el funcionamiento de los sectores estratégicos de la economía, la sociedad y el Estado. Dicho catálogo será administrado por el Consejo de Seguridad Nacional de conformidad a las disposiciones aplicables en la Ley de Seguridad Nacional.**

**Artículo 80. Se establecerán medidas de protección y seguridad específicas, tanto físicas cómo lógicas, para garantizar la integridad y disponibilidad de las infraestructuras críticas, incluyendo la implementación de controles de acceso, sistemas de detección de intrusos y mecanismos de respuesta ante incidentes cibernéticos.**

**Artículo 81. Las entidades responsables de las infraestructuras críticas deberán realizar un análisis de riesgos cibernéticos e informáticos, teniendo como base la información digital generada, con la finalidad de que adopten medidas de seguridad proporcionales al nivel de riesgo y la importancia estratégica de sus activos, así como colaborar con las autoridades competentes en la implementación de políticas y estándares de ciberseguridad.**

**Artículo 82. Se creará un registro nacional de incidentes cibernéticos específico para infraestructuras críticas, con el fin de recopilar, analizar y compartir información relevante sobre amenazas, ataques y vulnerabilidades que afecten a dichas infraestructuras.**

**Artículo 83. Las entidades responsables de las infraestructuras críticas estarán obligadas a reportar cualquier incidente cibernético que afecte la integridad o disponibilidad de sus sistemas, en un plazo máximo de cuarenta y ocho horas de que se haya resuelto en su caso el incidente, elaborando un informe completo y detallado, sobre las medidas de mitigación y respuesta adoptadas.**

**En caso de que no se resolviera la amenaza o evento cibernético que ponga en riesgo la información, los sistemas e intereses del Estado, se debe informar de manera inmediata, preparando un documento detallado con los pormenores, alcance y magnitud del posible daño o vulneración, así como las medidas adoptadas para solucionarlo, con la intención de establecer el inicio y preparación de los planes de contingencia y recuperación de desastres.**

**Artículo 84. El registro nacional de incidentes cibernéticos en infraestructuras críticas será gestionado por el Consejo de Seguridad Nacional, conforme a lo dispuesto en la Ley de Seguridad Nacional garantizando la confidencialidad y protección de la información sensible, así como su utilización para la mejora continua de la seguridad cibernética en el país.**

## Título séptimo

## Sobre la confianza digital

### Capítulo Primero

### Fomento de la confianza digital.

**Artículo 85. El Consejo deberá establecer los mecanismos de supervisión y control para garantizar la identificación, erradicación y sanción de todas las formas de discriminación, acoso, intimidación, violencia y violación de la privacidad en línea, así como cualquier actividad que atente contra la dignidad humana, la libertad de expresión y otros derechos fundamentales en el entorno digital.**

**Artículo 86. El Consejo a través de la ENC promoverá la educación y la concientización sobre los derechos humanos en el ciberespacio, con especial atención a grupos vulnerables, mediante programas de capacitación, campañas de sensibilización y materiales educativos accesibles y culturalmente relevantes.**

**Artículo 87. El Consejo a través de la ENC debe establecer mecanismos de protección y reparación para las víctimas de violaciones de derechos humanos en línea, incluyendo la atención integral, el acceso a la justicia y la garantía de no repetición de los actos de violencia o discriminación. De conformidad a lo dispuesto en la Ley General de Víctimas.**

**Artículo 88. El Instituto promoverá el uso seguro, responsable y ético de las tecnologías de la información y la comunicación, con el fin de fomentar la confianza de los usuarios en el entorno digital y fortalecer la seguridad cibernética a nivel nacional.**

**Artículo 89. El instituto divulgará las medidas para garantizar la integridad, la disponibilidad y la confidencialidad de la información en línea, incluyendo la adopción de estándares de seguridad, la implementación de buenas prácticas y la promoción de herramientas de protección digital.**

**Artículo 90. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital deben incentivar la colaboración entre el sector público, el sector privado, la sociedad civil y otros actores relevantes, con el fin de desarrollar iniciativas conjuntas para mejorar la confianza digital, compartir información y mejores prácticas, y promover la ciberseguridad en todos los ámbitos.**

**Artículo 91. El Consejo a través de la ENC debe establecer mecanismos de evaluación y seguimiento para medir el nivel de confianza digital en el país, identificar áreas de mejora y tomar acciones correctivas para fortalecer la seguridad y la protección de los usuarios en línea.**

## Capítulo Segundo

## Prevención de campañas de desinformación.

**Artículo 92. El Consejo a través de la ENC debe establecer mecanismos para prevenir y contrarrestar la difusión de desinformación en línea, incluyendo la promoción de la alfabetización mediática y digital, la verificación de datos, y la promoción de fuentes de información fiables y transparentes. Que incluyan cuando menos:**

I. **Establecimiento de protocolos de actuación para la detección y el seguimiento de campañas de desinformación, con la participación de autoridades competentes, organizaciones de la sociedad civil, medios de comunicación y otros actores relevantes.**

II. La promoción de transparencia y la rendición de cuentas en la información en línea, mediante la identificación de fuentes y responsables de contenidos, la promoción de la verificación de hechos y la sanción de prácticas fraudulentas o engañosas.

III. Fomentar la educación y el pensamiento crítico entre los usuarios de Internet, con el objetivo de identificar, cuestionar y rechazar la desinformación y los discursos de odio en línea, así como para promover un uso responsable y ético de la tecnología.

## Título octavo

## Uso ético de nuevas tecnologías y tecnologías emergentes

### Capítulo Único

**Artículo 93.** Se reconoce la importancia de promover un uso ético y responsable de nuevas tecnologías y de tecnologías emergentes como lo son: la inteligencia artificial, computación cuántica, neuro tecnologías y universos digitales inmersivos, con el fin de proteger los derechos y la dignidad de las personas, así como de promover el bienestar social y el desarrollo sostenible.

**Artículo 94.** Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital deben establecer principios éticos para guiar el desarrollo, la implementación y el uso de las tecnologías emergentes, incluyendo la transparencia, la equidad, la responsabilidad, la inclusión y el respeto a la diversidad y a los derechos humanos.

**Artículo 95.** El Consejo Nacional de Ciberseguridad establecerá un marco regulatorio flexible y adaptable, denominado "Sandbox", para la autorización de desarrollos, innovaciones, aplicaciones y modelos de negocio que incorporen nuevas tecnologías en materia de ciberseguridad, bajo un esquema que cumpla con los criterios de seguridad, privacidad y uso ético.

El marco regulatorio permitirá a los desarrolladores, innovadores, empresas y demás entidades interesadas probar y lanzar al mercado desarrollos, innovaciones, aplicaciones y modelos de negocio que incorporen nuevas

**tecnologías en el campo de la ciberseguridad, bajo la supervisión y regulación del Consejo, conforme a lo siguiente:**

I. **Requisitos para la participación en el Sandbox:**
   A. **Presentar una solicitud ante el Consejo Nacional de Ciberseguridad, que incluya información detallada sobre la innovación en ciberseguridad que se pretende desarrollar o implementar.**
   B. **Cumplir con los principios y criterios de seguridad, privacidad y uso ético establecidos en la presente Ley.**
   C. **Contar con un plan de pruebas y evaluación que demuestre la viabilidad y seguridad de la innovación en ciberseguridad.**
   D. **Suscribir un acuerdo con la Autoridad Competente en el que se establezcan las condiciones de participación en el Sandbox.**

II. **La participación bajo este esquema regulatorio tendrá una duración máxima de 24 meses, prorrogables por un periodo adicional de 12 meses.**

III. **Supervisión y evaluación.**
   A. **El Consejo establecerá los criterios y requisitos que los participantes en el régimen de Regulación Sandbox deben cumplir, incluyendo, entre otros, estándares de seguridad cibernética, protección de datos personales y principios éticos en el uso de tecnologías emergentes.**
   B. **El Consejo en coordinación con el Instituto supervisará y evaluará el desarrollo y la implementación de las innovaciones en ciberseguridad autorizadas en el Sandbox.**
   C. **Los participantes de este tipo de autorizaciones estarán obligados a informar regularmente al Consejo sobre el progreso de sus actividades, los resultados obtenidos y cualquier incidente relevante que pueda afectar la seguridad, privacidad o ética de sus tecnologías.**

IV. **El Consejo podrá revocar la autorización para participar en el Sandbox en caso de que se incumpla con las condiciones establecidas en la presente Ley, en el acuerdo suscrito o si se identifican riesgos significativos para la seguridad, privacidad o ética**

V. **El Consejo podrá emitir los reglamentos y lineamientos necesarios para la implementación de este tipo de marcos regulatorios transitorios.**

VI. **Los participantes del marco regulatorio estarán sujetos a un proceso de autorización simplificado y acelerado, que incluirá la evaluación de los**

**riesgos potenciales para la seguridad, privacidad y ética, así como la implementación de medidas adecuadas para mitigar dichos riesgos.**

**Artículo 96. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital deben fomentar la investigación y el desarrollo de tecnologías emergentes que contribuyan al beneficio social y al mejoramiento de la calidad de vida de las personas, priorizando la innovación responsable y el uso de tecnologías para resolver desafíos sociales y ambientales.**

**Artículo 97. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital deben promover el diálogo y la colaboración entre diferentes actores, incluyendo el sector público, el sector privado, la sociedad civil, la academia y la comunidad técnica, con el fin de abordar los riesgos y desafíos éticos asociados al desarrollo y uso de tecnologías emergentes.**

**Artículo 98. Se establece la obligación de incorporar principios de privacidad y seguridad por diseño en el desarrollo y la implementación de sistemas y servicios digitales, con el fin de garantizar la protección de datos personales y la seguridad de la información desde su concepción y a lo largo de todo su ciclo de vida, de conformidad a los principios establecidos en la Legislación Nacional aplicable en materia de protección de datos personales.**

**Artículo 99. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital promoverán la adopción de medidas técnicas y organizativas apropiadas para garantizar la privacidad y seguridad de la información, incluyendo la encriptación de datos, la gestión de accesos y la anonimización de información sensible; de conformidad a los principios establecidos en la legislación nacional aplicable en materia de protección de datos personales.**

**Sujeto al reconocimiento de los derechos humanos en el ciberespacio previstos en esta Ley, toda persona física o moral que transmita, enrute, o suministre conexiones para comunicaciones digitales, o bien, preste servicios en línea a través de dichas conexiones, estarán facultados para que, voluntariamente de buena fe, o bien, previo mandamiento por escrito de cualquier autoridad competente, y en observancia a lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión, den de baja o restrinjan el**

**acceso a direcciones de IP o limiten la disponibilidad de contenidos en portales web en los que se originen o materialicen la comisión de conductas ilícitas en términos de la presente Ley y demás disposiciones aplicables.**

**Esta disposición será igualmente aplicable para portales web cuyo único propósito sea hospedar contenidos que tengan por objeto causar un detrimento a los derechos y libertades cibernéticas que protege esta Ley, y que represente incitación al terrorismo o a la comisión de genocidios, apología al odio nacional, racial o religioso que incite violencia en contra de alguna comunidad en específico, o pornografía infantil.**

**Artículo 100. El INFOTEC deberá establecer estándares y mejores prácticas para la protección de datos y la seguridad de la información, incluyendo la realización de evaluaciones de impacto en la privacidad y la seguridad, la implementación de controles de acceso y la notificación oportuna de brechas de seguridad.**

## Título noveno

## Educación, capacitación y cultura digital

### Capítulo Único

**Artículo 101. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital fomentarán la educación y la sensibilización sobre la importancia de la privacidad y la seguridad de la información, tanto entre los responsables de procesar datos como entre los usuarios finales, con el objetivo de promover una cultura de protección de datos y seguridad digital en la sociedad.**

**Artículo 102. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital promoverán la implementación de programas de concientización y capacitación en ciberseguridad dirigidos a todos los niveles de la sociedad mexicana, con el fin de promover una cultura de seguridad digital y concientizar sobre los riesgos y amenazas cibernéticas.**

**Artículo 103. El Instituto desarrollará materiales educativos, campañas de sensibilización y actividades de formación en ciberseguridad, dirigidas tanto a la población general como a grupos específicos, como estudiantes,**

**profesionales de la tecnología y funcionarios públicos, con el objetivo de mejorar la comprensión y las habilidades en materia de ciberseguridad.**

**Artículo 104. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital fomentarán la colaboración con instituciones educativas, organizaciones de la sociedad civil, el sector privado y otros actores relevantes para promover la adopción de buenas prácticas y el intercambio de conocimientos en ciberseguridad, contribuyendo así a fortalecer la resiliencia y seguridad del ecosistema digital en México.**

**Artículo 105. El Instituto establecerá programas de capacitación en ciberseguridad dirigidos a diferentes poblaciones en México, con el objetivo de fortalecer la conciencia y las habilidades en materia de seguridad digital en diversos sectores de la sociedad.**

**Las poblaciones objetivo de los programas de capacitación incluirán, entre otras, las siguientes:**

I. **Funcionarios públicos: Se impartirán cursos de formación en ciberseguridad dirigidos a empleados del gobierno en todos los niveles y áreas, con énfasis en la protección de sistemas y datos gubernamentales y la prevención de incidentes cibernéticos.**

II. **Sector empresarial: Se desarrollarán programas de entrenamiento para empresarios, directivos y empleados de empresas de todos los tamaños y sectores, con el fin de promover la implementación de buenas prácticas en seguridad informática y la protección de la información confidencial y sensible.**

III. **Profesionales de TI: Se ofrecerán cursos, licenciaturas, ingenierías, posgrados de especialización en ciberseguridad para profesionales de tecnologías de la información y comunicación (TIC), con el objetivo de mejorar sus habilidades en detección, análisis y respuesta ante amenazas cibernéticas.**

IV. **Ciudadanía en general: Se desarrollarán campañas de sensibilización y capacitación en ciberseguridad dirigidas al público en general, con el objetivo de promover una cultura de seguridad digital y concientizar sobre las amenazas y los riesgos en el ciberespacio.**

V. Se integrarán contenidos de ciberseguridad en los programas educativos de todos los niveles, desde la enseñanza básica hasta la educación superior, con el fin de sensibilizar a estudiantes y docentes sobre los riesgos y las medidas de protección en el entorno digital.

Artículo 106. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital en colaboración con la autoridad educativa federal y estatal, integrarán contenidos de ciberseguridad en los programas educativos de todos los niveles, desde la enseñanza básica hasta la educación superior, con el fin de sensibilizar a estudiantes y docentes sobre los riesgos y las medidas de protección en el entorno digital.

Artículo 107. Las autoridades que formen parte del Sistema Nacional para la Ciberseguridad y Confianza Digital establecerán estrategias integrales de concientización y promoción de una cultura de ciberseguridad en México, con el objetivo de sensibilizar a la población sobre los riesgos y las buenas prácticas en el uso seguro de las tecnologías de la información y comunicación.

Las estrategias de concientización y cultura de ciberseguridad incluirán, entre otras, las siguientes acciones:

I. Campañas de sensibilización: Se desarrollarán campañas de comunicación y difusión dirigidas a la población en general, con mensajes claros y accesibles sobre los riesgos cibernéticos y las medidas de protección recomendadas.

II. Eventos y actividades educativas: Organización seminarios, talleres, conferencias y eventos públicos sobre ciberseguridad, en colaboración con instituciones educativas, organizaciones civiles y el sector privado, con el fin de promover el intercambio de conocimientos y experiencias en este ámbito.

III. Material educativo: Se producirán y distribuirán materiales educativos y recursos didácticos sobre ciberseguridad, incluyendo folletos, guías, manuales y videos informativos, dirigidos a diferentes grupos de edad y niveles de educación.

**IV. Participación comunitaria: Se fomentará la participación activa de la comunidad en la promoción de la ciberseguridad, mediante la creación de redes de apoyo y colaboración entre ciudadanos, organizaciones locales y autoridades, para compartir información y buenas prácticas en la prevención de incidentes cibernéticos.**

**V. Evaluación y seguimiento: Se realizarán evaluaciones periódicas de las estrategias de concientización y cultura de ciberseguridad, con el fin de medir su impacto y efectividad, y realizar ajustes y mejoras en función de los resultados obtenidos.**

**Artículo 108. Se establecerán programas de capacitación en ciberseguridad específicamente diseñados para comunidades indígenas, personas con discapacidad y otros grupos vulnerables en México, con el objetivo de garantizar su acceso equitativo a la información y promover su inclusión digital segura en el entorno cibernético.**

**Los programas de capacitación considerarán las particularidades culturales, lingüísticas y sociales de las comunidades indígenas, así como las necesidades específicas de las personas con discapacidad, con el fin de adaptar los contenidos y metodologías de enseñanza para garantizar su comprensión y participación efectiva en los cursos de ciberseguridad.**

**Los programas de capacitación incluirán contenidos sobre los riesgos y las amenazas cibernéticas específicas que enfrentan las comunidades indígenas, las personas con discapacidad y otros grupos vulnerables, así como medidas de protección y buenas prácticas para prevenir y mitigar estos riesgos.**

**Artículo 109. Se promoverá la colaboración con organizaciones indígenas, asociaciones de personas con discapacidad y grupos de la sociedad civil que trabajen en la promoción de los derechos digitales y la inclusión digital de estos sectores de la población, con el fin de desarrollar programas de capacitación adecuados a sus necesidades y realidades.**

**Artículo 110. Se establecerán mecanismos de seguimiento y evaluación de los programas de capacitación, con el fin de verificar su efectividad y realizar ajustes según sea necesario para garantizar su impacto positivo en la seguridad digital y la inclusión de los grupos destinatarios.**

**Las violaciones a esta Ley que constituyan delitos serán sancionadas conforme a lo establecido en el Código Penal Federal y demás disposiciones aplicables.**

**SEGUNDO.- Se reforman los artículos 168 Bis, 177, 199 Septies, 199 Octies 200, 202, 202 Bis, 211 Bis 1, 211 Bis 2, 211 Bis 3, 211 Bis 4, 211 Bis 5, 390, 403 y 424 bis y se adicionan los artículos 200 Bis, 211 Bis 8, 211 Ter, 211 Quáter, 387 fracciones XXII y XXIII, 403 fracción IV y 424 bis fracción II del Código Penal Federal, para quedar como sigue:**

## TITULO QUINTO
## Delitos en Materia de Vías de Comunicación y Correspondencia

### CAPÍTULO I
### Ataques a las vías de comunicación y violación de correspondencia

**Artículos 165 a 168.- ...**

**Artículo 168 Bis.-** Se impondrán de seis meses a dos años de prisión y multa de trescientos a tres mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien deliberada e ilegítimamente:

I. a II.

III. Produzca, venda, obtenga para su utilización, arriende, importe, difunda o que mediante cualquier otra forma ponga a disposición:

a) Dispositivos, incluidos programas informáticos diseñados o adaptados principalmente para la intervención de comunicaciones privadas, geolocalización o la interceptación de datos de navegación en internet sin consentimiento;

b) Contraseñas, códigos de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático sin consentimiento.

IV. Produzca, venda, obtenga para su utilización, arriende, difunda o que mediante cualquier otra forma ponga a disposición dispositivos electrónicos, programas informáticos o tecnologías de comunicación que permitan la obtención encubierta de datos, información confidencial o que atenten contra la privacidad.

V. Posea alguno de los elementos contemplados en la fracción anterior, con la intención de ser utilizados para cometer ilícitos relacionados con la violación de

confidencialidad, integridad, privacidad y disponibilidad de la información y sistemas informáticos.

**Artículos 169 a 176.- ...**

**Artículo 177.-** Se impondrán de seis a doce años de prisión y multa de trescientos a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien, sin mandato de autoridad judicial competente, intercepte o intervenga comunicaciones privadas o los datos transmitidos a través de las redes o servicios públicos de telecomunicaciones o por cualquier medio o método, datos informáticos en transmisiones dirigidas a un sistema o equipo informático, originadas desde otro sistema o equipo, o realizadas dentro del mismo, incluidas las emisiones electromagnéticas y radiofrecuencias provenientes de un sistema o equipo informático que transporte dichos datos informáticos.

La pena prevista en este artículo se duplicará para el caso de servidores públicos que en ejercicio de sus funciones o aprovechando su cargo, ordenen, permitan, autoricen o realicen las conductas señaladas en este artículo, además de la privación del cargo y la inhabilitación para ocupar otro hasta por cinco años.

## TITULO OCTAVO

## DELITOS CONTRA EL LIBRE DESARROLLO DE LA PERSONALIDAD.

### CAPÍTULO I
### Corrupción de Menores de Edad, de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo.

**Artículo 199 Septies.-** Se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil días multa a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo y le requiera imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual.

**Se impondrá la misma sanción a quien haciendo uso de sistemas, software, y/o herramientas basados en inteligencia artificial, cree audios, fotografías o**

**videos de índole sexual, en las que simulen aparecer personas que correspondan a las señaladas en el párrafo anterior.**

**Artículo 199 Octies.-** Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.

Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.

**Se impondrá la misma sanción a quien haciendo uso de sistemas, software, y/o herramientas basados en inteligencia artificial, cree audios, fotografías o videos de índole sexual, en las que simulen aparecer personas que correspondan a las señaladas en el párrafo anterior.**

Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización.

**Artículo 200.-** Se impondrán de seis meses a cinco años de prisión y multa de trescientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que financie, comercie, distribuya, exponga, ponga en circulación, oferte, difunda o transmita a menores de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales, simulados o creados por medios tecnológicos, sea de manera física, o a través de cualquier medio electrónico, digital o de dispositivos de almacenamiento de datos informáticos.

...

**Artículo 200 Bis.-** Comete el delito de acoso cibernético quien utiliza la tecnología para amenazar, intimidar, acosar o humillar a alguien con la intención de dañarlo social, psicológica o físicamente. A quien cometa el delito de acoso cibernético se le impondrán de seis meses a cinco años de prisión y multa de trescientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente.

## TITULO NOVENO

**Revelación de secretos y acceso ilícito a sistemas y equipos de informática**

**Capítulo II**
**Acceso ilícito a sistemas y equipos de informática**

**Artículo 211 Bis 1.-** Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información o datos informáticos contenidos en equipos, redes, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos por algún mecanismo de seguridad físico y/o digital.

Se le impondrán de tres meses a un año de prisión y multa de cincuenta a ciento cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización modifique, cause daño u obstaculice por cualquier medio o método, el funcionamiento de equipos o sistemas informáticos protegidos contra el acceso no autorizado.

Se le impondrán de uno a tres años de prisión y multa de ciento cincuenta a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización, por cualquier medio o método, modifique, dañe, deteriore, suprima o provoque la pérdida parcial o total de información o datos informáticos contenidos en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos contra el acceso no autorizado.

**Artículo 211 Bis 2.-** Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización altere, modifique, destruya o provoque por cualquier medio o método, la pérdida, inaccesibilidad, parcial, o total de información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, protegidos por algún mecanismo de seguridad.

Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, infringiendo medidas de seguridad con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Se le impondrán de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización acceda, conozca, obtenga, copie, extraiga o utilice información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales de seguridad pública, protegidos por algún mecanismo de seguridad.

Si el responsable es o hubiera sido servidor público en una institución de seguridad pública o de justicia penal, se le destituirá y se le impondrá una inhabilitación de cuatro a diez años para desempeñarse en otro cargo público.

...

**Artículo 211 Bis 3.-** Se le impondrán de dos a ocho años de prisión y multa de trescientos a novecientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que, estando autorizado para acceder a equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, del Estado, indebidamente, por cualquier medio o método altere, modifique, extraiga, destruya, dañe, deteriore, suprima, encripte o provoque pérdida parcial o total de información contenida en dichos equipos, sistemas o medios de almacenamiento del Estado.

Se le impondrán de uno a cuatro años de prisión y multa de ciento cincuenta a cuatrocientos cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado, indebidamente copie o reproduzca información contenida en equipos, sistemas o medios de almacenamiento, físicos o virtuales del Estado.

Se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales, en materia de seguridad pública, indebidamente obtenga, extraiga, copie, facilite o utilice información que contengan. 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 establecida, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro cargo público.

**Artículo 211 Bis 4.-** Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización cause daño, altere u obstaculice, por cualquier medio o método, el funcionamiento de sistemas o equipos de informática

de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad físico y/o digital.

Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización, por cualquier medio o método, modifique, altere, deteriore, suprima, encripte, destruya o provoque la pérdida parcial o total de información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

Se le impondrán de tres meses a dos años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga, reproduzca, o difunda, para beneficio propio o de un tercero, por cualquier medio o método, información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

**Artículo 211 Bis 5.-** Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero indebidamente altere, modifique, destruya, inhiba, bloquee o provoque pérdida parcial o total de información contenida en sistemas o equipos de informática por cualquier mecanismo o método.

Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales de las instituciones que integran el sistema financiero, indebidamente copie, extraiga, reproduzca, o difunda información, para beneficio propio o de un tercero.

...

**Artículo 211 Ter.-** Se le impondrán de cuatro a ocho años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización introduzca, altere, borre o suprima datos informáticos que

generen datos no auténticos con la intención de que sean tomados o utilizados como auténticos para efectos legales, con independencia de que los datos sean directamente legibles e inteligibles.

Se impondrá pena de cuatro a diez años de prisión y multa de doscientos a quinientos de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente en los casos siguientes:

a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito, lucrar; y,

b) Cuando los actos descritos en el inciso anterior se realicen para inducir a usuarios a la provisión de datos confidenciales, personales y/o financieros, tanto de personas físicas como de personas morales.

**Artículo 211 Quáter.-** Se le impondrán de uno a cuatro años de prisión y multa de cien a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien usurpe la identidad de otra persona, a través de un sistema o medio informático, o infringiendo medidas de seguridad físicas o digitales, con la intención de causar un daño o perjuicio a una persona, u obtener un beneficio indebido, para sí mismo o para otra persona.

Las penas señaladas en este artículo se incrementarán hasta en una mitad cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su formación, profesión o empleo para ello.

## TITULO VIGESIMO SEGUNDO
## Delitos en Contra de las Personas en su Patrimonio

### CAPÍTULO III
### Fraude

**Artículo 386.- ...**

**Artículo 387.-** Las mismas penas señaladas en el artículo anterior, se impondrán:

**I a XXI.-** ...

**XXII.** Al que causare un perjuicio patrimonial a otro, mediante la introducción, alteración, borrado o supresión de datos informáticos.

Asimismo, a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.

**XXIII.** A quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.

## CAPITULO III BIS
## Extorsión

**Artículo 390.-** Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa.

Las penas se aumentarán hasta un tanto más si el constreñimiento se realiza por una asociación delictuosa, o por servidor público o ex-servidor público, o por miembro o ex-miembro de alguna corporación policial o de las Fuerzas Armadas Mexicanas. En este caso, se impondrá además al servidor o ex-servidor público y al miembro o ex-miembro de alguna corporación policial, la destitución del empleo, cargo o comisión y la inhabilitación de uno a cinco años para desempeñar cargo o comisión público, y si se tratare de un miembro de las Fuerzas Armadas Mexicanas en situación de retiro, de reserva o en activo, la baja definitiva de la Fuerza Armada a que pertenezca y se le inhabilitará de uno a cinco años para desempeñar cargos o comisión públicos.

**Las penas previstas en este artículo se duplicarán si el constreñimiento se realiza a través de un medio de comunicación digital o electrónica.**

**Las penas previstas en este artículo se triplicarán si la extorsión es con motivo de la divulgación de contenido íntimo sexual de una persona, real o simulado.**

**Artículo 403.-** Se impondrán de veinte a doscientos días multa y prisión de uno a seis años, a quien:

I. a III. (...)

**IV. Obstaculice, impida o interfiera dolosamente, de manera física o virtual, la organización y el desarrollo normal de las votaciones, el escrutinio y cómputo, el traslado y entrega de los paquetes y documentación electoral, el adecuado ejercicio de las tareas de los funcionarios electorales, o que pretenda alterar los resultados de las elecciones;**

...

## TITULO VIGESIMO SEXTO
## De los Delitos en Materia de Derechos de Autor

**Artículo 424.- ...**

**Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. ...

**II.** A quien fabrique con fin de lucro un dispositivo o sistema **físico o digital,** cuya finalidad sea desactivar, inhibir o alterar los dispositivos electrónicos de protección de un programa de computación.

## RÉGIMEN TRANSITORIO

**PRIMERO.** El presente decreto entrará en vigor a los sesenta días posteriores al de su publicación en el Diario Oficial de la Federación.

**SEGUNDO.** La persona Titular del Ejecutivo Federal nombrará al Titular del Consejo Nacional de Ciberseguridad dentro de los treinta días posteriores a la entrada en vigor del presente.

**TERCERO.** El Consejo deberá quedar instalado y celebrar su primera reunión, durante los sesenta días siguientes al inicio de la vigencia de la presente Ley.

**CUARTO.** El Ejecutivo Federal expedirá y publicará las disposiciones reglamentarias de esta Ley, dentro de los 180 días posteriores a la entrada en vigor del presente ordenamiento.

**QUINTO.** El Ejecutivo Federal deberá establecer dentro de los 30 días posteriores a la entrada en vigor del presente ordenamiento, las medidas presupuestarias necesarias para el cumplimiento de la presente Ley.

**SÉPTIMO.** El Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad deberá adecuar su estatuto orgánico, dentro de los sesenta días naturales siguientes a la entrada en vigor del presente Decreto.

**OCTAVO.** Las disposiciones reglamentarias y administrativas y las normas oficiales mexicanas en vigor, continuarán aplicándose hasta en tanto se expidan los nuevos

ordenamientos que los sustituyan, salvo en lo que se expide por virtud del presente Decreto.

**NOVENO.** La Fiscalía General de la República y la Guardia Nacional, deberán implementar un programa permanente de capacitación especializada en materia de ciberseguridad y ciberdelincuencia dirigido a las autoridades y personal de las entidades gubernamentales federales responsables de la denuncia e investigación de los delitos en la materia.

**DÉCIMO.** El Consejo de la Judicatura Federal deberá implementar un programa permanente de capacitación judicial continua y especializada en materia de ciberseguridad y ciberdelincuencia dirigido a las autoridades de los órganos jurisdiccionales federales responsables en sancionar los delitos en la materia.

**DÉCIMO PRIMERO.** Se derogan todas las disposiciones que contravengan al presente decreto.

Dado en el Salón de Sesiones de la Comisión Permanente del H. Congreso de la Unión, a 14 de agosto de 2024.

**Atentamente**

**Senadora Alejandra Lagunes Soto Ruíz**