CÁMARA DE DIPUTADOS
LXV LEGISLATURA

Gaceta Parlamentaria

Año XXVII | Palacio Legislativo de San Lázaro, miércoles 20 de marzo de 2024 | Número 6488-II-4-1

CONTENIDO

Anexo II-4-1

Miércoles 20 de marzo

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD

Quien suscribe, **Diputado Javier Joaquín López Casarín**, integrante del Grupo Parlamentario del Partido Verde Ecologista de México, de la LXV Legislatura del honorable Congreso de la Unión, con fundamento en lo dispuesto por los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, así como 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a la consideración de esta asamblea la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD**, al tenor de la siguiente:

Exposición de Motivos

En los últimos años, el uso de las tecnologías de información y telecomunicaciones (TIC), se han desarrollado de manera acelerada.

Hoy en día, los sectores productivos de los países, los servicios en los ámbitos social, político, económico, cultural y de seguridad, se llevan a cabo por medio de infraestructuras tecnológicas que almacenan, procesan y transmiten información.

En esta era digital, el uso de las tecnologías ha transformado la forma en que las personas interactúan, en el trabajo, estudio, en su vida familiar y en cómo se comunican con su entorno, el cual, por medio del internet no se reduce al físico inmediato sino al ciberespacio que por tanto genera acceso a una conexión global.

A nivel mundial, este ciberespacio, se ha constituido, por tanto, en un entorno virtual de desarrollo, integrado por redes de computadoras y telecomunicaciones, tecnologías de operación (TO) usadas en la industria, pero también, por cualquier dispositivo por pequeño que sea, capaz de almacenar, procesar o transmitir información, incluidos los dispositivos de Internet de las Cosas (Internet of Things o IoT) que son dispositivos de uso común y de la vida diaria como bocinas, cámaras, puertas, refrigeradores, automóviles, etc, con capacidades de comunicarse y conectarse con redes de computadoras, principalmente Internet.

Cada vez más, los servicios vitales para la sociedad están siendo dependientes de las infraestructuras tecnológicas, a tal grado, que fallas en

ellas, pueden causar enormes daños humanos y financieros, e inclusive riesgos a la seguridad nacional.

De acuerdo a la Unión Internacional de Telecomunicaciones (UIT), se estima que, en el 2021, cerca de 4.9 billones de personas en todo el mundo tienen acceso a internet, lo que representa aproximadamente el 60% de la población mundial.

La Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) realizada por el INEGI, estimó que en México en 2021 había 88.6 millones de personas usuarias de internet, lo que representa el 75.6 % de la población de seis años o más, siendo esta cifra 4.1 puntos porcentuales mayor respecto a la de 2020. (71.5 %)[1]

En el resguardo e intercambio de datos e información en la red, a través de los distintos protocolos utilizados, existen riesgos de intrusión, robo, suplantación, manipulación, entre otros; para proteger a los sistemas informáticos de cualquiera de estos ataques, se aplican un conjunto de procesos, prácticas y tecnologías diseñadas para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información, a estas medidas se le denomina ciberseguridad.

La ciberseguridad implica el uso de herramientas de seguridad informática, como firewalls, software antivirus, autenticación, cifrado de datos, con el fin de resguardar, prevenir, detectar y responder a amenazas cibernéticas.

La implementación de políticas y procedimientos de seguridad cibernética, la capacitación de los usuarios sobre buenas prácticas de seguridad en línea y la realización de evaluaciones y pruebas de seguridad para identificar y mitigar vulnerabilidades son elementos imprescindibles en un entorno adecuado de ciberseguridad, lo anterior derivado de la creciente cantidad de información que se maneja en línea, incluyendo información confidencial de empresas, de los propios usuarios, y de las entidades de gobierno, pudiendo algunas de ellas en caso de ser afectadas representar riesgos de seguridad nacional.

Para la UIT, la Ciberseguridad es "El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y

[1] https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/OtrTemEcon/ENDUTIH_21.pdf

tecnologías que pueden utilizarse para proteger los activos de la organización y usuarios en el ciberentorno".[2]

Para el Estado mexicano, la importancia de la seguridad informática, radica en que, a través del llamado ciberespacio, fluye la información prácticamente de forma instantánea, lo que conlleva grandes beneficios, pero al mismo tiempo se convierte en un reto, si no se consideran los riesgos de seguridad que implican los medios digitales.

El uso natural de dispositivos electrónicos para la vida diaria como lo son teléfonos, tabletas, relojes y bocinas inteligentes, sólo por mencionar algunos, hace que perdamos de vista que todo el tiempo se genera y recopila información a través de ellos.

Es importante considerar que muchos datos tales como información personal, financiera, de salud, y del trabajo que viven en los dispositivos electrónicos pueden vulnerar al dueño de la información, en caso de que las condiciones de seguridad no sean las adecuadas.

En este sentido la ciberseguridad se ha convertido en una prioridad para los gobiernos y sociedades de todo el mundo; la cual radica en integrar los diferentes esfuerzos legislativos, técnicos y humanos a fin de mitigar posibles riesgos y amenazas que están presentes en la red.

Actualmente, el objetivo principal de muchos grupos de hackers y otros antagonistas son las infraestructuras críticas y los servicios esenciales a la población.

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

La Ciberseguridad es la piedra angular para evitar ataques en contra de la confidencialidad, integridad y disponibilidad de la información al permitir

[2] Unión Internacional de Telecomunicaciones (UIT). https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

dotar a los equipos técnicos y humanos de las capacidades y legislación necesaria para combatir eficazmente los riesgos cibernéticos.

Por lo que debe existir un marco legislativo robusto en la materia que apoye y dé certidumbre a todas las entidades que participan en las tareas asignadas, es por esto y ante las condiciones actuales, que es importante materializar los esfuerzos encaminados hacia el fortalecimiento de la ciberseguridad en México.

La pandemia COVID-19 acrecentó la dependencia de los sistemas digitales, acelerando el trabajo remoto y con ello la adopción de plataformas y dispositivos que permiten que los datos confidenciales sean compartidos por terceros, mediante intermediarios relacionados con tecnología como servicios en la nube, aplicaciones, interfaces de programación (API), entre otras.

Un problema importante que tiene México, para organizar y establecer la ciberseguridad en el país y para combatir y sancionar las actividades irregulares o lesivas en el internet consiste en establecer una adecuada definición de los delitos cometidos mediante el uso de las tecnologías de la información, también llamados ciberdelitos ya que no hay una legislación específica.

Adicionalmente, la definición de delitos cibernéticos no guarda homogeneidad con los conceptos establecidos en otros países, lo que dificulta también que el país se integre a iniciativas legales internacionales, lo que permitiría sancionar a los cibercriminales independientemente de la nación en la que se encuentren. Como señala el Wilson Center's Mexico Institute, "si las leyes no se crean y fortalecen México puede ser un objetivo vulnerable para las amenazas de los agentes criminales". [3]

Entre las necesidades que se buscan cubrir a través del proyecto de Ley Federal de Ciberseguridad, se encuentra la definición de un modelo de operación de la Ciberseguridad en México, el cual abarca un amplio espectro de temáticas por resolver que van desde la seguridad individual de las personas, hasta la seguridad y defensa nacional del Estado, por lo que es necesario delimitar atribuciones, competencias y responsabilidades

[3] Parragez Kobek, L. (2017). The State of Cybersecurity in Mexico: An Overview. México: Wilson Center's Mexico Institute.

que permitan a cada uno de los actores involucrados tener una visión clara de los objetivos que tienen que cumplir para fortalecerla.

En ese sentido, se requiere de un organismo que coordine los diferentes esfuerzos a nivel nacional y que se encargue de generar estrategias y políticas públicas a seguir. Para tal efecto se considera pertinente crear una Agencia Nacional de Ciberseguridad.

Es necesario establecer convenios de colaboración que permitan al Estado mexicano, afrontar los delitos cibernéticos en todo el territorio nacional, buscando la homologación de estructuras, de criterios y de preparación de los impartidores de justicia.

Se requiere establecer las bases de colaboración del gobierno con la iniciativa privada a través de las diferentes cámaras industriales, empresas y la población, para combatir delitos cibernéticos en especial aquellos que puedan poner en riesgo el suministro de servicios básicos a la población y protección de infraestructuras críticas de información.

Actualmente no existe la obligación de reportar o denunciar incidentes que permita determinar de forma precisa el estado que guarda la ciberseguridad en nuestro país por lo que es necesario contar con datos y estadísticas oficiales sobre incidentes y ciberdelitos ocurridos en México.

En la mayoría de los casos los organismos y personas que sufren incidentes omiten reportar este tipo de información ya sea por miedo a que afecte su reputación o prestigio, desconocimiento de los medios o simplemente consideran que, aunque lo reporten no será resuelto.

Es indispensable determinar un organismo encargado de concentrar la información sobre incidentes, ciberataques y delitos cibernéticos suscitados en organizaciones públicas y privadas, con lo cual se podrá constituir un parámetro para determinar el nivel de ciberseguridad del país y con ello tener un indicador para mejorarla día con día.

Para atender delitos cibernéticos trasnacionales o supranacionales que afecten al país u otros países de la comunidad internacional, es importante que México se adhiera a tratados internacionales, que posibiliten el castigo de los responsables.

Se requiere una regulación que obligue a los proveedores de servicios de comunicaciones y contenido de Internet, para que, con pleno respeto a los

derechos humanos, brinden información relacionada con la investigación de delitos cibernéticos.

En ese mismo sentido, es necesario que las empresas extranjeras que brinden servicios en México, cuenten con representación jurídica en nuestro país, quien deberá servir como punto de contacto y colaborar con las autoridades mexicanas, siempre que exista un ordenamiento legal de por medio.

Diferentes organizaciones civiles y periodistas, han manifestado que han visto afectada su esfera jurídica por intervenciones a sus comunicaciones, asimismo cada vez es más posible acceder a equipos y tecnología que tenga este tipo de capacidades tanto por grupos de delincuencia organizada como por actores que no tienen la facultad legal para utilizarla.

En ese sentido, es necesario regular la venta de tecnología para intervención de comunicaciones para dar certeza jurídica a los ciudadanos mexicanos; sin vulnerar las capacidades y facultades de las dependencias que tiene la posibilidad legal de utilizarlos, con pleno apego a los derechos humanos.

Si bien existen diferentes instrumentos jurídicos a nivel federal y local que regulan algunas conductas relacionadas con delitos informáticos; estos se encuentran desagregados y no son homogéneos.

Lo anterior, dificulta la procuración de justicia quedando impunes la mayor parte de las conductas ilícitas cometidas a través del ciberespacio; lo cual se agrava por la falta de profesionalización por parte de jueces, ministerios públicos y ausencia de una cultura de ciberseguridad entre la ciudadanía que desconoce los mecanismos legales existentes.

Bajo este contexto resulta indispensable emitir una Ley Federal de Ciberseguridad, para lograr un entendimiento común entre todos los sectores interesados, impulsar la profesionalización del poder judicial, establecer a una Agencia de Ciberseguridad que sea el responsable en la materia, así como constituir la bases para la generación de estrategias, y políticas públicas desarrolladas con la participación de los tres órdenes de gobierno, sector privado y sociedad en general.

Durante el primer semestre de 2022, México sufrió 85 mil millones de intentos de ciberataques, lo que representó un incremento del 40%, con relación al mismo periodo en 2021; con lo cual se considera que fue el país más atacado en América Latina, seguido por Brasil con 31.5 mil millones de ciberataques durante el mismo periodo de tiempo y Colombia en tercer lugar con 6.3 mil millones.[4]

De acuerdo con el informe de la Junta Internacional de Fiscalización de estupefacientes 2021, perteneciente a la ONU, el uso de criptomonedas y el ciberespacio es cada vez más frecuente entre las organizaciones criminales en México, que se disputan el control de los enormes mercados delictivos de drogas, armas, sexo y personas, "lavan" aproximadamente 25,000 millones de dólares al año, utilizando monedas electrónicas y el ciberespacio para su compunción y ejecución de actividades ligadas con estos ilícitos.[5]

De acuerdo al Informe "El Estado del Ransomware 2022" de Sophos, 74% de las empresas mexicanas fueron víctimas de este tipo de ataque, quienes realizaron un pago promedio de $482,446 dólares para restaurar el acceso a sus datos.[6]

La CONDUSEF registró un total de 24,215 fraudes bancarios y 76,000 denuncias por presuntos fraudes en 2021; en lo que va de la pandemia se totalizan 252,170 denuncias.[7]

Conforme al Censo Nacional de Seguridad Pública Federal 2021 (INEGI)[8], la Guardia Nacional atendió los siguientes incidentes:

1. Tentativa de extorsión telefónica (48,099);
2. Delitos en Internet (4,996);
3. Investigaciones cibernéticas (1,104);
4. Sitios web desactivados (5,920);

[4] https://www.idc.com/getdoc.jsp?containerId=prLA49766122

[5] https://www.incb.org/documents/Publications/AnnualReports/AR2021/Annual_Report/E_INCB_2021_1_spa.pdf

[6] https://assets.sophos.com/X24WTUEQ/at/npk6g4rwkmqc4s5j7hcrvfpn/sophos-state-of-ransomware-2022-wpes.pd

[7] https://www.condusef.gob.mx/documentos/comercio/FraudesCiber-1erTrim2021.pdf

[8] https://www.inegi.org.mx/contenidos/programas/cnspf/2021/doc/cnspf_2021_resultados.pdf

5. Reportes de Incidentes electrónicos (21,290)

6. Incidentes de seguridad informática (133,469).

Por otra parte, los problemas asociados a la falta de ciberseguridad ocupan el 8º riesgo a nivel mundial de acuerdo al Reporte de Riesgos Global 2023 del Foro Económico Mundial.[9]

Las principales afectaciones por grupos de Amenazas Persistentes Avanzadas (APT) en México en los últimos años han sido por orden cronológico:

1. Ataque al sistema de interconexión de bancos comerciales al sistema financiero de pagos electrónicos interbancarios (SPEI) en donde hubo un robo de 300 millones de pesos. (mayo 2018)

2. Petróleos Mexicanos fue víctima de ransomware (Doppel Paymer) afectando al 5% de sus computadoras y vulnerando 60 áreas. (noviembre 2019)

3. La Secretaría de Economía sufrió un ataque cibernético en algunos servidores, sin embargo, la información sensible de sus usuarios no se vio comprometida. (febrero 2020)

4. La Secretaría del Trabajo y Previsión Social informó que parte de su infraestructura de cómputo fue afectada lo que provocó que algunos servidores dejaran de operar correctamente. (marzo 2020)

5. El Instituto Nacional de Migración sufrió un ciberataque sin que la secrecía de la información relacionada con trámites migratorios fuera vulnerada. (abril 2020)

6. Ciberataque a la Comisión Nacional para la Protección y Defensa de los Usuario de Servicios Financieros por parte del grupo Anonymous. (julio 2020)

7. El Banco de México fue objeto de un intento de ataque cibernético, lo cual provocó fallas e intermitencias en sus sistemas. (julio 2020)

8. Hackeo a la Lotería Nacional por el grupo ruso Avaddon. (junio 2021)

---

[9] https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf?_gl=1*i5iw4z*_up*MQ..&gclid=EAIaIQobChMIoPW3 hs-W_gIVuQznCh1_qA7GEAAYASAAEgJJifD_BwE

9. Afectación de 12 empresas del sector industrial y manufacturero por parte del grupo

10. BlackCat. (abril 2022)

11. Afectación de empresas en CDMX, Veracruz, Hidalgo, Sinaloa, Querétaro y Nuevo León por el grupo LAPSUS$. (junio 2022)

12. Afectación a la fábrica Foxconn México por el grupo ruso Lockbit (junio 2022)

13. Robo de información del Buró de Crédito del historial crediticio de decenas de miles de personas del año 2016 (febrero 2023).

Derivado de todo lo anteriormente expuesto, podemos concluir que México al igual que todos los países de la comunidad internacional ha experimentado un desarrollo económico y social gracias a las TIC y TO, de tal forma que varias de sus actividades vitales están soportadas por estas tecnologías, lo que ahora constituyen infraestructuras críticas de información (ICI), y cuyo daño provoca impactos negativos para el funcionamiento de los servicios básicos de la sociedad y del gobierno, poniendo en riesgo la estabilidad, integridad y permanencia del Estado mexicano.

Es de suma importancia destacar que en la actualidad la mayoría de incidentes o ciberdelitos no se reportan o se denuncian, lo que significa que las estadísticas pueden subestimar la magnitud real del problema.

De igual forma, el Internet de las cosas (IoT o Internet of Things), que se refiere a la interconexión de objetos cotidianos a Internet, representará nuevas vías para delinquir y mayores riesgos, por lo que se requerirá aún más la consolidación de iniciativas integrales de ciberseguridad para la coordinación en la atención de ciberdelitos que atenten contra la seguridad nacional.

La Iniciativa de Ley Federal de Ciberseguridad tiene como parte de su objeto, el aumentar la seguridad cibernética bajo un esquema de corresponsabilidad, prevención, combate y persecución de los delitos cibernéticos o ciberdelitos, a su vez la protección de datos personales y el respeto a los derechos humanos.

Por lo aquí expuesto, someto a la consideración de esta asamblea el siguiente:

PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE CIBERSEGURIDAD

ARTÍCULO ÚNICO. Se expide la Ley Federal de Ciberseguridad, para quedar como a continuación se presenta:

LEY FEDERAL DE CIBERSEGURIDAD

TÍTULO PRIMERO

DISPOSICIONES GENERALES

Artículo 1. Las disposiciones de la presente Ley son de orden público y observancia general en todo el territorio nacional en materia de Ciberseguridad y tienen por objeto:

I. Definir las instituciones responsables de la Ciberseguridad, así como los principios y lineamientos generales a los que debe sujetarse la Política Nacional en la materia;

II. Establecer las facultades, atribuciones, competencias y coordinación entre las dependencias y entidades de la Administración Pública Federal, así como sentar las bases de colaboración con Entidades Federativas, Organismos Constitucionales Autónomos, Academia e instancias del Sector privado del país;

III. Establecer las bases para la prevención y persecución de los delitos cibernéticos, así como el marco regulatorio que fortalezca el ciclo de gestión de incidentes cibernéticos y resiliencia cibernética;

IV. Establecer y coordinar el marco regulatorio de prevención, vigilancia y control sobre infraestructuras críticas de información;

V. Establecer los derechos y obligaciones de los usuarios en el Ciberespacio;

VI. Establecer las bases para el fomento de una cultura de Ciberseguridad;

VII. Definir las facultades, atribuciones y funciones de las autoridades dentro de su ámbito de competencia y establecer los derechos y obligaciones de las personas y las entidades privadas responsables que cuenten con, posean o administren tecnologías de la información y comunicación;

VIII. Impulsar la organización, capacidad operativa, integralidad, transversalidad y profesionalización de las instituciones de la Administración Pública Federal, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e instancias del Sector privado del país;

IX. Establecer las bases para sancionar conductas ilícitas en materia de Ciberseguridad; y

X. Sancionar las conductas delictivas que sean descritas en la presente ley, acorde a los principios establecidos en el código penal federal; fortalecer las atribuciones otorgadas a las autoridades encargadas de perseguirlas, con respeto a las garantías procesales, el derecho a la intimidad, las libertades civiles y los derechos humanos.

Artículo 2. Las acciones en materia de Ciberseguridad que regula la presente Ley se rigen por los principios de legalidad, objetividad, profesionalismo, eficiencia, honradez y respeto a los Derechos Humanos.

Artículo 3. Para los efectos de esta Ley, se entenderá por:

I. Activo: Una persona, estructura, instalación, información y registros, sistemas y recursos de tecnología de la información, material, proceso, relaciones o reputación que tiene valor para quien lo posee, utiliza o administra.

II. Agencia: Agencia Nacional de Ciberseguridad.

III. Análisis de riesgos: Proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto

de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

IV. Aplicaciones: Programa o conjunto de programas informáticos que realizan el procesamiento de registros para una función específica, diseñado para el beneficio del usuario final.

V. Autenticación: Procedimiento para comprobar fehacientemente la identidad de un usuario para acceder a un dispositivo, aplicación, sistema, plataforma o servicio en línea, mediante conocimiento, basado en: información que solo conoce el usuario, pertenencia, basado en algo que posee el usuario, o característica, basada en alguna característica del usuario como datos biométricos.

Respecto de los proveedores de servicios bancarios y financieros se estará a lo dispuesto por el artículo 37 de la presente Ley.

VI. Autenticidad: característica de la seguridad informática que se refiere a la comprobación y confirmación de la identidad real de los activos.

VII. Base de Datos: Recopilación de datos estructurados almacenados de manera digital.

VIII. CERT-MX: Centro Nacional de Respuesta a Incidentes Cibernéticos de la Agencia Nacional de Ciberseguridad.

IX. Ciberamenaza: fuente potencial interna o externa a través del Ciberespacio, con capacidad de provocar un funcionamiento incorrecto, pérdida de valor o efecto adverso en los activos.

X. Ciberataque: cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, denegar, degradar o destruir los recursos del sistema de información o la propia información con la finalidad de afectar la disponibilidad, integridad y confidencialidad del activo.

XI. Ciberdefensa: capacidad de un Estado sujeto de derecho internacional traducida en acciones, recursos y mecanismos en materia de Seguridad y Defensa nacionales en el ciberespacio, para prevenir, identificar y neutralizar Ciberamenazas o Ciberataques, incluidos los que atentan contra Infraestructuras Críticas de Información y la seguridad nacional.

XII. Ciberespacio: entorno o ámbito intangible de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones, en

XIII. el que se comunican e interactúan las entidades públicas, privadas y la sociedad en general, haciendo uso del ejercicio de sus derechos y libertades.

XIV. Ciberseguridad: Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de cualquier organización y usuarios en el ciberespacio.

XV. Comisión o CITICSI: Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información.

XVI. Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

XVII. Datos Informáticos: información en formato electrónico que permite su recuperación o transmisión, incluyendo cantidades, caracteres o símbolos, en forma de señales eléctricas o grabación en medios magnéticos, ópticos o mecánicos

XVIII. Delitos cibernéticos o ciberdelitos: Acciones u omisiones que constituyen una conducta delictiva donde se utilice como medio o como fin a las tecnologías de la información y comunicación, las que se encuentran tipificadas en un código penal u otro, instrumento internacional o normativa exigible al Estado mexicano.

XIX. Disponibilidad: Capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

XX. Dispositivo: Combinación de diversos elementos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas para cumplir un propósito específico

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

XXII. Estrategia Nacional de Ciberseguridad: Documento que establece la visión, principios y objetivos del Estado Mexicano alineados a las prioridades en materia de Ciberseguridad.

XXIII. Evidencia Digital: información almacenada en cualquier clase de medio tecnológico que puede ser recolectada y analizada con herramientas y técnicas especiales y ser también utilizada en una investigación o proceso judicial

XXIV. Incidentes de Ciberseguridad o incidentes cibernéticos: uno o varios eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer o comprometan las operaciones organizacionales y amenazar la seguridad de la información.

XXV. Infraestructuras Críticas de Información: Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de Tecnologías de Información y Comunicaciones, y de Tecnologías de Operación TO, cuya afectación, interrupción o destrucción, tendría un impacto en la provisión de bienes y prestación de servicios públicos o privados esenciales que pudieran comprometer la Seguridad Nacional en términos de las leyes en la materia.

XXVI. Integridad: propiedad de la información, por la que se garantiza la exactitud de los datos transmitidos o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

XXVII. Instancias de Seguridad Nacional: instituciones o autoridades que en función de sus atribuciones participan directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional.

XXVIII. Ley: Ley Federal de Ciberseguridad.

XXIX. 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.

XXX. No repudio: Condición de un sistema informático que registra la actividad o acción de un usuario permitiendo generar la evidencia de las acciones realizadas.

XXXI. Operaciones militares en el Ciberespacio: Actividades que realiza el Estado-Nación en el ciberespacio con la finalidad de garantizar la permanencia del Estado.

XXXII. Proveedor de Servicios de Internet: Los concesionarios y autorizados, para proveer servicios públicos de Telecomunicaciones establecidos en el artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión.

XXXIII. Proveedor de Servicios en Línea: Los proveedores de servicios de aplicaciones y contenidos en Internet establecidos en el artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión.

XXXIV. Riesgo: La probabilidad de que una amenaza aproveche una vulnerabilidad y cause un determinado impacto, pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información.

XXXV. Seguridad de la Información: La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, trazabilidad y no repudio de la misma.

XXXVI. Sistema de Información o Sistema Informático: Conjunto de aplicaciones, servicios, activos u otros componentes para el almacenamiento y procesamiento de datos o información.

XXXVII. Sistema o medio Telemático: Medio que combina los sistemas de telecomunicaciones e informáticos como método para transmitir datos o información.

XXXVIII. TIC o Tecnologías de la Información y Comunicación: Conjunto de software y hardware utilizados para almacenar, procesar y transmitir datos o información.

XXXIX. Tecnología para Intervención legal de comunicaciones: Todo equipo, herramienta, medio, dispositivo, o software diseñados o modificados específicamente para interceptar, monitorear, registrar o manipular las comunicaciones electrónicas.

XL. Telecomunicaciones: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión.

XLI. Usuario: Persona o entidad autorizada para acceder a un sistema de información.

XLII. Vulnerabilidad: Estado o situación de un activo que permite que una amenaza afecte la confidencialidad, integridad y disponibilidad del mismo.

Artículo 4. En lo no previsto por la presente Ley, se aplicarán, conforme a su naturaleza y de forma supletoria, las disposiciones contenidas en:

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

II. La Ley de Seguridad Nacional;

III. La Ley de la Guardia Nacional;

IV. La Ley Federal de Telecomunicaciones y Radiodifusión;

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

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

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

VIII. La Ley Federal de Protección de Datos Personales en Posesión de Particulares.

TÍTULO SEGUNDO

DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD

Artículo 5. El Estado establecerá una Política Nacional de Ciberseguridad que contendrá las acciones necesarias para reducir riesgos cibernéticos,

proteger la información, los bienes, los derechos de las personas y su seguridad.

Artículo 6. El objetivo de la Política Nacional de Ciberseguridad es establecer un sistema de responsabilidad compartida entre los actores públicos, privados y sociales que permita reducir los incidentes y la posible comisión de delitos, a través de la coordinación y atención de los riesgos cibernéticos.

Artículo 7. En el desarrollo de la Política Nacional de Ciberseguridad se deberán considerar los siguientes ejes rectores: seguridad nacional, seguridad pública, economía y educación digital.

Los ejes rectores establecidos deberán observar el respeto y protección a los derechos humanos.

Artículo 8. La Política Nacional de Ciberseguridad promoverá:

I. Crear el Consejo Nacional de Ciberseguridad, el cual estará integrado por las instancias públicas y privadas competentes para el impulsar y fortalecer la política nacional en la materia, dicho Consejo será presidido por la Agencia Nacional de Ciberseguridad;

II. Que todos los sectores participen en el desarrollo de una Estrategia Nacional de Ciberseguridad incluyente, de acuerdo con el Sistema de Planeación Nacional;

III. Que se contribuya al diseño de mecanismos encaminados a la reducción de vulnerabilidades en las infraestructuras tecnológicas;

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

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

VI. El combate a la delincuencia en el ciberespacio;

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

VIII. Que los responsables de Infraestructura Crítica de Información actúen diligentemente y adopten medidas necesarias para prevenir y mitigar

IX. incidentes de Ciberseguridad o de ciberataques y su posible propagación a otros sistemas informáticos;

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

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

a) Garantizar los derechos de los usuarios de los sistemas y servicios que ofrecen con base en los tratados internacionales y los criterios que

b) establezcan los más altos tribunales de nuestro país, eliminando las disposiciones de carácter general que atenten contra su bienestar y patrimonio.

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

d) Colaborar con las autoridades para la investigación y persecución de los delitos

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

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

XII. Las dependencias y entidades de la Administración Pública Federal deberán cumplir con los requisitos mínimos de seguridad que, al efecto determine la Agencia Nacional de Ciberseguridad, los cuales deberán considerar:

a) La designación de un responsable de la Seguridad de la Información;

b) El establecimiento de un Marco de Gestión de Seguridad de la Información;

c) El establecimiento de un equipo de respuesta a incidentes.

XIII. Así mismo, en el marco de la Ley General del Sistema Nacional de Seguridad Pública y la Ley de Seguridad Nacional, las Entidades Federativas, municipios, y demás instancias públicas y privadas podrán considerar:

a) La designación de un responsable de la Seguridad de la Información;

b) El establecimiento de un Marco de Gestión de Seguridad de la Información;

c) El establecimiento de un equipo de respuesta a incidentes.

XIV. En cumplimiento a las obligaciones de seguridad de los sistemas de información, los responsables de Infraestructura Crítica de Información

XV. públicos y privados, y aquellos que administren información de las autoridades de la administración pública federal, tendrán la obligación de reportar y denunciar incidentes cibernéticos confirmados, a las autoridades facultadas, bajo los procedimientos establecidos en esta ley.

CAPÍTULO I

DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD

Artículo 9. La Agencia Nacional de Ciberseguridad, dependerá directamente del Titular del Ejecutivo Federal.

La Agencia contará con las siguientes atribuciones:

I. Coordinar el desarrollo, implementación, evaluación, actualización y mejora continua de la Estrategia Nacional de Ciberseguridad;

II. Generar un Registro de Centros de Respuesta a Incidentes Cibernéticos Públicos y Privado

III. Establecer los esquemas de coordinación e intercambio de información entre los Centros de Respuesta a Incidentes Cibernéticos Públicos y Privados, establecidos en el país;

IV. Establecer esquemas de cooperación con las Entidades Federativas, los organismos constitucionalmente autónomos., instancias del sector privado y la academia, entre otros;

V. Establecer esquemas de cooperación con organismos internacionales y autoridades extranjeras en materia de Ciberseguridad;

VI. Desarrollar, implementar, evaluar y actualizar las disposiciones de seguridad de la información, estándares y guías en materia de Ciberseguridad;

VII. Diseñar criterios técnicos para la detección, monitoreo, pronóstico y medición de riesgos en las tecnologías de la información y comunicaciones;

VIII. Analizar y proponer la armonización legal en materia de Ciberseguridad;

IX. Coordinar entre las instituciones y entidades de la Administración Pública Federal el desarrollo de programas de capacitación y certficaciones que fortalezcan las capacidades en Ciberseguridad;

X. Operar el Registro Nacional de Incidentes de Ciberseguridad, así como generar las estadísticas en la materia;

XI. Requerir en el marco del Sistema Nacional de Seguridad Pública a las autoridades competentes y particulares, la información sobre incidentes cibernéticos ocurridos dentro de su infraestructura tecnológica, cuando se ponga en riesgo la protección a la seguridad nacional o se afecten infraestructuras críticas para establecer las acciones que correspondan;

XII. Fungir como órgano de consulta y coordinación de acciones del gobierno federal y de las entidades federativas para convocar, concertar,

inducir e integrar las actividades de los diversos participantes e interesados en materia de Ciberseguridad;

XIII. Desarrollar e implementar un programa que promueva el fortalecimiento de la cultura nacional de Ciberseguridad;

XIV. Promover la denuncia ciudadana en materia de ciberdelitos;

XV. Establecer los protocolos de prueba en coordinación con las instancias competentes y fabricantes de tecnologías de información y comunicación a efecto de identificar los mecanismos el nivel de ciberseguridad con los que cuenta y en su caso emitir las recomendaciones para su mejora.

XVI. Definir e implementar una metodología de medición y seguimiento a la política pública y a la Estrategia Nacional de Ciberseguridad, con énfasis en las Infraestructuras Críticas de Información

XVII. Integrar y mantener actualizado un Catálogo Nacional de Infraestructuras Críticas de Información; así como salvaguardar su confidencialidad, integridad y disponibilidad;

XVIII. Definir medidas estandarizadas de seguridad de las Infraestructuras Críticas de Información, basadas en un análisis transversal de riesgos que considere a todos los sectores críticos;

XIX. Apoyar, en el ámbito de sus atribuciones, a las autoridades competentes en el análisis de riesgos de las Infraestructuras Críticas de Información;

XX. Promover mecanismos de prevención, atención y respuesta frente a ataques cibernéticos contra las Infraestructuras Críticas de Información, en coordinación con las instancias competentes;

XXI. Fortalecer las actividades de inteligencia en materia de Ciberseguridad;

XXII. Promover campañas nacionales de prevención y concenciación de delitos cibernéticos;

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

XXIV. Colaborar con las instancias de seguridad nacional y administradores de las Infraestructuras Críticas de Información, en la atención de incidentes cibernéticos, así como promover ejercicios y simulacros para su protección;

XXV. Elaborar el mapa de riesgos de las Infraestructuras Críticas de Información, así como los programas correspondientes para mitigarlos;

XXVI. Crear un Consejo Consultivo Ciudadano de Ciberseguridad, que genere la colaboración Pública-Privada en todos los sectores de la sociedad;

XXVII. Generar los Protocolos y mecanismos de la Evidencia Digital, en términos de la legislación aplicable;

XXVIII. Diseñar, definir e implementar, en coordinación con los organismos y autoridades competentes, las políticas normativas y legales, los mecanismos técnicos que permitan la contención y mitigación de actividades ilícitas y tráfico malicioso que atente contra la seguridad pública y la seguridad nacional;

XXIX. La Agencia, elaborará en el marco de las Conferencias Nacionales Conjuntas de Procuración de Justicia y de Secretarios de Seguridad Pública el Protocolo de preservación, procesamiento, traslado, análisis, almacenamiento y presentación de evidencia digital, el cual será de observancia obligatoria a nivel nacional;

XXX. Conformar y dirigir el equipo Nacional de Respuesta a Incidentes Cibernéticos, y promover la creación de Equipos de Respuesta a Incidentes de carácter sectorial, así como la coordinación de equipos existentes nacionales e internacionales;

XXXI. La Agencia Nacional de Ciberseguridad integrará y administrará un Catálogo Nacional de Infraestructuras Críticas de Información en términos de la presente Ley, su Reglamento y demás disposiciones que al efecto se emitan;

XXXII. La Agencia Nacional de Ciberseguridad emitirá los lineamientos para la identificación de Infraestructuras Críticas de Información y realizará la evaluación para la integración del Catálogo correspondiente;

XXXIII. La Agencia deberá establecer un plan nacional de protección de las infraestructuras críticas de información y se coordinará con las instancias correspondientes encargadas de la seguridad física de las mismas;

XXXIV. Promoverá un mecanismo de análisis e intercambio de información con la colaboración de instancias de gobierno y sector privado nacionales e internacionales, con la finalidad de intercambiar información con otras instancias para prevenir incidentes cibernéticos; y

XXXV. Las demás que establezcan otras disposiciones legales y las que sean necesarias para el desarrollo de la Política Nacional de Ciberseguridad.

CAPÍTULO II

DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Artículo 10. Corresponderá a la Agencia Nacional de Ciberseguridad, formular, conducir e impulsar el cumplimiento de una Estrategia Nacional de Ciberseguridad, misma que será actualizada de acuerdo con el Sistema Nacional de Planeación, y contendrá al menos, lo siguiente:

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

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

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

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

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

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

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

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

IX. Definir esquemas de información y participación ciudadana, mecanismos de proximidad para atender a la población, así como acciones tendientes al fomento de la cultura de Ciberseguridad que contemplen orientar y concientizar a la población sobre la importancia de la ciberseguridad, impulsar el desarrollo y aplicación de criterios homologados en la materia y promover programas de capacitación para una efectiva adopción y cumplimiento de mecanismos de ciberseguridad; y

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

XI. Las demás que se consideren necesarias

CAPITULO III

DEL REGISTRO NACIONAL DE INCIDENTES CIBERNÉTICOS Y CIBERDELITOS

Artículo 11. El Registro Nacional de Incidentes Cibernéticos y de Ciberdelitos se integrará con la información de los eventos que afecten la confidencialidad, integridad y disponibilidad de la información de acuerdo a lo establecido en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

En el caso de que éstos constituyan una conducta delictiva, o bien, afecte de forma grave la infraestructura tecnológica de un organismo público o privado dicho registro deberá acompañarse de las acciones legales conducentes a notificar a las demás autoridades competentes.

Artículo 12. El Registro Nacional de Incidentes Cibernéticos y de Ciberdelitos, será administrado por la Agencia Nacional de Ciberseguridad y la información contenida en éste registro deberá atender lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Artículo 13. Para la conformación del Registro Nacional de Incidentes, están obligados a entregar información a la Agencia:

I. La Secretaría de Seguridad y Protección Ciudadana, lo correspondiente al ámbito de su competencia en el marco del Sistema Nacional de Seguridad Pública;

II. La Guardia Nacional, a través de sus unidades especializadas remitirá la información que sea requerida respecto a los incidentes cibernéticos que le sean reportados;

III. Las dependencias de la Administración Pública Federal, respecto de sus incidentes de Ciberseguridad;

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

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

TÍTULO TERCERO

DE LA DISTRIBUCIÓN DE COMPETENCIAS

CAPÍTULO I

DE LA SEGURIDAD NACIONAL

Artículo 14. Para efectos de la presente Ley, se consideran amenazas a la Seguridad Nacional en materia de Ciberseguridad, aquellas que:

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

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

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

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

Artículo 15. Cuando se investiguen amenazas cibernéticas inminentes y concretas a la seguridad nacional, las entidades públicas y privadas proporcionarán de manera inmediata la información que les sea solicitada por la autoridad que tenga a su cargo el proceso, en términos de las disposiciones jurídicas y administrativas aplicables.

Artículo 16. Corresponde a las instancias de seguridad nacional, dentro del ámbito de sus competencias, coordinar las acciones necesarias para prevenir y contener cualquier amenaza cibernética que pudiera constituir un riesgo a la seguridad nacional.

CAPÍTULO II

DE LA SEGURIDAD PÚBLICA

Artículo 17. Las instituciones de seguridad pública de los tres órdenes de gobierno se coordinarán en el marco del Sistema Nacional de Seguridad Pública, para:

I. Suministrar e intercambiar la información obtenida mediante los sistemas e instrumentos tecnológicos respectivos;

II. Generar y difundir campañas orientadas a prevenir y evitar el uso ilícito de las tecnologías de la información y comunicación;

III. Colaborar con las autoridades competentes, así como con las organizaciones públicos y privados con el objetivo de orientar a la sociedad en las medidas que deben adoptar para prevenir los delitos establecidos en esta Ley u otros ordenamientos legales;

IV. Coadyuvar en la generación del Registro Nacional de Incidentes Cibernéticos;

V. Colaborar con las instancias competentes en la prevención, investigación y persecución de los delitos cibernéticos, en el ámbito de sus competencias; y

VI. Observar las demás obligaciones establecidas en otros ordenamientos.

Artículo 18. La Fiscalía General de la República contará con una fiscalía especializada en delitos cibernéticos, cuyas funciones serán investigar y perseguir los delitos cibernéticos, misma que actuará bajo los principios del sistema penal acusatorio.

Artículo 19. Las Fiscalías y policías especializadas en delitos cibernéticos contarán con las herramientas tecnológicas necesarias para la preservación, procesamiento y análisis de la evidencia digital que será aportada en los procedimientos judiciales relacionados con ciberdelitos.

Artículo 20. En el marco del Sistema Nacional de Seguridad Pública, se promoverá:

I. La creación de procuradurías o fiscalías estatales especializadas para la investigación de las conductas en materia de ciberdelitos, promoviendo Ministerios Públicos y policías especializados, recursos humanos, financieros y materiales que requieran para su efectiva operación.

II. La operación de al menos una unidad de policía Cibernética en las entidades federativas, bajo un Modelo Homologado de Policías Cibernéticas cuyos objetivos serás los siguientes:

a) Prevenir, por medio del monitoreo y ciber patrullaje en el ciberespacio, conductas que puedan constituir un evento delictivo.

b) Promover una cultura de respeto y civismo digital estableciendo un estrecho vínculo con la ciudadanía que promueva la denuncia de conductas delictivas.

c) Realizar alertas preventivas, pláticas informativas, acopio y análisis de información para la prevención de ciberdelitos.

d) Realizar bajo el mando y conducción del Ministerio Público la investigación de hechos probablemente delictivos.

Artículo 21. Las Unidades de Policía Cibernética de las Entidades Federativas, en el marco del Sistema Nacional de Seguridad Pública se coordinará con la Unidad Especializada en Cibercrimen de la Guardia Nacional, con el fin de compartir información sobre incidentes, alertas, actores, entre otros datos que puedan ser relevantes en un proceso de investigación.

Estos entes, serán los encargados de operar el Modelo Homologado de Unidades de Policía Cibernética.

Artículo 22. El Poder Judicial de la Federación contará con jueces especializados en materia de cibercrimen y promoverá la capacitación continua en esta materia.

Así mismo, promoverá la colaboración nacional e internacional para contar con las herramientas tecnológicas necesarias para la recepción de la evidencia digital que será aportada a los procedimientos judiciales relacionados con ciberdelitos.

CAPÍTULO III

DE LA CIBERDEFENSA

Artículo 23. Corresponderá a la Secretaría de la Defensa Nacional y la Secretaría de Marina en el ámbito de sus competencias y a través de las unidades administrativas que determinen sus titulares, la atención única y exclusivamente ,de los incidentes cibernéticos que atenten contra la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional, para lo cual previa publicación de los lineamientos correspondientes por parte de dichas Secretarías contarán con las atribuciones siguientes:

I. Monitorear el ciberespacio para prevenir, identificar y neutralizar ciberamenazas y ciberataques que atenten contra la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

II. Considerar dentro de su planeación estratégico-militar a las operaciones militares en el ciberespacio que atenten contra la integridad, estabilidad y permanencia del Estado mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

III. Establecer convenios de colaboración con otros países en materia de ciberdefensa y operaciones militares conjuntas en el ciberespacio por

IV. cuanto hace a hechos que atenten contra la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

V. Desarrollar y ejecutar mecanismos para la ciberdefensa del país únicamente por cuanto hace a hechos que atenten contra la integridad,

estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

VI. Ejercer el derecho de legítima defensa ante toda ciberamenaza y ciberataque que ponga en riesgo la soberanía, los intereses nacionales y las Infraestructuras Críticas de Información y que atenten contra la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

VII. Realizar operaciones militares y navales en el ciberespacio, a fin de disminuir los riesgos en materia de Ciberseguridad, únicamente por cuanto hace a hechos que atenten contra la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

VIII. Coadyuvar en coordinación con las entidades y autoridades competentes, en la gestión de riesgos y gestión de incidentes que afecten la seguridad nacional que atenten contra la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

IX. Establecer mecanismos permanentes de comunicación con los operadores de las Infraestructuras Críticas de Información para, en su caso, emitir alertas tempranas y recomendaciones que atenten contra la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo establecido en la Ley de Seguridad Nacional;

X. Crear unidades para llevar a cabo operaciones militares en el ciberespacio, en cumplimiento de las misiones conferidas en sus Leyes Orgánicas, así como organizar, equipar, mantener dichas unidades y adiestrar continuamente al personal dedicado a estas actividades de acuerdo a lo establecido en la Ley de Seguridad Nacional; y

XI. Las demás que le confieran esta ley u otros ordenamientos aplicables.

CAPÍTULO IV

DE LAS INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN

Artículo 24. Se considerarán infraestructuras críticas de información los siguientes sectores:

I. Químico.

II. Comunicaciones.

III. Presas.

IV. Servicios de Emergencia.

V. Servicios Financieros.

VI. Instalaciones de Gobierno.

VII. Tecnologías de Información.

VII. Sistemas de Transporte.

IX. Instalaciones comerciales.

X. Manufactura crítica.

XI. Industria de defensa.

XII. Energético.

XII. Alimentación y Agricultura.

XIV. Salud Pública.

XV. Materiales, desechos y reactores nucleares

XVI. Sistemas de aguas y aguas residuales

Artículo 25. La ciberseguridad de las Infraestructuras Críticas de Información estará a cargo de aquellas entidades públicas o privadas que tengan la responsabilidad legal de la administración de las mismas.

Artículo 26. Los lineamientos para la identificación de Infraestructuras Críticas de Información deberán considerar al menos los siguientes aspectos:

I. La relación de sectores considerados críticos;

II. El impacto de una posible interrupción o mal funcionamiento de los componentes de la infraestructura de la información, a partir de la cantidad de usuarios potencialmente afectados y su extensión geográfica;

III. El efecto e impacto en la operación y servicios de sectores regulados cuya afectación es relevante para la población;

IV. La potencial afectación de la vida, integridad física o salud de las personas;

V. Las pérdidas financieras estimadas por fallas o ausencia del servicio a nivel nacional o regional asociada al producto interno bruto;

VI. El grado de afectación y relevancia del funcionamiento del Estado y sus órganos; y,

VII. Impacto en la seguridad nacional y el mantenimiento de la soberanía.

Artículo 27. Las autoridades de la federación, entidades federativas, órganos constitucionales autónomos y los particulares están obligados a evaluar sus infraestructuras e identificar si las mismas cumplen con los criterios establecidos para ser consideradas como Infraestructuras Críticas de Información, en cuyo caso deberán notificarlo a la Agencia, para su evaluación e inscripción en el catálogo correspondiente.

Artículo 28. Las autoridades de la federación, entidades federativas, órganos constitucionales autónomos y los particulares, que tengan a su cargo Infraestructuras Críticas de Información, designarán ante la Agencia Nacional de Ciberseguridad, a un responsable para el desarrollo de acciones de prevención y atención a incidentes cibernéticos.

Artículo 29. Todo aquel responsable de administrar Infraestructuras Críticas de Información que cumpla con los criterios establecidos por la Agencia Nacional de Ciberseguridad para ser identificados como tal, están obligados a:

I. Realizar la identificación de activos estableciedo su nivel de criticidad e impacto de acuedo a la metodología definida por la Agencia Nacional de Ciberseguridad;

II. Aplicar permanentemente medidas de seguridad tecnológica, organizacionales, físicas e informativas necesarias para prevenir, reportar y resolver incidentes de Ciberseguridad, así como gestionar riesgos para contener y mitigar el impacto sobre la continuidad operacional;

III. Aplicar medidas para salvaguardar la confidencialidad, integridad y disponibilidad de la información del servicio prestado;

IV. Notificar ante la Agencia Nacional aquellos incidentes de Ciberseguridad considerados como relevantes, de acuerdo con los criterios a la que se refiere el artículo 37 de la presente Ley;

V. Proporcionar información y apoyo a las autoridades para el seguimiento de casos de investigación;

VI. Promover una cultura de Ciberseguridad y el desarrollo de normatividad interna que se haga del conocimiento de los empleados, proveedores y usuarios;

VII. Realizar continuamente revisiones, ejercicios, simulacros y análisis, a fin de fortalecer las medidas de protección;

VIII. Cumplir con lo establecido en el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos y lo demás establecido en esta Ley o en otros ordenamientos aplicables;

IX. Designar un encargado de cumplimiento para la atención y respuesta a incidentes cibernéticos;

X. Establecer un domicilio legal en territorio nacional, para oír y recibir notificaciones de la autoridad; y

XI. Las demás establecidas en la presente Ley, u otros ordenamientos legales.

Artículo 30. La información del Catálogo Nacional de Infraestructuras Críticas de Información contiene información sensible por motivos de Seguridad Nacional, debido a que su revelación indebida podría potenciar una amenaza que ponga en entredicho la integridad, permanencia y estabilidad del Estado mexicano.

Artículo 31. Cuando exista un riesgo a la seguridad nacional, las Secretarías de la Defensa Nacional y de Marina, así como la Guardia Nacional y el Centro Nacional de Inteligencia, en el ámbito de sus competencias, podrán solicitar a la Agencia Nacional de Ciberseguridad el acceso a la información contenida en el Catálogo Nacional de Infraestructuras Críticas de Información.

Artículo 32. Los servidores públicos que tengan acceso al Catálogo Nacional de Infraestructuras Críticas de Información, y a cualquier dato proporcionado por los enlaces responsables de las mismas, deberán abstenerse de difundir la información ahí contenida, y adoptar las medidas necesarias para evitar su publicidad. Además, deberán suscribir una promesa de confidencialidad que se mantendrá vigente en todo tiempo, aún después de que hayan cesado en el cargo en razón del cual se les otorgó el acceso.

CAPÍTULO V

DE LA NOTIFICACIÓN DE INCIDENTES

Artículo 33. Los responsables de Infraestructura Crítica de Información públicos y privados, y aquellos que administren información de las autoridades de la administración pública federal, notificarán en un plazo no mayor a 72 horas, a la autoridad competente respectiva, los incidentes que puedan tener afectaciones a la seguridad pública y a la seguridad nacional.

Para tal efecto, se observará el nivel de impacto alto, muy alto o crítico, de acuerdo al detalle que se especifica en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

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

La notificación de un incidente, no excluirá ni sustituirá la notificación que deba realizarse a otros organismos nacionales e internacionales, o al Instituto Nacional de Transparencia, a la Información y Protección de Datos Personales.

Artículo 34. Los responsables de Infraestructura Crítica de Información públicos y privados, y aquellos que administren información de las autoridades de la administración pública federal, deberán realizar la notificación correspondiente mediante los medios de comunicación establecidos en el PNHGIC.

Artículo 35. Las notificaciones deberán incluir mínimamente la siguiente información, en cuanto la misma, se encuentre disponible: Indicadores de Compromiso, técnicas, tácticas y procedimientos, así como la afectación económica y aquellos datos que permitan determinar cualquier efecto transfronterizo del incidente.

Artículo 36. Los responsables de Infraestructura Crítica de Información públicos y privados, y aquellos que administren información de las autoridades de la administración pública federal, comunicarán al Ministerio Público los hechos probablemente delictivos de acuerdo a lo establecido en el Código Penal Federal, el Código Nacional de Procedimientos Penales y el PNHGIC, y al efecto podrán requerir del Centro Nacional de Respuesta de Incidentes Cibernéticos, la información relacionada con el incidente que se estime necesaria para el inicio de la investigación.

TÍTULO CUARTO

DE LA PRESTACIÓN DE SERVICIOS, USO DE INFRAESTRUCTURA DIGITAL Y TELECOMUNICACIONES

Artículo 37. Los proveedores de servicios de internet y los proveedores de servicios de línea que operen en territorio nacional están obligados a atender todo mandamiento por escrito, en formato físico o digital, fundado y motivado por la autoridad competente en los términos que establezca la Constitución Política de los Estados Unidos Mexicanos y demás leyes.

Para lo cual estarán sujetos a las siguientes obligaciones específicas:

I. Contar con una representación legal para la atención de requerimientos de autoridades competentes.

Dicha representación podrá ser a través de un representante legal establecido en el territorio nacional o bien a través de medios electrónicos.

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

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

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

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

II. Contar con una unidad de cumplimiento para la atención y respuesta de incidentes de ciberseguridad;

III. Registrarse ante la Agencia Nacional de Ciberseguridad;

IV. Establecer medidas de autenticación y cifrado para el acceso a servicios donde se ingresen datos personales;

V. Establecer en sus servicios medidas de seguridad tecnológica, que permitan salvaguardar la integridad, confidencialidad y disponibilidad de la información de los usuarios;

VI. En caso de que la información contenga datos que pudieran vulnerar la seguridad nacional, deberá almacenarse en territorio nacional;

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

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

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

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

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

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

Artículo 38. De conformidad con el principio de cooperación internacional, los proveedores de servicios en línea constituidos en el extranjero que tengan y operen plataformas, sistemas de información, productos o servicios digitales a través de Internet o algún otro medio tecnológico que cuenten con usuarios registrados y activos en México, podrán ser requeridos mediante orden judicial, a colaborar con las autoridades mexicanas de procuración de justicia o encargadas de la seguridad pública y nacional, según corresponda en términos de las disposiciones aplicables en la materia.

Para efectos del párrafo anterior, los proveedores antes citados, deberán sujetarse a lo dispuesto en el Título Octavo "De la Colaboración con la Justicia", de la Ley Federal de Telecomunicaciones y Radiodifusión.

Artículo 39. Los proveedores de servicios bancarios y financieros están obligados a establecer las medidas de Ciberseguridad necesarias para evitar delitos que afecten la seguridad y el patrimonio de los ciudadanos por conductas delictivas que se realicen en las plataformas y los servicios que prestan de acuerdo con las leyes especiales y las disposiciones de carácter general que les son aplicables y que no afecten los derechos de la ciudadanía.

Artículo 40. Los proveedores que desarrollen, operen, comercialicen o pretendan comercializar la tecnología a que se refiere el artículo 3 fracción XXXVIII, dentro del territorio nacional, están obligados a inscribirse en el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones y, a comercializar dicha tecnología únicamente con las autoridades con competencia legal.

Artículo 41. El Centro Nacional de Inteligencia conformará el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones, en términos de lo dispuesto en el Reglamento de la presente Ley.

Artículo 42. La información contenida en el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones será tratada con el carácter de información sensible en materia de Seguridad Nacional, debido a que su revelación indebida podría actualizar o potenciar una amenaza que ponga en riesgo la integridad, permanencia y estabilidad del Estado mexicano.

Artículo 43. El uso de Tecnología para Intervención de Comunicaciones es exclusivo para las Instituciones de seguridad pública o nacional; las autoridades observarán en todo momento el respeto a las formalidades legales, y los derechos humanos, por lo que su venta queda prohibida para fines distintos a los establecidos.

Quedan exceptuados de esta disposición las personas físicas y morales que desarrollen actividades profesionales, económicas, académicas utilicen aquellas tecnologías para la prevención e identificación de vulnerabilidades, con la finalidad de fortalecer la ciberseguridad de las empresas públicas y privadas.

TÍTULO QUINTO

DE LA CULTURA Y EDUCACIÓN

Artículo 44. Los poderes de la Unión, en el ámbito de sus respectivas atribuciones, desarrollarán y difundirán una cultura de ciberseguridad, con el objetivo de:

I. Orientar y concientizar a la población sobre la importancia de la ciberseguridad en los ámbitos público y privado;

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

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

IV. Informar qué áreas y procedimientos institucionales existen para denunciar una posible vulnerabilidad o amenaza en materia de ciberseguridad, así como para denunciar la comisión de un posible delito cibernético;

V. Promover programas de capacitación para una efectiva adopción y cumplimiento de los mecanismos de ciberseguridad en el ejercicio de sus funciones;

VI. Impulsar el desarrollo científico y tecnológico en la materia; y

VII. Los demás que se identifiquen para consolidar una cultura de ciberseguridad en el país.

Artículo 45. Corresponde a las instituciones públicas y privadas de educación, investigación e innovación:

I. Desarrollar programas educativos y de profesionalización, en todos los niveles de escolaridad, que fomenten una cultura de ciberseguridad;

II. Proporcionar acciones formativas a todo el personal de los centros educativos, en materia de ciberseguridad;

III. Fomentar a través de los Centros de Investigación y demás instituciones educativas públicas y privadas, la cultura en materia de ciberseguridad, y

IV. Participar como asesores para la implementación de políticas públicas en materia de ciberseguridad.

TÍTULO SEXTO

DE LAS INFRACCIONES Y SANCIONES

Artículo 46. Los administradores de Infraestructuras Críticas de Información, los proveedores de servicios e instancias públicas y privadas que incumplan con los dispuesto en los artículos 13, 27,28, 29, 32, 37, 38, 39 y 40 podrán ser

acreedores a multas de mil a veinte mil veces el valor diario de la Unidad de Medida y Actualización, por parte de la Agencia.

En su caso, respecto de la aplicación de multas serán impuestas por la entidad reguladora correspondiente al sector respectivo, y conforme a las normas y montos establecidos en la legislación especial en la materia

Artículo 47. A fin de que la calificación de la sanción sea proporcional a la conducta respectiva, la Agencia tomará en cuenta los siguientes criterios:

I. Si el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones;

II. La probabilidad de ocurrencia del riesgo;

III. La gravedad de los efectos de los ataques;

IV. La reiteración en la infracción dentro del plazo de tres años; y

V. La capacidad económica del infractor.

Artículo 48. Las infracciones cometidas por funcionarios de la Administración Pública Federal y demás autoridades competentes para la imposición de las sanciones se regirán por los procedimientos para el establecimiento de sanciones respectivos en términos de la normatividad aplicable.

TÍTULO SÉPTIMO

DE LOS DELITOS CIBERNÉTICOS

CAPÍTULO I

DE LOS CIBERDELITOS

SECCIÓN PRIMERA

De los delitos contra la Confidencialidad, Integridad y Disponibilidad de la información

Artículo 49. Al que por cualquier medio o método, sin autorización o excediendo de la autorización que posea de la persona física o moral que legalmente pueda otorgarlo, dolosamente acceda, copie, extraiga, modifique, altere, destruya o elimine la información provocando la pérdida de la confidencialidad, integridad y disponibilidad de la misma contenida en equipos, sistemas o medios informáticos, electrónicos o telemáticos, que estén protegidos o no por un mecanismo de seguridad, se le impondrán de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Artículo 50. Al que con motivo de la conducta descrita en el artículo 49, cifre, exfiltre y/o controle o manipule la información o el funcionamiento de cualquier dispositivo electrónico que forme parte interna o externa del sistema informático con la finalidad de obligar a otro de hacer o dejar de hacer, usar o no divulgar información obtenida, o bien para obtener un lucro indebido o cualquier tipo de beneficio para sí o para un tercero, se sancionará con pena de diez a quince años de prisión y multa de quince mil a veinticinco mil unidades de actualización.

Artículo 51. La sanción a las conductas descritas en los artículos 49 y 50 se incrementarán en una mitad, cuando el acceso ilícito y el lucro indebido, beneficio, uso divulgación de información, provengan de personas físicas o morales contratadas para proporcionar servicios de seguridad de la información.

SECCIÓN SEGUNDA

Del ataque a la integridad de un Sistema Informático

Artículo 52. Al que sin autorización o excediendo de la autorización que posea, de la persona física o moral que legalmente pueda otorgarlo, obstaculice o impida mediante la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, el funcionamiento total o parcial de un sistema informático, electrónico o telemático, se le impondrá una pena de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

SECCIÓN TERCERA

De la interceptación de datos

Artículo 53. Quien, a través de cualquier medio o método, intercepte sin autorización o sin una orden judicial, cualquier tipo de datos informáticos, electrónicos telemáticos, incluidas las emisiones electromagnéticas y radiofrecuencias, originadas y/o provenientes desde otro sistema o equipo o realizadas dentro del mismo, se le impondrá de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización.

Artículo 54. A quien sin tener facultades legales para tal efecto adquiera o arriende Tecnología para Intervención de Comunicaciones, se le impondrán de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización.

Quedan exceptuados de esta disposición las personas físicas y morales que desarrollen actividades profesionales, económicas, académicas utilicen aquellas tecnologías para la prevención e identificación de vulnerabilidades, con la finalidad de fortalecer la ciberseguridad de las empresas públicas y privadas.

Artículo 55. Al quien sin estar registrado para tal efecto comercialice Tecnología para Intervención de Comunicaciones en territorio nacional, se le impondrán de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización.

Quedan exceptuados de esta disposición las personas físicas y morales que desarrollen actividades profesionales, económicas, académicas utilicen aquellas tecnologías para la prevención e identificación de vulnerabilidades, con la finalidad de fortalecer la ciberseguridad de las empresas públicas y privadas.

A quien sin estar sujeto a una ciberamenaza o ciberataque real e inminente o que estando bajo una ciberamenaza o ciberataque real e inminente no presente la denuncia correspondiente ante la unidad especializada de la Fiscalía General de la República, utilice cualesquiera equipos, medios, dispositivos, o software que permitan identificar comunicaciones, se le impondrán de cinco a diez años de prisión y multa de cinco mil a diez mil unidades de medida de actualización.

SECCIÓN CUARTA

De la falsificación informática

Artículo 56. Quien sin autorización de la persona física o moral que legalmente pueda otorgarlo introduzca, altere, bloqueé, borre o suprima datos informáticos, electrónicos telemáticos previamente almacenados en un sistema o base de datos con la intención de que sean tomados como auténticos o utilizados como auténticos para efectos legales, con independencia de que los datos sean legibles e inteligibles directamente. Se le impondrá de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

SECCIÓN QUINTA

Del abuso de dispositivos tecnológicos

Artículo 57. El que para la comisión de los delitos descritos en los artículos 49 a 56, produzca, venda, adquiera para su uso, importe, exporte programas informáticos, equipos, o dispositivos se sancionará con la pena de cinco a

vente años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Las disposiciones del presente artículo no se aplicarán a los casos cuando la producción, venta, adquisición para uso, importación, exportación u otras formas de prestación para la utilización de los dispositivos estén relacionados, con una prueba autorizada para la identificación de vulnerabilidades con fines preventivos, capacitación o bien para innovación tecnológica, o cualquier otra actividad comercial lícita.

SECCIÓN SEXTA

Del fraude por medio informático

Artículo 58. Al que por medio del engaño aprovechándose del error en que otro se halle, mediante cualquier medio método informático, electrónico o telemático obtenga cualquier bien o derecho patrimonial en perjuicio de un tercero o del Estado, será sancionado con pena de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Esta pena se incrementará hasta en una mitad cuando el medio informático, electrónico o telemático utilizado, suplante la identidad de una Entidad del gobierno federal o estatal.

Artículo 59. A quien mediante el engaño, y a través de sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica, se haya allegado de información personal, documentos, datos financieros verdaderos o apócrifos con independencia de la autorización del titular, con el fin de vulnerar los mecanismos de gestión y/u obtener un beneficio económico a través del otorgamiento de créditos solicitados ante alguna entidad financiera o crediticia o de empresas de servicios de financiamiento tecnológico emergentes, para cobro a través de depósitos transferencias bancarias nacionales e internacionales de divisas o en su defecto mediante la conversión a algún tipo de moneda digital, se le impondrá una sanción de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

La sanción económica y pena se aumentará en una mitad, en los siguientes supuestos:

I. La conducta ha sido repetida en reiteradas ocasiones ante una misma o en diferentes instancias;

II. Exista el consentimiento de una de las partes involucradas para hacer mal uso de su información o datos;

III. Una de las partes involucradas trabajó o formó parte de algunas de las instancias vulneradas, y aprovechándose de sus conocimientos sobre el proceso de selección y tramites auxilió a vulnerar o facilitar de manera dolosa el otorgamiento de un crédito.

SECCIÓN SÉPTIMA

De los delitos contra la integridad y libertad de las personas

Artículo 60. Al que dolosamente trate datos personales mediante el engaño o aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos. Mediante las tecnologías de la información y comunicación, con la finalidad de obtener un lucro indebido o cualquier tipo de beneficio, se le impondrá de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Por tratamiento deberá atenderse lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Artículo 61. El que suplante la identidad o se apropie de un medio de identificación de otra persona con el propósito de realizar una conducta tipificada como delito, será sancionado con una pena de cinco a veinte años de prisión y multa de mil a veinte mil unidades de medida de actualización.

Para fines de este delito, medio de identificación debe entenderse como cualquier dato o información que pueda ser utilizado por sí o junto con otros para identificar a una persona de manera directa o indirecta en entornos digitales, incluyendo datos biométricos, tales como huellas, grabación de voz, retina, imagen del iris o cualquier representación digital particularizada

Artículo 62. Al que describa, diseñe, distribuya 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 o material, a sí mismas o a terceros, se sancionará con una pena de tres a seis años de prisión y una multa de quinientas a mil unidades de medida y actualización. Los proveedores de servicios digitales y de telecomunicaciones a través de cuyas plataformas se hayan exhibido, publicado o compartido los materiales antes referidos, no tendrán responsabilidad al respecto, salvo que hubieran participado directa o indirectamente en la elaboración o edición del material correspondiente.

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 provoque, incite o apoye acciones basadas en odio, violencia o contra cualquier persona o grupo de personas o realización de genocidio o de pornografía infantil.

Serán consideradas 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.

Lo anterior, sin perjuicio de la responsabilidad civil por daños o perjuicios que se hayan podido generar con motivo de la conducta.

Artículo 63. 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.

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.

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

Artículo 64. 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 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.

Para efectos de esta Ley Federal se entenderá por connotación sexual los actos que tengan como característica o finalidad conseguir una gratificación, o placer sexual para el espectador o escucha e inclusive para el sujeto activo.

Artículo 65. 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.

Artículo 66. Cuando exista sentencia firme por cualquier delito comprendido en esta sección, la autoridad competente, ordenará el borrado seguro relacionado con pornografía infantil o en su caso la destrucción del dispositivo que contenga la información que haya motivado la sentencia del imputado y que se encuentre en poder o bajo control del Tribunal de Enjuiciamiento o del Ministerio Público.

SECCIÓN OCTAVA

De la propiedad intelectual

Artículo 67. Cuando las conductas descritas en la Ley Federal de Derechos de Autor y en la Ley de Propiedad Industrial, vigente al momento de los

hechos, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones, de conformidad con el principio penal de especificidad.

SECCIÓN NOVENA

De los sistemas gubernamentales e infraestructuras críticas de información

Artículo 68. 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 infraestructuras críticas de información o sistemas gubernamentales, se le impondrán de seis a veinte años de prisión y multa de cinco mil a veinte mil unidades de medida y actualización.

Artículo 69. A la persona que dolosamente, 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 infraestructuras críticas de información o sistemas gubernamentales, se le impondrán de seis a veinte años de prisión y multa de cinco mil a veinte mil unidades de medida y actualización.

Artículo 70. 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 infraestructuras críticas de información o sistemas gubernamentales, se le impondrán de ocho a veinticinco años de prisión y multa de ocho mil a veinte mil unidades de medida y actualización.

Artículo 71. Como regla común y en cuanto a las penas previstas en esta sección 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 72. A los empleados o ex empleados de las empresas prestadoras de servicios tecnológicos que tengan o hayan tenido relación comercial o contractual con instituciones públicas, y del sistema financiero o de infraestructuras críticas de información, se les aumentará hasta una mitad de las penas previstas en el presente capítulo.

Artículo 73. Las penas a que se refiere el artículo anterior se incrementarán hasta en una mitad cuando los empleados hayan firmado un acuerdo o carta de confidencialidad.

CAPÍTULO II

DE LAS TÉCNICAS ESPECIALES DE INVESTIGACIÓN

Artículo 74. El Ministerio Público atendiendo a la urgencia del caso particular y con la debida diligencia, puede solicitar al juez de control la actuación de agentes encubiertos a efecto 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.

La orden judicial que autorice la realización de este acto de investigación, deberá indicar circunstanciadamente el nombre real, alias o nombre de usuario, dirección física o electrónica del afectado, señalar el tipo y la duración de la misma.

El juez de control competente, podrá prorrogar la duración de este acto de investigación, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el párrafo anterior.

El agente encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de referidas comunicaciones.

El agente encubierto estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.

CAPÍTULO III

REPARACIÓN DEL DAÑO

Artículo 75. El responsable de la comisión de un delito cibernético deberá resarcir los daños directos generados, 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, y

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

Artículo 76. Asimismo, la autoridad deberá:

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

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

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 expedirá y publicará el Reglamento de esta Ley dentro de los seis meses posteriores a la entrada en vigor del presente Decreto.

TERCERO. Se conformará la Agencia Nacional de Ciberseguridad dentro de los treinta y seis meses posteriores a la entrada en vigor del presente Decreto, en tanto sus funciones estarán a cargo de la Coordinación de la Estrategia Digital Nacional (CEDN) de Presidencia.

CUARTO. A la entrada en vigor del presente Decreto, la Fiscalía General de la República, contará con treinta y seis meses para implementar la fiscalía especializada en la materia.

QUINTO. A partir de la emisión de los Lineamientos que contienen los criterios para la clasificación de Infraestructuras Críticas de Información, los particulares contarán con doce meses para notificar ante la instancia competente las infraestructuras a su cargo.

SEXTO. El Centro Nacional de Inteligencia contará con 90 días posteriores a la publicación del presente Decreto para expedir las reglas de operación del Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones.

SÉPTIMO. Los proveedores que desarrollan, operan, proporcionan mantenimiento o comercializan Tecnología para Intervención de Comunicaciones dentro del territorio nacional, contarán con seis meses

posteriores a la entrada en vigor del presente Decreto, para darse de Alta en el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones.

OCTAVO. Las instituciones que previamente tengan Tecnología para Intervención de Comunicaciones, contarán con 60 días hábiles a partir de la entrada en vigor del presente Decreto, para informar al Centro Nacional de Inteligencia el nombre de los proveedores de la misma, así como el tipo y características de la tecnología adquirida.

Dado en el Palacio Legislativo de San Lázaro, a 20 de marzo de 2024

Atentamente

Diputado Javier López Casarín

Grupo Parlamentario Verde Ecologista de México

Cámara de Diputados del Honorable Congreso de la Unión, LXV Legislatura

Junta de Coordinación Política

Diputados: Jorge Romero Herrera, presidente; Moisés Ignacio Mier Velasco, Morena; Rubén Ignacio Moreira Valdez, PRI; Carlos Alberto Puente Salas, PVEM; Alberto Anaya Gutiérrez, PT; Braulio López Ochoa Mijares, MOVIMIENTO CIUDADANO; Francisco Javier Huacus Esquivel, PRD.

Mesa Directiva

Diputados: Marcela Guerra Castillo, presidenta; vicepresidentas, Karla Yuritzi Almazán Burgos, MORENA; Joanna Alejandra Felipe Torres, PAN; Blanca María del Socorro Alcalá Ruiz, PRI; secretarios, Brenda Espinoza López, MORENA; Diana Estefania Gutiérrez Valtierra, PAN; Fuensanta Guadalupe Guerrero Esquivel, PRI; Nayeli Arlen Fernández Cruz, PVEM; Pedro Vázquez González, PT; Vania Roxana Ávila García, MOVIMIENTO CIUDADANO; Karina Isabel Garivo Sánchez, PRD.

Secretaría General

Secretaría de Servicios Parlamentarios

Gaceta Parlamentaria de la Cámara de Diputados

Director: Juan Luis Concheiro Bórquez, **Edición:** Casimiro Femat Saldívar, Ricardo Águila Sánchez, Antonio Mariscal Pioquinto.

Apoyo Documental: Dirección General de Proceso Legislativo. **Domicilio:** Avenida Congreso de la Unión, número 66, edificio E, cuarto nivel, Palacio Legislativo de San Lázaro, colonia El Parque, CP 15969. Teléfono: 5036 0000, extensión 54046. **Dirección electrónica: http://gaceta.diputados.gob.mx/**