INICIATIVA DE LA SENADORA JESÚS LUCIA TRASVIÑA WALDENRATH, CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD CIUDADANA Y SE DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL

SENADOR GERARDO FERNÁNDEZ NOROÑA
PRESIDENTE DE LA MESA DIRECTIVA
DEL SENADO DE LA REPUBLICA
P R E S E N T E.-

La suscrita, **Jesús Lucia Trasviña Waldenrath**, Senadora de la República en la LXVI Legislatura e integrante del Grupo Parlamentario del Movimiento de Regeneración Nacional (MORENA), con fundamento en los artículos 71, fracción II, 72, 73 de la Constitución Política de los Estados Unidos Mexicanos; los artículos 8 numeral 1, fracción I, 163, fracción I, 164, 169, 171 y 172 del Reglamento del Senado de la República, me permito someter a consideración de esta Soberanía la siguiente **Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad Ciudadana** y se derogan diversas disposiciones del Código Penal Federal, al tenor de las siguientes:

Consideraciones

La ciberseguridad se ha convertido en una prioridad global en la última década, ya que la interconexión digital entre ciudadanos, gobiernos, empresas e infraestructuras críticas de información se incrementa continuamente. Aunado al uso de la Inteligencia Artificial (IA) en los servicios de las Tecnologías de la Información y Comunicación (TIC) y la Internet de las Cosas (IoT), está transformando la forma en que las personas interactúan, trabajan, estudian, conviven y comunican con su entorno. Mientras aumenta el número de usuarios conectados a internet, la seguridad y la resiliencia no se ha tomado en cuenta como parte de una cultura tecnológica, lo que provoca insuficiencias en la ciberseguridad. En este contexto, se aprecia la necesidad imperante de una legislación actualizada y sólida en materia de ciberseguridad ciudadana para proteger a los individuos y a la sociedad en su conjunto frente a los riesgos asociados al uso indebido de las Tecnologías de la Información y Comunicación y la Internet.

De acuerdo a la Unión Internacional de Telecomunicaciones (UIT), se estima que en 2023 el sesenta y siete porciento de la población mundial, lo que equivale a 5,400 millones de personas, estaban conectadas a Internet. De esta población mundial, el setenta nueve por ciento de las personas de entre 15 y 24 años utilizan Internet.[1]

La Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023 realizada por el INEGI, se estimó que en México en 2023 había poco más 97

[1] Medición del desarrollo digital. Datos y cifras 2023, disponible en: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

millones de personas usuarias de internet, lo que representa el ochenta y dos punto dos por ciento de la población de seis años o más.[2]

La ciberseguridad son todas aquellas actividades necesarias para la protección de: las redes y sistemas de información; de los usuarios de estos sistemas; y de todas las personas afectadas. La ciberseguridad también implica el desarrollo de políticas y procedimientos de seguridad cibernética, la capacitación de los usuarios sobre buenas prácticas de seguridad de información y la realización de evaluaciones y pruebas de seguridad de información para identificar y mitigar vulnerabilidades.

Para el Estado Mexicano la importancia de la ciberseguridad no solo se trata de proteger datos y sistemas, sino también de preservar el bienestar de los individuos en un entorno digital cada vez más complejo. En un contexto global donde el uso de dispositivos móviles y redes sociales se ha vuelto universal, es fundamental que existan leyes que salvaguarden la información personal, regulen el acceso a los datos y sancionen las acciones malintencionadas delictivas.

Los marcos legales adecuados en ciberseguridad pueden reducir la incidencia de ciberataques, pero en muchos países, incluyendo México, la normativa actual aún no es insuficiente. Según el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT, 2021), México se posiciona en el lugar 52 de 194 países, lo que refleja la necesidad de actualizar y robustecer sus políticas de seguridad digital.

Varios incidentes internacionales recientes en el ámbito de la ciberseguridad han tenido un impacto devastador, destacando la importancia de una legislación adecuada.

El ataque de ransomware a Colonial Pipeline (EE. UU., 2021) provocó la interrupción de una de las principales infraestructuras energéticas de Estados Unidos, afectando a millones de personas y generando una crisis de combustible. El ataque fue perpetrado por el grupo de ransomware DarkSide, quienes lograron cifrar sistemas clave de la empresa. Como respuesta, el gobierno estadounidense anunció el fortalecimiento de su ciberseguridad, especialmente para infraestructuras críticas.[3]

La filtración de datos de Facebook en 2019, donde, aproximadamente, 530 millones de usuarios de Facebook en todo el mundo vieron comprometidos sus datos personales, los cuales se expusieron en un foro de hackers. Entre la información filtrada se incluían nombres, números de teléfono y correos electrónicos. Este incidente subraya la importancia de que los gobiernos regulen y supervisen la seguridad de las grandes plataformas sociales para proteger a los usuarios.[4]

Encuanto a SolarWinds y el ciberespionaje en 2020, el ataque se considera uno de los incidentes de ciberseguridad más importantes de la década. Fue un ciberataque dirigido a empresas de tecnología y a agencias gubernamentales en los Estados Unidos, afectando a decenas de organizaciones públicas y privadas. El ataque reveló la vulnerabilidad de las infraestructuras críticas de información

[2] Personas usuarias de TIC. Disponible en: https://www.inegi.org.mx/programas/endutih/2023/#informacion_general
[3] Department of Homeland Security, 2021. Cybersecurity report on Colonial Pipeline attack.
[4] Sveen, S. (2020). "Understanding Facebook's data breach and its implications". Global Information Security, 7(1), 10-15.

y la necesidad de regulaciones de ciberseguridad más estrictas para proteger los sistemas gubernamentales y de empresas que manejan información.[5]

Durante 2022 ha sido evidente el incremento de la actividad por parte de grupos APT (Amenaza Persistente Avanzada, por sus siglas en inglés "Advanced Persistent Threat"), cuyos ataques han afectado incluso a la estabilidad de algunos Estados-Nación, el ejemplo más claro es la actual guerra entre Rusia y Ucrania, que ha puesto de manifiesto el potencial dañino de los ciberataques.

Estos incidentes demuestran que la falta de normas estrictas y actualizadas en ciberseguridad puede generar graves consecuencias para las infraestructuras críticas y la vida de millones de personas.

En México, se ha incrementado los incidentes de ciberseguridad, y han afectan tanto al sector privado como al público. La falta de regulación eficaz en este ámbito expone a la ciudadanía a riesgos significativos.[6]

De acuerdo con el Registro Nacional de Incidentes Cibernéticos del Sistema Nacional de Información de Seguridad Pública, en enero de 2022 comenzó en funciones y hasta noviembre de 2024, se han contabilizado poco más de 200 mil incidentes, reportados por las 32 entidades federativas.

Relativo al ataque al Banco de México en el 2018, el Sistema de Pagos Electrónicos Interbancarios (SPEI) fue atacado, lo que resultó en un robo de aproximadamente 300 millones de pesos. Este incidente subrayó la necesidad de fortalecer las defensas cibernéticas del sistema financiero en México y provocó que las autoridades revisaran los protocolos de seguridad de las instituciones bancarias.[7]

El hackeo a PEMEX en 2019, consistió en que la empresa estatal Petróleos Mexicanos fue víctima de un ataque de ransomware que afectó sus operaciones internas. Este ataque generó una pérdida económica y provocó interrupciones en las operaciones de la empresa. Fue un claro ejemplo de cómo las infraestructuras críticas de información en México están en riesgo frente a los ciberataques y de la necesidad de medidas regulatorias y preventivas.[8]

En 2022 un grupo de hacktivistas llamados Guacamaya penetraron las bases de datos de la Secretaría de la Defensa Nacional (SEDENA) y obtuvieron determinada información comprimida y almacenada en seis terabytes. Estos contenían documentos, fotografías, videos y correos relacionados con las actividades de esa dependencia, tanto de sus miembros como de otros individuos y colectivos nacionales.[9]

---

[5] Romm, T. (2021). "SolarWinds cyberattack: What it means for the US and global cybersecurity". The Washington Post.
[6] Registro Nacional de Incidentes Cibernéticos, SNI Plataforma México. Secretaría de Seguridad y Protección Ciudadana.
[7] Banco de México. (2018). Annual report on cybersecurity in the financial system. Disponible en: https://www.banxico.org.mx/publications-and-press/financial-system-reports/financial-system-reports-supe.html
[8] Flores, J. (2020). "El ataque a Pemex y sus implicaciones en la ciberseguridad de México". Revista Mexicana de Seguridad Informática, 14(2), 12-19.
[9] Cossío, J. (2023). Una Guacamaya(leak) que no hizo primavera. Disponible en: https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/17689/18069

También hubo aumento en ciberataques a ciudadanos durante la pandemia de COVID-19. Durante el confinamiento, los ataques de phishing y las estafas en línea se incrementaron, afectando a miles de usuarios. Según la Unidad de Inteligencia Financiera de México en 2021, estos ataques son una amenaza continua y destacan la importancia de concientizar a la población sobre la ciberseguridad.

Estos incidentes en México no solo reflejan la vulnerabilidad de las infraestructuras críticas de información, sino también la necesidad de crear políticas que protejan a los ciudadanos frente a amenazas cibernéticas.

La legislación en ciberseguridad es esencial por varias razones:

Es la pieza clave para contar con mecanismos para prevenir ciberataques en contra de la confidencialidad, integridad y disponibilidad de la información, al permitir dotar a los equipos técnicos y humanos de las capacidades y legislación necesaria para combatir eficazmente los riesgos cibernéticos.

Protección de la privacidad y derechos digitales. Los ciudadanos tienen derecho a que su información personal esté protegida. La legislación ayuda a asegurar que las empresas y los gobiernos manejen y resguarden adecuadamente los datos personales.

Prevención y sanción de delitos cibernéticos. La ley permite tipificar y penalizar conductas delictivas en el ámbito digital, como el ciberacoso, la violencia de genero digital, el fraude y extorsión en línea y el ciberespionaje.

Fortalecimiento de la infraestructura crítica de información, como las Secretarías de Estado, PEMEX, CFE, CONAGUA, Banco de México, entre otras, es esencial para la seguridad pública. La legislación en ciberseguridad ciudadana ayuda a que estas infraestructuras adopten estándares mínimos de seguridad. La falta de regulación en materia de ciberseguridad genera un vacío que permite la proliferación de ataques y afecta el bienestar y la seguridad de los ciudadanos. Una legislación sólida ayuda a prevenir ciberataques y establece protocolos de respuesta rápida y efectiva ante incidentes.

El presente proyecto de Ley General de Ciberseguridad Ciudadana busca, entre otros aspectos, cubrir las necesidades de contar con un modelo de coordinación de la Ciberseguridad en México, el cual abarca las instancias de seguridad pública de los tres órdenes de gobierno, la Fiscalía General de la Republica y las Fiscalías o Procuradurías Generales Estatales, y la participación de las instancias de Seguridad Nacional, por lo que es necesario definir el marco de coordinación que permita a cada uno de los actores involucrados tener una visión clara de los objetivos que tienen que cumplir para fortalecerla.

En ese sentido, la Secretaría de Seguridad y Protección Ciudadana es la instancia que coordina los diferentes esfuerzos a nivel nacional y que se encarga de generar estrategias y políticas públicas a seguir. Para tal efecto se considera pertinente crear una Agencia Nacional de Ciberseguridad.

Además, es necesario establecer convenios de colaboración internacional que permitan al Estado Mexicano, afrontar los delitos cibernéticos, buscando la homologación de estructuras, de criterios y de preparación de los impartidores de justicia.

Conjuntamente se requiere establecer las bases de colaboración del gobierno con la iniciativa privada a través de las diferentes cámaras industriales, empresas y la población, para combatir delitos cibernéticos en especial aquellos que puedan poner en riesgo a la ciudadanía.

Actualmente las instancias de los tres órdenes de gobierno, paraestatales, instancias autónomas o desconcentradas, empresas de cualquier sector, etcétera, no tienen la obligación de reportar o denunciar incidentes que permitan determinar de forma precisa el estado que guarda la ciberseguridad en su contexto, por lo que es necesario reglamentar el reporte estos incidentes dentro del Registro Nacional de Incidentes Cibernéticos para contar con datos y estadísticas oficiales.

La legislación en ciberseguridad es un imperativo en un mundo cada vez más digitalizado, donde los ciudadanos dependen de la tecnología para realizar transacciones financieras, comunicarse, trabajar y recibir servicios básicos. Los incidentes de ciberseguridad recientes en México y el mundo subrayan la necesidad de establecer políticas que protejan a las personas y garanticen la integridad de las infraestructuras críticas de información. Para avanzar en la protección de la ciudadanía y la soberanía digital, los gobiernos deben actuar con urgencia en la creación y actualización de normas en ciberseguridad, promoviendo un entorno digital más seguro y confiable.

Al tenor de lo anteriormente expuesto y motivado, se pone a la consideración de esta Honorable asamblea el siguiente:

Proyecto de decreto por el que se expide la Ley General de Ciberseguridad Ciudadana y se derogan diversas disposiciones del Código Penal Federal

PRIMERO. Se derogan diversos artículos del Código Penal Federal para quedar como sigue:

Código Penal Federal

Artículo 211 Bis. - Derogado.

Artículo 211 bis 1.- Derogado.

Artículo 211 bis 2.- Derogado.

Artículo 211 bis 3.- Derogado.

Artículo 211 bis 4.- Derogado.

Artículo 211 bis 5.- Derogado.

Artículo 211 bis 6.- Derogado.

Artículo 211 bis 7.- Derogado.

SEGUNDO. Se expide la Ley General de Ciberseguridad Ciudadana, para quedar como sigue:

LEY GENERAL DE CIBERSEGURIDAD CIUDADANA

LIBRO I

TÍTULO PRIMERO

DISPOSICIONES PRELIMINARES

CAPÍTULO I

Disposiciones Generales

Artículo 1.- La presente Ley es reglamentaria de los artículos 4, 6, 21 y 73 fracción XVII de la Constitución Política de los Estados Unidos Mexicanos en materia de Ciberseguridad y tiene por objeto establecer las bases, principios, y distribución de competencias a fin de fortalecer la ciberseguridad para proteger la información digital de los sistemas y aplicaciones, así como las infraestructuras críticas de información, los datos personales y los derechos digitales de los ciudadanos para prevenir las amenazas y daños cibernéticos, estableciendo los mecanismos de coordinación necesarios para la protección y fomento de una cultura en ciberseguridad.

Artículo 2.- Para los efectos de esta Ley, se entenderá por:

I. ANCI: Agencia Nacional de Ciberseguridad.
II. Ciberamenaza: Intentos maliciosos de dañar, interrumpir u obtener acceso no autorizado a sistemas, redes o dispositivos informáticos, a través de medios cibernéticos. Con la intención de producir un riesgo potencial, relacionado a las vulnerabilidades de los sistemas informáticos y de infraestructura física y pasiva de las redes públicas de telecomunicaciones de permitir causar daño a los procesos y continuidad de la seguridad de las personas.
III. Ciberataque: Acción realizada a través de las redes de telecomunicaciones con el objetivo de amenazar, afectar, inhabilitar, destruir, vulnerar, eliminar, negar o modificar la información contenida en un sistema de información, o de dañar en general a organizaciones gubernamentales o de la iniciativa privada, así como la seguridad de las personas.
IV. Ciberdelincuencia: Actividades que llevan a cabo uno o más individuos en el que utilizan como medio o como fin a las Tecnologías de la Información y Comunicación.
V. Ciberespacio: Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico.
VI. Ciberseguridad: Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y en el ciberespacio y las redes públicas de telecomunicación.
VII. Confidencialidad: Propiedad de la información por la que se garantiza que su acceso se encuentra restringido a personal, entidades o procesos autorizados.
VIII. Delito Cibernético: Acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional. Y en la esfera de competencia internacional, son los delitos

cometidos contra datos informáticos, medios de almacenamiento de datos informáticos, sistemas informáticos, y proveedores de servicios.

IX. Estrategia Nacional de Ciberseguridad Ciudadana: Documento que establece la visión, principios y objetivos del Estado Mexicano alineados a las prioridades en materia de ciberseguridad. Implica el desarrollo, implementación, medición y seguimiento de planes y acciones de la visión de un gobierno en materia de ciberseguridad ciudadana.

X. Evidencia Digital: Información almacenada o transmitida en formato digital de tal manera que una parte o toda, y esta pueda ser utilizada en un proceso ante la autoridad que conozca de un caso en concreto.

XI. Información: Todo aquel conjunto de datos organizados y procesados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (física, mensajes de datos, impresa en papel, almacenada electrónicamente, proyectada, transmitida por medios físicos, electrónicos, ópticos o cualquier otra tecnología), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

XII. Infraestructuras Críticas de Información: Las infraestructuras Críticas de información por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.

XIII. Internet: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única. Lo anterior, de conformidad con el artículo 3, fracción XXXII de la Ley Federal de Telecomunicaciones y Radiodifusión.

XIV. Ley: Ley General de Ciberseguridad Ciudadana.

XV. Proveedor de Servicios de Internet: Es la empresa que proporciona una conexión de acceso a Internet a sus clientes (ISP), que incluye tránsito y registro de nombres de dominio.

XVI. Tecnologías de la Información y Comunicación: Conjunto de herramientas, sistemas, programas, recursos, procedimientos que sirven para el almacenamiento y facilitar la emisión, acceso y tratamiento de la información mediante códigos variados que pueden corresponder a textos, imágenes, videos, sonidos, y otros tipos de formatos digitales.

XVII. Vulnerabilidad: Es una deficiencia o fallo de un programa que puede permitir el acceso ilegítimo a la información o el desarrollo de operaciones no permitidas

Artículo 3.- Las disposiciones de esta ley son de orden público y observancia general en todo el territorio nacional y deberán ser aplicadas conforme a su distribución de competencias federal, estatal, y municipal.

Artículo 4.- Son sujetos obligados al cumplimiento de la presente Ley:

a) Las dependencias y entidades de la Administración Pública federal y sus equivalentes en los estados, y municipios.
b) Los poderes legislativo y judicial.
c) Los organismos constitucionales autónomos, y demás instituciones públicas.
d) El sector privado, que incluye a las empresas, organizaciones y operadores de infraestructuras críticas de información.

e) La ciudadanía, en lo que refiere al uso de las Tecnologías de la Información y Comunicación, la Internet, la protección de sus datos personales y la adopción de buenas prácticas en materia de ciberseguridad.

Artículo 5.- El cumplimiento de esta Ley y la función de la ciberseguridad ciudadana se realizará en los diversos alcances de su competencia, estas serán por conducto de la seguridad pública.

La coordinación será el eje rector de las actuaciones en la materia por los tres órdenes de gobierno, para garantizar el debido cumplimiento de esta Ley.

El estado auspiciará la participación privada y social en la integración y ejecución de la Política Nacional de Ciberseguridad.

Artículo 6.- Con el objetivo de coadyuvar con la Secretaría de Seguridad y Protección Ciudadana, se crea la Agencia Nacional de Ciberseguridad, misma que integrará y ejecutará las políticas, instrumentos, acciones y servicios previstos en la presente Ley, tendientes a cumplir los fines de la ciberseguridad.

Artículo 7.- La coordinación, evaluación y supervisión de lo dispuesto en esta Ley, se hará con respeto a lo establecido en los artículos 4, 6, 21 y 73 fracción VXII Constitucional, y conforme a las atribuciones que le correspondan a la Secretaría de Seguridad y Protección Ciudadana. Los gobiernos federal, estatal y municipal, así como las personas físicas y morales en el ámbito de su competencia y atribuciones y en los términos de esta Ley, deberán coordinarse y en su caso realizar concurrencia para cumplir con las atribuciones y obligaciones definidas.

Artículo 8.- 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 Federal de Telecomunicaciones y Radiodifusión;

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

III. La Ley Federal del Derecho de Autor;

IV. La Ley Federal de Protección de Datos Personales en Posesión de Particulares;

V. La Ley para Regular las Instituciones de Tecnología Financiera;

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

VII. La Ley General en materia de Humanidades, Ciencias, Tecnologías e Innovación;

VIII. La Ley General de Títulos y Operaciones de Crédito;

IX. El Código Penal Federal;

X. El Código Nacional de Procedimientos Penales;

XI. La Ley General del Sistema Nacional de Seguridad Pública;

XII. La Ley de Seguridad Nacional; y

XIII. La Ley de la Guardia Nacional.

Artículo 9.- La Agencia Nacional de Ciberseguridad observará lo dispuesto en las resoluciones y acuerdos generales que emita la Secretaría de Seguridad y Protección Ciudadana.

TÍTULO SEGUNDO

POLÍTICA NACIONAL DE CIBERSEGURIDAD

CAPÍTULO I

Principios Rectores

Artículo 10.- Esta Ley General tendrá como principios, los de:

I. Territorialidad. Esta Ley se aplicará por las conductas típicas cometidas dentro del territorio nacional y el ciberespacio, conforme a la competencia que corresponda a las autoridades en los tres órdenes de gobierno.

Se consideran como realizados dentro del territorio nacional y el ciberespacio, no obstante que hayan intervenido ciudadanos mexicanos o extranjeros y éstas puedan haber utilizado las tecnologías de la información y comunicación, ya sea como medio o como fin, y todo tipo de redes, sistemas informáticos, activos de información y procesos para su comisión, los delitos donde el Estado mexicano ejerza su jurisdicción, incluyendo las conductas típicas realizadas:

a) En alta mar, a bordo de buques nacionales;

b) A bordo de algún buque de guerra nacional surto en puerto o en aguas territoriales de otra nación. Esto se extiende al caso en que el buque sea mercante, si la persona imputada no ha sido juzgada en la nación a que pertenezca el puerto;

c) A bordo de un buque extranjero surto en puerto nacional o en aguas del territorio nacional;

d) A bordo de aeronaves nacionales o extranjeras que se encuentren en el territorio, atmósfera, orbita satelital o en aguas territoriales nacionales o extranjeras, en casos análogos a los que señalan para buques las fracciones anteriores.

e) En las embajadas y representaciones mexicanas, y

f) Los cometidos en el ciberespacio que, conforme a los niveles de impacto, organización y sofisticación, dañen o pongan en peligro bienes jurídicos tutelados dentro del territorio nacional.

En los casos anteriores, la competencia será de la Federación;

II. Extraterritorialidad. Esta Ley se aplicará también a personas mexicanas o extranjeras por:

a) Las conductas y delitos que se inicien, preparen o cometan en el extranjero incluido el ciberespacio, así como aquellos que utilicen las tecnologías de la información y comunicación, además de todo tipo de sistemas informáticos y de procesos para su

comisión, cuando se produzcan o que tengan efectos, en el territorio nacional y en todo tipo de sistemas informáticos incluyendo los dominios de internet, o que las consecuencias consistan en poner en peligro o dañar cualquier bien jurídico tutelado.

b) Los delitos permanentes o continuados incluyendo aquellos que utilicen las tecnologías de la información y comunicación, así como las redes y procesos.

c) Las conductas y delitos cometidos tanto en embajadas como en los consulados mexicanos o en contra de su personal, cuando no hubieren sido juzgados en el país en que se cometieron, incluyendo aquellos que utilicen el ciberespacio y las tecnologías de la información y comunicación, así como todo tipo de sistemas informáticos para su comisión, incluyendo los dominios dentro de éste que se empleen o que dañen cualquier bien jurídico tutelado.

Lo previsto en los incisos anteriores será competencia de la autoridad federal pudiéndose realizar con la coordinación y concurrencia de las autoridades locales, municipales y con las demarcaciones territoriales de la Ciudad de México, como se prevé en el artículo 39 de la Ley General del Sistema Nacional de Seguridad Pública.

Las treinta y dos Entidades Federativas y los Municipios que integran la Federación, habrán de colaborar en la aplicación de esta Ley General, por las conductas y por los delitos iniciados o preparados en otra Entidad Federativa, cuando produzcan, o que tengan efectos en su territorio, así como en los delitos permanentes o continuados que se sigan cometiendo en su territorio, refiriéndose a aquellos que utilicen el ciberespacio, los sistemas de las tecnologías de la información y comunicación, y que dañen o pongan en peligro cualquier bien jurídico tutelado y todo tipo de sistemas informáticos para su comisión.

III. Supremacía del Derecho internacional. En el caso en que un Tratado, del que el Estado Mexicano sea parte, establezca una regla de competencia más amplia que la contemplada en esta Ley General, se estará a lo previsto por aquél. Así mismo, deberá tomarse en consideración lo establecido por Organismos Internacionales Especializados en la Materia, y las Tecnologías de la Información y Comunicación.

En cuanto al cumplimiento de la obligación o facultad de extraditar o procesar a extranjero o a persona alguna se estará a lo previsto por el Tratado aplicable. En ningún caso serán competentes los órganos jurisdiccionales nacionales cuando la Corte Penal Internacional haya establecido su competencia y la admisibilidad de un asunto. Lo anterior no obsta para que las policías, fiscalías nacionales, instancias competentes y la Guardia Nacional, investiguen hechos distintos derivados de la misma situación.

Para efectos del ejercicio de la jurisdicción de la Corte Penal Internacional, se estará a lo dispuesto tanto en las Leyes Reglamentarias del artículo 21 de la Constitución Política de los Estados Unidos Mexicanos como en esta Ley General.

IV. Momento y lugar de la comisión del hecho. El hecho de que la ley señale a determinadas conductas como delitos, ello debe comprenderse como lo realizado tanto en el momento y lugar de la manifestación de la conducta como en el momento y lugar en que haya acontecido

el resultado típico, incluyendo aquellos que se desplieguen a través de las tecnologías de la información y comunicación, y cualquier otra tecnología actual o emergente.

V. Validez temporal. Eficacia jurídica de la aplicación respectiva de esta ley general como del derecho vigente en concordancia con los Instrumentos Internacionales aplicables en la materia, tanto en el momento como en el lugar del hecho y de la conducta que se cometa y se encuentre regulada o en su caso sancionada.

VI. Criterio especializado en materia de delitos informáticos. Las conductas típicas, que involucren el ciberespacio, las tecnologías de la información y comunicación, las redes, los sistemas activos de información, que afecten la confidencialidad, la integridad y disponibilidad de la información o cualquier otra tecnología, se atenderá tanto en el ámbito de la puesta en peligro o amenaza como ante el hecho o acto que causó el resultado formal o material, así como por el daño causado a los bienes jurídicos tutelados tanto de las personas físicas como de las personas jurídicas del ámbito público como del privado. Cuando se presenten diferentes interpretaciones se atenderá a lo establecido en la Constitución, en los Tratados Internacionales, así como en los Organismos Internacionales Especializados en la Materia.

CAPÍTULO II

De la Política Nacional de Ciberseguridad Ciudadana

Artículo 11.- La Secretaría de Seguridad y Protección Ciudadana establecerá una Política Nacional de Ciberseguridad Ciudadana que contendrá las acciones necesarias para evaluar riesgos tanto en el sector público como en el privado, promueva las mejores prácticas en el uso de las Tecnologías de Información y Comunicación, proteja los derechos de las personas y su seguridad en el ciberespacio.

Artículo 12.- El objetivo de la Política Nacional de Ciberseguridad Ciudadana es establecer un sistema de coordinación y responsabilidad compartida entre los actores públicos, privados y sociales que permita reducir los incidentes y la posible comisión de delitos cibernéticos, a través de la coordinación y atención de los riesgos que conlleva el uso de las Tecnologías de Información y Comunicación.

Artículo 13.- En el desarrollo de la Política Nacional de Ciberseguridad Ciudadana se deberán considerar los siguientes ejes rectores:

I. Crear la Agencia Nacional de Ciberseguridad Ciudadana, para impulsar y fortalecer la política nacional en la materia;

II. Que todos los sectores participen en el desarrollo de una Estrategia Nacional de Ciberseguridad Ciudadana incluyente, de acuerdo con la Estrategia Nacional de Seguridad Pública y el Plan Nacional de Desarrollo;

III. El acceso a Internet y disponibilidad de servicios de telecomunicaciones;

IV. El respeto a los derechos humanos durante la investigación y persecución de Ciberdelitos;

V. El combate a la delincuencia en el ciberespacio;

VI. Que la seguridad de la información sea responsabilidad de aquel que la ofrece, administra u opera, con independencia de la naturaleza pública o privada del organismo, a partir de las obligaciones y derechos de las partes interesadas;

VII. Que los responsables de Infraestructura Crítica de Información actúen diligentemente y adopten medidas necesarias para prevenir y mitigar incidentes de ciberseguridad o de ciberataques y su posible propagación a otros sistemas informáticos;

VIII. Que los responsables de Infraestructura Crítica de Información públicos y privados tengan la obligación de cooperar con la autoridad para reportar y resolver los incidentes de Ciberseguridad, y cooperar entre diversos sectores, en caso de ser necesario, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios;

IX. Los entes reguladores de los sectores de Infraestructura Crítica definidos en la presente ley deberán mantener actualizadas las normativas especiales y las disposiciones de carácter general considerando al menos lo siguiente:

   a. Garantizar los derechos de los usuarios de los sistemas y servicios que ofrecen con base en los tratados internacionales y los criterios que establezcan los más altos tribunales del Estado Mexicano, eliminando las disposiciones de carácter general que atenten contra su bienestar y patrimonio.

   b. Impulsar la colaboración pública privada para la protección de los servicios esenciales de la población.

   c. Colaborar con las autoridades para la investigación y persecución de los delitos cibernéticos.

   d. Implementar la gestión del riesgo cibernético conforme a las mejores prácticas nacionales e internacionales alineado con el cumplimiento de la misión y objetivos de la instancia que corresponda.

   e. Considerar y atender las disposiciones que emita la Agencia Nacional de Ciberseguridad en el ámbito de su competencia.

X. Las dependencias y entidades de las dependencias y entidades de seguridad pública deberán cumplir con el Marco de Gobierno, Riesgo y Cumplimiento que se define en esta Ley; y

XI. En cumplimiento a las obligaciones de seguridad de los sistemas de información, los responsables de Infraestructura Crítica de Información públicos y privados, y aquellos que administren información de las autoridades de la administración pública estatal, tendrán la obligación de reportar y denunciar incidentes cibernéticos confirmados, a las autoridades facultadas, bajo los procedimientos establecidos en esta ley.

CAPÍTULO III

De la Estrategia Nacional de Ciberseguridad Ciudadana

Artículo 14.- Corresponderá a la Agencia Nacional de Ciberseguridad formular, conducir e impulsar el cumplimiento de una Estrategia Nacional de Ciberseguridad Ciudadana, de su seguimiento y operación en el país. Dicha Estrategia contendrá al menos, lo siguiente:

I. Un diagnóstico general sobre Ciberseguridad en el país, así como la prospectiva de largo plazo;

II. Objetivos específicos, acciones y autoridades de la Entidad responsables de su ejecución;

III. Los indicadores estratégicos que permitan dar seguimiento al logro de los objetivos;

IV. Mecanismos para la generación de esquemas de cooperación nacional e internacional en materia de Ciberseguridad;

V. Promover mecanismos para prevenir y combatir los delitos cibernéticos, utilizando enfoques basados en riesgos;

VI. Promover la investigación científico-tecnológica, programas de formación académica, creación y adopción de estándares, así como el desarrollo de una industria de la ciberseguridad;

VII. Acciones de capacitación, certificación, asistencia, intercambio de información, tecnología y cualquier otro fin relacionado con el análisis y desarrollo de esquemas estandarizados de Ciberseguridad, así como con el uso y protección de las Tecnologías de Información y Comunicación;

VIII. Realizar acciones para gestionar el riesgo, así como la prevención de ataques cibernéticos a los sistemas informáticos, digitales y de las telecomunicaciones tanto públicas como privadas;

IX. Definir esquemas de información y participación ciudadana, mecanismos de proximidad para atender a la población, así como acciones tendientes al fomento de la cultura de la ciberseguridad que contemplen orientar y concientizar a la población sobre la importancia de la Ciberseguridad, uso adecuado de las Tecnologías de Información y Comunicación, la Identidad Digital, e impulsar el desarrollo y aplicación de criterios homologados en la materia y promover programas de prevención para una efectiva adopción y cumplimiento de estos mecanismos;

X. Definir el rol de responsabilidad de los titulares de las dependencias y entidades en la instrumentación de los planes, programas y recursos en ciberseguridad para la protección de sus activos; y

XI. Las demás que se consideren necesarias.

Artículo 15.- La Estrategia Nacional de Ciberseguridad será obligatoria para los tres órdenes de gobierno.

La vigencia de la Estrategia Nacional en materia de Ciberseguridad, no deberá exceder del período constitucional de la gestión gubernamental en que se apruebe, aunque sus previsiones y proyecciones se refieran a un plazo mayor.

TÍTULO III

COORDINACIÓN Y DISTRIBUCIÓN DE COMPETENCIAS

CAPÍTULO I

Distribución de Competencias

Artículo 16.- La Federación, las Entidades Federativas y los Municipios, coadyuvarán para el cumplimiento de los objetivos de esta ley de conformidad con las competencias previstas en el presente ordenamiento y demás instrumentos legales aplicables, para lo cual tomarán las medidas presupuestales y administrativas correspondientes.

La Federación y las entidades federativas deberán contar con fiscalías especializadas para atender los delitos en materia cibernética.

Capítulo II

De la Federación

Artículo 17.- Son facultades y obligaciones de la Federación:

I. Integrar la Comisión Nacional de Ciberseguridad y, coordinar, evaluar y supervisar sus objetivos y fines;
II. Formular la Política Nacional de Ciberseguridad integral, sistemática, continua y medible, asegurando el respeto a los derechos humanos fundamentales, como igualdad, justicia, accesibilidad, confidencialidad, protección de datos, libertad y seguridad;
III. Coordinar el desarrollo, implementación y evaluación de la Estrategia Nacional de Ciberseguridad Ciudadana, en concurrencia con las autoridades competentes;
IV. Ejecutar y, brindar un seguimiento a la evaluación de las políticas, estrategias y acciones, a través de las instancias previstas en esta ley;
V. Distribuir a los integrantes de la Agencia Nacional de Ciberseguridad, actividades específicas para el cumplimiento de los fines de la ciberseguridad;
VI. Determinar criterios uniformes de homologación para la organización, operación y modernización tecnológica de las Instituciones especializadas en materia de Ciberseguridad;
VII. Generar, compartir, intercambiar, ingresar, almacenar y proveer información, archivos y contenidos a las Bases de Datos que integren al Centro Nacional de Información Plataforma México, de conformidad con lo dispuesto en la legislación en la materia;

VIII. Coordinar acciones y operativos en conjunto con las Instituciones de Ciberseguridad y de las áreas especializadas de las instituciones de Seguridad Pública, aplicando los protocolos correspondientes tanto para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, así como para la gestión de incidentes cibernéticos para la contención y mitigación de amenazas cibernéticas a las infraestructuras críticas de información.

IX. Colaborar en la protección y vigilancia de las Infraestructuras Críticas de Información y Estratégicas del país en los términos de esta ley y demás disposiciones aplicables;

X. Coordinar la protección y vigilancia de las Infraestructuras Críticas de Información del país;

XI. Que las instancias responsables del control estadístico tanto del Poder Judicial de la Federación como de los Poderes Judiciales de las Entidades Federativas proporcionen de manera permanente y oportuna la información estadística sobre todos los procedimientos relacionados con los ciberdelitos;

XII. Determinar la participación de la comunidad, de instituciones académicas y de las instancias especializadas en la materia en coadyuvancia de los procesos de evaluación de las políticas de ciberseguridad, así como de las Instituciones de Seguridad Pública, a través de mecanismos eficaces;

XIII. Promover acuerdos de cooperación y coordinación entre las distintas instancias públicas, privadas, académicas e internacionales para fortalecer la ciberseguridad;

XIV. Apoyar la economía digital, fomentando la adopción de medidas de ciberseguridad en empresas, especialmente micro, pequeñas y medianas empresas (MIPYMES);

XV. Supervisar el cumplimiento de esta Ley y de los tratados internacionales aplicables;

XVI. Fomentar la participación de la iniciativa privada en el fortalecimiento de la ciberseguridad del país;

XVII. Impulsar la investigación y el desarrollo de tecnologías avanzadas en ciberseguridad, facilitando la colaboración entre gobierno, sector privado y academia;

XVIII. Implementar mecanismos de evaluación de los tres órdenes de Gobierno, en el cumplimiento de la presente Ley y en su caso de los fondos de ayuda federal para la ciberseguridad; y

XIX. Realizar las demás acciones que sean necesarias para incrementar la eficacia en el cumplimiento de los fines de la Ciberseguridad.

CAPÍTULO III
De la Agencia Nacional de Ciberseguridad

Artículo 18.- La Agencia Nacional de Ciberseguridad es un área de trabajo dependiente de la Secretaría de Seguridad y Protección Ciudadana y está integrada por:

I. Un Titular quien desempeña las funciones de Secretario de Seguridad y Protección Ciudadana, de la Secretaria de Seguridad y Protección Ciudadana;

II. Un Secretario General, quien desempeñe las funciones de Subsecretario de Seguridad Pública, quien, en los casos de ausencia del Titular de esta Agencia, desempeñara sus funciones;

III. Un Coordinador de Ciberseguridad, que desempeña las funciones de Director General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico, y

IV. Los funcionarios del Gobierno Federal que de acuerdo con sus funciones y atribuciones puedan ser invitados por el Titular de esta Agencia para colaborar de manera permanente o temporal en la Agencia Nacional de Ciberseguridad.

Artículo 19.- La Agencia Nacional de Ciberseguridad tendrá las atribuciones siguientes:

I. Coordinar el desarrollo, implementación, evaluación, actualización y mejora continua de la Estrategia Nacional de Ciberseguridad Ciudadana;
II. Impulsar ante las instancias Federales, Entidades Federativas y Organismos Constitucionalmente Autónomos, el cumplimiento de la Estrategia Nacional de Ciberseguridad Ciudadana;
III. Evaluar, en coordinación con las autoridades competentes, el cumplimiento de la Estrategia Nacional Ciberseguridad, así como coordinar la formulación de propuestas de actualización y modificación de la Estrategia para su presentación al Titular del Ejecutivo Federal;
IV. Instituir un modelo homologado de Policías Cibernéticas que opere en las 32 entidades federativas y promover su conformación, desarrollo, capacitación y certificación.
V. Establecer mecanismos de coordinación y colaboración de los equipos de respuesta a incidentes públicos y privados a través del establecimiento de un Equipo Nacional de Respuesta a Incidentes de Ciberseguridad;
VI. Generar protocolos y mecanismos para preservar evidencia digital y establecer un protocolo nacional para su manejo, en coordinación con las autoridades competentes.
VII. Conformar y dirigir el Centro Nacional de Respuesta a Incidentes Cibernéticos, promoviendo la creación de Centros de Respuesta a Incidentes Sectoriales y la cooperación internacional en esta materia.
VIII. Desarrollar un plan nacional para la protección de Infraestructuras Críticas de Información.
IX. Integrar y mantener actualizado el Catálogo Nacional de Infraestructuras Críticas de Información, asegurando su confidencialidad, integridad y disponibilidad.
X. Definir y promover medidas de seguridad para Infraestructuras Críticas de Información, basadas en análisis de riesgos, y coordinar la respuesta ante ataques cibernéticos.
XI. Realizar las actividades de coordinación de los tres órdenes de gobierno y la iniciativa privada para realizar las funciones de Ciberseguridad en el país;
XII. Desarrollar, implementar, evaluar y actualizar las políticas públicas, disposiciones de seguridad de la información, estándares, y guías en materia de ciberseguridad para instancias públicas y privadas;
XIII. Proponer criterios técnicos de vanguardia para la detección, monitoreo, pronóstico y medición de riesgos en las tecnologías de la información y comunicaciones del sector público y privado;
XIV. Promover el establecimiento de mecanismos de coordinación y colaboración entre los equipos de respuesta a incidentes cibernéticos públicos y privados;
XV. Proponer la armonización legal en la materia de Ciberseguridad, para contar con instrumentos nacionales e internacionales para el cumplimiento de los objetivos de esta Ley;
XVI. Realizar mediciones de la ciberseguridad de las instituciones públicas y privadas a fin de que se establezcan mecanismos de mejora continua para mantener los mecanismos de

ciberseguridad vigentes y adecuados, para responder a las amenazas derivadas de las nuevas tecnologías;

XVII. Coordinar programas de cultura y capacitación de los funcionarios de gobierno y público en general, con instituciones educativas, centros de investigación, entidades públicas y privadas tanto nacionales como internacionales;

XVIII. Implementar mecanismos de coordinación pública y privada con procedimientos y recursos específicos que permitan el cumplimiento de la presente ley en materia de prevención, investigación, procuración e impartición de justicia conforme a la atribución de cada instancia de colaboración;

XIX. Las demás que se establezcan en otras disposiciones jurídicas o le asigne, en el ámbito de su competencia el Presidente de la República.

Artículo 20.- Corresponderá a la Agencia Nacional de Ciberseguridad la facultad para participar e intervenir en la integración de convenios, acuerdos, convenciones y cooperación Internacional que emplean el uso de las Tecnologías de la Información y la Comunicación que establezca México con otros países.

I. La Agencia Nacional de Ciberseguridad podrá celebrar convenios de colaboración con agencias de otras naciones y organismos internaciones para realizar acciones conjuntas y acciones de cooperación internacional.

II. Para tal efecto, ejercerá las funciones generales asignadas en la presente Ley, y aquellas disposiciones y acuerdos que se generen en la Comisión Nacional de Ciberseguridad y disposiciones legales reglamentarias que le correspondan, y conforme a las disposiciones legales aplicables.

CAPÍTULO IV
Del Registro Nacional de Incidentes Cibernéticos

Artículo 21.- El Registro Nacional de Incidentes Cibernéticos estará contenido dentro de las Bases de Datos del Sistema Nacional de Información de Seguridad Pública. La información contenida en este registro deberá atender lo establecido en la Ley General del Sistema Nacional de Seguridad Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Artículo 22.- Para la conformación del Registro Nacional de Incidentes, están obligados a entregar información al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública:

I. Las Secretarías de Seguridad Ciudadana estatal, lo correspondiente al ámbito de su competencia en el marco del Sistema Nacional de Seguridad Pública;

II. Los Centros de Control, Comando, Comunicaciones, Cómputo, Coordinación e Inteligencia (C5i) respecto a los reportes que recibe del 9-1-1 y 089;

III. Las dependencias y entidades de la Administración Pública Estatal, respecto de sus incidentes de Ciberseguridad;

IV. El Poder Judicial de la Federación, lo correspondiente a todos los incidentes de ciberseguridad que le sean reportados; y

V. Los administradores de Infraestructuras Críticas de Información públicos y privados, reportarán todos aquellos incidentes de ciberseguridad que hayan puesto en riesgo su operación a través de sus organismos reguladores correspondientes.

CAPÍTULO V

De la Autoridad de Seguridad Ciudadana en Materia Cibernética

Artículo 23.- Corresponde a la Secretaría de Seguridad y Protección Ciudadana:

I. Dirigir la Agencia Nacional de Ciberseguridad;
II. Capacitar al personal de las instancias de seguridad y las fuerzas policiales en ciberseguridad, con enfoque en derechos humanos, género, privacidad y protección de datos, para responder adecuadamente a los delitos cibernéticos;
III. Coordinar acciones con las demás autoridades federales, estatales y municipales para cumplir los objetivos de esta Ley y garantizar la seguridad en el ciberespacio;
IV. Desarrollar y mantener un sistema de resiliencia cibernética que permita la rápida recuperación y continuidad de las infraestructuras críticas y servicios esenciales;
V. Dar seguimiento y ejecutar las acciones que le correspondan en el marco de la Estrategia Nacional de Ciberseguridad Ciudadana;
VI. Fomentar la cultura de ciberseguridad, a través de programas y acciones que promuevan el respeto a los derechos digitales, la protección de la privacidad y el uso seguro de las tecnologías;
VII. Supervisar y mejorar los sistemas e instrumentos utilizados para la gestión de riesgos y respuesta ante incidentes cibernéticos, en coordinación con las instancias nacionales e internacionales;
VIII. Celebrar convenios de cooperación y coordinación en materia de ciberseguridad con instituciones públicas y privadas, tanto nacionales como internacionales, para fortalecer la protección en el ciberespacio;
IX. Implementar un portal digital que permita el reporte ciudadano de incidentes cibernéticos y la colaboración pública para la detección de amenazas cibernéticas, actualizado en tiempo real y accesible para toda la población;
X. Establecer mecanismos de accesibilidad para recabar denuncias y testimonios de personas con discapacidad que hayan sido víctimas de delitos cibernéticos, incluyendo procedimientos ajustados a sus necesidades;
XI. Verificar que los Centros de Respuesta a Incidentes Cibernéticos sean considerados como componentes estratégicos de prioridad nacional en el marco de la ciberseguridad;
XII. Establecer directrices y protocolos para la preservación de evidencia digital, en coordinación con las autoridades judiciales y peritos especializados, para asegurar su integridad y validez en procesos legales;
XIII. Las demás atribuciones necesarias para el cumplimiento de la presente Ley.

CAPÍTULO VI

De las Fiscalías y Procuradurías

Artículo 24.- La Fiscalía General de la República y las Fiscalías y Procuradurías de las Entidades Federativas deberán contar con Fiscalías Especializadas en la investigación y persecución de delitos cibernéticos, cuya función será la protección del ámbito digital y la prevención de delitos cibernéticos en todo el territorio nacional.

Dichas Fiscalías Especializadas contarán con recursos humanos, financieros, materiales y técnicos especializados y multidisciplinarios, así como una unidad de análisis que permita la efectiva operación y coordinación de la persecución de estos delitos, asegurando la participación de personal ministerial, policial, pericial y apoyo técnico especializado.

Las autoridades competentes, en el ámbito de sus atribuciones, deberán colaborar de manera eficaz con las Fiscalías Especializadas para el cumplimiento de la Ley.

Artículo 25.- Los servidores públicos que integren las Fiscalías Especializadas en delitos cibernéticos deberán cumplir, como mínimo, con los siguientes requisitos:

I. Contar con el perfil y las competencias establecidas por la Comisión Nacional de Ciberseguridad; y
II. Acreditar los cursos de especialización, capacitación y actualización en ciberseguridad, análisis forense digital y legislación aplicable que establezca la Agencia Nacional de Ciberseguridad.

Las Fiscalías deberán capacitar a sus servidores públicos conforme a estándares internacionales en derechos humanos, protección de datos personales, atención a las víctimas de delitos cibernéticos y en el uso adecuado de herramientas de investigación digital.

Artículo 26.- La Fiscalía Especializada en Delitos Cibernéticos de la Fiscalía General de la República, en el ámbito de su competencia, tendrá las siguientes atribuciones:

I. Recibir las denuncias relacionadas con la probable comisión de delitos cibernéticos e iniciar la carpeta de investigación correspondiente;
II. Coordinarse con instituciones nacionales e internacionales para realizar todas las acciones relativas a la investigación y persecución de delitos cibernéticos, conforme a los protocolos de colaboración y cooperación vigentes;
III. Informar de manera inmediata a las autoridades correspondientes sobre el inicio de una investigación en materia de delitos cibernéticos y compartir información relevante de conformidad con los protocolos aplicables;
IV. Proporcionar información y evidencia digital a las autoridades judiciales y organismos de ciberseguridad, conforme a los lineamientos de homologación y custodia de evidencia;
V. Mantener comunicación continua y permanente con otros organismos de seguridad cibernética para intercambiar información sobre amenazas y tendencias delictivas en el ciberespacio;

VI. Solicitar a la autoridad judicial competente la autorización para la obtención de datos o la intervención de comunicaciones en investigaciones relacionadas con delitos cibernéticos, en los términos establecidos en el Código Nacional de Procedimientos Penales;
VII. Conformar grupos de trabajo interinstitucionales para la investigación de delitos cibernéticos de alcance transnacional o que involucren la participación de redes delictivas organizadas;
VIII. Solicitar el apoyo de otras instituciones para la realización de operativos y tareas de campo necesarias para la recolección de evidencia digital;
IX. Colaborar en la capacitación y actualización continua de sus servidores públicos, en coordinación con organismos nacionales e internacionales, para el fortalecimiento de capacidades en ciberseguridad y análisis forense digital;
X. Establecer mecanismos de cooperación con entidades públicas y privadas para la prevención de delitos cibernéticos y la sensibilización de la ciudadanía sobre prácticas seguras en el entorno digital;
XI. Facilitar la participación de las víctimas en el proceso de investigación, brindándoles información periódica sobre los avances y resultados de las investigaciones en materia de delitos cibernéticos;
XII. Celebrar convenios de colaboración con organizaciones nacionales e internacionales para optimizar la prevención, investigación y sanción de delitos en el ámbito digital; y
XIII. Las demás atribuciones que establezcan otras disposiciones jurídicas aplicables en materia de delitos cibernéticos y ciberseguridad.

Artículo 27.- Las Fiscalías Especializadas en Delitos Cibernéticos de las Entidades Federativas deberán contar, como mínimo, con los recursos, características y atribuciones necesarias para garantizar una adecuada capacidad operativa, técnica y de investigación en el ámbito de los delitos cibernéticos.

Cuando se advierte que pudiera actualizarse la competencia federal, las Fiscalías Especializadas de las Entidades Federativas remitirán de inmediato a la Fiscalía Especializada de la Fiscalía General de la República los expedientes correspondientes.

En los casos no contemplados expresamente como competencia de la Federación, las Fiscalías Locales iniciarán la carpeta de investigación correspondiente de manera inmediata y de conformidad con los protocolos homologados que emita el Centro Nacional de Ciberseguridad.

Artículo 28.- En caso de que un servidor público sea señalado como imputado en un delito cibernético y exista el riesgo de que, debido a su cargo o influencia, interfiera o impida el desarrollo de las investigaciones, podrá ser sujeto a medidas cautelares, tales como la suspensión temporal de su cargo. La autoridad jurisdiccional competente ordenará estas medidas, en conformidad con el Código Nacional de Procedimientos Penales, con la finalidad de asegurar la transparencia y efectividad en las investigaciones.

El superior jerárquico del imputado podrá aplicar medidas administrativas adicionales para evitar interferencias o posibles actos de obstrucción, conforme a los lineamientos institucionales y normativas aplicables.

Artículo 29.- Las Fiscalías Especializadas en Delitos Cibernéticos deberán desarrollar criterios y metodologías específicas de investigación adaptados a los estándares internacionales y a las

mejores prácticas en ciberseguridad, gestión de evidencia digital, y análisis forense. Estas metodologías permitirán un enfoque eficiente y confiable en la recopilación, custodia y presentación de pruebas digitales, asegurando la transparencia, la legalidad y el respeto a los derechos humanos.

Artículo 30.- En situaciones excepcionales, la Fiscalía Especializada de la Fiscalía General de la República deberá continuar la investigación de los delitos cibernéticos previstos en esta Ley sin interrupciones, aplicando el Protocolo Homologado de Investigación que emita el Centro Nacional de Ciberseguridad, el Código Nacional de Procedimientos Penales, y la normatividad aplicable.

Artículo 31.- Todas las autoridades de los distintos niveles de gobierno están obligadas a prestar el auxilio e información que las Fiscalías Especializadas en Delitos Cibernéticos soliciten, en el marco de sus competencias y en los términos de esta Ley, para facilitar la investigación y persecución de delitos en el ámbito cibernético.

Artículo 32.- La Fiscalía General de la República celebrará acuerdos y protocolos interinstitucionales con autoridades y organismos internacionales, con el propósito de coordinar las acciones de investigación de delitos cibernéticos que involucren a ciudadanos mexicanos en el extranjero o a extranjeros en el territorio nacional, respetando los marcos jurídicos y estándares internacionales de ciberseguridad y derechos humanos.

Artículo 33.- La Fiscalía General de la República podrá solicitar el apoyo técnico de la Secretaría de Seguridad y Protección Ciudadana, del Centro Nacional de Inteligencia, del Centro Nacional de Ciberseguridad y de las Unidades de Policía Cibernética Estatales para el desarrollo de las investigaciones correspondientes.

Artículo 34.- Las personas físicas o jurídicas que cuenten con información relevante que pueda contribuir a la investigación y persecución de los delitos cibernéticos previstos en esta Ley están obligadas a proporcionar dicha información a las Fiscalías Especializadas.

Esta información puede ser entregada a través de los canales previstos en esta Ley o cualquier medio adecuado y accesible, siempre en conformidad con la normativa aplicable, garantizando la confidencialidad y la integridad de los datos aportados.

Artículo 35.- Las Fiscalías Especializadas en Delitos Cibernéticos deberán recibir la información aportada por personas físicas o jurídicas de forma expedita y sin requerir el cumplimiento de formalidades que pudieran dificultar la colaboración. La recepción y gestión de dicha información se realizarán de acuerdo con los principios de simplicidad, transparencia y respeto a los derechos fundamentales.

Artículo 36.- Las Fiscalías Estatales Especializadas en Delitos Cibernéticos podrán recibir apoyo técnico de la Secretaría de Seguridad Pública Estatal o Municipal, así como de la Unidad de Policía Cibernética Estatal para el desarrollo de las investigaciones correspondientes.

Artículo 37.- Las atribuciones antes descritas deberán ejercerse respetando los principios de legalidad, debido proceso, protección de datos personales y derechos humanos, garantizando que las actuaciones de las diferentes autoridades se realicen de forma ética, transparente y respetando los derechos digitales de los ciudadanos.

Artículo 38.- Se promoverá que el Poder Judicial de la Federación cuente con jueces especializados en materia de cibercrimen y promoverá la capacitación continua en esta materia.

Así mismo, promoverá la colaboración nacional e internacional para contar con las herramientas tecnológicas necesarias para la recepción de la evidencia digital que será aportada a los procedimientos judiciales relacionados con delitos cibernéticos. Y proporcionar de manera permanente y oportuna la información estadística sobre todos los procedimientos relacionados con los ciberdelitos.

CAPÍTULO VII

De las Autoridades en Seguridad Nacional

Artículo 39.- Para efectos de la presente Ley, se consideran amenazas a la Seguridad Nacional debido al uso indebido de las Tecnologías de Información y Comunicación, y la Internet, aquellas que:

I. Comprometan la operación y capacidades de las instancias de seguridad nacional;

II. Potencialicen el impacto de amenazas previstas en la Ley de Seguridad Nacional;

III. Afecten el funcionamiento de algún sistema o Infraestructura Crítica, y

IV. Los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

Artículo 40.- Cuando se investiguen amenazas cibernéticas inminentes y concretas a la seguridad nacional, se dará aviso y proporcionará información a la autoridad que tenga a su cargo el proceso, en términos de las disposiciones jurídicas y administrativas aplicables.

Artículo 41.- Corresponde a las instancias de seguridad nacional, dentro del ámbito de sus competencias, coordinar las acciones necesarias para prevenir y contener cualquier amenaza cibernética que pudiera constituir un riesgo a la seguridad nacional.

CAPÍTULO VIII

De las Infraestructuras Críticas de Información

Artículo 42.- Se consideran Infraestructuras Críticas de información los siguientes sectores:

I. Químico;
II. Instalaciones comerciales y recreativas;
III. Comunicaciones;
IV. Fabricación crítica;

V. Presas/represas;
VI. Base industrial de defensa;
VII. Servicios de emergencia;
VIII. Energía;
IX. Servicios financieros;
X. Alimentación y agricultura;
XI. Instalaciones gubernamentales;
XII. Salud y salud pública;
XIII. Tecnología de información;
XIV. Reactores nucleares, materiales y residuos;
XV. Sistemas de transporte;
XVI. Sistemas de agua y aguas residuales.

Artículo 43.- La ciberseguridad de las Infraestructuras Críticas de Información estará a cargo de aquellas entidades públicas o privadas que tengan la responsabilidad legal de la administración de las mismas.

Artículo 44.- Los responsables de Infraestructura Crítica de Información públicos y privados, y aquellos que administren información de las autoridades de la administración pública estatal, notificarán en un plazo no mayor a 48 horas, a la autoridad competente respectiva, los incidentes que puedan tener afectaciones a la seguridad pública y a la seguridad nacional.

De igual forma, notificarán los sucesos o incidencias que, por su nivel de impacto puedan afectar a las redes y sistemas de información empleados para la prestación de servicios esenciales, aun cuando no hayan tenido todavía un efecto adverso.

La notificación de un incidente se realizará de acuerdo a lo que especifica el Protocolo de Gestión de Incidentes Cibernéticos, y no excluye ni sustituye, la notificación que deba realizarse a otros organismos nacionales e internacionales, o al Instituto Nacional de Transparencia, a la Información y Protección de Datos Personales.

CAPÍTULO IX

De los Prestadores de Servicios de Internet y Servicios Web

Artículo 45.- Los proveedores de servicios de internet y los proveedores de servicios de web o en línea que operen en territorio nacional están obligados a atender todo mandamiento por escrito, en formato físico o digital, fundado y motivado por la autoridad competente en los términos que establezca la Constitución Política de los Estados Unidos Mexicanos y demás leyes. Para lo cual estarán sujetos a las siguientes obligaciones específicas:

I. Contar con una representación legal para la atención de requerimientos de autoridades competentes. Dicha representación podrá ser a través de un representante legal establecido en el territorio nacional o bien a través de medios electrónicos:

a. En relación con la representación legal en territorio nacional, se indicará a la autoridad competente el domicilio y el nombre del representante al cual se le solicitará la información requerida y de igual forma se indicarán los requisitos correspondientes para la tramitación de dichas solicitudes.

b. Para el caso de la representación por medios electrónicos, el proveedor dispondrá de una plataforma digital, la cual operará las 24 horas los 365 días del año para la atención de requerimientos de las autoridades competentes, la cual actuará como ventanilla única de atención.

Dicha plataforma proveerá los mecanismos para seguimiento de las solicitudes que se realicen, hasta la conclusión de la petición realizada.

El tiempo de atención de las solicitudes, que sean de urgencia al existir un riesgo a la vida, integridad de las personas, o alguno de los delitos contemplados en los artículos 123 al 141 del Código Penal Federal, se atenderán de acuerdo a lo establecido en el artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión y sus Lineamientos, para el resto de las solicitudes se atenderán en los tiempos que determine la autoridad competente.

II. Informar a los usuarios de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de seguridad de la información y permitan, entre otros, la protección frente a malware;

III. Informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para los menores de edad;

IV. Facilitar información a los usuarios acerca de las posibles responsabilidades en que puedan incurrir por el uso indebido de sus servicios, en particular, para la comisión de delitos y vulneración de la legislación en materia de propiedad intelectual e industrial;

V. Suspender de manera provisional, las direcciones IP, aplicaciones, dominios y sitios de internet dentro de las 72 horas posteriores a la notificación que le realicen la Fiscalía General de la República y autoridades judiciales competentes para su inhabilitación, precisando que el afectado podrá hacer valer los recursos legales para contrarrestar la suspensión referida;

VI. Conservar la información sobre las IP y datos de registro; y

VII. Lo anterior, sin perjuicio en lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión y demás leyes en la materia.

Artículo 46.- De conformidad con el principio de cooperación internacional, los proveedores de servicios en línea constituidos en el extranjero que tengan y operen plataformas, sistemas de información, productos o servicios digitales a través de Internet o algún otro medio tecnológico que cuenten con usuarios registrados y activos en México, podrán ser requeridos mediante orden judicial, a colaborar con las autoridades mexicanas de procuración de justicia o encargadas de la seguridad pública y nacional, según corresponda en términos de las disposiciones aplicables en la materia.

Artículo 47.- Los proveedores de servicios bancarios y financieros están obligados a establecer las medidas de Ciberseguridad necesarias para evitar delitos que afecten la seguridad y el patrimonio de los ciudadanos por conductas delictivas que se realicen en las plataformas y los servicios que prestan de acuerdo con las leyes especiales y las disposiciones de carácter general que les son aplicables y que no afecten los derechos de la ciudadanía.

CAPÍTULO X

De la Cibercultura y la Vinculación con Autoridades del Sistema Educativo Nacional

Artículo 48.- La Secretaría de Seguridad y Protección Ciudadana, con la participación de la Agencia Nacional de Ciberseguridad, en el ámbito de sus respectivas atribuciones, desarrollará y difundirá una cultura de ciberseguridad, con el objetivo de:

I. Orientar y concientizar a la población sobre la importancia de las mejores prácticas en el uso de las Tecnologías de Información y Comunicación en los ámbitos público y privado;

II. Promover la adopción de mecanismos de seguridad utilizando enfoques basados en riesgos, respecto a los sistemas informáticos de cualquier individuo u organización pública o privada;

III. Impulsar el desarrollo y aplicación de criterios de ciberseguridad para la protección de la información en el ciberespacio;

Artículo 49.- La Secretaría de Seguridad y Protección Ciudadana, en coordinación con la Secretaría de Educación Pública, deberá establecer los mecanismos de colaboración a fin de que se diseñe, implemente y evalúe, un Programa Nacional de Prevención Escolar contra la ciberdelincuencia a todos los niveles, y deberá considerar, de manera enunciativa, mas no limitativa:

I. Las acciones de prevención desde los niveles básico, medio superior y superior;

II. La participación de la comunidad educativa;

III. El grado de intervención y colaboración de las autoridades, siempre con pleno respeto a los Derechos Humanos de los educandos; y

IV. Las acciones de carácter transversal.

CAPÍTULO XI

De las Entidades Federativas

Artículo 50.- Son facultades y obligaciones de las Entidades Federativas:

I. Participar en la elaboración de la Estrategia Nacional de Ciberseguridad, a través de la Secretaría de Seguridad Pública y su Unidad de Policía Cibernética;

II. Instituir a la Unidad de Policía Cibernética estatal, cuando sea el caso, como el ente coordinador de las unidades cibernéticas a nivel municipal;
III. Instrumentar y articular políticas públicas en concordancia con la Estrategia Nacional de Ciberseguridad y de acuerdo a la Política Nacional de Ciberseguridad Ciudadana;
IV. Crear el Registro Estatal de Incidentes Cibernéticos que se integrará con la información de los reportes que afecten la confidencialidad, integridad y disponibilidad de la información, así como la reputación de la ciudadanía de acuerdo al Registro Nacional de Incidentes Cibernéticos.
V. Promover, en coordinación con la Federación, programas y proyectos de atención, prevención, educación, formación y capacitación, investigación y cultura de la ciberseguridad;
VI. Proveer de los recursos presupuestarios, humanos y materiales, en coordinación con las autoridades que integran el sistema estatal de seguridad pública;
VII. Promover programas de cultura, prevención y atención a la población en la materia;
VIII. Rendir un informe semestral sobre los avances de la Estrategia y los programas de ciberseguridad implementados, mismo que será desarrollado por la Unidad de Policía Cibernética, y que será enviado al titular del ejecutivo estatal y a la Agencia Nacional de Ciberseguridad;
IX. Impulsar la participación de las organizaciones privadas, en el tema de ciberseguridad;
X. Proporcionar la información de los incidentes de ciberseguridad reportados a la Secretaría de Seguridad Pública Estatal, C5 o C5i estatal y la Procuraduría o Fiscalía General del Estado, a través del Registro Nacional de Incidentes de Cibernéticos;
XI. Impulsar reformas a la legislación local, así como convenios de cooperación, coordinación y concertación en el ámbito de su competencia, para el cumplimiento de los objetivos de la presente ley;
XII. Conocer y resolver sobre los ciberdelitos del fuero Estatal conforme a las legislaciones locales que para tales efectos emitan las Entidades Federativas;
XIII. Especializar a las y los agentes del Ministerio Público, peritos y personal en la actualización y el desarrollo de competencias, para asesorar, atender y judicializar los delitos cibernéticos;
XIV. Aplicar los protocolos homologado tanto para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital de los delitos cibernéticos, así como para la gestión de incidentes cibernéticos para la contención y mitigación de amenazas cibernéticas a las infraestructuras críticas de información;
XV. Crear, fomentar y mantener una estrecha coordinación y concurrencia por parte de la Unidad de Policía Cibernética tanto de la Secretaría de Seguridad Pública Estatal como de la Procuraduría o Fiscalía General del Estado, C5 o C5i estatal, la Fiscalía General de la República con la Agencia Nacional de Ciberseguridad;
XVI. Apoyar la investigación del ciberdelito y la procuración de justicia tanto de su competencia Estatal, como en su caso en auxilio de la competencia Federal, es decir, en apoyo a los procedimientos penales relativos a los ciberdelitos Federales, y de igual forma aplicar los protocolos correspondientes a la identificación, recolección, preservación, procesamiento y presentación de la evidencia digital;
XVII. Que los Tribunales Superiores de Justicia de las treinta y dos Entidades Federativas proporcionen de manera permanente y oportuna la información estadística a la Agencia Nacional de Ciberseguridad sobre todos los procedimientos relacionados con los ciberdelitos;
XVIII. Colaborar de manera permanente en las acciones, estrategias y programas en materia de ciberseguridad vinculadas a la seguridad pública;

XIX. Colaborar en las campañas nacionales de prevención de conductas ilegales en el ciberespacio;
XX. Ejercer sus facultades reglamentarias para la aplicación de la presente ley;
XXI. Las demás que le confieran esta ley u otros ordenamientos aplicables.

CAPÍTULO XII

De las Unidades de Policía Cibernética Estatales

Artículo 51.- Las Unidades de Policía Cibernética estatales tendrán las siguientes atribuciones:

I. Proteger a la ciudadanía de la Entidad Federativa en el entorno digital, a través de la prevención, detección e investigación de delitos cibernéticos que atenten contra la seguridad, integridad y bienestar de las personas y las instituciones.
II. Actuar en coordinación con las autoridades municipales, estatales y federales competentes, y empleando el protocolo para identificar y mitigar actividades ilícitas en el ámbito digital y cualquier otra actividad que ponga en riesgo la ciberseguridad de la ciudadanía.
III. Alertar de manera temprana, de acuerdo al protocolo correspondiente, sobre amenazas y riesgos de ciberseguridad en las infraestructuras críticas dentro del territorio del estado, así como la sensibilización y capacitación de la comunidad en el uso seguro y responsable de las tecnologías de la información y comunicación.
IV. Colaborar en el intercambio de información con organismos de seguridad cibernética a nivel nacional e internacional, bajo los principios de protección de derechos digitales, privacidad y legalidad.
V. Investigar y recolectar evidencia de delitos cibernéticos, que atenten contra la seguridad cibernética de las personas y de las instituciones en el estado.
VI. Realizar monitoreos preventivos de redes y sistemas públicos en el estado para detectar amenazas y prevenir posibles incidentes cibernéticos, garantizando el respeto a la privacidad de los ciudadanos y ajustándose a las disposiciones legales.
VII. Coordinar y colaborar con los proveedores de servicios de Internet y telecomunicaciones en la detección y mitigación de actividades ilícitas en línea que afecten a la población del estado, en cumplimiento de las leyes de protección de datos personales y con la correspondiente autorización judicial.
VIII. Gestionar el bloqueo temporal o definitivo de contenidos o sitios web en el estado que inciten o faciliten actividades ilícitas o representen un riesgo a la seguridad pública, previo procedimiento legal y en coordinación con las autoridades judiciales.
IX. Participar en el intercambio de información sobre amenazas y vulnerabilidades cibernéticas con otras instancias de seguridad a nivel municipal, estatal, federal e internacional, en el marco de tratados y acuerdos de cooperación, para fortalecer la capacidad de respuesta ante delitos cibernéticos transnacionales.
X. Colaborar de forma inmediata y coordinada ante incidentes de ciberseguridad que puedan afectar las infraestructuras críticas del estado, en coordinación con entidades de seguridad pública y privada.

XI. Desarrollar y promover programas de capacitación y concientización sobre ciberseguridad dirigidos a la población, las instituciones y las empresas del estado, con el fin de fomentar el uso seguro y responsable de las tecnologías de la información y comunicación.
XII. Asesorar a las entidades gubernamentales del estado en la implementación de medidas de ciberseguridad, protección de datos personales y salvaguarda de derechos digitales, así como colaborar en la creación de políticas y protocolos de seguridad informática.
XIII. Llevar a cabo acciones de sensibilización pública para informar a la ciudadanía sobre riesgos y buenas prácticas en el ciberespacio, promoviendo el respeto y la protección de los derechos digitales y la privacidad.
XIV. Colaborar en la investigación y desarrollo de tecnologías y técnicas para mejorar la ciberseguridad en el ámbito estatal y nacional, así como fortalecer los mecanismos de protección contra delitos cibernéticos.
XV. Fomentar la denuncia ciudadana.
XVI. Colaborar en la armonización legislativa, a fin de fortalecer el marco jurídico a nivel estatal y nacional.
XVII. Las demás que le confieran esta ley u otros ordenamientos aplicables.

CAPÍTULO XIII

De los Municipios

Artículo 52.- Son facultades y obligaciones de los Municipios:

I. Instrumentar y articular, en concordancia con la política y estrategia nacional y estatal, la política municipal en materia de Ciberseguridad;
II. Colaborar de manera permanente en las acciones, estrategias y programas en materia de ciberseguridad vinculadas a la seguridad pública;
III. Colaborar en las campañas nacionales de prevención de conductas ilegales en el ciberespacio;
IV. Colaborar con las Unidades de Policía Cibernética Estatales;
V. Promover, en coordinación con las entidades federativas, cursos de capacitación a los servidores públicos encargados del tema de Ciberseguridad;
VI. Ejecutar las acciones necesarias para el cumplimiento de la Estrategia Nacional de Ciberseguridad y de los Programa Estatales que para tal efecto se establezcan;
VII. Participar y coadyuvar en la prevención, atención y erradicación de delitos cibernéticos;
VIII. Celebrar convenios de cooperación, coordinación y concertación en la materia;
IX. Las demás que le confieran esta ley u otros ordenamientos aplicables.

LIBRO SEGUNDO

DELITOS CIBERNÉTICOS

CAPÍTULO I

De los Delitos contra la Confidencialidad, la Integridad y la Disponibilidad de la Información

Artículo 53.- Acceso ilícito a tecnologías de la información y comunicaciones, sistemas informáticos, electrónicos o telemáticos.

Al que, por cualquier medio o método, sin autorización legitima, dolosamente acceda, copie, extraiga, modifique, destruya o elimine la información contenida en sistemas informáticos, electrónicos o telemáticos, se le impondrán de dos a ocho años de prisión y multa de seiscientos a seis mil unidades de medida de actualización (UMA).

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de instituciones públicas, así como bienes o servicios que brinda el Estado, y cuando el acceso no autorizado sea para la clonación, venta, distribución o cualquier otra utilización de un dispositivo de acceso a un servicio o sistema informático, electrónico o de telecomunicaciones, aumentándose la penalidad hasta en una tercera parte.

Artículo 54.- Interceptación de Datos o Señales.

A quien intercepte de forma no autorizada o sin una orden judicial, cualquier tipo de comunicación informática, electrónica o telemática, incluidas las emisiones electromagnéticas y de radiofrecuencias, por cualquier medio o método, originadas o provenientes desde otro sistema o equipo o realizadas dentro del mismo, se le impondrá de dos a seis años de prisión y multa de seiscientas a cuatro mil unidades de medida de actualización (UMA).

Artículo 55.- Intervención de Datos o Señales.

A quien intervenga de forma no autorizada o sin una orden judicial, cualquier tipo de comunicación informática, electrónica o telemática, incluidas las emisiones electromagnéticas y de radiofrecuencias, por cualquier medio o método, originadas o provenientes desde otro sistema o equipo o realizadas dentro del mismo, se le impondrá de cuatro a diez años de prisión y multa de mil a diez mil unidades de medida de actualización (UMA).

Artículo 56.- Falsificación informática.

Quien sin autorización legitima introduzca, altere, impida el acceso, elimine datos informáticos, electrónicos o telemáticos previamente almacenados en un sistema, nube, plataforma o base de datos informáticos locales o remotos, que generen datos erróneos o falsos, se le impondrá de dos a ocho años de prisión y multa de mil doscientos a doce mil unidades de medida de actualización (UMA).

Artículo 57.- Abuso de Dispositivos Tecnológicos.

El que produzca, utilice, posea, venda, obtenga o distribuya sin causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo uso fundamental sea el de emplearse como herramienta para cometer conductas que de forma dolosa modifiquen, destruyan o provoquen la pérdida parcial o total de información digital contenida en equipos, sistemas o medios de almacenamiento informáticos, electrónicos o telemáticos, se impondrá la pena de dos a seis años de prisión y multa de mil a diez mil unidades de medida de actualización (UMA).

En estos casos, se incrementará hasta en una tercera parte la pena, cuando derivado del uso ilegal de dispositivos tecnológicos se solicite dar, hacer, dejar de hacer o tolerar algo con la finalidad de obtener cualquier beneficio para sí o para un tercero con independencia de la existencia de un perjuicio patrimonial.

CAPÍTULO II.

De los delitos contra el patrimonio

Artículo 58.- Fraude por medio informático.

Al que engañe o se aproveche del error en que otra persona se encuentra, debido al uso mal intencionado que cualquier medio o método informático, electrónico o telemático, y obtenga con ellos cualquier bien o beneficio patrimonial, se le impondrá una pena de tres a nueve años de prisión y multa de seiscientos a ocho mil unidades de medida de actualización (UMA).

La autoridad jurisdiccional deberá tomar en cuenta al momento de individualizar la sanción, cuando el inculpado repare el daño causado a satisfacción del agraviado.

CAPITULO III.

De los delitos contra la libertad de las personas

Artículo 59.- Acceso y uso Indebido de datos personales.

El que, sin estar facultado para ello o mediante el engaño, con provecho propio o de un tercero, mediante las tecnologías de la información y comunicación, obtenga, almacene, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o trate dolosamente datos personales, será sancionado con seis a quince años de prisión y de ocho mil a doce mil unidades de medida de actualización (UMA).

Artículo 60.- Usurpación de identidad.

El que se apropie mediante el uso de las tecnologías de la información y comunicación de un medio de identificación digital de otra persona, usurpando su identidad con el propósito de causar algún daño a la víctima u obtener algún tipo de beneficio, será sancionado con una pena de tres a nueve años de prisión y multa de seiscientos a ocho mil unidades de medida de actualización (UMA).

La sanción a imponer para la conducta señalada, se incrementará hasta una tercera parte, cuando:

I. Aprovechándose de la apropiación ilegal de identidad, haya incurrido en la realización de transacciones comerciales o de cualquier otra índole que afecte derechos patrimoniales de la víctima.

II. La conducta haya sido reiterada ante una misma o en diferentes instancias bancarias, comerciales o entidades del Sistema Financiero.

III. Exista colaboración intencional de algún integrante, o exintegrante de alguna entidad financiera tercera que facilite la conducta comisiva ilícita.

Artículo 61.- Incitación a la violencia digital.

Al que diseñe o grabe cualquier tipo de material digital, con el propósito de difundirlo a través de medios digitales, incitando a cometer desmanes, robo, o violencia generalizada para afectar a personas físicas o morales en su integridad física o su patrimonio, se le aplicarán de dos a diez años de prisión y multa de seiscientas a seis mil unidades de medida de actualización (UMA).

No serán motivo de sanción aquellas expresiones que se realicen en estricto apego a la libertad de expresión, siempre y cuando no inciten a afectar la esfera de derechos y seguridad jurídica de las personas.

Artículo 62.- Delitos contra la privacidad personal.

A quien, haciendo violencia moral sobre la víctima, divulgue, distribuya, comercialice, arriende, publicite, o difunda imágenes, comunicaciones escritas, verbales, audiovisuales, a través de medios digitales, con contenido erótico, sexual o pornográfico, de una persona o

personas, obtenidas o falsamente creadas, se le impondrá de cinco a diez años de prisión y multa de seiscientos a ocho mil unidades de medida y actualización (UMA).

Las sanciones se aumentarán hasta una tercera parte cuando el sujeto activo sea el cónyuge, concubina o concubinario, o la persona que mantenga o haya mantenido una relación sentimental, afectiva o de confianza con la víctima, o similar relación de afectividad, aún sin convivencia o una relación laboral.

CAPÍTULO IV.

De los Delitos contra niñas, niños o adolescentes

Artículo 63.- Acoso sexual a menores de edad.

Al que, a través de medios digitales, induzca o influencie, a un menor de dieciocho años de edad, con el propósito de aprovecharse de éste, orillándolo a que se exponga desnudo, o que realice cualquier comportamiento con fines sexuales, se le impondrá de cinco a diez años de prisión y multa de seiscientos a ocho mil unidades de medida y actualización (UMA).

Artículo 64.- Corrupción de menores de edad a través de medios digitales.

Al que solicite, procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio digital, a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o no tiene capacidad de resistir la conducta, a realizar actos sexuales o de exhibición corporal con fines lascivos o sexuales, con el objeto de crear algún material de abuso sexual de niñas, niños y adolescentes, se le impondrá de siete a catorce años de prisión y multa de mil a diez mil unidades de medida de actualización (UMA).

La autoridad jurisdiccional podrá ordenar el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados.

Si se hiciere uso de violencia física o moral o psicoemocional, o se aproveche de la ignorancia, extrema pobreza o cualquier otra circunstancia que disminuya o elimine la voluntad de la víctima para resistirse, la pena se aumentará hasta en una mitad.

Se impondrá hasta una mitad de la pena que corresponde a la corrupción de menores, a quien, con fines comerciales, financie, elabore, reproduzca, o almacene, a través de medios digitales, material de abuso sexual de niñas, niños y adolescentes.

Artículo 65.- Exposición sexual de menores a través de medios digitales.

A quien, haciendo uso de medios digitales, mediante la persuasión psicológico-sexual, extorsión, o pago económico, induzca a un menor de dieciocho años de edad, a realizar la transmisión en vivo o video llamadas en tiempo real, o le solicite compartir archivos electrónicos que contengan material sexual explicito, se le impondrá una pena de cinco a doce años de prisión y multa de mil a diez mil unidades de medida de actualización (UMA).

Artículo 66.- Turismo sexual y exposición digital.

Quien en el contexto de viajes y turismo sexual, promueva, publique, divulgue, publicite, invite, facilite o gestione, a través de medios digitales, a que una o más personas viajen en territorio nacional, con la finalidad de realizar cualquier tipo de actos sexuales reales o simulados, con una o varias personas menores de dieciocho años de edad, o con una o varias personas que no tienen capacidad para comprender el significado del hecho, se les impondrá una pena de seis a doce años de prisión y multa de dos mil a quince mil unidades de medida de actualización (UMA).

Artículo 67.- Destrucción de Material de Abuso Sexual de niñas, niños y adolescentes.

Cuando exista sentencia firme por cualquier delito comprendido en este Capítulo, la autoridad competente, ordenará el borrado seguro y la destrucción física de los medios de almacenamiento respecto del material relacionado con las conductas descritas que hayan motivado la sentencia del imputado y que se encuentre en poder o bajo control del Tribunal de Enjuiciamiento o del Ministerio Público y/o Fiscalía.

CAPÍTULO V.

De los delitos contra la violencia de género en el ámbito digital

Artículo 68.- Acoso digital de género diversidad.

Al que, hostigue, amenace, intimide o acose a una mujer o personas miembros de la diversidad sexual, valiéndose del uso de medios digitales y le cause un daño en su dignidad personal, o afecte su paz y tranquilidad, y aún su propia seguridad, se le impondrá de tres a siete años de prisión y multa de seiscientos a diez mil unidades de medida y actualización (UMA).

Artículo 69.- Violencia digital de género contra la libertad de las mujeres o personas miembros de la diversidad sexual.

A quien imponga, coaccione, exija o intimide a cualquier mujer o persona miembro de la diversidad sexual a compartir contraseñas, geolocalización e intervención de diferentes tecnologías de uso personal, o de manera dolosa intervenga con dispositivos o tecnologías de dispositivos inteligentes, con el fin de tener el monitoreo y vigilancia de las actividades

de una persona en línea y fuera de la internet, se le impondrá de tres a siete años de prisión y multa de dos mil a siete unidades de medida y actualización (UMA).

Artículo 70.- Apoderamiento de materiales digitales de contenido sexual.

A quien, con el propósito de uso personal, o bien para comercializarlo, solicite a otra persona, o sustraiga sin su consentimiento, materiales sexuales realizados mediante el uso de medios digitales, a fin de recibir algún beneficio, se le impondrá de cuatro a doce años de prisión y multa de dos mil a diez mil unidades de medida y actualización (UMA).

Artículo 71.- Extorsión digital sexual.

A quien con el propósito de obtener un beneficio o causar daño, amenace con divulgar, compartir, distribuir, o publicar la imagen de una persona desnuda parcial o totalmente, o realizando actividad de contenido erótico sexual, valiéndose de medios digitales, se le impondrá de cuatro a diez años de prisión y multa de tres mil a doce mil unidades de medida y actualización (UMA).

CAPÍTULO VI.

De los delitos digitales contra la propiedad intelectual

Artículo 72.- Los delitos previstos y sancionados en la Ley General de Derechos de Autor y en la Ley de Propiedad Industrial, vigentes al momento de los hechos, y se cometan a través del empleo de medios digitales, se sancionará aumentando hasta una tercera parte de la pena privativa de la libertad que corresponda, y aumentando igualmente hasta una tercera parte la multa conforme a dicha legislación.

CAPÍTULO VII.

De los delitos contra el Sistema Financiero

Artículo 73.- Al que, por cualquier medio digital, dolosamente ponga en peligro o cause daño, altere u obstaculice el debido funcionamiento de los sistemas informáticos, electrónicos o telemáticos de las instituciones que integran el sistema financiero, se le impondrá de seis a veinte años de prisión y multa de cinco mil a doce mil Unidades de Medida y Actualización (UMA).

Artículo 74.- A la persona que, por cualquier medio digital, modifique, altere, destruya o provoque pérdida parcial o total de información contenida en sistemas o medios

informáticos, electrónicos o telemáticos, de las instituciones que integran el sistema financiero, se le impondrán de seis a veinte años de prisión y multa de seis mil a doce mil Unidades de Medida y Actualización (UMA).

Cuando la finalidad sea obtener un beneficio ilícito, patrimonial, económico o de otra naturaleza para sí o para un tercero, se aumentará la sanción hasta una mitad de la pena privativa de la libertad y de la multa.

CAPITULO VIII.

Disposiciones comunes a los delitos en materia de las tecnologías de la Información y comunicación, que afectan redes de sistemas informáticos, electrónicos o telemáticos.

Artículo 75.- Con independencia de las penas establecidas por esta Ley y otros ordenamientos legales, se aumentará hasta una tercera parte la pena privativa de la libertad, cuando los delitos a que se refiere el presente título, se cometan por:

I. Un servidor o un ex servidor público, miembro o exmiembro de alguna corporación de seguridad privada;

II. De igual forma, al servidor o ex servidor público o, miembro de alguna corporación de seguridad pública se le destituirá del empleo, cargo o comisión que desempeñe, y se le inhabilitará de acuerdo a la Ley General de Responsabilidades Administrativas de los Servidores Públicos para desempeñar cargos, empleos, o comisiones públicas;

III. Al mismo tiempo, se le suspenderá el derecho para ejercer actividades en corporaciones de seguridad privada.

Artículo 76.- Las autoridades competentes, actuarán con la celeridad requerida para preservar la evidencia digital contenida en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

Artículo 77.- Las Policías, la Guardia Nacional y el Ministerio Público, en apego a lo establecido en el Código Nacional de Procedimientos Penales, podrán solicitar a la autoridad judicial:

I. La cooperación con empresas proveedoras de servicios de Internet, y de servicios en la Red Pública de Internet nacionales o internacionales, para neutralizar sitios, páginas electrónicas y perfiles de redes sociales, siempre y cuando no se afecte la libertad de expresión, en los siguientes casos:

a) Cuando inciten a la violencia, realicen la apología del odio de género, racial, sexual o religioso;

b) Cuando se realice incitación a la discriminación, la hostilidad o agresión;

c) Cuando la instigación sea directa y pública a cometer crímenes o delitos;

d) Cuando se suplante la identidad de una persona para cometer fraude, extorsión y/o robo de datos personales;

e) Cuando de persistir su difusión, se dañe la imagen pública y la reputación de una persona o Institución, de manera dolosa y con falsedades;

II. La preservación de la información digital por los proveedores de servicios y contenidos de Internet, nacionales e internacionales cuando tengan efecto en territorio nacional.

III. Solicitar a los proveedores de servicios detener o no aumentar la proliferación de la exposición de materiales digitales que afecten o puedan afectar la imagen de una persona o personas que hayan sido víctimas de un delito cibernético.

Se podrá solicitar la colaboración de los proveedores de servicios de Internet en términos de lo dispuesto en la Ley Federal de Telecomunicaciones y Radiodifusión y sus Lineamientos de Colaboración en Materia de Seguridad y Justicia.

Las peticiones podrán ser realizadas por las policías, la Guardia Nacional y el Ministerio Público en casos de urgencia, de conformidad a lo establecido en el Código Nacional de Procedimientos Penales.

IV. Solicitar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa días, pudiendo esta orden ser renovada por períodos sucesivos.

Artículo 78.- El Ministerio Público atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa en el ciberespacio o mediante tecnologías de la información y comunicación, de conformidad con lo establecido en los ordenamientos jurídicos aplicables.

Artículo 79.- El responsable de los daños causados por una conducta delictiva, deberá resarcir a la víctima, como se describe a continuación:

I. Gastos generados para restituir el daño de la conducta, incluyendo el pago de cualquier deuda u obligación que haya adquirido.

II. Gastos correspondientes a servicios médicos, psicológicos, psiquiátricos y todos aquellos que se generen con motivo de una afectación a la salud física o mental.

Asimismo, la autoridad deberá:

a) Solicitar a las instancias competentes, la corrección de cualquier documento público o privado que contenga información falsa en perjuicio de la víctima.

b) Ordenará la cancelación de créditos que no hayan sido solicitados por la víctima.

c) Ordenará la destrucción de los dispositivos con los cuales se haya cometido la conducta ilícita incluyendo la información contenida en éstos.

TRANSITORIOS

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

SEGUNDO. El Ejecutivo Federal emitirá los Reglamentos de la Ley dentro de los 90 días siguientes a la entrada en vigor del presente Decreto.

TERCERO. Cuando el Ejecutivo Federal emita el Reglamento, la Fiscalía General de la República, las Procuradurías y Fiscalías de las Entidades Federativas contaran con 180 días para la creación de la Unidad de Procuración de Justicia especializadas en la materia.

CUARTO. El Ejecutivo Federal, tendrá 90 días para la publicación de la Estrategia Nacional de Ciberseguridad del Estado Mexicano.

QUINTO. Los recursos para llevar a cabo los programas y la implementación de las acciones que se deriven de la presente Ley, se cubrirán con cargo al presupuesto autorizado a la Secretaría de Seguridad y Protección Ciudadana, para el presente ejercicio fiscal y se proveerá en los subsecuentes.

SEXTO. A partir de la entrada en vigor de la presente Ley, se derogan todas las disposiciones normativas que contravengan la misma.

SEPTIMO. Los procedimientos que se encuentren en trámite a la entrada en vigor del presente ordenamiento, continuarán con su substanciación de conformidad con la legislación aplicable al inicio de los mismos.

SUSCRIBE

JESÚS LUCÍA TRASVIÑA WALDENRATH

Salón de Sesiones, a los 10 días del mes de diciembre de 2024.