Ciudad de México, martes, 1 de septiembre de 2020

SENADOR EDUARDO RAMÍREZ AGUILAR
PRESIDENTE DE LA MESA DIRECTIVA
DEL SENADO DE LA REPÚBLICA
PRESENTE.

El suscrito Senador **Miguel Ángel Mancera Espinosa,** integrante y Coordinador del Grupo Parlamentario del Partido de la Revolución Democrática de la LXIV Legislatura del H. Congreso de la Unión, con fundamento en lo establecido en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos, 8, párrafo 1, fracción I y 164 párrafo 3, del Reglamento del Senado de la República, someto a consideración de esta Honorable Asamblea, la siguiente **INICIATIVA CON AVAL DEL GRUPO PARLAMENTARIO QUE CONTIENE PROYECTO DE DECRETO POR EL QUE SE MODIFICA LA DENOMINACIÓN DEL CAPÍTULO II, DEL TITULO NOVENO, DEL LIBRO SEGUNDO Y SE REFORMA EL ARTÍCULO 211 BIS 1 Y SE DEROGAN DIVERSOS ARTÍCULOS DEL CÓDIGO PENAL FEDERAL; SE REFORMAN Y ADICIONAN DIVERSOS ARTÍCULOS DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA; SE ADICIONA UNA FRACCIÓN XIV AL ARTÍCULO 5° DE LA LEY DE SEGURIDAD NACIONAL; Y SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD,** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

➢ GENERALIDADES

De acuerdo con las manifestaciones vertidas durante el Foro Económico Mundial en 2018, el mundo está atravesando por lo que podría considerarse una "cuarta revolución industrial".

"La globalización y la tecnología están íntimamente entrelazadas. Las nuevas formas de transporte y comunicación agilizan y aumentan el movimiento de personas, bienes e ideas. A su vez, la diversidad de ideas y la mayor escala que proviene del alcance mundial potencian el avance tecnológico". En todas las fases de la globalización, la tecnología ha desempeñado un papel fundamental en la configuración tanto de oportunidades como de riesgos. A medida que la cuarta revolución industrial impulsa una nueva fase de la globalización —la "globalización 4.0"— aquí le presentamos cinco cosas que podemos aprender al mirar hacia atrás, y hacia adelante, en el impacto de la tecnología".[1]

Las tecnologías de la información y de la comunicación han transformado las actividades de los gobiernos, las actividades

[1] La cuarta revolución industrial impulsa la globalización 4.0. https://es.weforum.org/agenda/2018/11/la-cuarta-revolucion-industrial-impulsa-la-globalizacion-4-0/

productivas y la manera en que las personas interactúan. Los sistemas cibernéticos o informáticos tienen la propiedad de ser sistemas agregativos, es decir, conforme más personas usuarias se conectan, aumenta el valor que estas redes ofrecen.

Según el Reporte Global para Riesgos, en 2019, el robo y fraude de datos y los ciber ataques se encuentran entre los cinco riesgos con más probabilidad de ocurrencia.[2]

La transformación digital que se vive actualmente, hace que las leyes y regulaciones referidas a estas tengan que redactarse o modificarse con cierta frecuencia para adaptarse a la coyuntura actual.

La ciberseguridad se ha convertido en un aspecto relevante. Cada vez se producen más ciberataques que pueden crear grandes problemas a empresas, organismos públicos y particulares.

En noviembre de 2001, los Estados miembros del Consejo de Europa firmaron el *"Convenio sobre la Ciberdelincuencia"*[3], en Budapest. Dicho Convenio reconoce la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como proteger los intereses legítimos en la utilización y el desarrollo de tecnologías de la información.

---

[2] The Global Risks Report 2019 14th Editionhttp://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[3] Convenio sobre la ciberdelincuencia https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

El Convenio previene los actos que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, facilitando su detección, investigación y sanción.

Las implicaciones económicas de los ciberataques no son menores, algunos estudios cifran las pérdidas globales por virus maliciosos en 350.000 millones de euros en 2016, y el coste conjunto de la criminalidad digital y la apropiación de propiedad intelectual en 445.000 millones de dólares y que la industria de seguridad informática mundial, que maneja entre 60.000 y 70.000 millones de euros en la actualidad (80.000, según McAfee), podría triplicar su negocio global en 2020, hasta superar los 200.000 millones.[4]

Sobre el particular, las Naciones Unidas, la OCDE, la Unión Europea y el G8 han realizado diversas iniciativas destinadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la delincuencia cibernética.

- **La necesidad de contar con una Ley General de Ciberseguridad en México**

[4] https://www.publico.es/internacional/industria-ciberseguridad-coge-musculo-oleada.html

En México, diversas voces se han manifestado sobre la urgencia de discutir una Ley General de Cibserguridad, entre esas voces se encuentra la del titular de la Secretaría de Seguridad y Protección Ciudadana al manifestar que esto es así en virtud de que “parte de los delitos que se cometen en el país se dan en el ciberespacio”.[5]

Ante ello, estamos ciertos que no es una tarea sencilla, pues se debe garantizar el equilibrio entre los intereses de la acción penal y el respeto a los Derechos Humanos contenidos en la Constitución Política de los Estados Unidos Mexicanos, así como en los tratados internacionales de los que el Estado Mexicano sea parte.

Y es que en México el uso del internet por las personas es medido en millones, y prueba de ello son los datos que el Instituto Nacional de Estadística y Geografía (INEGI), en colaboración con la Secretaría de Comunicaciones y Transportes (SCT) y el Instituto Federal de Telecomunicaciones (IFT), publicaron en virtud de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2019.[6]

Dicha encuesta, **respecto al uso de internet,** señala que en México hay 80.6 millones de personas usuarias de internet, que representan

---

[5] https://tecnoempresa.mx/index.php/2020/01/30/urge-aprobar-ley-general-de-ciberseguridad-alfonso-durazo/

[6] http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-mexico-hay-806-millones-de-usuarios-de-internet-y-865-millones-de-usuarios-de-telefonos-celulares

70.1% de la población de seis años o más. Esta cifra revela un aumento de 4.3 puntos porcentuales respecto de la registrada en 2018 (65.8%) y de 12.7 puntos porcentuales respecto a 2015 (57.4 por ciento).

Se estima en 20.1 millones el número de hogares que disponen de internet (56.4%), ya sea mediante una conexión fija o móvil, lo que significa un incremento de 3.5 puntos porcentuales con respecto a 2018 y de 17.2 puntos porcentuales en comparación con los resultados de 2015 (39.2 por ciento).

De los 80.6 millones de personas usuarias de internet de seis años o más, 51.6% son mujeres y 48.4% son hombres.

Entre 2017 y 2019, las personas usuarias en la zona urbana pasaron de 71.2% a 76.6%, mientras que en la zona rural el incremento fue de 39.2% a 47.7% de personas usuarias de 6 años o más.

Los tres principales medios para la conexión de personas usuarias a internet en 2019 fueron: celular inteligente (smartphone) con 95.3%; computadora portátil con 33.2%, y computadora de escritorio con 28.9 por ciento.

Las principales actividades de las personas usuarias de internet en 2019 correspondieron a entretenimiento (91.5%), obtención de información (90.7%) y comunicarse (90.6 por ciento).

Las personas usuarias de internet identificaron como principales problemas al conectarse a la red la lentitud en la transferencia de la

información (50.1%), interrupciones en el servicio (38.6%) y exceso de información no deseada (25.5 por ciento).

Por cuanto hace al **uso de telefonía celular,** la encuesta refiere que el país cuenta con 86.5 millones de personas usuarias de esta tecnología, lo que representa el 75.1% de la población de seis años o más; y un incremento de 3.6 puntos porcentuales respecto de 2015.

Nueve de cada diez personas usuarias de teléfono celular disponen de un celular inteligente (smartphone).

La proporción de personas usuarias que sólo dispusieron de un celular inteligente tuvo un crecimiento de 23 puntos porcentuales entre 2015 y 2019 (65.1 contra 88.1%, respectivamente).

Sin duda, estos números que seguirán en aumento en los próximos años, con ello el riesgo de delitos o ciberataques aumentará. Esto hace que la vida social, económica y política de la población mexicana esté expuesta a delitos cibernéticos.

- **Los ciberataques a nivel mundial**

La seguridad del ciberespacio y de los datos contenidos en éste, es uno de los mayores problemas al que se enfrenta el mundo actualmente, es por ellos que se requiere una respuesta oportuna, proporcionada, eficaz y coordinada que garantice la libre y segura utilización del mismo.

Un ciberataque es un conjunto de acciones ofensivas contra sistemas de información como bases de datos, redes computacionales, etc., hechas para dañar, alterar o destruir instituciones, personas o empresas.[7]

El 12 de mayo del 2017, se conoce como el día del *"WannaCry",* un ciberataque masivo dirigidos al sistema operativo *Windows de Microsoft.* Esto hace que los datos de la persona son encriptados, y se solicita un rescate económico pagado con la criptomoneda *Bitcoin,* para poder volver a tener el acceso a los datos.

El ataque ha infectado a más de 230,000 computadoras en más de 150 países, el ataque comenzó a través de una e-mail, el cual al ser abierto instala el programa en los servidores, y se extiende a través de las redes locales y anfitriones remotos que no hayan recibido la actualización de seguridad más reciente.

Los países más afectados que han sido reportados fueron Rusia, Ucrania, India y Taiwán, partes del Servicio Nacional de Salud de Gran Bretaña, *Telefónica de España, FedEx, Deutsche Bahn*, las aerolíneas de *LATAM*, entre otros.

En el 2017, la entonces Procuraduría General de la República, en conjunto con el Buró Federal de Investigaciones (FBI por sus siglas en

[7] https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos, Consultado el 2 de noviembre del 2019.

inglés), informaron que identificaron y destruyeron un virus cibernético proveniente de Corea del Norte, este virus tenía como objetivo obtener información y controlar equipos de cómputo, el virus se conoció como *FALLCHILL,* el cual estaba alojado en computadoras pertenecientes a una empresa privada de telecomunicaciones.

Una de las capacidades del virus fue la posibilidad de extraer información de discos duros de los equipos que infectó, además de finalizar procesos como leer, escribir o ejecutar archivos.

En las últimas décadas, casos como la explosión en el sistema de distribución de gas en la URSS (1982), el ciberataque contra empresas estadounidenses conocido como Titan Rain (2003 – 2005), el ciberataque contra Estonia (2007), el ciberataque contra Siria (2007), las acciones de ciberguerra durante la guerra en Osetia del Sur (2008) y el ciberataque contra el programa nuclear iraní (2010) han constituido episodios destacados de ciberguerra (Torres, 2013). También en 2016, un informe conjunto de la Organización de los Estados Americanos (OEA) y del Banco Interamericano de Desarrollo (BID)[8] señaló que el cibercrimen le cuesta anualmente al mundo unos 575.000 millones de dólares, es decir, un 0,5% del PIB global. En el caso concreto de América Latina y el Caribe, la cifra es de unos 90.000 millones anuales (BID y OEA, 2016).

[8] https://www.elfinanciero.com.mx/tech/america-latina-no-esta-preparada-para-un-ataque-cibernetico-bid

Se debe determinar qué tan grande es la brecha entre la tecnología y la legislación, debido a que los sistemas se desarrollan a gran velocidad, las sociadades dentro de sus ecosistemas gubernamentales y legislativos, tardan mucho en reaccionar para generar marcos legales y procesos judiciales adecuados, lo que está generando vacíos legales dentro del marco jurídico que dejan indefensos a las personas usuarias ante la ciberdelincuencia.

Cada vez en mayor medida las actividades sociales, económicas y hasta militares de un Estado se hacen más dependientes del uso de las Tecnologías de la Información y de la Comunicación, lo que implica una mayor vulnerabilidad y exposición a los ciberataques.

Lamentablemente, México[9] cayó 35 lugares en el Índice Global de Ciberseguridad (ICG) de la Unión Internacional de Telecomunicaciones (UIT). Entre 2017 y 2018, México pasó del lugar 28 al 63 dentro de la lista de países que integran el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (ITU). El país fue además desplazado por Uruguay de entre los tres primeros lugares del continente americano.

Mientras que en 2017, México ocupaba la posición 28 de 165 países, con un índice de 0.660, en 2018, el país cayó a la posición 63 de 175 países, con un índice de 0.629. Pese a que la ITU cambió detalles de la

[9] https://www.eleconomista.com.mx/tecnologia/Mexico-cae-35-lugares-en-Indice-Global-de-Ciberseguridad-de-la-ITU-20190506-0054.html

metodología entre ambos años y aumentó el número de países estudiados, México ha retrocedido de forma significativa respecto a las mediciones que hace la institución basada en Ginebra, Suiza.

El uso de las Tecnologías de la Información y de la Comunicación se ha incorporado de forma general a la vida cotidiana de nuestra nación. Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero al mismo tiempo, conlleva serios riesgos y amenazas que pueden afectar a la Seguridad Nacional.

Los distintos perfiles de atacantes que explotan las vulnerabilidades tecnológicas con el objeto de recabar información, sustraer activos de gran valor y amenazar los servicios básicos, pueden afectar al normal funcionamiento de nuestro país. El disfrute pacífico de ciertos derechos fundamentales consagrados en nuestra Constitución y en el ordenamiento jurídico internacional puede verse seriamente comprometido como consecuencia de este tipo de acciones.

- **Los ciberataques en México**

La información de diversos ciberataques en nuestro país es constante, y ello demuestra que México no ha estado exento de dichos ataques cibernéticos, y estos, se realizan cada vez con mayor frecuencia, y prueba de ello son las siguientes notas al menos de 2020:

- **Febrero de 2020. Hackers atacan a la secretaría de Economía.** La dependencia señaló que detectó un ataque cibernético en algunos servidores sin que fuera afectada información sensible y de sus usuarios.[10]

- **Febrero de 2020. Hackeo a empresas en México deja pérdidas por 3 mil mdd al año.** El experto en ciberseguridad, Fernando Thompson, señaló que el 87% de las organizaciones fueron atacadas en 2019.[11]

- **Marzo de 2020. El costo por ciberataques en México creció 38.4% en 2019.** El costo de un hackeo en México en 2018 fue de 2.5 mdp. En 2019 esta cifra alcanzó los 6.5 mdp, según cifras de Sophos.[12]

- **Marzo de 2020. Bancos, principal objetivo de ciberataques en México.** Fortinet, empresa global en materia de ciberseguridad, revela que nuestro país sufrió más de 12,8 billones de intentos de ciberataques en el 2019, la mayoría de éstos siguen la tendencia

[10] https://expansion.mx/economia/2020/02/25/hackers-atacan-a-la-secretaria-de-economia

[11]

[12] https://expansion.mx/tecnologia/2020/03/11/el-costo-por-ciberataques-en-mexico-crecio-38-4-en-2019

de Latinoamérica y están diseñados para entrar en redes bancarias, obtener información financiera y robar dinero[13].

- **Junio de 2020. Alertan por aumento de ciberataques en México.** En México, más del 50 por ciento de las empresas han tenido un ciberataque y el país se encuentra en el lugar número 12 de los más atacados con malware.[14]

- **Julio de 2020. Anonymous México ataca página del Banco de México, y amenaza a la Secretaría de Hacienda.** "Hacienda sigues tú", indicaron presuntos integrantes de Anonymous México tras atacar brevemente la página del Banco de México.[15]

- **Julio de 2020. Hackers buscan atacar al INE a un año de las elecciones.** El experto Israel Reyes Gómez advierte que estos ataques no son coincidencias y que ahora los piratas informáticos tienen un nuevo objetivo en la mira: los comicios de 2021.[16]

---

13 https://www.revistamasseguridad.com.mx/ciberataques-en-mexico-bancos-ciberseguridad/

14 https://www.milenio.com/tecnologia/alertan-por-aumento-de-ciberataques-en-mexico

15 https://www.unotv.com/nacional/anonymous-hackea-portal-de-banxico-amenaza-ahora-a-hacienda/

16 https://www.elsoldesanluis.com.mx/mexico/sociedad/hackers-buscan-atacar-al-ine-a-un-ano-de-las-elecciones-2021ciberataques-seguridad-tecnologia-ciberseguridad-5515569.html

➢ La regulación de la Ciberseguridad en América Latina

La mayor parte de los Estados en América Latina, disponen de capacidad de respuesta ante ciberataques, seis de ellos han diseñado una Estrategia de Ciberseguridad. Sin embargo, faltan diversos Estados en adoptar una estrategia de seguridad en este tema, esto puede deberse a la falta de recursos dedicados a esta problemática, así como la carencia de experiencia práctica y conocimientos especializados para diseñar e implementar este tipo de medidas. La OEA juega un papel importante a lo que a apoyo técnico se refiere.

Es por ello por lo que para tener un mejor panorama de lo que los Estados Americanos han implementado en este aspecto, lo ejemplificamos en el siguiente cuadro:

Colombia	Panamá	Paraguay	Costa Rica	Chile
Marco Institucional.	Derechos Fundamentales de los ciudadanos.	Sensibilización y cultura.	Coordinación Nacional.	Infraestructura.
Gestión de Riesgo.	Prevenir y detener conductas delictivas.	Investigación, Desarrollo e Innovación.	Conciencia Pública.	Garantizar los derechos de los ciudadanos.
Fortalecer la seguridad del individuo y el Estado.	Infraestructura	Infraestructura.	Capacidad Nacional de Seguridad.	Cultura de la Ciberseguridad

	Tejido Empresarial Nacional	Capacidad de Respuesta.	Marco Jurídico.	Cooperación con otros actores.
	Cultura de Seguridad Cibernética.	Capacidad de Investigación y Persecución.	Infraestructura.	Industria de la Ciberseguridad
	Capacidad de respuesta.	Administración Pública.	Gestión de riesgo.	
		Sistema Nacional.	Cooperación Internacional.	
			Implementación, Seguimiento y Evaluación.	

Colombia.

Fue el primer país en aprobar una Estrategia Nacional de Ciberseguridad, en el 2011. Para el 2016 se reformó y cambió su nombre a Política Nacional de Seguridad Digital, incluyendo la gestión de riesgo, esto para fortalecer la protección de las personas usuarias en el ciberespacio, así como las capacidades de los potenciales afectados, intenta reducir la probabilidad de que las amenazas sean efectivas.

Las cinco estrategias que implementa son:

1. *Gobernanza de la seguridad digital:* mediante la articulación de las partes interesadas, bajo el liderazgo del Gobierno de la Nación.
2. *Marco Legal y Regulatorio de la seguridad digital:* que recoja los aspectos necesarios para adoptar la Estrategia.

3. *Gestión sistemática y cíclica del riesgo de la seguridad digital*: a través de los procedimientos, metodologías e iniciativas necesarias.
4. *Cultura Ciudadana para la seguridad digital*: mediante la sensibilización de las partes interesadas.
5. *Fortalecimiento de las capacidades para la gestión del riesgo de seguridad digital* de todas las partes interesadas.

Los cinco objetivos específicos que incluye la Estrategia son:

1. *Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos, involucrando a las partes interesadas.*
2. *Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de la seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.*
3. *Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos.*
4. *Fortalecer la defensa y la soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.*

5. *Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.*

Las entidades encargadas de ejecutar la Estrategia son el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Nacional de Planeación y la Dirección Nacional de Inteligencia.

Panamá.

Tiene la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, la cual alude al estado de la ciberseguridad en los ámbitos nacional e internacional, tiene como objetivo aunar los esfuerzos de sus ciudadanos, empresas e instituciones públicas para lograr un incremento de la seguridad cibernética que permita el uso confiable de tecnologías de la información en todos los ámbitos nacionales, sin dejar de lado la salvaguarda de los derechos y libertades fundamentales de los ciudadanos y un entorno económico regulatorio favorable al crecimiento y desarrollo de las empresas y permitiendo el buen funcionamiento del Estado.

Los objetivos de la Estrategia se basan en la protección de los Derechos Humanos y las libertades fundamentales, corresponsabilidad en el uso de las TIC.

La Estrategia tiene seis pilares fundamentales:

1. Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio.
2. Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos.
3. Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales.
4. Fomentar el desarrollo de un tejido empresarial nacional fuerte en seguridad cibernética, como referencia para la región.
5. Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares.
6. Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes de los organismos públicos.

Objeto de la iniciativa

El objeto de la presente iniciativa es proteger a las instituciones del Estado y a la sociedad frente a los ciberataques, lo anterior, a través de la instrumentación de acciones legislativas que permitan prevenir y sancionar los actos perpetrados por la ciberdelincuencia.

Para ello, se propone la expedición de una Ley General de Ciberseguridad, y entre sus objetivos se encuentra el establecer los

tipos penales en la materia e integrar la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea, con el fin de garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, incluido el de banda ancha e internet en forma segura, en virtud de lo anterior, se derogan diversas disposiciones del Código Penal Federal toda vez que dichos tipos penales se incorporan a la nueva Ley General de Ciberseguridad.

También se establece dentro de la Ley General del Sistema Nacional de Seguridad Pública la creación de la Comisión Permanente de Ciberseguridad dentro de la estructura del Consejo Nacional de Seguridad Pública.

Esta comisión se coordinará con el Secretario Ejecutivo para dar seguimiento al cumplimiento de las disposiciones aplicables por parte de los Centros Nacionales que integran el Secretariado Ejecutivo. Sobre el funcionamiento, integrantes y deberes, el Consejo Nacional lo determinará.

Aunado a lo anterior, se crea el Centro Nacional de Ciberseguridad dentro de la estructura del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, para ello, conforme al artículo 17 de la Ley Genera del Sistema Nacional de Seguridad Pública, la persona titular

del Centro Nacional de Ciberseguridad será nombrada y removida libremente por el Consejo Nacional de Seguridad Pública.

En suma, la Ley General de Ciberseguridad que se propone, cuenta con 47 artículos divididos en IX Títulos.

El Titulo I es el relativo a las Disposiciones Generales, en dicho apartado se encuentra el glosario, así como los diferentes objetos de la ley.

El Titulo II es el concerniente a la Comisión Permanente de Ciberseguridad, así como su adscripción, su funcionamiento, y quienes podrán participar en ella.

El Titulo III contempla la Infraestructura de Información Crítica y lo relativo al Centro Nacional de Ciberseguridad, así como sus atribuciones, integración y funcionamiento.

El Titulo IV nos refiere la seguridad en las operaciones en la red, para ello, el Centro Nacional deberá definir como parte de la Estrategia Nacional de Ciberseguridad un sistema de protección multinivel de ciberseguridad.

El Titulo V nos reseña a las amenazas a la ciberseguridad y la seguridad de la información en la red

El Titulo VI nos habla de los proveedores de servicios de ciberseguridad, para tal efecto, el Centro Nacional deberá establecer los requerimientos necesarios para que las empresas proveedoras de ciberseguridad cuenten con los certificados requeridos para la provisión de dichos servicios, de acuerdo con los mejores estándares internacionales en la materia.

El Titulo VII de la Estrategia Nacional de Ciberseguridad que deberá ser desarrollada por el Centro Nacional.

El Titulo VIII lo relativo a los delitos y sus respectivas sanciones.

Y el Titulo IX de la Cooperación Internacional.

En conclusión, el marco normativo propuesto debe servir como base para iniciar la discusión en un tema que no se debe postergar en beneficio de las instituciones del Estado y de las personas que se sienten vulnerables ante los ciberataques.

Por tanto, se pone a su consideración la siguiente iniciativa:

CON PROYECTO DE DECRETO POR EL QUE SE MODIFICA LA DENOMINACIÓN DEL CAPÍTULO II, DEL TITULO NOVENO, DEL

LIBRO SEGUNDO Y SE REFORMA EL ARTÍCULO 211 BIS 1 Y SE DEROGAN DIVERSOS ARTÍCULOS DEL CÓDIGO PENAL FEDERAL; SE REFORMAN Y ADICIONAN DIVERSOS ARTÍCULOS DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA; SE ADICIONA UNA FRACCIÓN XIV AL ARTÍCULO 5° DE LA LEY DE SEGURIDAD NACIONAL; Y SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD.

PRIMERO.- Se modifica la denominación del Capítulo II del Titulo Noveno del Libro Segundo, se reforma el artículo 211 bis 1 y se derogan diversos artículos del Código Penal Federal para quedar como sigue:

DE LOS DELITOS COMETIDOS EN MATERIA DE CIBERSEGURIDAD

Artículo 211 bis 1.- **Los delitos cometidos en contra de los sistemas informáticos, sus personas usuarias o en materia de ciberseguridad, se sancionarán de conformidad con lo previsto en la legislación especial en la materia.**

Artículo 211 bis 2.- **Derogado.**

Artículo 211 bis 3.- **Derogado.**

Artículo 211 bis 4.- **Derogado.**

Artículo 211 bis 5.- **Derogado.**

Artículo 211 bis 6.- **Derogado.**

SEGUNDO.- Se reforman y adicionan diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública para quedar como sigue:

Artículo 16.- Son comisiones permanentes del Consejo Nacional, las siguientes:

I. ...

II. ...

III. ...

IV. De Ciberseguridad.

Artículo 17.- El Secretariado Ejecutivo es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y presupuestal. Contará con los Centros Nacionales de Información, de Prevención del Delito y Participación Ciudadana, de Certificación y Acreditación, **así como de Ciberseguridad**. El Titular del Ejecutivo Federal expedirá el Reglamento del Secretariado, que establecerá las atribuciones y articulación de estos Centros.

...

Artículo 22 Bis. El Centro Nacional de Ciberseguridad tendrá, entre otras, las siguientes atribuciones:

I. Monitorear, prevenir y manejar los riesgos, peligros y amenazas de ciberseguridad que surgen dentro y fuera del territorio nacional;

II. Proteger la infraestructura de información crítica contra ataques, intrusiones, interferencias, negaciones de servicio y destrucción;

III. La prevención de los delitos en contra de la infraestructura de información crítica.

IV. Elaborar y actualizar continuamente la Estrategia Nacional de Ciberseguridad;

V. Coordinarse con el Instituto Federal de Telecomunicaciones para determinar la política en la materia de Ciberseguridad.

VI. Contar con un registro de infraestructura de información crítica, así como con un atlas de la misma.

VII. Integrar y supervisar un padrón de empresas o personas que presten servicios de ciberseguridad.

TERCERO.- Se adiciona una fracción XIV al artículo 5° de la Ley de Seguridad Nacional para quedar como sigue:

Artículo 5.- …

I a la XIII. …

XIV. Actos tendentes a amenazar, afectar, inhabilitar o destruir la infraestructura activa o pasiva de telecomunicaciones que sean indispensable para la provisión de bienes o servicios públicos o para el adecuado funcionamiento de las instituciones del Estado.

CUARTO.- Se expide la Ley General de Ciberseguridad para quedar como sigue:

Ley General de Ciberseguridad

TITULO I

DISPOSICIONES GENERALES

Capítulo Único

Articulo 1.- La presente ley es reglamentaria del párrafo tercero del artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, de orden público, de interés social y de observancia general en todo el territorio nacional.

Artículo 2.- Para los efectos de la presente ley, se entenderá por:

I. Centro Nacional: El Centro Nacional de Ciberseguridad.

II. Ciberataque: Acción realizada a través de uno o varios sistemas informáticos con el objeto de amenazar, afectar, inhabilitar, destruir vulnerar, eliminar, negar o modificar la información contenida en un sistema de información, bases de datos y/o registro digital.

III. Ciberseguridad: Todas las actividades o acciones necesarias necesarias para la protección de las redes y sistemas de información, de las personas usuarias de tales sistemas y de otras personas afectadas por las amenazas a la seguridad;

IV. Ciberamenaza: Cualquier situación potencial, hecho o acción que pueda amenazar, dañar, eliminar, modificar, perturbar, negar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a las personas usuarias de tales sistemas y a otras personas que puedan resultar afectadas;

V. Ciberdefensa: Conjunto de acciones, recursos y mecanismos en materia de seguridad para prevenir, identificar, reaccionar y neutralizar las amenazas, ciberamenazas o ciberataques.

VI. Ciberespacio: Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas, empresas, todos los órdenes de gobierno, dispositivos electrónicos y sistemas informáticos.

VII. Comisión Permanente: La Comisión Permanente de Ciberseguridad.

VIII. Datos Personales: Los definidos como tal en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.

IX. Estrategia: La Estrategia Nacional de Ciberseguridad.

X. Infraestructura activa: La definida como tal en la Ley Federal de Telecomunicaciones y Radiodifusión en materia de telecomunicación;

XI. Infraestructura pasiva: La definida como tal en la Ley Federal de Telecomunicaciones y Radiodifusión en materia de telecomunicación;

XII. Infraestructura Informática Crítica: Infraestructura activa o pasiva que se encuentra total o parcialmente en territorio mexicano y cuyo daño o pérdida implica una afectación en el adecuado funcionamiento de las actividades de las autoridades del Estado o la provisión de servicios públicos.

XIII. Internet: La definida como tal en la Ley Federal de Telecomunicaciones y Radiodifusión;

XIV. Red de telecomunicaciones: La definida como tal en la Ley Federal de Telecomunicaciones y Radiodifusión;

XV. Registro Nacional de Infraestructuras Informáticas Críticas: Base de datos en la que obra la información referente a las Infraestructuras Criticas de Información de los diferentes sectores del país.

XVI. Operador de red: Operador que posee, tanto la adjudicación de espectro radioeléctrico, como la infraestructura necesaria para prestar cualquiera de los servicios de acceso a Internet;

XVII. Proveedor de servicios: Entidad pública o privada que ofrezca servicios de comunicación a través de un sistema informático o sistema de comunicaciones;

XVIII. Riesgo: La posibilidad de que una ciberamenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los sistemas informáticos, la información contenida en estos o las infraestructuras críticas;

XIX. Sistema Informático: todo dispositivo o conjunto de dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el procesamiento de datos digitales;

XX. Tecnologías de la Información y Comunicación (TIC): Son los equipos de cómputo, programas de computación, servicios y dispositivos de impresión que sean utilizados para almacenar, procesar, con convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

XXI. Vulnerabilidades: las características o defectos de un sistema informático que pueden ser utilizadas o explotadas por una o más ciberamenazas;

XXII. Administración de riesgos: proceso mediante el cual se identifican, mitigan, eliminan, aceptan o transfieren los riesgos de infraestructura informática crítica;

XXIII. Disponibilidad: atributo de datos o sistemas que denota la capacidad de que estos sean usados o accesibles;

XXIV. Integridad: atributo de datos o sistemas que garantiza la exactitud de estos, que no sean modificados a propósito por alguien no autorizado o de manera accidental; y,

XXV. Confidencialidad: atributo de datos o sistemas que controla el acceso a datos o sistemas, el cual busca garantizar que las personas adecuadas puedan accesar datos o sistemas.

Artículo 3.- La presente ley tiene por objeto:

I. Establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la ciberseguridad, en sus respectivos ámbitos de competencia;

II. Establecer los tipos penales en la materia e integrar la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea, con el fin de garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, incluido el de banda ancha e internet en forma segura;

III. Establecer la obligación del Estado de tomar medidas para monitorear, prevenir y manejar los riesgos, peligros y amenazas de ciberseguridad que surgen dentro y fuera del territorio nacional, así como de proteger la infraestructura de información crítica contra ataques, intrusiones, interferencias, negaciones de servicio y destrucción;

IV. Establecer la garantía para la investigación y desarrollo de productos y servicios de red que conduzcan a la educación saludable de menores de edad, así como sancionar el uso de redes para participar en actividades que pongan en peligro su bienestar psicológico, moral y físico, para ello, el Estado deberá proporcionar un entorno de red seguro y saludable para los menores de edad.

V. Mejorar continuamente la Estrategia Nacional de Ciberseguridad, definiendo los requisitos fundamentales y los objetivos principales para garantizar la seguridad cibernética;

VI. Presentar políticas y procedimientos de ciberseguridad para sectores estratégicos;

VII. Sancionar las actividades en el ciberespacio ilegales y criminales de conformidad con la Ley, preservando la seguridad y el orden del ciberespacio; y,

VIII. Fomentar la educación de ciberseguridad en la población a través de la Federación, las entidades federativas, los municipios y las alcaldías de la Ciudad de México.

TITULO II
DE LA COMISIÓN PERMANENTE DE CIBERSEGURIDAD

Artículo 4.- El Consejo Nacional de Seguridad Pública contará con una Comisión Permanente de Ciberseguridad, y su funcionamiento se sujetará a lo previsto en la presente ley, en la Ley General del Sistema Nacional de Seguridad Pública y en su reglamento.

Artículo 5.- Dicha Comisión se coordinará con el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública para dar seguimiento al cumplimiento de las disposiciones aplicables por parte del Centro Nacional de Ciberseguridad.

Artículo 6.- En la Comisión podrán participar expertos de instituciones académicas, de investigación y agrupaciones del sector social y privado relacionados con su objeto.

TITULO III
DE LA INFRAESTRUCTURA DE INFORMACIÓN CRÍTICA Y DEL CENTRO NACIONAL DE CIBERSEGURIDAD

Artículo 7.- El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública contará con un Centro Nacional de Ciberseguridad,

sus atribuciones, integración y funcionamiento se sujetará a lo previsto en la Ley General del Sistema Nacional de Seguridad Pública y en su reglamento.

Artículo 8.- El Centro Nacional se coordinará con el Instituto Federal de Telecomunicaciones, para determinar la política en la materia de Ciberseguridad.

Artículo 9.- El Centro Nacional deberá designar aquella infraestructura activa o pasiva, así como los sistemas informáticos que serán considerados infraestructura de información crítica.

Artículo 10.- El Centro Nacional contará con un registro de infraestructura de información crítica, así como con un atlas de esta, los cuales deberán ser revisados y actualizados, cuándo menos, anualmente.

Artículo 11.- El Centro Nacional será el encargado de la prevención de los delitos en contra de la infraestructura de información crítica.

Artículo 12.- El Centro Nacional deberá expedir los lineamientos de ciberseguridad y administración de riesgos que tendrán que seguir aquellas personas físicas o morales, públicas o privadas que tengan en su poder infraestructura de información crítica.

Además, deberá llevar a cabo las visitas de revisión y verificación correspondientes a las autoridades para asegurar el cumplimiento de los lineamientos referidos en el párrafo anterior.

Artículo 13.- El Centro Nacional deberá expedir los requisitos mínimos y prácticas que deberán seguir las autoridades de los tres órdenes de gobierno en materia de ciberseguridad.

Artículo 14: El Centro Nacional implementara la protección estratégica sobre la base del sistema de protección multinivel de ciberseguridad para los servicios públicos de comunicación e información, energía, tráfico, recursos hídricos, finanzas, servicios públicos, gobierno electrónico y otra infraestructura de información crítica que, si es destruido, o sufre pérdida alguna de una función operativa o una fuga de datos, ponga en peligro la seguridad nacional.

La Comisión definirá el alcance específico y las medidas de protección de seguridad para la infraestructura de información crítica.

Artículo 15.- El Centro Nacional implementará un sistema de monitoreo de ciberseguridad, alerta temprana y comunicación de información. Las entidades de seguridad apoyarán en la recopilación, análisis e informes de ciberseguridad, y seguirán las regulaciones para la consolidación de la información de monitoreo y alerta temprana de ciberseguridad.

Artículo 16.- Las dependencias y organismos con infraestructura de información crítica que cuenten con responsables de ciberseguridad, o seguridad informática, se coordinarán con la Comisión para establecer y completar mecanismos de evaluación de riesgos de ciberseguridad y esfuerzos de respuesta a emergencias, formular planes de respuesta a emergencias de incidentes de ciberseguridad para sus respectivas industrias o sectores y organizar periódicamente simulacros.

Los planes de respuesta a emergencias de incidentes de ciberseguridad clasificarán los incidentes de ciberseguridad en función de factores como el grado de daño después de que ocurra el incidente y el alcance del impacto, y proporcionarán las medidas de manejo de respuesta de emergencia correspondientes.

TITULO IV

DE LA SEGURIDAD DE LAS OPERACIONES EN LA RED

Artículo 17.- El Centro Nacional deberá definir como parte de la Estrategia Nacional de Ciberseguridad un sistema de protección multinivel de ciberseguridad.

Artículo 18.- La construcción y operación de redes, o la provisión de servicios a través de redes, se realizará de acuerdo a los requisitos

obligatorios de las normas jurídicas nacionales así como de los tratados internacionales de los que el Estado Mexicano sea parte, adoptando las medidas necesarias para salvaguardar la ciberseguridad y la estabilidad operativa, responder eficazmente a incidentes de ciberseguridad, la prevención de delitos cibernéticos y actividades ilegales, así como preservar la integridad, el secreto y la usabilidad de los datos.

Artículo 19.- Los operadores de red que lleven a cabo actividades comerciales y de servicios deben cumplir con las leyes y regulaciones administrativas, así como con las obligaciones de proteger la ciberseguridad, aceptar la supervisión del Gobierno Federal en los términos de la ley, y asumir la responsabilidad social.

Artículo 20.- Los operadores de red deberán garantizar que la red esté libre de interferencias, daños o acceso no autorizado, para evitar fugas de datos, robos o falsificaciones; los operadores de red deberán desarrollar al menos las siguientes acciones:

I. Adoptar medidas técnicas para prevenir virus informáticos, ataques cibernéticos, intrusiones en la red y otras acciones que pongan en peligro la seguridad nacional;

II. Establecer sistemas de gestión de seguridad y normas internas de funcionamiento, determinar a las personas que son responsables de la ciberseguridad;

III. Adoptar medidas técnicas para monitorear y registrar los estados operativos de la red y los incidentes de seguridad, y seguir las disposiciones para almacenar registros de la red durante al menos un año; y,

IV. Adoptar medidas tales como clasificación de datos, copia de seguridad de datos importantes y cifrado.

Artículo 21.- Los proveedores de productos o servicios de red no deberán instalar programas maliciosos, al detectar que sus productos y servicios presentan fallas o vulnerabilidades de seguridad, deberán adoptar de inmediato medidas correctivas e informar a las personas usuarias.

Artículo 22.- El equipo de red crítico y los productos especializados de ciberseguridad deberán cumplir con las normas y requisitos obligatorios, contar con la certificación de seguridad de un proveedor autorizado, antes de ser vendidos o suministrados.

El Centro Nacional formulará y expedirá un catálogo de equipos de red críticos y productos especializados de ciberseguridad, y promoverá el reconocimiento recíproco de las certificaciones de seguridad y los

resultados de las inspecciones de seguridad para evitar duplicaciones de certificaciones e inspecciones.

Artículo 23.- Los operadores que proveen el acceso a la red de los servicios de registro de nombres de dominio para las personas usuarias, que manejan el acceso a la red de telefonía fija o móvil, o que brindan servicios de publicación de información o mensajería instantánea, requerirán que las personas usuarias proporcionen información de identidad real al firmar acuerdos o confirmar la prestación de servicios. Cuando las personas usuarias no proporcionen información de identidad real, los operadores de red no deberán proporcionar los servicios.

Artículo 24.- Los operadores de red formularán al Centro Nacional planes de respuesta de emergencia para incidentes de seguridad y atenderán las vulnerabilidades del sistema, virus informáticos, ataques cibernéticos, intrusiones en la red y otros riesgos de ciberseguridad.

Cuando se produzcan incidentes de ciberseguridad, los operadores de red deberán iniciar de inmediato un plan de respuesta de emergencia, y adoptar las medidas correctivas correspondientes e informar inmediatamente a la Comisión.

TITULO V
DE LAS AMENAZAS A LA CIBERSEGURIDAD Y LA SEGURIDAD DE LA INFORMACIÓN EN LA RED

Artículo 25.- El Centro Nacional deberá publicar e informar al Secretario Ejecutivo del Sistema Nacional de Seguridad Pública de manera continua un reporte de amenazas a la ciberseguridad para la población en general y generar un informe anual sobre el estado que guarda la ciberseguridad, con el fin de que las personas conozcan los mayores riesgos a los que están expuestos por el uso de sistemas de telecomunicación, información y comunicación.

Artículo 26.- El Centro Nacional deberá informar a las autoridades de las ciberamenazas que enfrentan en el desempeño de sus funciones, así como establecer los lineamientos de capacitación de las y los servidores públicos en la materia.

Artículo 27.- Los operadores de red deberán de implementar sistemas de protección para garantizar la confidencialidad de la información de las personas usuarias.

Artículo 28.- Los operadores de red adoptarán las acciones necesarias para garantizar al máximo la seguridad de la información personal que

recopilan y para evitar que la información personal se divulgue, destruya o se pierda.

Artículo 29.- Todas las personas y empresas serán responsables del uso de sus sitios web y por ningún motivo deberán establecer sitios de internet o grupos de comunicación para realizar actividades ilícitas, difundir o perpetrar fraudes, impartir métodos criminales, elaborar o comercializar artículos prohibidos o controlados, u otras actividades ilegales.

Artículo 30.- Los operadores de red gestionarán la información publicada por las personas usuarias y, al descubrir que está prohibida la publicación o transmisión, deberán detener inmediatamente la transmisión de esa información, evitar la difusión de la información, guardar registros e informar de forma inmediata a las autoridades competentes.

TITULO VI
DE LOS PROVEEDORES DE SERVICIOS DE CIBERSEGURIDAD

Artículo 31.- El Centro Nacional deberá establecer los requerimientos necesarios para que las empresas proveedoras de ciberseguridad cuenten con los certificados requeridos para la provisión de dichos

servicios, de acuerdo con los mejores estándares internacionales en la materia.

Artículo 32.- El Centro Nacional podrá celebrar convenios con terceros con el objeto de expedir los certificados para la prestación de servicios de ciberseguridad.

Artículo 33.- Quienes lleven a cabo la certificación de ciberseguridad, pruebas, evaluación de riesgos u otras actividades relacionadas, o publiquen información de ciberseguridad, como vulnerabilidades del sistema, virus informáticos, ataques a la red o incursiones en la red, deberán cumplir con los lineamientos que para tal efecto emita la Comisión.

Artículo 34.- El Centro Nacional deberá integrar un padrón de empresas o personas que presten servicios de ciberseguridad, para ello emitirá los lineamientos para el registro respectivo.

TITULO VII
DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Artículo 35.- El Centro Nacional contará con una Estrategia Nacional de Ciberseguridad que será actualizada al menos cada dos años.

Artículo 36. La Estrategia es el instrumento mediante el cual se llevará a cabo la coordinación de las autoridades federales, estatales y locales en materia de ciberseguridad.

Artículo 37.- La Estrategia establecerá los lineamientos mínimos para el manejo de riesgos, vulnerabilidades y ciberamenazas a las que estén sujetas la infraestructura informática crítica y los sistemas informáticos; así como los planes de prevención y de los delitos que se establecen en la presente ley.

Artículo 38. La Estrategia deberá prever el fomento de la cultura de ciberseguridad en la población a través de la Federación, las entidades federativas, los municipios y las alcaldías de la Ciudad de México.

TITULO VIII
DE LOS DELITOS
Capítulo I
Delitos contra la Infraestructura Informática Crítica

Artículo 39.- Al que realice actos tendientes a acceder de manera ilegítima, vulnerar, inhabilitar, robar, intervenir, destruir o afectar la infraestructura informática crítica se le impondrán de 10 a 15 años de prisión y una multa que va desde las 1000 a 3000 veces la unidad de medida y actualización vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta se encuentre a cargo, controle u opere la infraestructura objeto de esta conducta, se le aumentará la pena hasta en una mitad.

Cuando la persona que realice la conducta del párrafo anterior sea una servidora o servidor público, se le aumentará la pena hasta en una tercera parte, lo anterior, sin perjuicio de aquellas responsabilidades que incurra en el marco legal aplicable en materia de responsabilidad de las y los servidores públicos.

Artículo 40.- Al que contribuya en la preparación o realización de los actos contenidos en el artículo anterior, se le impondrán de 4 a 9 años de prisión y una multa de 900 a 2800 veces la Unidad de Medida y Actualización vigente al momento de la realización de la conducta.

Cuando la persona que realice la conducta se encuentre a cargo, controle u opere la infraestructura objeto de esta conducta, se le aumentará la pena hasta en una mitad.

Cuando la persona que realice la conducta del párrafo anterior sea una servidora o servidor público, se le aumentará la pena en una mitad, lo anterior sin perjuicio de aquellas responsabilidades que incurra en el marco legal aplicable en materia de responsabilidad de las y los servidores públicos.

Artículo 41.- A quien sin autorización legitima copie, modifique, limite el acceso, corrompa o destruya información en sistemas informáticos, considerados infraestructura informática crítica se le impondrán de 10 a 12 años de prisión y una multa de 800 a 2500 veces la unidad de medida y actualización vigente al momento de la realización de la conducta

Cuando la persona que realice la conducta del párrafo anterior sea una servidora o servidor público, se le aumentará la pena en una mitad, lo anterior sin perjuicio de aquellas responsabilidades que incurra en el marco legal aplicable en materia de responsabilidades de las y los servidores públicos.

Capítulo II
Delitos en contra de los Sistemas Informáticos

Artículo 42.- Al que por si o por interpósita persona, sin autorización del dueño, operador o controlador de un sistema informático acceda a la información contenida en el mismo se le impondrán de 2 a 6 años de prisión y multa que va de las 200 a 800 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Artículo 43.- Al que por si o por interpósita persona, sin autorización del titular, acceda a una cuenta de servicios proveídos total o parcialmente a través de internet, se le impondrán de 1 a 2 años de prisión y multa

que va de las 200 a 800 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Artículo 44.- A quien, sin autorización del dueño, operador o controlador de un sistema informático, obtenga datos o información referente al tráfico de datos, actividad en internet o mensajes digitales del dueño del equipo o de algún otro usuario autorizado por este a utilizarlo, se le impondrán de 2 a 6 años de prisión y una multa de 400 a 1000 veces la unidad de medida y actualización.

Cuando los datos o información de actividad sean referentes a datos personales o a contenido íntimo, las penas aumentarán hasta en una mitad.

Artículo 45.- A quien, sin autorización del dueño, operador o controlador de un sistema informático, copie, corrompa, limite el acceso, modifique o destruya información reservada o que ponga en riesgo el adecuado funcionamiento de las instituciones del Estado, la integridad de instalaciones estratégicas o física de las personas se le impondrán de 10 a 20 años de prisión y multa que va de las 1000 a 3000 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Artículo 46.- A quién lleve a cabo programas informáticos, aplicativos o

cualquier otro conjunto de datos que tenga cómo función el acceder a los datos de un sistema informático sin la autorización del dueño, operador o controlador del sistema, se le impondrán de 8 a 15 años de prisión y multa de 1000 a 1500 unidades de medida y actualización.

Cuando la persona que lleve a cabo la conducta prevista en el párrafo anterior tenga como actividad directa o indirecta la provisión de servicios de ciberseguridad, las penas aumentarán hasta en una mitad.

Artículo 47.- A quien acceda de manera autorizada a un sistema informático, pero que de manera no autorizada copie, modifique, **limite el acceso**, corrompa o destruya datos o información contenida en dicho sistema o **realice chantaje para permitir el acceso a dicho dato o sistema**, se le impondrán de 5 a 7 años de prisión y multa que va de las 200 a 800 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Cuando la información o datos del párrafo anterior se refieran a información o datos contenida en la infraestructura informática crítica, las penas aumentarán hasta en dos terceras partes.

Capítulo III
Delitos contra las personas usuarias

Artículo 48.- Al que acceda de manera ilegítima a uno o más sistemas informáticos, de manera física o a través de otro u otros sistemas informáticos, para copiar información considerada datos personales, se le impondrán de 4 a 6 años de prisión y multa que va de las 200 a 600 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta

Artículo 49.- Al que, a través de información personal en formato digital, suplante la identidad de una persona para realizar actos con consecuencias jurídicas de cualquier índole, se le impondrán de 6 a 8 años de prisión y multa que va de las 200 a 800 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Artículo 50.- A quien cree, opere, controle o administre sitios de internet que simulen ser sitios oficiales del estado o de empresas que soliciten y guarden información de la persona usuaria, se le impondrán de 6 a 8 años de prisión y multa que va de las 300 a 800 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Las penas previstas en este artículo aumentarán hasta en una mitad cuándo la información solicitada sean datos personales o información bancaria

Artículo 51.- A quien intencionalmente y sin la debida autorización por cualquier medio cree, capture, grabe, copie, altere, duplique, clone o elimine datos informáticos contenidos en una tarjeta inteligente o en cualquier instrumento con fines de participación en el sistema financiero; con el objeto de incorporar, modificar la información de personas usuarias, transacciones, simular transacciones o eliminarlas, se le impondrán de 7 a 10 años de prisión y multa que va de las 1500 a 2500 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Artículo 52.- A quien utilice el ciberespacio para publicar, almacenar y compartir contenidos que sean constitutivos de delitos, se le impondrán de 5 a 10 años de prisión sin perjuicio de las penas que les sean impuestas por la comisión de los delitos y multa que va de las 1000 a 2000 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

En aquellos casos en los que la información a la que se refiere el párrafo anterior sea constitutiva de delitos de pornografía o explotación de niñas, niños y adolescentes, las penas aumentarán hasta en dos terceras partes.

Capítulo IV
Delitos contra la Ciberseguridad

Artículo 53.- A quien lleve a cabo modificaciones no autorizadas en los sistemas informáticos que tengan como consecuencia la generación de una vulnerabilidad se le impondrán de 8 a 12 años de prisión y multa que va de las 800 a 2000 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Cuando la conducta anterior sea realizada por una persona que tenga como actividad directa o indirecta la provisión de servicios de ciberseguridad, las penas aumentarán hasta en una mitad.

Cuándo las conductas previstas en este artículo sean realizadas en sistemas informáticos considerados infraestructura informática crítica, las penas aumentarán hasta en dos terceras partes.

Artículo 54.- A quien distribuya a través del ciberespacio programas, códigos u otro tipo de información con el fin de generar o aprovechar vulnerabilidades en los sistemas informáticos, se le impondrán de 7 a 10 años de prisión y multa que va de las 800 a 1500 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Artículo 55.- A quien utilice sistemas informáticos de manera parcial o total, con autorización o sin ella, para buscar, generar y aprovechar vulnerabilidades en los sistemas informáticos sin autorización del

dueño, administrador, controlador u operador, se le impondrán de 6 a 11 años de prisión y multa que va de las 400 a 800 veces la unidad de medida y actualización vigente al momento de la realización de la conducta.

Artículo 56.- A quien afecte la disponibilidad, la integridad y la confidencialidad de los datos o sistemas de infraestructura informática crítica o que con ánimo de conseguir un lucro o provecho, amenazare al Estado con daños físicos o patrimoniales a datos, sistemas o infraestructura informática crítica, ya sea por vía telefónica, comunicación electrónica o cualquier medio físico o electrónico, se le impondrán de 10 a 20 años de prisión y multa que va de las 1000 a 3000 veces la unidad de medida y actualización vigente al momento de la realización de la conducta.

TITULO IX
DE LA COOPERACIÓN INTERNACIONAL

Articulo 57.- El Estado Mexicano podrá celebrar tratados o acuerdos interinstitucionales en el ámbito internacional en materia de ciberseguridad con uno o varios sujetos de derecho internacional público.

En materia de prevención, el Centro Nacional podrá intercambiar

información con dependencias internacionales cuando se detecten amenazas a la ciberseguridad que surjan dentro o fuera del territorio nacional.

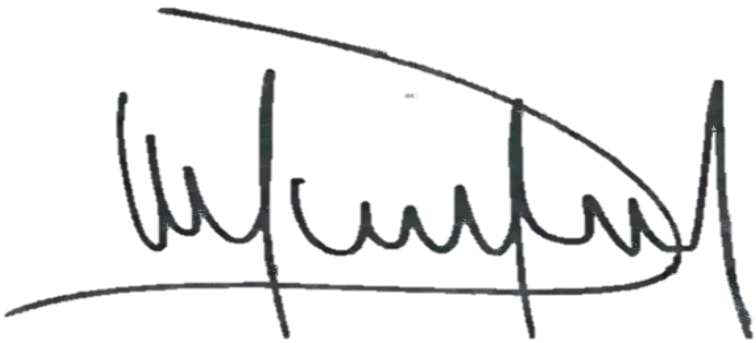
TRANSITORIOS

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

Segundo. La Persona Titular del Centro Nacional de Ciberseguridad será designada por el Presidente del Consejo Nacional de Seguridad Pública en un plazo no mayor a 180 días naturales contados a partir de la entrada en vigor del presente Decreto.

Tercero. El Centro Nacional de Ciberseguridad contará con un plano no mayor a seis meses a partir del nombramiento de la persona titular del Centro Nacional para expedir la Estrategia Nacional de Ciberseguridad e integrar el Registro de Infraestructura Informática Crítica, así como los lineamientos de ciberseguridad que tendrán que seguir aquellas personas físicas o morales, públicas o privadas que tengan en su poder infraestructura informática crítica.

Cuarto. Para el adecuado cumplimiento de sus funciones, el Centro Nacional de Ciberseguridad, contará con los recursos humanos, materiales y financieros suficientes de acuerdo con las normas presupuestales aplicables.



SEN. MIGUEL ÁNGEL MANCERA ESPINOSA