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

SENADOR EDUARDO RAMIREZ AGUILAR
PRESIDENTE DE LA MESA DIRECTIVA
DEL SENADO DE LA REPÚBLICA
P R E S E N T E.-

La suscrita, **Jesús Lucía Trasviña Waldenrath**, Senadora de la República en la LXIV Legislatura e integrante del Grupo Parlamentario del Movimiento 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 y se derogan diversas disposiciones del Código Penal Federal**, al tenor de las siguientes:

Consideraciones

Los avances tecnológicos en el mundo son cada vez más grandes, su crecimiento exponencial en algunos casos rebasa, a la propia actividad humana, esto va dando certeza de futuro en diversos campos como la medicina, investigación científica, educación, economía y casi en todos los aspectos del desarrollo de la humanidad, lamentablemente estos avances también han generado diversos y múltiples factores de riesgo, desde los que tienen que ver con la seguridad nacional de un país, hasta los dispositivos móviles, de una ama de casa, un estudiante o cualquier otro miembro de la población en general, la imperiosa necesidad de generar la seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información.

Consideramos que este factor debe ser atendido en una competencia federal tanto por la capacidad de operación de las actividades cibernéticas e informáticas en todo el territorio nacional como por su inmediatez de desplazamiento, además de que con tales actividades tecnológicas sin regulación se incurre actualmente en conductas irregulares, ilegales e ilícitas que ponen en peligro y dañan valores y bienes jurídicos tutelados del más alto impacto del interés nacional, del interés social, del orden público, por lo que con el fin de prevenir, disuadir, disminuir y erradicar el mal uso de las herramientas dentro del campo de las tecnologías de la información y comunicaciones, con las cuales se puede amenazar y atacar actividades estratégicas y prioritarias para

la subsistencia y permanencia del Estado Mexicano y su desarrollo, por lo que se emite esta Ley Federal ya que estos actos dañinos influyen, amenazan y atacan directamente al desarrollo democrático de la República Mexicana.

Por ello dentro de la presente iniciativa de Ley se define que los ciberdelitos, son los llamados delitos en el ciberespacio, y que estos abarcan tanto las actividades que atentan contra la confidencialidad, integridad y disponibilidad de la información, los sistemas informáticos, redes de telecomunicaciones, entre otros, así como a las personas en su carácter individual como sujetos de derecho que, ante la evolución social constante en sus formas de interacción, es necesario legislar con miras al avance tecnológico y a las necesidades que emergen de las mismas.

Por los planteamientos de los problemas emanados en materia de ciberseguridad, se plantea que la transformación digital se ha convertido en los últimos años en la prioridad de muchos países. Los gobiernos locales alrededor del mundo han impulsado estrategias para el fortalecimiento de la administración electrónica, la modernización de las telecomunicaciones, el comercio electrónico, la cobertura de Internet, la promoción de habilidades digitales, entre otros, con objetivos tan amplios como garantizar el acceso a Internet, los servicios gubernamentales y la información, buscando que las naciones emerjan en un ámbito global cada vez más competitivo.

Actualmente la conectividad y el acceso a las TIC constituyen una línea de vida social, política y económica a través de la cual se está forjando el desarrollo.

En México de conformidad con la ENDUTIH[1] del año 2019, existen 74.3[2] millones de usuarios. De ellos, el 13.3% son niñas, niños y adolescentes. Destaca que el año 2018 ha mostrado un cambio importante respecto del uso que los mexicanos damos a Internet. Si bien con antelación el principal uso era el acceder a la información, para el año 2018 las cifras de ENDUTIH muestran que el principal uso constituye el entretenimiento (90.5%), en segundo lugar, la comunicación (90.3%) y en tercero para acceder a la información (86.9%). Este cambio tendrá un impacto en la forma en qué se desarrolle política pública dirigida a educar y capacitar a los ciudadanos en el uso seguro de esta tecnología. Así como la sensibilización en la importancia de su seguridad y estabilidad. De esta forma la actividad diaria de más de la mitad de la población en nuestro país se encuentra ligada al uso de TIC. Tecnología empleada principalmente por los jóvenes, con la generación que ha crecido en el mundo de Internet. No obstante, el desconocimiento por parte de las personas de mayor edad acerca del empleo de las TIC, en general, también resulta preocupante.

[1] Instituto Nacional de Estadística y Geografía (INEGI), Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2018, disponible en: https://www.gob.mx/cms/uploads/attachment/file/534997/INEGI_SCT_IFT_ENDUTIH_2019.pdf (Consultado el 2 de abril de 2019)

[2] La población se cuenta a partir de los 6 años de edad.

Aunque las bondades y beneficios que traen consigo las TIC superan por mucho a los riesgos y amenazas, no podemos soslayar estos últimos.

El recurso humano continúa siendo un factor crítico. Es por ello que la capacitación, sensibilización y educación digital, así como la especialización de capital humano resulta indispensable en el desarrollo de políticas en la materia.

Derechos Humanos en el contexto tecnológico.

Las TIC constituyen herramientas que nos ayudan en el ejercicio de los Derechos Humanos. La Resolución A/HRC/20/L.132 del Consejo de Derechos Humanos de la Organización de Naciones Unidas (en adelante ONU), titulada "Promoción, protección y disfrute de los derechos humanos en Internet"[3] reconoció, en lenguaje de Derechos Humanos, una serie de derechos de acceso y empleo del Internet para todas las personas. La Resolución reconoce que los DDHH de las personas deben ser reconocidos y garantizados en el mundo *offline*, así como en el *online*. Adicionalmente, se exhorta a los Estados para que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países.

En México, con la reforma constitucional al artículo 6º, se adiciona el tercer párrafo, que refiere: "El Estado garantizará el derecho a las tecnologías de la información y comunicación… incluido el de banda ancha e Internet"[4]. De esta forma su acceso se vuelve una garantía exigible.

Para el año 2016, en su 32º periodo de sesiones, el Consejo de Derechos Humanos de la ONU aprobó otra Resolución[5] en donde, además de confirmar lo referido en la Resolución A/HCR/20/L.132, reconoce la expansión e importancia de las TIC, así como la interconexión mundial, como aceleradores del progreso humano. También reconoce la importancia del derecho a la privacidad, en línea, para materializar el derecho a la libertad de expresión, de reunión, así como de asociación pacífica, entre otros.

Destacando la importancia de aplicar un enfoque basado en DDHH para facilitar y ampliar el acceso a Internet. A lo anterior se suman medidas en torno a generar confianza en Internet (ciberseguridad). Destaca también la mención de que todas las medidas que se tomen, deben ser ejercidas a través del enfoque de gobernanza de Internet de múltiples partes interesadas. Además, pone en relieve la importancia del derecho humano de acceso a la información, no sólo para difundir, solicitar, investigar información, sino como una habilitador del derecho a la educación, y por tanto, la necesidad de una adecuada educación digital, para la reducción de la brecha digital, en específica la de género, entre otras.

[3] Consejo de Derechos Humanos de Naciones Unidas, Resolución A/HRC/20/L.13, "Promoción, protección y disfrute de los derechos humanos en Internet", de 29 de junio el 2018, disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf
[4] Párrafo adicionado mediante Decreto publicado en el *Diario Oficial de la Federación* el 11 de junio del año 2013.
[5] ONU, Resolución A/HRC/32/L.20, "Promoción protección y disfrute de los Derechos Humanos en Internet",

Por ello insta a los Estados a examinar la forma en que Internet y otras TIC pueden ser una importante herramienta para fomentar la participación ciudadana, en aras de alcanzar el ejercicio de los DDHH, así como el desarrollo sostenible.

Ciberespacio y ciberseguridad.

El ciberespacio es más que Internet, no sólo incluye el software, hardware, activos y sistemas de información, redes y la infraestructura. El ciberespacio es un espacio global y multidimensional, sustentado por elementos físicos y lógicos donde existe presencia virtual del ser humano.

Las amenazas y riesgos en el ciberespacio se desarrollan en un espacio común global. Las redes están tan interconectadas[6] que puede ser difícil limitar los efectos de un ataque contra una parte del sistema sin dañar otras o interrumpirlo del todo. Los activos de información de los individuos, empresas y gobiernos fluyen por igual en el ciberespacio. El intercambio y la salvaguarda de estos hoy en día resultan críticos para proteger los intereses públicos y privados en el área de la seguridad (pública, nacional, así como la paz y estabilidad internacional), la protección de los derechos humanos, la economía y el desarrollo.

En los últimos años hemos sido testigos de cómo las acciones negativas o el uso malicioso del ciberespacio han aumentado. Lo anterior consecuencia de una mayor accesibilidad a las herramientas, así como mejoras en las metodologías y capacidades técnicas de ataque, lo que permite la sofisticación de los actores empeñados en causar estragos o interrupciones. Sus efectos también se han incrementado y en un futuro no muy lejano podrían traer consecuencias humanitarias devastadoras[7].

La *European Union Agency For Network and Information Security*[8] (en adelante ENISA) reconoció como las principales tendencias dentro del panorama de amenazas cibernéticas del 2020[9] las siguientes: *Malware; Web Based Attacks; Web application Attacks; Phishing; DDos; Spam; Botnets; Data Breaches; Insider*

[6] Situación que ha sido materia de preocupación en el seno de la Asamblea General de la ONU donde se ha reconocido"que esa creciente interdependencia tecnológica se basa en una red completa de componentes de las infraestructuras de información esenciales"; *Cfr.* Preámbulo Resolución A/RES/58/199 de fecha 30 de enero 2004, disponible en: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (Consultado _____).

[7] El Comité Internacional de la Cruz Roja ya ha alertado sobre el uso de operaciones cibernéticas en conflictos armados y las consecuencias humanitarias devastadoras que pueden traer consigo; *Cfr.* Cordula Droege (ICRC Legal Adviser), "No legal vacuum in cyber space," Interview on 16 Aug. 2011, *ICRC Resource Centre,* disponible en: https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (Consultado el 28 de junio de 2019)

[8] Agencia Europea de Seguridad de las Redes y de la Información

[9] En el documento "Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe", ENISA, hace referencia a las "existential threats", entendidas como las amenazas, que en caso de llegar a ocurrir "tienen el potencial de destruir la parte directamente afectada de la sociedad, la industria o las empresas" (*Those threats that if enacted have potential to destroy the directly impacted part of society, industry and business*); *Cfr.* European Union Agency for Network and Information Security ENISA, *Analysis of the European R&D Priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe*, European Union Agency For Network and Information Security, 2018, disponible en: https://www.enisa.europa.eutopics/threat-risk-management/threats-and-trends (Actualizado al 2020)

Threat; Physical manipulation/damage/theft/loss; Information Leakage; Identity Thieft; Cryptohacking[10]*; Ramsomware; Cyber Espionage*[11].

Las predicciones para este año no son alentadoras. El Foro Económico Mundial (en adelante FEM), recientemente publicó su informe "*The Global Risks Report 2019"*[12], en donde sitúa al robo o fraude de datos y a los ciberataques dentro de los primeros cinco[13] lugares en su "Encuesta de Percepción de Riesgos Globales" (*Global Risks Perception Survey*, GRPS), consolidando su posición junto con los riesgos medioambientales en el cuadrante de alto impacto y probabilidad del panorama de riesgos globales[14]. Para el caso de los ciberataques, tuvo un aumento de 82%, a nivel global. Dentro del informe el FEM también reconoció que el año pasado proporcionó evidencia adicional de los riesgos que los ciberataques plantean para la infraestructura crítica de los países.

El uso malicioso de la tecnología amenaza la seguridad, paz y estabilidad internacional. Es por lo que la ciberseguridad se ha vuelto una preocupación para la comunidad internacional. La ONU ha emitido diversas recomendaciones en donde enfatiza que "la difusión y el uso de las tecnologías y los medios de la información afectan los intereses de toda la comunidad internacional"[15], reconociendo que las tecnologías "también pueden ser empleadas con finalidades distintas de los objetivos de mantener la estabilidad internacional y la seguridad"[16].

La ciberseguridad en el ámbito personal, empresarial y gubernamental es uno de los desafíos clave de nuestro tiempo, por lo que debe ser una política pública de alto nivel en nuestro país tanto en la Estrategia Nacional de Ciberseguridad bajo sus tres principios: respeto de los Derechos Humanos, gestión de riesgos y un enfoque multidisciplinario, con involucramiento de todas las partes interesadas, así como en esta ley.

Los países cada vez más dependen de Internet, para mantener sus servicios, infraestructura y economías en el ciberespacio; por tanto, deben ser los más preocupados en mantenerlo seguro. De esta forma los encargados de la

[10] De conformidad con ENSIA, el *cryptohacking* o *cryptomining* es un ejemplo del funcionamiento del cibercrimen como servicio (*Cybercrime-as-a Service)*, conpetualizando así a los programas que emplean el poder del procesamiento de dispositivos de la víctima para extraer criptomonedas sin consentimiento, para más tarde obtener dinero en el mundo real, monetizado después de intercambios y transacciones legales. Este poder se utiliza para resolver rompecabezas criptográficos que se registran en la cadena de bloques; *Cfr*. European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, p. 09, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el ----------)

[11] European Union Agency for Network and Information Security, "ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends", European Union Agency For Network and Information Security, 2019, p. 09, disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (Consultado el 28 de enero 2019)

[12] Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, p. 5, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado --------)

[13] En primer lugar se encuentran los acontecimientos climáticos extremos, seguido de el fracaso de la mitigación y adaptación al cambio climático y en tercero los desastres naturales.

[14] Foro Económico Mundial, "*The Global Risk Report 2019*", Foro Económico Mundial, Ginebra, 2019, p. 16, disponible en: https://es.weforum.org/reports/the-global-risks-report-2019/articles/ (Consultado ----------

[15] "*… the dissemination and use of information technologies and means affect the interests of the entire international community*"; *Cfr.* Asamblea General de Naciones Unidas, Preámbulos de las Resoluciones A/RES/55/28 de 20 de Noviembre del año 2000; A/RES/56/19 de 29 de noviembre de 2001; A/RES/59/61 de 3 de diciembre de 2004; A/RES/60/45 de 8de diciembre de 2005; A/RES/61/54 de 6 de Diciembre de 2006; A/RES/62/17 de 05 de diciembre de 2007; A/RES/63/37 de 2 de diciembre de 2008; A/RES/64/25 de 2 de diciembre de 2009.

[16] Preámbulos de las Resoluciones A/RES/58/32 de 08 de diciembre de 2003; A/RES/59/61 de 3 de diciembre de 2004; A/RES/60/45 de 8 de diciembre de 2005; A/RES/61/54 de 6 de diciembre de 2006; A/RES/62/17 de 5 de diciembre de 2007; A/RES/63/37 de 2 de diciembre de 2008; A/RES/64/25 de 2 de diciembre de 2009.

formulación de políticas públicas no sólo enfrentan una inmensa tarea para seguir el rápido ritmo del cambio tecnológico en medio de una gran incertidumbre sobre la configuración del futuro[17].

En ese orden de ideas, y ante la progresividad de los Derechos Humanos, la Libertad de Expresión resulta ser clave para asegurar no solo la integridad de las personas, sino también para conservar la legitimidad de los Estados y sus Instituciones democráticas; lo cual ante el avance de todo tipo de tecnologías tales como inteligencia artificial, computo en la nube, criptomonedas, tecnologías emergentes que entre otras, requieren adecuada regulación. Resulta igualmente relevante mencionar que, la CCN-CERT señala que: "… El principal objetivo de una campaña de desinformación es suministrar en el proceso de formación de la opinión pública de un país noticias falsas, medias verdades, información altamente subjetiva presentada como objetiva (confusión deliberada entre opinión e información) e información diseñada para producir un efecto emocional en el receptor, minimizando la probabilidad de que la persona la procese aplicando un juicio crítico generando con ello una manipulación de su percepción del contexto que le rodea.

Esta información se distribuye desde plataformas y perfiles que aparentan ser creíbles, pero que ocultan su verdadero origen, significado, y dificultan su trazabilidad. La distribución maliciosa y sistemática de información es de escasa calidad en el debate público pretende quebrar la confianza entre los ciudadanos de un país y en los principales actores responsables de mantener la cohesión social: instituciones y medios de comunicación… …"[18], en tal sentido se transgrede la libertad de expresión y ocasiona la pérdida de confianza no solo hacia las personas que de forma individual se pueden ver afectadas por la desinformación, sino que también se altera negativamente el ánimo social de la nación manipulado por un interés ilegítimo que afecta la soberanía nacional y pone en riesgo el desarrollo económico político y social del país.

Resulta necesario tomar en consideración que los indicadores anuales de 2018 de la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) señalan que el número de cibernautas en el mundo se duplicó, pasando de 1,991 millones en 2010 a 3,896 millones en 2018, aunque el ritmo de crecimiento decayó de 10 por ciento a 7 por ciento en este mismo periodo.[19]

En otra perspectiva, el Panorama de Riesgos 2019, del Foro Económico Mundial (WEF por sus siglas en inglés), muestran que el fraude o robo de datos y los ataques cibernéticos son las principales amenazas globales, sólo detrás de los eventos meteorológicos extremos, el fracaso a la mitigación del cambio climático y los desastres naturales. Una señal de que los países deben poner mucha atención en la adopción de tecnologías, el crecimiento de usuarios y las

[17] United Nations Conference on Trade and Development (UNCTAD), *Informe sobre la Economía de la Información, 2017. Digitalización, Comercio y Desarrollo. Panorama General*, Organización de Naciones Unidas, Nueva York/Ginebra, 2017, p. 6.
[18] CCN-CERT BP/13, Desinformación en el Ciberespacio, 2019, p. 19.
[19] Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés, 2018): https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

tecnologías emergentes en términos de los riesgos y amenazas que esto pudiera representar.

El reporte anual de riesgos globales del Foro Económico Mundial también señala que:

"…

Las preocupaciones relacionadas con el fraude de datos y los ataques cibernéticos fueron prominentes otra vez en la GRPS, que también puso de manifiesto otras vulnerabilidades tecnológicas: alrededor de dos tercios de los encuestados creen que en el 2019 aumentarán los riesgos asociados con noticias falsas y el robo de identidades, en tanto que tres quintas partes dijeron lo mismo acerca de la pérdida de privacidad ante compañías y gobiernos. En el 2018 hubo más filtraciones masivas de datos, se revelaron nuevas debilidades de hardware y la investigación apuntó a usos potenciales de la inteligencia artificial para dar lugar a ataques cibernéticos más potentes. El año pasado también proporcionó evidencia adicional de que los ataques cibernéticos plantean riesgos a la infraestructura esencial, ya que orillan a los países a fortalecer su filtrado de asociaciones transfronterizas por motivos de seguridad nacional.

…" [20]

La firma de software Symantec afirmó en su reporte anual 2019 que a nivel mundial los costos del cibercrimen ascendieron a cerca de 126 mil millones de dólares en 2016, y en México alcanzó los 5 mil 500 millones de dólares. México fue el segundo país de América Latina donde se detectaron mayores amenazas cibernéticas, sólo superado por Brasil.[21]

La constante evolución de las tecnologías de la información y comunicación implica a su vez una permanente necesidad de protección y seguridad en un entorno digital donde los incidentes cibernéticos son cada vez más frecuentes, complejos y de mayor magnitud, con un alto impacto en la economía y la sociedad.

En el "Estudio exhaustivo sobre el delito cibernético"[22] realizado en el año 2013 por la ONU se establece que el delito informático es un fenómeno establecido desde hace tiempo, los antecedentes refieren a aquellos actos relacionados con computadoras, incluyendo los daños físicos a sistemas informáticos y datos almacenados; el uso no autorizado de sistemas informáticos y la manipulación de datos electrónicos; el fraude informático, y la piratería de programas

[20] World Economic Forum, Informe de Riesgos Mundiales 14ª Edición, 2019, p. 2. Disponible en https://www.zurich.com.mx/-/media/project/zwp/mexico/docs/wef-global-risks-report-2021.pdf?la=es-mx&rev=66c4d8ed609e4413b44ca534c40941a9&hash=30E981EBE8DDC61DDCD7EEF4F11BCD76

[21] Medios electrónicos: El Economista, 06 de junio de 2017. https://esemanal.mx/2019/02/informe-anual-de-amenazas-de-symantec/

[22] Organización de las Naciones Unidas, Estudio exhaustivo del delito cibernético" versión en español 2020. https://www.unodc.org/documents/Cybercrime/IEG_Cyber_website/UNODC_CCPCJ_EG.4_2020_2/UNODC_CCPCJ_EG.4_2020_2_S.pdf

informáticos, que han sido reconocidos como delitos penales desde la década de los 60.

En este contexto, la evolución del delito informático ha venido quedando únicamente en este enfoque, y por ende, se han generado diversas definiciones que involucran otras conductas propias de la modernización, el crimen y los abusos de la tecnología; el Dr. Julio Téllez Valdés establece en su libro “Derecho Informático” que al delito informático se le puede definir en forma típica y atípica, las conductas típicas son “*antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin*", y las atípicas como las "*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin*".[23]

De esta manera, se plantea que el delito informático evoluciona con las tecnologías de la información y comunicación a la par con la conectividad mundial, lo que conlleva de manera inseparable al desarrollo del delito cibernético contemporáneo.

Las actividades actuales del delito cibernético se enfocan en utilizar tecnologías de la información y comunicación globalizada para cometer actos delictivos con alcance transnacional lo que implica que los esquemas actuales de colaboración y cooperación internacional se vuelven laxos e inoperantes, favoreciendo la delincuencia y la impunidad.

En este contexto, la legislación mexicana ha venido reformando a nivel federal y local, diversas conductas relacionadas a los delitos cibernéticos, no obstante, que se encuentra dispersa y en gran parte con definiciones que en la práctica pudieran generar la falta de aplicación de las mismas.

Por otra parte, datos del Instituto Nacional de Estadística, Geografía e Informática (INEGI) señalan que en México hay 71.3 millones de usuarios de Internet, que representan el 63.9 por ciento de la población de seis años o más.[24]

La Asociación Mexicana de Internet MX en su 15°Estudio sobre los Hábitos de los Usuarios de Internet en México 2018[25] se identifica que el 26 por ciento de la población cibernauta se encuentra entre los 6 y los 17 años, una población que en la mayoría de los casos adopta las tecnologías sin una adecuada guía y supervisión haciéndolos vulnerables ante los abusos propios del Internet. A diferencia de la población de más de 34 años que en lo general aún presenta la dificultad en el uso de los dispositivos electrónicos, que a su vez también son usualmente víctimas del robo de identidad, principalmente los adultos mayores. Dicho estudio revela a su vez que ha crecido significativamente el uso de consolas de videojuegos y aparatos electrónicos, así como el uso de la banca electrónica.

En México, la División Científica de la Policía Federal atiende en promedio anual más de 3 mil solicitudes de investigación de autoridades competentes, de las

[23] Téllez Valdés, Julio. Derecho Informático. 2ª. ed. México. Mc Graw Hill 1996.
[24] INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2019.
[25] Asociación Mexicana de Internet MX, 15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018, 2019.

cuales de enero a mayo de 2019, los delitos que más resaltan son: pornografía infantil (17%), secuestro (13%), personas desaparecidas (11%), fraude (8%) y trata de personas (7%).

La pornografía infantil representa un problema global que en nuestro país se ha duplicado en los últimos tres años, respecto a la cantidad de indicios que son identificados por transmisión de contenidos a través de redes punto a punto (peer to peer), pasando de 15 mil en 2015 a 31 mil registros en 2018.

A fin de establecer un criterio, la División Científica de la Policía Federal por conducto de la Coordinación para la Prevención de Delitos Electrónicos realiza la clasificación de las diversas afectaciones que atiende conforme a lo siguiente:

- Conductas que afectan la confidencialidad, integridad y disponibilidad de la información:
    - Modificación y/o destrucción de contenido no autorizado a datos y sistemas de información
    - Negación o degradación del servicio
    - Creación, utilización, propagación e infección de código malicioso
    - Obtención ilegal, comercialización, divulgación o publicación no autorizada de información oficial reservada y/o datos personales
    - Ataques de fuerza bruta o escaneos de equipos y redes
    - Envío de correo SPAM
    - Phishing

En esta clasificación, con más de 20 mil incidentes cibernéticos registrados por la División Científica de la Policía Federal de enero a mayo de 2019, el primer lugar es infección de código malicioso con el 56%, seguido por los ataques de fuerza bruta con 18% y el Phishing con 12%.

- Conductas que afectan el patrimonio de los ciudadanos:
    - Robo de identidad y Fraudes
        - Fraude al comercio electrónico
        - Fraude nigeriano
        - Fraude al usuario de la banca electrónica
        - Extorsión
        - Robo de identidad

En esta clasificación, con más de 3 mil eventos reportados por la ciudadanía en el periodo enero a mayo de 2019, la principal afectación es el fraude al comercio electrónico con el 67 por ciento, seguido de la extorsión con 22 por ciento,

comúnmente por Ransomware (código malicioso que cifra la información del usuario dejándola inaccesible, lo que aprovechan los delincuentes cibernéticos para exigir una recompensa -de ahí la palabra “ransom”- a cambio del descifrado); y en tercer sitio el robo de identidad con 7 por ciento.

- Conductas que afectan psicológica y físicamente a la persona
    - Difamación
    - Amenazas
    - Acoso cibernético
    - Delitos contra la libertad de expresión
    - Actos ilícitos contra menores
        - Sexting
        - Sextorsión
        - Grooming
        - Cyberbullying
        - Pedofilia
        - Pornografía infantil
        - Trata de personas
        - Usurpación de identidad
        - Corrupción de menores
        - Abuso sexual

En esta clasificación, con más de 250 eventos registrados en el periodo enero a mayo de 2019, la principal afectación es la amenaza a menores con 27 por ciento, el acoso a menores con 26 por ciento y la pornografía infantil con 18 por ciento, usualmente las dos primeras conductas delictivas son utilizadas para la tercera.

- Conductas que afectan la propiedad intelectual:
    - Las relacionadas con obras protegidas por la Ley Federal del Derecho de Autor
    - Las relacionadas al descifrado ilegal de señales de satélite sin autorización de su distribuidor legal
    - El uso de otro nombre en la propiedad del código y el uso sin autorización de su propietario

- Utilización de técnicas para violar la protección de programas de cómputo y/o servicios informáticos

Así mismo, la regulación del Estado se reforma a un ritmo muy por debajo de lo que lo hace la tecnología, y en ese sentido, se considera imperante la necesidad de actualizar y reformar la legislación actual para adecuarla a un marco nacional y trasnacional de actuación que permita definir y tipificar las conductas que generan afectaciones de una forma homologada, armonizada a un contexto global, de orden nacional y con las estructuras en el ámbito ejecutivo y judicial que mediante el uso de instrumentos y mecanismos jurídicos así como la especialización generen las condiciones para el tratamiento del delito cibernético en un marco fortalecido.

Por otra parte, la propuesta de Ley que se desarrolla considera los aspectos más relevantes para cumplir con los avances en la armonización legislativa que los países de la ONU se han propuesto, incluyendo al menos la tipificación como delito de los principales actos del delito cibernético:

- Los delitos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos y los datos que correspondan a personas físicas, morales e instancias gubernamentales, que son perpetrados con el uso de sistemas informáticos.
- El uso de instrumentos y mecanismos para realizar solicitudes de preservación de datos y la obtención de datos almacenados y en tiempo real.
- El uso de técnicas de investigación con base en la legislación internacional sobre derechos humanos, incluyendo las protecciones de la privacidad que están basadas en tratados.
- Considerar la obligación de establecer en casos concretos la respuesta rápida para proporcionar evidencia electrónica y acordar lapsos para la respuesta.
- El desarrollo de programas, instrumentos y mecanismos de cooperación internacional y la consolidación del servicio 24/7.
- Las acciones de prevención del delito cibernético como elemento medular de las estrategias y políticas públicas.[26]

Con el objeto de prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, y garantizar la lucha eficaz contra la ciberdelincuencia, dado que es un hecho innegable que el desarrollo de las tecnologías de la información y la comunicación (TIC), ha propiciado un cambio en el desarrollo de la sociedad,

[26] Recopilación de algunas propuestas del Cuestionario de delito cibernético sobre el Estudio exhaustivo aplicado por la ONU, 2013.

desde las formas más sencillas de la existencia hasta la forma en la que se regula la vida cotidiana.

Entidades de aplicación de la Ley.

Bajo el contexto anterior, es necesario que existan entidades especializadas para la investigación y persecución de las conductas que se proponen en ésta Iniciativa, ante el aumento en el número de investigaciones vinculadas a la utilización de las nuevas tecnologías y más específicamente de internet, al ser cada vez más numerosos los bienes jurídicos objeto de protección penal, que pueden verse comprometidos por quienes utilizan los avances de la ciencia para llevar a efecto acciones criminales, aprovechando las ventajas que ofrecen las nuevas tecnologías.

En ese orden de ideas, se considera necesaria la creación de Fiscalías Especializadas en Delitos Informáticos, derivado de la incidencia de las manifestaciones cometidas directamente contra los sistemas informáticos o que se sirven de ellos para atentar contra los más variados bienes jurídicos, desde la intimidad, pasando los de carácter personal como la propia seguridad del Estado, pues en la actualidad existen dificultades para la presentación de denuncias derivado de los hechos ocurridos en un sistema informático, hasta las evidencias que deben presentarse a la autoridad y continuar con las líneas de investigación correspondientes.

Así mismo, la actividad ministerial se verá reforzada con la actuación de las policías especializadas las cuales en apego a lo establecido en el artículo 21 Constitucional, auxiliarán a la autoridad en la investigación, mismas que con la aprobación del Modelo Homologado de Unidades de Policía Cibernética que se implementó a partir de 2017, para lo cual las entidades federativas se comprometieron a asignar recursos del Fondo de Aportaciones para la Seguridad Pública de los Estados y del DF (FASP), con base en los artículos 44 y 45 de la Ley de coordinación Fiscal, y con ello dar cumplimiento a los acuerdos: 12/XL/16 referente a la elaboración de un Modelo Homologado de Unidades de Policía Cibernética, y 06/XLI/16. Modelo Homologado de las Unidades de Policía Cibernética, del Consejo Nacional de Seguridad Pública, fortalecerán no solo la investigación y persecución de éstas conductas delictivas, sino también se construirán las acciones de prevención en materia de ciberseguridad.[27]

De igual forma, no se omite mencionar que debe considerarse para la continuidad del desarrollo del Estado Mexicano en materia de ciberseguridad e infraestructuras críticas de información, la existencia de organismos especializados que actúe proactivamente para el impulso y el cumplimiento de objetivos en materia de ciberseguridad, en conjunto con otras instancias gubernamentales y el sector privado, donde se generen estándares de seguridad de la información, promoción de esquemas de cooperación interinstitucional

[27] http://www.dof.gob.mx/nota_detalle.php?codigo=5452136&fecha=09/09/2016, http://www.dof.gob.mx/nota_detalle.php?codigo=5468583&fecha=04/01/2017.

nacionales como internacionales, que permitan el desarrollo de mecanismos estandarizados de seguridad de la información y el impulso de programas de capacitación, concientización y desarrollo en ésta materia.

En suma, con las acciones propuestas en la presente iniciativa, el Estado Mexicano contará con la posibilidad de avanzar en materia de ciberseguridad al contar con una Estrategia Nacional de Ciberseguridad, una legislación más robusta e instancias que puedan investigar, perseguir y diseñar políticas públicas en la materia.

Infraestructuras Críticas de Información y Seguridad Nacional

En materia de seguridad nacional, han surgido ataques cibernéticos que han paralizado a países enteros dejando inutilizados sus servicios hacia la sociedad como el ocurrido en Estonia en 2007, que afectó a medios de comunicación, bancos y diversas entidades, e instituciones gubernamentales[28] ,o el sucedido en 2008 en Georgia que bloqueó sitios gubernamentales de forma generalizada, y en ambos casos se culpó a Rusia, quien negó que su gobierno estuviera detrás de estas acciones, pues es muy difícil de comprobar quienes son los responsables y bajo qué mando están[29].

A estos tipos de ataques se les ha denominado ciberguerra, que se define como ataques cibernéticos sistemáticamente realizados por parte de un Estado nación a otro, en donde el campo de batalla es el ciberespacio. El enorme impacto que han tenido los delitos cibernéticos y ciberataques entre países es tal que, ahora el ciberespacio ha sido considerado por los Estados Unidos, así como por la Organización del Tratado del Atlántico Norte y la mayor parte de los países del mundo, como la quinta dimensión de la guerra, existiendo entonces cinco dimensiones: tierra, mar, aire, espacio y ciberespacio[30]. En el caso de México, también se han cometido ciberdelitos que por sus implicaciones políticas, económicas y sociales, han puesto en riesgo la defensa y seguridad nacional del país, pues los ciberdelitos ahora constituyen un riesgo mundial sobre todo desde inicios del siglo XXI, lo que también afecta a nuestra nación.

Con relación a México, desde el año 2000, el país ha sufrido ataques cibernéticos, tanto en instituciones privadas (bancos) y públicas (gobiernos municipales, estatales y federales). Además, las infraestructuras de Tecnologías de Información y Comunicación mexicanas tienen alto grado de vulnerabilidad, pues de acuerdo con el reporte Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos, México ocupa el primer lugar en hospedaje de URL maliciosos y es el principal país originador de spam[31]. Asimismo, en 2010 México fue el segundo país afectado por el virus Zeus, después de Egipto, lo que provocó que miles de computadoras dentro del territorio nacional fueran comprometidas para ser utilizadas en lanzamiento de

[28] Kimburg A. (2012). National cyber security framework manual. NATO Coopertive Cyber Defense Center of Excellence.
[29] Instituto Español de Estudios Estratégicos (2011), Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio. Cuaderno de Estrategia 149. España: Ministerio de Defensa.
[30] Murphy, Matt (2010). Cyberwar: War in the fifth domain. Economist, July,3.
[31] Organizacion de Estados Americanos y Trend Micro. (Mayo de 2013). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. Washintong D.C.

ataques a otros países[32] 31. De igual forma, el sector académico de México experimenta más ataques que otro sector con el 39% del total de incidentes, y las ciberamenazas en México han afectado a la población civil por el phishing en 409% en 2013[33].

México al igual que todos los países de la comunidad internacional, ha experimentado un desarrollo económico y social gracias a las tecnologías de la información y comunicación , de tal forma que varias de sus actividades vitales están soportadas por estas tecnologías, lo que ahora constituyen infraestructuras criticas de información y cuyo daño provocaría impactos negativos para el funcionamiento de la sociedad y del gobierno, poniendo así en riesgo la estabilidad, integridad y permanencia del Estado Mexicano.

Es por ello que es importante implementar un Programa rector de ciberseguridad en materia de Seguridad Nacional como parte de una iniciativa del Gobierno de la República, que defina las acciones y determine las responsabilidades para la protección de Infraestructuras Críticas de Información del país, así como para fortalecer la Seguridad Nacional en el ciberespacio.

Las infraestructuras críticas de información son aquellas que comunican, operan, monitorean y controlan las funciones societales y de gobierno más importantes, así como servicios, incluidos pero no limitados, de generación, distribución, y transmisión de energía; telecomunicaciones (móviles, terrestres, Internet, etc.); transportación (aire, tierra, vías férreas, marítima), defensa, etc.[34]

La infraestructura Crítica de Información ha venido incrementándose en las diferentes áreas vitales del Estado mexicano, por lo que su relevancia aumenta dramáticamente conforme el mundo se desarrolla tecnológicamente. La contribución de estos servicios así como su impacto es muy importante por lo que una falla o interrupción repentina de estas, puede provocar un impacto negativo en el bienestar de los ciudadanos y en la Seguridad Nacional de nuestro país.

Una característica importante es el incremento de una profunda interdependencia en una red profunda de interacción entre diversas infraestructuras de carácter critico de información, por lo que una interrupción, distorsión o disrupción en el funcionamiento de una o varias traerá un potencial problema generalizado en cascada a otras y, como consecuencia una inestabilidad nacional que constituirá un riesgo potencial a la Seguridad Nacional del Estado Mexicano.

Es por ello que, debido a la dinámica del ciberespacio, el reto inherente es garantizar el buen funcionamiento de nuestra red de Infraestructura nacional, las cuales se están incrementando exponencialmente generando una ubicuidad presente en servicios dependientes de ellas. Por otro lado se ha considerado

[32] Unisys Stealth Solution Team. (2010). Zeus Malware: Threat Banking Industry. Recuperado el 7 de marzo de 2017, de http://botnetlegalnotice.com/citadel/files/Guerrino_Decl_Ex1.pdf
[33] Parragez Kobek, L. (2017). The State of Cybersecurity in Mexico: An Overview. México: Wilson Center's Mexico Institute
[34] The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.

que hay un alto grado de vulnerabilidad a los ciberataques con motivos y objetivos diversos, usando múltiples metodologías de ataque por lo que su protección es el tema más crítico de ciberseguridad en el país. Es por ello que es importante establecer un Programa Rector de Ciberseguridad en materia de Seguridad Nacional para atender los riesgos y las amenazas.

Algunos de los ataques importantes a nivel mundial que han puesto el riesgo la seguridad nacional de diferentes naciones se mencionan a continuación:

a. Red GhosNet.

Fue el caso de la red de espionaje electrónico cuyo origen se atribuye a un Estado nación, y que fue descubierta en 2009 después de 10 meses de investigación por especialistas del Centro Munk de la Universidad de Toronto; esta había infiltrado al menos 1295 computadoras en 103 países alrededor del mundo, y entre algunas ubicaciones se encuentran los centros de exilio tibetano del Dalái Lama en la India, Brúcelas, Londres, Nueva York; así como las embajadas de India, Corea del Sur, Malta, Alemania, y Pakistán entre otros[35].

b. Espionaje de gobiernos a través de empresas globales.

Según informes públicos, señalan que empresas de telecomunicaciones han proporcionado información privada de sus clientes a gobiernos, lo que ha llevado a varios Estados a tomar medidas al respecto, lo cierto es que empresas globales tienen equipos de red y comunicaciones conectados en todas partes y de comprobarse estos hechos, podría ser una amenaza a nivel global de grandes dimensiones[36] [37].

c. Programas de espionaje.

A nivel mundial se han publicado información sobre programas de espionaje electrónico promovidos por gobiernos para la recopilación masiva de datos de compañías de Internet, como los dados a conocer en 2013 tras las revelaciones de Edward Snowden.[38]

d. Stuxnet.

Stuxnet es un gusano informático que ataca a los Sistemas de Control Industrial (ICS por sus siglas en inglés) que se utilizan para controlar instalaciones como plantas de energía eléctrica, presas, sistemas de procesamiento de desechos entre otras operaciones industriales. Stuxnet busca sistemas de control industrial y luego modifica el código en ellos para permitir que los atacantes tomen control de los sistemas sin que los operadores lo noten. En otras palabras, esta

[35] Munk Centre. (29 de Marzo de 2009). Tracking GhostNet:Investigating a Cyber Espionage Network. (T. University, Ed.) Recuperado el 14 de Marzo de 2017, de http://www.nartv.org/mirror/ghostnet.pdf
[36] Riley, C. (19 de Julio de 2013). Ex-CIA director says Huawei spied for China. CNNMoney Recuperado el 14 de Marzo de 2017, de http://money.cnn.com/2013/07/19/news/huawei-china-spy/
[37] Matt Apuzzo and Michael S. Schmidt (5 de noviembre del 2016), Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say. The New York Times. Recuperado el 30 de julio del 2019 en: https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html
[38] Chappell, Bill (June 6, 2013). "NSA Reportedly Mines Servers of US Internet Firms for Data". The Two-Way (blog of NPR). Recuperado el 31 de julio del 2019 en: https://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/

amenaza está diseñada para permitir a los hackers manipular infraestructura física, lo cual lo hace extremadamente peligroso.

Fue descubierto en junio de 2010, y se sospecha que fue usado para atacar la central nuclear de uranio en Irán, Natanz, usando cuatro vulnerabilidades 0-day (no descubiertas previamente). Así, Stuxnet se puede considerar la primer ciberarma, siendo pionero en su tipo, mostrando también lo vulnerable que pueden llegar a ser los sistemas industriales hoy en día[39].

- Conductas que afectan al estado de derecho y la seguridad nacional
    - Los servicios que operan en el territorio nacional a través de infraestructura del Estado Mexicano o a través de permisionarios y/o concesionarios que son regulados por el Estado Mexicano para la provisión de energéticos, telecomunicaciones, agua, electricidad y otros por cuya definición sean considerados como críticos por su impacto económico, político o social incluyendo los del uso de las fuerzas armadas.
    - Los delitos electorales.

Como puede verse, las amenazas son muchas y los riesgos innumerables por lo que es necesario desarrollar medidas coordinadas y legislativas a nivel de país para poder responder a los riesgos mundiales, regionales y nacionales que atenten contra el Estado Mexicano.

Al tenor de lo anteriormente expuesto, con el espíritu y motivación antes señalados, ponemos a la consideración de esta Honorable asamblea el siguiente:

Decreto por el que se expide la Ley General de Ciberseguridad 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.

[39] Mueller, P., & Yadegari, B. (2012). The Stuxnet Worm. Département des sciences de l'informatique, Université de l'Arizona, http://www.cs.arizona.edu/~ collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report. pdf.

Artículo 211 bis 6.- Derogado.

Artículo 211 bis 7.- Derogado.

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

LEY GENERAL DE CIBERSEGURIDAD

LIBRO PRIMERO

TÍTULO PRIMERO

CAPÍTULO I
Disposiciones Preliminares

Artículo 1.- La presente Ley es reglamentaria de los artículos 6 y 21 de la Constitución Política de los Estados Unidos Mexicanos en materia de Ciberseguridad y tiene por objeto regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad, así como establecer la distribución de competencias y las bases de coordinación entre la Federación, las Entidades Federativas y los Municipios, en esta materia.

Sus disposiciones son de orden público e interés general, social y de observancia general en todo el territorio nacional.

Artículo 2.- La Ciberseguridad es una función a cargo de la Federación, las Entidades Federativas y Municipios, que tiene como fines salvaguardar el uso seguro y responsable de las redes, los sistemas de información y comunicaciones, a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable, así como preservar las libertades, el orden y la paz pública, y comprende la prevención especial y general de las esferas política, económica y social, así como de los delitos cometidos en el ciberespacio, la investigación y la persecución de dichos delitos por parte de instituciones especializadas en el materia, en términos de esta Ley, en las respectivas competencias establecidas en la Constitución Política de los Estados Unidos Mexicanos.

El Estado desarrollará políticas en materia de ciberseguridad con carácter integral, sobre las causas que generan la comisión de los delitos y conductas antisociales cometidas en el ciberespacio, así como programas y acciones para fomentar en la sociedad el uso adecuado del ciberespacio, en conjunto de los valores educativos, culturales y cívicos, que induzcan el respeto a la legalidad y a la protección de las víctimas.

Artículo 3.- La función de la ciberseguridad se realizará en los diversos alcances de su competencia, estas serán por conducto de las diversas instancias de seguridad nacional, seguridad pública y de las demás Instituciones Policiales, en colaboración con los cuatro ámbitos de la seguridad pública consistentes en prevención del delito; investigación del delito y procuración de justicia; sanciones administrativas y penales; y de la reinserción social.

Contribuirán a la colaboración concurrente al auxilio y asesoría de las diversas dependencias, e instituciones de impartición de justicia, así como por las demás autoridades que en razón de sus atribuciones deban contribuir directa o indirectamente al objeto de la ciberseguridad, la Agencia Nacional de Ciberseguridad y otros organismos que administren infraestructuras críticas de información, de seguridad pública y nacional que componen la Comisión Nacional de Ciberseguridad.

Artículo 4.- La Comisión Nacional de Ciberseguridad contará para su funcionamiento y operación con las instancias, instrumentos, políticas, acciones y servicios previstos en la presente Ley, tendientes a cumplir los fines de la Ciberseguridad, la cual estará presidida por la o el Titular de la Secretaría de Seguridad y Protección Ciudadana y en suplencia por el Titular de la Agencia Nacional de Ciberseguridad.

La coordinación y concurrencia, en un marco de respeto a las atribuciones entre las instancias de la Federación, las Entidades Federativas y los Municipios, será el eje de la Ciberseguridad.

Artículo 5.- La coordinación de Estrategia Digital Nacional de Presidencia de la República, será coadyuvante en proponer herramientas, instrumentos, innovación y directrices digitales, en materia de Ciberseguridad. Así mismo podrá proponer la integración y ejecución de la implementación estratégica de Tecnologías de Información y Comunicación de la Agencia Nacional de Ciberserguridad.

Artículo 6.- Para los efectos de esta Ley, se entenderá por:

I. **Activo:** Se refiere a información, procesos, personas y tecnología que aporta valor y son relevantes para el objeto principal de una empresa, Institución, así como datos personales.

II. **Activo virtual:** La representación en valor registrado electrónicamente y utilizado entre el público como medio de pago para todo tipo de actos jurídicos, cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. Los cuales se encuentran sujetos a la normativa que Banco de México formule. (Ley para Regular las Instituciones de Tecnología Financiera, art. 30).

III. **ANCI:** Agencia Nacional de Ciberseguridad.

IV. **Algoritmo:** Conjunto ordenado de operaciones o funciones matemáticas que permite solucionar un determinado problema o lograr un resultado definido.

V. **Aplicación:** Programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas. Esto lo diferencia principalmente de otros tipos de programas, como los sistemas operativos, las utilidades, y las herramientas de desarrollo de software.

VI. **Autenticación:** Procedimiento para comprobar que alguien es quien dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

VII. **Autenticidad:** O no repudio, constituye un pilar de la seguridad de la información, el cual consiste en la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

VIII. **Archivo Informático:** Conjunto organizado de unidades de información (bits) almacenados en un dispositivo electrónico el cual puede ser modificado o asignado a voluntad del usuario o del programador, y que contiene un nombre y extensión que determina qué tipo de archivo es y qué funciones cumple.

IX. **Base de Datos:** Colección de datos o información relacionados entre sí que tienen un significado implícito.

X. **Borrado Seguro:** Proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.

XI. **Ciberamenaza:** Riesgo potencial relacionado a las vulnerabilidades de los sistemas informáticos e infraestructura física y pasiva de las redes públicas de telecomunicaciones de permitir causar daño a los procesos y continuidad de las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas.

XII. **Ciberataque:** Acción realizada a través de las redes de telecomunicaciones con el objetivo de dañar las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas.

XIII. **Ciberdefensa:** Conjunto de acciones, recursos y mecanismos del estado en materia de seguridad nacional para prevenir, identificar y neutralizar todo ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional.

XIV. **Ciberdelincuencia:** Actividades que llevan a cabo individuo(s) realiza(n) en el que utilizan como medio o como fin a las Tecnologías de la Información y Comunicación.

XV. **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.

XVI. **Ciberseguridad:** Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación.

XVII. **Confidencialidad:** propiedad de la información por la que se garantiza que su acceso se encuentra restringido a personal, entidades o procesos autorizados.

XVIII. **Contraseña:** También llamada clave o password. Una contraseña es una palabra formada por caracteres que sirve a uno o más usuarios para acceder a un determinado recurso.

XIX. **Datos Biométricos:** Cualquier registro o dato que hace referencia al reconocimiento de personas basado en sus características fisiológicas como el ADN (ácido desoxirribonucleico), huellas dactilares, retina, iris de los ojos, patrones faciales o de voz, así como las medidas de las manos a efectos de autenticación de identidad.

XX. **Datos Informáticos:** Representación simbólica mediante números o letras de una recopilación de información, la cual puede ser cualitativa o cuantitativa que faciliten la deducción de un hecho.

XXI. **Delitos cibernéticos o ciberdelitos:** 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.

XXII. **Dispositivo:** Aparato, artificio, mecanismo, artefacto, órgano, periférico, gadget, producto, elemento de un sistema o componente electrónico.

XXIII. **Dispositivo de Acceso:** Es toda tarjeta, placa, código, número, u otros medios o formas de acceso, a un sistema o parte de éste, que puedan ser usados independientemente o en conjunto con otros dispositivos, para lograr acceso a un sistema de información o a cualquiera de sus componentes.

XXIV. **Dominio:** Espacio de aplicabilidad intangible que define el campo de acción del ciberdelito.

XXV. **Nombre de dominio:** Es un nombre fácil de recordar asociado a una dirección física de internet.

XXVI. **Emisiones Electromagnéticas:** Combinación de campos eléctricos y magnéticos oscilantes, que no necesitan un canal o medio para su propagación de un lugar a otro.

XXVII. **Entorno Digital:** Conjunto de canales, plataformas y herramientas que disponen cualquier individuo, marcas o negocios para tener presencia en Internet.

XXVIII. **Entorno Físico:** Es aquello que rodea algo o alguien y con lo cual interactúa.

XXIX. **Estrategia Nacional De Ciberseguridad:** 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.

XXX. **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.

XXXI. **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.

XXXII. **Infraestructuras Críticas de Información:** Las infraestructuras de información esenciales consideradas estratégicas, 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.

XXXIII. **Internet:** Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales.

XXXIV. **Ley:** Ley General de Ciberseguridad.

XXXV. **Medio de almacenamiento informático:** Dispositivo que escribe y lee datos digitales en un soporte de forma temporal o permanente, siendo su funcionamiento de tipo mecánico o electrónico.

XXXVI. **Metadatos:** Conjunto de datos únicos de origen que describen el contexto, contenido y estructura de la información a través del tiempo, sirviendo para identificarlos, facilitar su búsqueda, administración y control de acceso.

XXXVII. **Moneda digital:** Cualquier medio de intercambio monetario que se realiza a través de un medio electrónico que permite transacciones instantáneas.

XXXVIII. **Orbita satelital:** Son las trayectorias en las que se coloca un satélite para cumplir su misión; estas trayectorias están definidas por leyes matemáticas.

XXXIX. **Principio de confidencialidad:** Los datos transmitidos o almacenados deben ser privados y ser conocidos solamente por personal autorizado.

XL. **Principio de disponibilidad:** Los datos transmitidos o almacenados deben ser accesibles a personal autorizado con independencia del tiempo y momento en que sean requeridos.

XLI. **Principio de integridad:** Los datos transmitidos o almacenados deben ser auténticos, libres de errores que pudieran cometerse durante su almacenamiento o durante su transmisión.

XLII. **Principio de no repudio:** Los datos transmitidos o almacenados son de autenticidad indiscutible, especialmente cuando se respaldan por certificados digitales aceptables, firmas digitales u cualquier otro identificador explícito.

XLIII. **Programa Informático:** Es una serie de comandos ejecutados por aplicaciones y recursos que permiten desarrollar diferentes tareas en un dispositivo a través de lenguajes de programación que posibilitan la operación del sistema.

XLIV. **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.

XLV. **Proveedor de contenidos en Internet:** Persona física o moral que brinda servicios, aplicaciones, almacenamiento, infraestructura y soporte técnico de diversos productos basados en Internet, entre otros, bajo las políticas de privacidad y condiciones que él mismo establece.

XLVI. **Radiofrecuencia:** También denominado espectro de radiofrecuencia, es la distribución energética del conjunto de las ondas electromagnéticas, es decir, la radiación electromagnética que emite una antena de radiocomunicación.

XLVII. **Reconocimiento biométrico:** Identificación o verificación de la identidad de una persona a partir de la comparación de platillas biométricas.

XLVIII. **Red Pública de Internet:** Es un tipo de red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal.

XLIX. **Red Social:** Comunidad virtual que permite la interacción entre personas u organizaciones que se conectan a partir de intereses o valores comunes, basados en la estructura de conocido ha conocido.

L. **Registro de Cadena de Custodia Aplicable a Indicios Informáticos o Digitales:** Procedimiento controlado que se aplica a los indicios digitales relacionados con el delito electrónico, desde su localización hasta su valoración, fijación y preservación.

LI. **Riesgo:** La posibilidad de que una amenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información.

LII. **Seguridad de la Información:** Capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad, auditabilidad, protección a la duplicación, no repudio y legalidad.

LIII. **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantiza el origen de la información, validando el emisor para evitar la suplantación de identidades.

LIV. **Auditabilidad:** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

LV. **Protección a la duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario, así como en impedir que se grabe una transacción para su posterior reproducción, con el objeto de simular múltiples peticiones del remitente original.

LVI. **No repudio:** Se refiere a evitar que una entidad, órgano o persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

LVII. **Legalidad:** Referido al cumplimiento del marco jurídico al que está sujeta la institución de que se trate.

LVIII. **Seguridad Informática:** Técnicas desarrolladas para proteger los equipos informáticos conectados en una red frente a daños accidentales o intencionados, los cuales incluyen el mal funcionamiento del hardware, la pérdida física de datos el acceso a bases de datos por personas no autorizadas.

LIX. **Sistema de Información:** Dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitado a los sistemas electrónicos, informáticos, de telecomunicaciones y telemáticos, que separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros.

LX. **Sistema de Telecomunicaciones:** Conjunto de dispositivos relacionados, conectados o no, cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales, señales electromagnéticas, signos, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos o informaciones de cualquier naturaleza, por medio óptico, celular, radioeléctrico, electromagnético o cualquiera otra plataforma útil a tales fines. Este concepto incluye servicios de telefonía fija y móvil, servicios de valor agregado, televisión por cable, servicios espaciales, servicios satelitales y otros.

LXI. **Sistema Electrónico:** Conjunto de circuitos electrónicos (semiconductores o transistores) que interactúan entre sí para el procesamiento de información digital.

LXII. **Sistema Informático:** Dispositivo aislado o conjunto de dispositivos interconectado o relacionados entre sí, cuya función sea el tratamiento automatizado de datos en ejecución de un programa.

LXIII. **Sistema Telemático:** Sistema que combina los sistemas de telecomunicaciones e informáticos como método para transmitir la información.

LXIV. **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, entre otros.

LXV. **Transferencia de datos personales:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

LXVI. **Transferencia de la Información:** Es un término genérico para referirse al acto de transmisión de activos de información, a través de un medio.

LXVII. **Usuario:** Conjunto de permisos y recursos asignados a un operador como parte de una red informática, que puede ser una persona o programa informático, con privilegios válidos.

LXVIII. **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

LXIX. **Wi Fi:** Es una red de dispositivos inalámbricos interconectados entre sí y generalmente conectados a Internet a través de un punto de acceso inalámbrico. Se trata de una red LAN que no utiliza un cable físico para el envío de la información. Tecnología de interconexión de dispositivos electrónicos de forma inalámbrica, que funciona en base al estándar 802.11, que regula las transmisiones inalámbricas.

Artículo 7.- Conforme a lo previsto en los artículos 6 y 21 de la Constitución Política de los Estados Unidos Mexicanos, la Federación, las Entidades Federativas, los Municipios, 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 siguientes atribuciones y obligaciones:

I. Competencias de la Federación:

a) Integrar la Comisión Nacional de Ciberseguridad y cumplir con sus objetivos y fines;

b) Formular políticas integrales, sistemáticas, continuas y medibles, así como programas y estrategias, en materia de ciberseguridad;

c) Ejecutar y, brindar un seguimiento a la evaluación de las políticas, estrategias y acciones, a través de las instancias previstas en esta ley;

d) Proponer, ejecutar y evaluar la Estrategia Nacional de Ciberseguridad, el Programa Nacional de Ciberseguridad y demás instrumentos programáticos en la materia previstos en la Ley de Planeación;

e) Distribuir a los integrantes del Sistema, la Comisión Nacional de Ciberseguridad y Agencia Nacional de Ciberseguridad, actividades específicas para el cumplimiento de los fines de la ciberseguridad;

f) Determinar criterios uniformes de homologación para la organización, operación y modernización tecnológica de las Instituciones especializadas en materia de Ciberseguridad;

g) 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;

h) 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 a la preservación y conservación de la evidencia digital;

i) Coordinar y 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;

j) 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;

k) 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;

l) 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

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

II. Competencia de las Entidades Federativas

a) Conocer y resolver sobre los delitos cibernéticos del fuero Estatal conforme a las legislaciones locales que para tales efectos emitan las Entidades Federativas.

b) Cumplir con la obligación de mantener en perfecto estado y funcionamiento el flujo de información relativo al Centro Nacional de Información Plataforma México.

c) Reportar en el Informe Homologado de Incidentes Cibernéticos (IHIC), en cumplimiento al formato único nacional del IHIC, incluyendo en su caso el Registro Nacional de Detenciones.

d) Crear, fomentar y mantener una estrecha coordinación y concurrencia por parte de las Oficinas de Ciberseguridad tanto de la Secretaria de Seguridad

Pública Estatal como de la Procuraduría o Fiscalía General del Estado con la Agencia Nacional de Ciberseguridad.

e) 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 preservación y conservación de la evidencia digital.

f) Que los Tribunales Superiores de Justicia de las treinta y dos Entidades Federativas proporcionen de manera permanente y oportuna la información estadística sobre todos los procedimientos relacionados con los ciberdelitos.

g) Colaborar de manera permanente en las acciones, estrategias y programas en materia de ciberseguridad vinculadas a la seguridad pública y nacional.

h) Colaborar en las campañas nacionales de prevención de conductas ilegales en el ciberespacio.

III. Competencia de los Municipios:

a) Colaborar de manera permanente en las acciones, estrategias y programas en materia de ciberseguridad vinculadas a la seguridad pública y nacional.

b) Colaborar en las campañas nacionales de prevención de conductas ilegales en el ciberespacio.

IV. Derechos y obligaciones de las personas físicas y morales:

a) Prevenir y colaborar mediante estrategias y acciones que permitan reducir las afectaciones, así como impulsar la procuración e impartición de justicia de acuerdo a las atribuciones de la Agencia Nacional de Ciberseguridad.

Artículo 8.- La coordinación, medición y seguimiento de lo dispuesto en esta Ley, se hará con respeto a lo establecido en los artículos 6 y 21 Constitucional, y conforme a las atribuciones que le correspondan a la Comisión Nacional de Ciberseguridad.

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

TÍTULO II

DE LAS INSTANCIAS DE COORDINACIÓN Y LA DISTRIBUCIÓN DE COMPETENCIA DE LA COMISIÓN NACIONAL DE CIBERSEGURIDAD

CAPÍTULO I

De la Organización de la Comisión Nacional de Ciberseguridad

Artículo 10.- La Comisión Nacional de Ciberseguridad se integrará por:

I. La Conferencia de Ciberseguridad;

II. La Conferencia de Ciberdefensa;

III. La Agencia Nacional de Ciberseguridad; y

IV. Las Oficinas Estatales de Ciberseguridad.

La Agencia Nacional de Ciberseguridad será la instancia superior de coordinación y seguimiento a las políticas públicas en materia de ciberseguridad.

La Conferencia de Ciberseguridad, estará compuesta por los representantes de la Agencia Nacional de Ciberseguridad por parte del Gobierno Federal y por las personas designadas por parte de los gobiernos de las Entidades Federativas, los cuales deberán tener conocimientos en materia de ciberseguridad, y deberán ser asesorados o acompañados por representantes de la Fiscalía o Procuraduría y Secretarias de Seguridad Pública o sus equivalentes.

La Conferencia de Ciberdefensa, estará compuesta por los representantes de la Agencia Nacional de Ciberseguridad por parte del Gobierno Federal y por las personas designadas por parte de la Secretaría de la Defensa Nacional y la Secretaría de Marina, los cuales deberán tener conocimientos en materia de ciberseguridad.

Artículo 11.- Las Conferencias cumplirán con los mecanismos de coordinación y concurrencia establecidos en esta Ley, que permitan la formulación y ejecución de políticas, programas, acciones necesarias para el cumplimiento de sus funciones.

CAPÍTULO II

De la Comisión Nacional de Ciberseguridad

Artículo 12.- Para efectos de representar a la Comisión Nacional de Ciberseguridad ante el Consejo de Seguridad Nacional y ante el Consejo Nacional de Seguridad Pública dicha atribución ejercerá, la o el Titular de la Secretaría de Seguridad y Protección Ciudadana.

La Comisión Nacional de Ciberseguridad en su carácter de parte integrante tanto del Consejo de Seguridad Nacional como del Consejo Nacional de Seguridad Pública estará integrada por:

I. La o el Titular de la Secretaría de Seguridad y Protección Ciudadana, quien lo presidirá;

II. El Titular de la Agencia Nacional de Ciberseguridad, quien fungirá como suplente en ausencia del presidente;

III. A quien para tal efecto designe el Secretario de la Defensa Nacional;

IV. A quien para tal efecto designe el Secretario de Marina;

V. A quien para tal efecto designe el Fiscal General de la República;

VI. A quien para tal efecto designe el Secretario de Gobernación;

VII. A quien para tal efecto designe el Secretario de Relaciones Exteriores;

VIII. A quien para tal efecto designe el Secretario de Comunicaciones y Transportes;

IX. A quien para tal efecto designe el Secretario de Energía;

X. A quien para tal efecto designe el Secretario de Hacienda y Crédito Público;

XI. A quien para tal efecto designe el Secretario de Economía;

XII. A quien para tal efecto designe el Secretario Educación Pública, y

XIII. A quien para tal efecto designen los Gobernadores de los Estados;

La Comisión Nacional de Ciberseguridad podrá invitar, por el tipo de la naturaleza de los asuntos a tratar, a las personas físicas o morales, Instituciones Educativas y representantes de la Sociedad Civil que puedan exponer conocimientos y experiencias para el cumplimiento de los objetivos de la ciberseguridad, expresando que dicha participación es de carácter honorífico.

Artículo 13.- La Comisión Nacional de Ciberseguridad, es una instancia deliberativa cuya finalidad es establecer y articular la política pública en la materia de ciberseguridad y tendrá las siguientes atribuciones:

I. Establecer los instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendientes a cumplir los objetivos y fines de la Ciberseguridad;

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

III. Establecer los lineamientos para la formulación de políticas generales en materia de Ciberseguridad;

IV. Promover la efectiva coordinación de las instancias que integran la Comisión, y dar seguimiento de las estrategias y acciones que para tal efecto se establezcan;

V. Formular propuestas para los programas nacionales de Ciberseguridad en los términos de la Ley de la materia;

VI. Evaluar el cumplimiento de los objetivos y metas de los programas de Ciberseguridad y otros relacionados;

VII. Llevar a cabo la evaluación periódica de los programas de Ciberseguridad y otros relacionados;

VIII. Expedir políticas en materia de suministro, intercambio, sistematización y actualización de la información que sobre Ciberseguridad generen las Instituciones de los tres órdenes de gobierno y de los poderes judiciales;

IX. Establecer medidas para vincular a la Comisión con otros organismos internacionales, nacionales, regionales o locales;

X. Promover políticas de coordinación y colaboración tanto con el Poder Judicial de la Federación como con los Poderes Judiciales de las Entidades Federativas; con la finalidad de informar veraz y oportunamente la información estadística sobre todos los procedimientos relacionados con los ciberdelitos, a través de los mecanismos establecidos;

XI. Promover políticas de coordinación y colaboración con la Fiscalía General de la República y de los Estados; con la finalidad de informar veraz y oportunamente, estadística sobre todos los procedimientos relacionados con los ciberdelitos, a través de los mecanismos establecidos;

XII. Crear grupos de trabajo especializados en Ciberseguridad, para el apoyo de sus funciones, y

XIII. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento de la Comisión.

Artículo 14.- La Comisión Nacional de Ciberseguridad podrá funcionar en Pleno o en grupos de trabajo previstos por esta ley. El Pleno se reunirá por lo menos cada seis meses a convocatoria de la o el Titular de la Secretaría de Seguridad y Protección Ciudadana, quien integrará la agenda de los asuntos a tratar.

El quórum para las reuniones de la Comisión Nacional de Ciberseguridad se integrará con la mitad más uno de sus integrantes. Los acuerdos se tomarán por la mayoría de los integrantes presentes de la Comisión.

Corresponderá al Presidente de la Comisión Nacional de Ciberseguridad, además, la facultad de promover en todo tiempo la efectiva coordinación y funcionamiento del Sistema.

Los miembros de la Comisión Nacional de Ciberseguridad podrán formular propuestas de acuerdos que permitan el mejor funcionamiento y logro de los objetivos de la Comisión.

La Agencia Nacional de Ciberseguridad, será la encargada de la gobernanza de la generación de la política pública y acuerdos que se generen en la Comisión Nacional de Ciberseguridad y vinculación con actores del sector público y privado.

La Secretaría de Relaciones Exteriores, coordinará la cooperación con organismos internacionales para vincular las acciones en materia de Ciberseguridad con diversas Agencias y cooperación Internacional.

Y las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento de la Comisión.

Capítulo II

De la Agencia Nacional de Ciberseguridad

Artículo 15.- La Agencia Nacional de Ciberseguridad está integrada por:

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

II. Un Secretario General, quien desempeñe las funciones de la Dirección General de Gestión de Servicio, Ciberseguridad y Desarrollo Tecnológico, quien, en los casos de ausencia del Titular de esta Agencia, desempeñara sus funciones;

III. Un Coordinador de Ciberseguridad, que desempeña las funciones de Coordinador de Ciberseguridad, Administración y Análisis de Información de Seguridad Pública; 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 16.- 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;

II. Impulsar ante las instancias Federales, Entidades Federativas y Organismos Constitucionalmente Autónomos, el cumplimiento de la Estrategia Nacional de Ciberseguridad;

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. 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 Tecnológicos;

V. Realizar las actividades de coordinación de los tres órdenes de gobierno y la iniciativa privada para realizar las funciones de Ciberseguridad en el país;

VI. 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;

VII. 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;

VIII. Promover el establecimiento de mecanismos de coordinación y colaboración entre los equipos de respuesta a incidentes cibernéticos públicos y privados;

IX. 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;

X. 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;

XI. 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;

XII. Emitir la política de seguridad para las Infraestructuras Críticas de Información y coordinar las acciones derivadas de ésta, atendiendo los estándares y mejores prácticas internacionales en la materia;

XIII. Evaluar en coordinación con el personal especializado designado por las instituciones públicas o privadas que tengan a su cargo infraestructuras que puedan ser consideradas críticas de información, las características específicas de las infraestructuras conforme al procedimiento establecido para tales efectos, a fin de determinar su criticidad y el impacto de las afectaciones a su operación;

XIV. Requerir tanto a las Entidades Federativas como a los Órganos Constitucionalmente Autónomos y los particulares, información para la integración del Registro Nacional de las Infraestructuras Críticas de Información, conforme a las disposiciones reglamentarias que al efecto se emitan;

XV. Integrar, actualizar y administrar el Registro Nacional de las Infraestructuras Críticas de Información, conforme a las disposiciones de la presente Ley, su reglamento y demás disposiciones aplicables;

XVI. Supervisar los análisis de riesgos de las Infraestructuras Críticas de Información;

XVII. Desarrollar un Mapa de Riesgos de las Infraestructuras Críticas de Información que describa la afectación de cada una de ellas sobre las demás;

XVIII. Establecer mecanismos para el monitoreo y generación de alertas de Infraestructuras Críticas de Información;

XIX. Establecer mecanismos permanentes de comunicación con los operadores de las Infraestructuras Críticas de Información para, en su caso, la emisión de alertas tempranas;

XX. Definir estándares de Protección de Infraestructuras Críticas de Información;

XXI. Participar y coordinar ejercicios y simulacros para la protección de las Infraestructuras Críticas de Información;

XXII. Coordinar la atención de incidentes en las Infraestructuras Críticas de Información a través de un equipo especializado de respuesta en incidentes en Infraestructuras Críticas de Información;

XXIII. Desarrollar mecanismos para la evaluación de la ciberseguridad en Infraestructuras Críticas de Información;

XXIV. Impulsar marcos jurídicos relacionados con protección de Infraestructuras Críticas de Información;

XXV. Establecer esquemas de cooperación con organismos internacionales y autoridades extranjeras para la protección de las Infraestructuras Críticas de Información;

XXVI. Reportar ante las autoridades competentes la posible comisión de hechos que afecten la seguridad, a fin de determinar la responsabilidad penal a que haya lugar;

XXVII. 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.

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

Artículo 17.- El Mapa de Riesgos, así como el Registro Nacional de las Infraestructuras Críticas de Información será reservada, al considerarse información de seguridad nacional, en los términos de la Ley General del Sistema Nacional de Seguridad Pública artículo 110 y de la Ley de Seguridad Nacional artículo 51, 52, 59 y 64, y de las Leyes de Transparencia y Acceso a la Información Pública y demás ordenamientos.

Artículo 18.- Corresponde a las Fuerzas Armadas representadas por la Secretaría de Marina y la Secretaría de la Defensa Nacional, desarrollar y ejecutar mecanismos para la ciberdefensa del país, así mismo serán el punto de contacto para el establecimiento de convenios de colaboración en materia de ciberdefensa y operaciones militares conjuntas en el ciberespacio que establezca México con otros países.

Capítulo III

De las facultades, competencias y obligaciones de las Entidades Federativas

Artículo 19.- Las Entidades Federativas deberán implementar el modelo homologado de Policía Cibernética que defina la Federación a través de la Secretaria de Seguridad y Protección Ciudadana en el marco de la Ley General del Sistema Nacional de Seguridad Pública.

Las Entidades Federativas a través de las Unidades Cibernéticas deberán suministrar las incidencias y delitos cibernéticos conforme a los criterios que dicte la Comisión Nacional de Ciberseguridad.

Las Entidades Federativas y demás entidades públicas y privadas, deberán coordinarse con la Federación en materia de prevención e investigación de incidentes y delitos cibernéticos con la Secretaria de Seguridad y Protección Ciudadana a través de los mecanismos que definan para tal fin.

Artículo 20.- 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 la infraestructura crítica, 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 cibernéticos e informáticos. Las conductas típicas, que involucren el ciberespacio, sistemas de infraestructuras críticas de información, 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 Mexicana, en los Tratados Internacionales, así como en los Organismos Internacionales Especializados en la Materia.

Artículo 21.- Competencia. Las disposiciones de esta Ley serán de competencia federal en los siguientes casos:

Se considerarán delitos aquellas conductas ilícitas que se cometan a través de las tecnologías de la información y comunicación, redes, internet, y todo tipo de sistemas informáticos.

Para efectos de considerar delitos cibernéticos de la competencia federal ya sea por su redacción expresa o por circunstancias de atracción, se tomarán en cuenta los criterios correspondientes al nivel de impacto, al nivel de organización de la conducta y las personas que intervienen, y al nivel de sofisticación.

I. Por los delitos que se inicien, preparen o cometan en el extranjero, cuando produzcan o se pretenda que tengan efectos en el territorio de la República; o bien, por los delitos que se inicien, preparen o cometan en el extranjero, siempre que un tratado o convenio de cooperación internacional vinculativo para México prevea la obligación de extraditar o juzgar y no se extradite al probable responsable al Estado que lo haya requerido;

II. Por los delitos cometidos en los consulados mexicanos o en contra de su personal, cuando no hubieren sido juzgados en el país en que se cometieron;

III. Los delitos continuos cometidos en el extranjero, que se sigan cometiendo en la República, se perseguirán con arreglo a las leyes de ésta, sean mexicanos o extranjeros los delincuentes. La misma regla se aplicará en el caso de delitos continuados;

IV. Los delitos cometidos en territorio extranjero por un mexicano contra mexicanos o contra extranjeros, o por un extranjero contra mexicanos;

V. Los delitos cometidos por mexicanos o por extranjeros en alta mar, a bordo de buques nacionales;

VI. Los ejecutados a bordo de un 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 el delincuente no ha sido juzgado en la nación a que pertenezca el puerto;

VII. Los cometidos a bordo de un buque extranjero surto en puerto nacional o en aguas territoriales de la República, si se turbare la tranquilidad pública o si el delincuente o el ofendido no fueren de la tripulación. En caso contrario, se obrará conforme al derecho de reciprocidad;

VIII. Los cometidos a bordo de aeronaves nacionales o extranjeras que se encuentren en territorio o en atmósfera o aguas territoriales nacionales o extranjeras, en casos análogos a los que señalan para buques las fracciones anteriores;

IX. Los cometidos en las embajadas y legaciones mexicanas.

X. En caso de delitos cometidos en contra de niñas, niños y adolescentes que tengan como medio o fin el uso de las tecnologías de la información y comunicaciones, de acuerdo a la convención sobre los derechos de los niños;

XI. Aquellos que comprometan las infraestructuras críticas de información del país, y;

XII. Los que pongan en riesgo la seguridad nacional.

Las autoridades locales serán competentes para conocer de las conductas y delitos previstos en esta Ley que no sean del orden Federal.

Los Estados que integran la Federación, incluida la Ciudad de México, conforme a su respectiva competencia, aplicarán las disposiciones de esta Ley, por las conductas y delitos iniciados o preparados en otra Entidad Federativa, cuando produzcan, o se pretenda que tengan efectos en su territorio, así como en los delitos permanentes o continuados que se sigan cometiendo en su territorio, incluyendo aquellos que utilicen las tecnologías de la información y comunicación, en los dominios dentro de éste que se empleen o que dañen

cualquier bien jurídico tutelado y todo tipo de sistemas informáticos para su comisión.

Los órganos jurisdiccionales de la Federación serán competentes para aplicar esta Ley en términos de la Constitución Política de los Estados Unidos Mexicanos, del Código Nacional de Procedimientos Penales y de la Ley Orgánica del Poder Judicial de la Federación

Artículo 22.- La ciberseguridad se rige también por los principios de legalidad, objetividad, profesionalismo, eficiencia, honradez y respeto a los derechos humanos reconocidos por los Estados Unidos Mexicanos.

Artículo 23.- Los fines de la ciberseguridad tienen por objeto: vigilar, cuidar y proteger en todo momento la protección de datos personales, toda persona será propietaria de sus propios datos, por lo que cualquier uso de datos deberá ser autorizado por la misma persona.

LIBRO SEGUNDO

PARTE ESPECIAL

TÍTULO PRIMERO

Capítulo I

De los Delitos contra la confidencialidad, la Integridad y la disponibilidad de la Información

Artículo 24.- Acceso ilícito a tecnologías de la información y comunicaciones, sistemas informáticos, electrónicos o telemáticos.

Al que por cualquier medio o método, sin autorización de la persona física o moral que legalmente pueda otorgarlo, dolosamente acceda, copie, extraiga, modifique, destruya o elimine la información provocando la pérdida de la confidencialidad, integridad y disponibilidad de la misma contenida en equipos, sistemas o medios informáticos, electrónicos o telemáticos, modifique o altere los procesos locales o remotos, que estén protegidos o no por un mecanismo de seguridad, se le impondrán de cuatro a diez 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 propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

Artículo 25.- Las sanciones a las conductas descritas en los párrafos anteriores se incrementarán en una mitad 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.

Artículo 26.- Interceptación e Intervención de Datos o Señales. A quien intercepte o 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 27.- Falsificación informática. Quien sin autorización de la persona física o moral que legalmente pueda otorgarlo 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 no auténticos con la intención que sean tomados o utilizados como auténticos para efectos legales, con independencia de que los datos sean legibles e inteligibles directamente. Se le impondrá de tres a diez años de prisión y multa de ochocientos a ocho mil quinientas unidades de medida de actualización (UMA).

Artículo 28.- 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 o datos contenidos en equipos, sistemas o medios de almacenamiento informáticos, electrónicos o telemáticos, se sancionará con la pena de seis a doce años de prisión y multa de mil a doce mil unidades de medida de actualización (UMA).

La sanción a la conducta descrita en este apartado, se incrementará en una mitad cuando derivado del abuso 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 29.- Fraude por medio informático.

Al que engañe o se aproveche del error en que otro se halle mediante cualquier medio o método informático, electrónico o telemático obtenga cualquier bien o derecho patrimonial en perjuicio de un tercero o del Estado, será sancionado con pena de prisión de cuatro a doce años de prisión y multa de quinientas a cinco mil unidades de medida de actualización (UMA).

Capitulo III

De los delitos contra la libertad de las personas

Artículo 30.- 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 ochocientas a ocho mil unidades de medida de actualización (UMA).

Artículo 31.- Usurpación de identidad.

El que se apropie mediante el uso de las tecnologías de la información y comunicación de un medio de identificación de otra persona con el propósito de realizar cualquier acto ilícito, será sancionado con una pena de cuatro a quince años de prisión y multa de seiscientas a nueve mil unidades de medida de actualización (UMA).

Para fines de este delito, se contemplarán aquellos datos personales que puedan ser utilizados por sí o junto con otros para identificar a una persona de forma directa o indirecta en entornos físicos o digitales, lo cual se extiende también a datos sensibles.

La sanción impuesta para la conducta descrita en este artículo, se incrementará hasta una mitad, cuando:

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

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

III. Exista consentimiento de forma intencional de una de las partes involucradas para hacer mal uso de su información o datos.

IV. Si una de las partes involucradas laboró o formó parte de algunas de las instancias bancarias, comerciales o entidades del Sistema Financiero, y aprovechándose de sus conocimientos sobre el proceso de selección para el otorgamiento de créditos y trámites correspondientes, auxilió a la comisión de la conducta para el otorgamiento del crédito indebido.

Artículo 32.- Incitación a la Violencia y Alteración del Orden Social.

Al que describa, diseñe o grabe cualquier tipo de material digital, auditivo, fotográfico o video gráfico con el propósito de que sea exhibido, publicado o compartido a través de redes de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean producto de la evolución tecnológica mediante los cuales se incite, facilite, induzca u obligue a personas a ocasionar un daño físico, psicológico, material, a la imagen o reputación, a sí mismas o a terceros, 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 apego a la libertad de expresión, siempre y cuando no inciten o consistan en terrorismo, o realicen la apología del odio nacional, racial, sexual o religioso, o constituya

discriminación, hostilidad, instigación o realización de genocidio o de pornografía infantil.

Así mismo, será considerado como incitación o realización de violencia aquellas acciones que de forma sistemática, automatizada e intencional desinformen a la población provocando la manipulación individual o colectiva de las personas, transgrediendo los límites del derecho a la libertad de expresión.

No serán motivo de sanción aquellas conductas inherentes al ejercicio del derecho a la libertad de expresión y de ideas de cualquier ámbito o materia, que lleven a cabo personas físicas y morales por cualquier medio de comunicación.

Artículo 33.- Delitos contra la Imagen Personal.

A quien amenace con divulgar, o sin autorización divulgue, distribuya, comercialice, arriende, publicite, o difunda imágenes, comunicaciones escritas, verbales, audiovisuales, a través de redes de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean producto de la evolución tecnológica, con contenido erótico, sexual o pornográfico, obtenidas con o sin el consentimiento de otra persona, o bien hayan sido falsamente creadas, se le impondrá de seis a diez años de prisión y multa de mil a tres mil unidades de medida y actualización (UMA).

Las sanciones a que se refiere el párrafo anterior se aumentarán hasta el doble 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.

Artículo 34.- Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo.

A quien solicite, procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, a realizar actos sexuales o de exhibición corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, audio grabarlos, fotografiarlos, filmarlos, transmitirlos, exhibirlos o describirlos, a través de anuncios impresos, sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, se le impondrá de siete a catorce años de prisión y multa de mil a diez mil unidades de medida de actualización, así como 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 prevista en el párrafo anterior se aumentará en una mitad.

Se impondrán las mismas sanciones a quien financie, elabore, reproduzca, almacene haciendo uso de algún servicio de alojamiento local o remoto en sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, distribuya, comercialice, arriende, exponga, publicite, difunda, adquiera, intercambie o comparta por cualquier medio el material a que se refieren las conductas anteriores.

A quien permita directa o indirectamente el acceso de un menor a espectáculos transmitidos a través de las tecnologías de la información y comunicación, obras gráficas o audiovisuales de carácter lascivo o sexual, se le impondrá prisión de dos a ocho años de prisión y multa de seiscientos a seis mil unidades de medida de actualización.

No constituye pornografía el empleo en los programas preventivos, educativos o informativos que diseñen e impartan las instituciones públicas, privadas o sociales, que tengan por objeto la educación sexual, educación sobre la función reproductiva, prevención de infecciones de transmisión sexual y embarazo de adolescentes.

Para efectos de esta Ley Federal, se entenderá por exhibición corporal toda representación, presentación real o gráfica del cuerpo humano.

Se entenderá por fines lascivos o sexuales la intención de obtener un placer o satisfacer un deseo sexual en el ámbito de la pornografía, respecto de hechos descritos en el presente capítulo.

Artículo 35.- Seducción de menores a través de medios informáticos o digitales de la Internet o por medios electrónicos.

A quien haciendo uso de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, contacte, incite, facilite, induzca u obligue a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo, a realizar transmisión en vivo o video llamadas en tiempo real, o solicite o reciba archivos electrónicos de tipo imagen, audio, video, u otros, en los que aparezca la víctima realizando actividades sexuales explícitas, actos de connotación sexual, actos de exhibición corporal con fines lascivos o sexuales, o le solicite un encuentro con propósitos sexuales, 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).

Para efectos de esta Ley Federal se entenderá por connotación sexual los actos que tengan como característica o finalidad conseguir una gratificación, lucro o placer sexual para el espectador o escucha e inclusive para el sujeto activo ya sea en los ámbitos de autoría, coautoría, participación o coparticipación penal.

A quien haciendo uso de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, establezca contacto con una persona menor de 18 años de edad y por esa vía, mediante amenazas u otros actos le obligue o induzca a dar, hacer sobre sí mismo o sobre un tercero, dejar de hacer o tolerar conducta alguna que dañe sus componentes fisonómicos, fisiológicos, psicológicos, sociales o económicos, se le aplicarán de cinco a quince años de prisión y de mil a doce mil unidades de medida de actualización (UMA).

Artículo 36.- Turismo Sexual

Comete el delito de turismo sexual quien promueva, publique, divulgue, publicite, invite, facilite o gestione haciendo uso de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, a que una o más personas viajen al interior o exterior del territorio nacional con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados con 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 o acto o con una o varias personas que no tienen capacidad para resistirlo.

A los responsables de este delito se les impondrá una pena de ocho a dieciocho años de prisión y multa de dos mil a quince mil unidades de medida de actualización (UMA).

Artículo 37.- Lenocinio a través del uso de las tecnologías de información y comunicación.

Comete el delito de lenocinio a través del uso de las tecnologías de información y comunicación quien utiliza a personas menores de dieciocho años de edad o de personas vulnerables o que no tienen capacidad para comprender el significado del acto o de personas que no tienen capacidad para resistirlo, siendo tal sujeto activo o responsable:

I.- Al que mediante explotación sexual del cuerpo de las personas antes mencionadas, por medio del comercio u obtenga de él un lucro o beneficio cualquiera;

II.- Al que induzca o solicite a cualquiera de las personas antes mencionadas, para que comercie sexualmente con su cuerpo o le facilite los medios para que se entregue a la prostitución,

III.- Al que administre o sostenga directa o indirectamente, prostíbulos, casas de cita o lugares de concurrencia dedicados a explotar la prostitución de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, u obtenga cualquier beneficio con sus productos.

IV.- Al que compre, registre, programe, administre, publicite, o por cualquier medio se beneficie de sistemas informáticos, electrónicos, telemáticos,

programas o aplicaciones que sean fruto de la evolución tecnológica, a través de los cuales promueva, publicite, invite, facilite o gestione la prostitución de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, u obtenga cualquier beneficio con sus productos.

Al responsable de este delito de lenocinio a través del uso de las tecnologías de información y comunicación se le impondrá prisión de diez a veinte años de prisión y multa de dos mil a ocho mil unidades de medida de actualización (UMA).

Artículo 38.- Destrucción de material.

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.

Capitulo IV

De los delitos a la propiedad intelectual

Artículo 39.- Cuando las conductas descritas en la Ley Federal de Derechos de Autor y en la Ley de Propiedad Industrial, vigentes al momento de los hechos, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o en cualquiera de sus componentes, se sancionará con prisión de seis a doce años y con multa de dos mil a diez mil unidades de medida de actualización (UMA), sin perjuicio de las sanciones penales que sea procedente aplicar conforme a otras leyes, en apego al principio penal de especificidad que sobre conductas ilegales corresponde a esta Ley.

Capítulo V

De los delitos contra la nación

Artículo 40.- Serán considerados también delitos contra la Nación, los actos que se realicen a través de un sistema informático, electrónico, telemático o de telecomunicaciones, que atenten contra los intereses fundamentales y de Seguridad de la Nación, tales como los siguientes:

I.- Al que sin autorización de la persona física o moral que legalmente pueda otorgarlo por cualquier medio o método acceda, copie, extraiga, altere, modifique, destruya o elimine dolosamente la información provocando la pérdida de la confidencialidad, integridad y disponibilidad de la misma contenida en equipos, sistemas o medios informáticos, electrónicos, telemáticos, modifique o altere los procesos necesarios para la protección o empleo correcto de una infraestructura crítica de información o que afecte la seguridad nacional, servicios esenciales o bien sistema local o remoto del Estado Mexicano, protegidos o no por un mecanismo de seguridad, se le impondrán cinco a quince

años de prisión y multa de ochocientos a ocho mil quinientas unidades de medida de actualización (UMA).

II.- Si las conductas a que se refieren los artículos 39 y 40:

a) Se realizarán respecto de equipos, sistemas o medios informáticos, electrónicos o, telemáticos que sean considerados como una infraestructura crítica de información, o bien sistemas locales o remotos relacionados con Instituciones de Seguridad Pública de la Federación o de las Entidades Federativas, se le impondrá pena de seis a veinte años de prisión y multa de mil a diez mil unidades de medida de actualización UMA.

b) Si el que hubiere cometido las conductas descritas es o hubiera sido servidor público de alguno de los tres niveles de gobierno, se le impondrá, además de lo previsto en el párrafo anterior, destitución e inhabilitación acorde a la Ley General de Responsabilidades Administrativas de los Servidores Públicos para desempeñarse en otro empleo, puesto, cargo o comisión pública.

De igual forma, las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 41.- A la persona o grupo de personas que mediante el uso de equipos, sistemas o medios informáticos, electrónicos o telemáticos promueva o favorezca o ejecute de forma sistemática o automatizada o intencional, las amenazas a la seguridad nacional referidas en el artículo 5 de la Ley de Seguridad Nacional, se le impondrá pena de ocho a veinticinco años de prisión y multa de tres mil a quince mil Unidades de Medida de Actualización (UMA).

Artículo 42.- Al que dolosamente, siendo o habiendo sido servidor público de la federación o integrante del sector seguridad privada, ponga en peligro o afecte información o funcionalidad, mediante el uso de equipos, sistemas o medios informáticos, electrónicos o telemáticos que sean considerados como una infraestructura crítica de información, o bien sistemas locales o remotos relacionados, se le impondrá una pena de diez a treinta años de prisión y multa de seis mil a veinte mil días de Unidades de Medida de Actualización (UMA), además se le impondrá destitución e inhabilitación acorde a la Ley General de Responsabilidades Administrativas de los Servidores Públicos para poder desempeñar empleo, puesto, cargo o comisión en cualquier institución o instancia de alguno de los tres órdenes de gobierno o en el Poder Judicial Federal o Estatal.

De igual forma, las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados bajo confidencialidad por las autoridades competentes.

Artículo 43.- Las penas se aumentarán en dos terceras partes, con independencia de las penas establecidas, cuando los delitos a que se refiere el presente capítulo, se cometan por:

I. Servidor o ex servidor público, o miembro o ex miembro de seguridad privada,

II. De igual forma, al servidor o ex servidor público o miembro de alguna corporación de seguridad privada se le destituirá del empleo, cargo o comisión público, y se le inhabilitará acorde a la Ley General de Responsabilidades Administrativas de los Servidores Públicos para desempeñar cargos o comisión públicos;

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

IV. A quien aprovechándose de los conocimientos especializados en materia de tecnologías de la información y comunicación, realice alguna de las conductas comprendidas en el presente capítulo.

Capítulo VI

De los delitos contra el Sistema Financiero.

Artículo 44.- Al que dolosamente ponga en peligro o cause daño, altere u obstaculice por cualquier medio o método el funcionamiento de 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 cinco mil a doce mil Unidades de Medida y Actualización (UMA).

Artículo 45.- A la persona que por cualquier medio o método, 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).

Artículo 46.- A quien mediante el uso de tecnologías de la información y comunicación copie, extraiga, reproduzca, fabrique u obtenga ilícitamente un beneficio patrimonial, económico o de otra naturaleza para sí o para un tercero, así como por cualquier medio o método ilegalmente obtenga modifique dañe, altere o destruya parcial o totalmente información contenida en sistemas, equipos o medios informáticos, electrónicos o telemáticos, locales o remotos, de las instituciones que integran el sistema financiero, se le impondrán de ocho a veinticinco años de prisión y multa de ocho mil a quince mil Unidades de Medida y Actualización (UMA).

Artículo 47.- Como regla común y en cuanto a las penas previstas en estos artículos relativos a delitos financieros realizados a través del uso de tecnologías de la información y comunicación se incrementarán las sanciones hasta en una mitad cuando las conductas sean cometidas por empleados o ex empleados de las instituciones que integran el sistema financiero.

Artículo 48.- A los empleados o ex empleados de las empresas prestadoras de servicios que tengan o hayan tenido relación comercial o contractual con instituciones públicas, y del sistema financiero, se les aumentará hasta una mitad de las penas previstas en el presente capítulo.

Artículo 49.- Las penas a que se refiere el artículo anterior se incrementaran hasta en una mitad cuando los empleados hayan firmado un acuerdo o carta de confidencialidad.

Capitulo VII

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 50.- Las penas se aumentarán en dos terceras partes, con independencia de las penas establecidas, cuando los delitos a que se refiere el presente título, se cometan por:

I. Servidor o 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 público, y se le inhabilitará de acuerdo a la Ley General de Responsabilidades Administrativas de los Servidores Públicos para desempeñar cargos o comisión públicos;

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

IV. A quien aprovechándose de los conocimientos especializados en materia de tecnologías de la información y comunicación, realice alguna de las conductas comprendidas en el presente Título.

Artículo 51.- En los hechos relacionados con el presente Título, 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 conforme a los lineamientos que emita la autoridad competente del ejecutivo federal.

Artículo 52.- Las Policías, la Guardia Nacional y el Ministerio Público, en apego a lo establecido en el Código Nacional de Procedimientos Penales, podrán solicitar sin intervención de la autoridad judicial:

I. La cooperación con empresas proveedoras de servicios de Internet, y de servicios en la Red Pública de Internet nacionales e 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) Inciten al terrorismo realicen la apología del odio nacional, racial, sexual o religioso;

b) Que constituya incitación a la discriminación, la hostilidad o la violencia;

c) La instigación directa y pública a cometer genocidio y pornografía infantil;

d) Suplantación de identidad para fraude, y robo de datos personales;

e) Dañe la imagen pública y la reputación de una persona o Institución;

II. La preservación de la información, a los proveedores de servicios y contenidos en Internet, nacionales e internacionales.

III. En los hechos relacionados con el presente Titulo, y de conformidad con las políticas de privacidad de los proveedores de servicios y contenidos en Internet y cualquier otra entidad que contenga en su infraestructura indicios de hechos delictivos que pongan en riesgo las libertades, derechos humanos y otras garantías, la información correspondiente por los mecanismos establecidos por dichas personas físicas o morales.

En los casos de que los indicios se refieran a datos de contenido o datos personales deberá de solicitarse por control judicial y en caso de que se encuentren fuera del país también se deberá recurrir a los Tratados de Asistencia Jurídica Mutua o de Carta Rogatoria, según corresponda en términos de las disposiciones de Derecho Internacional.

De igual forma 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.

Así mismo, dichas 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 (90) días, pudiendo esta orden ser renovada por períodos sucesivos.

Artículo 53.- El Ministerio Público atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos 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 54.- Reparación del Daño.

El responsable deberá resarcir los daños generados 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:

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

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

III. 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. Las Secretarías de Seguridad Pública de las Entidades Federativas contaran con 180 días para la creación de las Unidades de Policía Cibernética.

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

SEXTO. 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 los subsecuentes.

SUSCRIBE

JESÚS LUCÍA TRASVIÑA WALDENRATH
Salón de Sesiones, a los 23 días del mes de marzo de 2021.