# INICIATIVA DE LA SENADORA JESÚS LUCÍA TRASVIÑA WALDENRATH, CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN Y DEROGAN DIVERSAS DISPOSICIONES DEL TÍTULO NOVENO, LIBRO SEGUNDO DEL CÓDIGO PENAL FEDERAL Y SE EXPIDE LA LEY DE SEGURIDAD INFORMÁTICA

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

## CONSIDERACIONES

### Objetivo de la Iniciativa

La presente Iniciativa propone reformar y derogar diversas disposiciones del Código Penal Federal relativos a ciberdelitos o delitos cometidos por medio de sistemas informáticos, dando paso a crear una Ley especializada en la materia de Ciberdelitos, a fin de erradicar el mal uso de las herramientas dentro del campo de la tecnología de la información, ya que estos influyen directamente sobre la sociedad moderna, y que actualmente dentro el ciberespacio es utilizado con fines ilegítimos.

Por ello dentro de la presente iniciativa de Ley se define que los Ciberdelitos, son los llamados delitos en el ciberespacio, y que estos abarcan tanto las actividades que atentan contra la integridad, la disponibilidad y la confidencialidad de los sistemas informativos y redes de telecomunicaciones, así como a las personas en su carácter individual como sujetos de derecho.

Derecho que, ante la evolución social constante en sus formas de interacción, es necesario legislar con miras al avance tecnológico y las necesidades que emergen de las mismas.

### Motivación de la Iniciativa

En estos días, somos cada vez más conscientes de que la tecnología es sumamente útil y necesaria para la vida diaria, gracias a ella podemos explorar el espacio, estudiar las profundidades del océano y acceder rápidamente a más información de la que nuestro cerebro puede contener. A su vez, nos permite almacenar miles de bits de información, acortar distancias con los medios de transporte y comunicación

y mantenernos contactados en todo momento. Sin ir más lejos, gracias a la tecnología los seres humanos poseemos el estilo de vida del que dependemos. Nos provee una vida mejor.

El nacimiento de la tecnología es sin duda un producto de las necesidades del hombre. Surge como una manera de superarse, perfeccionarse, analizarse y favorecer el progreso de la humanidad y la evolución del hombre. La mayoría de las nuevas tecnologías surgen como imitación y perfeccionamiento de la mente humana. Es importante destacar entonces, que la tecnología no es más que un instrumento, un medio para llegar a un fin que es la evolución y prosperidad del ser humano[1].

Y es precisamente en esta evolución que una herramienta elemental para cualquier persona en nuestros días, son las Tecnologías de la Información y Comunicación que incluso es un derecho constitucional consagrado en el articulo 6º, en el cual establece que:

> *El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.*

Derivado de lo anterior, podemos decir que a lo largo del citado artículo nos encontramos derechos implícitos como lo es el derecho al acceso a la información, a la vida privada y datos personales; entre otros más.

Mismos que al ser considerados, debemos respetarlos y proveer de herramientas que los puedan vigilar, proteger y garantizar plenamente.

En ese orden de ideas quiero mencionar que dentro de estas Tecnologías se encuentran diferentes elementos que en apariencia son tecnicismos pero que en la práctica necesitan aterrizarse en la legislación de una manera general que pueda digerirse por cualquier persona y por lo tanto pueda brindarse una interpretación conforme a las necesidades nacientes de regular el mal uso que se les dan.

Y es precisamente en el ciber espacio, donde últimamente nos encontramos ante nuevas amenazas.

Motivo por el cual es necesario recalcar que el ciberespacio, ese relativamente un nuevo entorno virtual en el que se desarrolla gran parte de nuestras vidas, y que no está en absoluto libre de amenazas.

---

[1] Extracto retomado del ensayo "El hombre y la tecnología: del hombre moderno al hombre primitivo", consultado en: http://www.santiagokoval.com/2011/04/27/el-hombre-y-la-tecnologia-del-hombre-moderno-al-hombreprimitivo/

Los ideales ciber-libertarios, con su visión del ciberespacio como un lugar inmune a la acción estatal, quedaron pronto arrumbados, entre otras razones por la necesidad de hacer frente a esas amenazas, ya que actualmente existen cibercriminales

La ciberseguridad, inicialmente una disciplina de carácter técnico ha pasado a conformar, así, un elemento esencial en las estrategias de seguridad nacionales.

Desde el punto de vista del Derecho internacional, el único avance producido para dotar de una regulación específica al ciberespacio es el que ha tenido lugar en el campo de la lucha contra la cibercriminalidad, mediante el Convenio de Budapest de 2001[2].

Por lo demás, parece existir consenso acerca de que los principios y normas del Derecho internacional preexistentes son aplicables a la conducta de los Estados en el ciberespacio, particularmente, en lo que se refiere a la amenaza o al uso de la fuerza y a la conducción de ciberhostilidades en caso de conflicto armado.

La ciberdelincuencia es uno de los delitos transnacionales de más rápido crecimiento a los que se enfrentan los países miembros de INTERPOL[3]. Aunque la rápida evolución de Internet y la tecnología informática han permitido el crecimiento económico y social, una mayor dependencia de Internet ha generado más riesgos y vulnerabilidades, y ha abierto nuevas posibilidades para las actividades delictivas[4].

Dentro de esta gran problemática encontramos la *Piratería informática. Programas maliciosos. Botnets. Red oscura. Ciberdelincuencia como servicio.* Con el uso de las nuevas tecnologías para cometer ataques cibernéticos contra gobiernos, negocios e individuos, palabras y frases que hace una década apenas existían, forman ahora parte de nuestro vocabulario diario. Estos delitos no conocen fronteras, ni físicas ni virtuales, causan importantes daños y suponen un peligro muy real para las víctimas de todo el mundo.

La «ciberdelincuencia pura» se refiere a delitos contra computadoras y sistemas de información, con el objetivo de lograr el acceso no autorizado a un dispositivo o negar el acceso a un usuario legítimo.

Las formas tradicionales de delincuencia también han evolucionado. Las organizaciones delictivas utilizan cada vez más Internet con el fin de facilitar sus actividades y maximizar los beneficios en el menor tiempo posible. Estos delitos facilitados por medios electrónicos no son necesariamente nuevos – robo, fraude,

---

[2] Convenio sobre la Ciberdelincuencia. Budapest, 23.XI.2001 consultado en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[3] México es uno de los 194 países miembros de Interpol, consultado en: https://www.interpol.int/es/Quienes-somos/Paises-miembros

[4] Retomado de la *ESTRATEGIA MUNDIAL CONTRA LA CIBERDELINCUENCIA* consultado en: *https://www.interpol.int/es/Media/Files/Crime-areas/Cybercrime/Estrategia-mundial-contra-la-ciberdelincuencia-Resumen/*

juegos de azar ilícitos, venta de medicamentos falsificados – pero han adquirido una nueva dimensión en línea.

La ciberdelincuencia crece a un ritmo muy acelerado, con nuevas tendencias emergiendo continuamente. La policía debe por tanto mantenerse al día en las nuevas tecnologías, con el fin de comprender las posibilidades que crean para los delincuentes y su uso como herramientas para luchar contra la ciberdelincuencia[5].

La naturaleza "sin fronteras" de la ciberdelincuencia implica que los organismos encargados de la aplicación de la ley tienen problemas para responder eficazmente, a causa de los límites en las investigaciones transfronterizas, problemas de tipo jurídico y la diversidad de capacidades en el mundo.

Si bien a nivel internacional se cuenta por parte de la Interpol la Estrategia contra la Ciberdelincuencia describe el plan de INTERPOL para apoyar los esfuerzos de los países miembros en su lucha contra la ciberdelincuencia, mediante la coordinación y facilitación de capacidades policiales especializadas de 2016 a 2020.

Misma que se revisará periódicamente para garantizar que mantiene su relevancia, continúa respondiendo a nuevas amenazas en el dinámico entorno en el que opera, y responde a las expectativas de los países miembros.

El principal ámbito de acción del Programa de INTERPOL sobre Ciberdelincuencia es abordar la "ciberdelincuencia pura", delitos contra ordenadores y sistemas de información en los que el objetivo es acceder sin autorización a un dispositivo o denegar el acceso a un usuario legítimo (típicamente mediante el uso de software malicioso).

No obstante, INTERPOL reconoce la importancia de la lucha contra los delitos cibernéticos en los que el uso de ordenadores y sistemas de información amplifican el delito, como el fraude financiero y el uso terrorista de los medios sociales.

Además, de que existe una creciente demanda de especialistas forenses informáticos para apoyar la lucha contra muchos tipos de delitos[6].

De los cuales quiero mencionar, que como bien hace alusión Interpol no son los únicos delitos en la materia, sino que hay más como es el caso del acoso, la trata de personas, la pornografía infantil, el chantaje sexual, la difamación el más uso de datos personales en la Red y los de carácter financiero.

Motivo por el cual es importante velar por la Seguridad Informática, puesto que las tecnologías de la información y comunicación (TIC) como un factor de desarrollo

---

[5] Extracto retomado de: *Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. Internet también facilita una serie de delitos más tradicionales*, consultado en https://www.interpol.int/es/Delitos/Ciberdelincuencia

[6] *Ibidem* p. 3

político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.

De acuerdo con el Director General de Fortinet[7] en México, Eduardo Zamora, quien dijo a Notimex que México es vulnerable debido a que no se tiene consciencia respecto la capacidad de los "hackers" para mejorar sus prácticas de ataque.

> *"México es tan atacado por cuestión cultural, por falta de conciencia y por la idea de 'a mí no me va a pasar', por ejemplo los ataques que se han escuchado a los diferentes retailers no son lo más evolucionados, lo que hacen es un distractor para robar las bases de datos, las identidades porque no se tiene una estrategia de seguridad, estamos en la tercer o cuarta generación de ciberseguridad y se está usando la primera cuando ya se ha encontrado cómo vulnerarla",* señaló.

Apuntó el directivo que, además, buena parte de los ataques que se llevan a cabo en la actualidad provienen de los móviles que son vulnerados, debido a los hábitos de los usuarios, quienes sin tomar medidas se conectan a redes abiertas o descargan programas que ya contienen software malicioso, el cual puede infectar las redes de las empresas.

> *"Los ataques están proliferando por diferentes razones, el mundo cambió: la cantidad de dispositivos móviles en el mercado es impresionante; si tú tomas en cuenta que poco más del 80 por ciento de las empresas te permiten utilizar tu móvil para meterte en las redes de la empresa, entonces tienes un mundo impresionante para atacar, ahora los delincuentes usan mucho el móvil para meterse a las empresas".*

Ricardo Alvarado, director ejecutivo de Riesgo de Lockton México, afirmó en un comunicado que los diversos ataques perpetuados en 2018 llegaron a una gran diversidad de usuarios, entre los que se encontraron algunas instituciones bancarias.

> *"Es un error pensar que difícilmente los ciberataques podrían ocurrir en una empresa, ha habido casos tan recientes como el de abril de 2018, cuando cinco entidades bancarias mexicanas fueron "hackeadas" a través de su plataforma SPEI, produciendo una pérdida aproximada de 300 millones de pesos, de acuerdo a Banxico",* sostuvo.

[7] Fortinet https://www.fortinet.com/

México es el tercer país que más ataques ha padecido a nivel mundial, y el número uno en Latinoamérica[8].

Paralelamente al incremento en el acceso de los mexicanos a Internet, ha aumentado el cibercrimen en el país, de acuerdo con el estudio "Perspectiva de ciberseguridad en México" realizado por la consultora global McKinsey & Company y el Consejo Mexicano de Asuntos Internacionales (COMEXI).

El incremento del cibercrimen se ha dado en prácticamente en todos los ámbitos, y la expectativa es que para 2025 la cantidad de dispositivos conectados a las redes en manos de mexicanos crezca casi 70%, hasta un total de 300 millones de aparatos.

Entre los ataques más comunes que se han incrementado para los sectores público y privado, precisa el documento, son los dirigidos o sistémicos que incluyen el riesgo de robo de información, ataques a infraestructura crítica y afectación a servicios clave.

Adicionalmente existen amenazas a nivel personal que se centran en el ciberacoso, las campañas de desinformación en redes sociales, el fraude y el robo de identidad.

El socio de McKinsey y coautor del estudio, Andrea Cristofori, indicó que la creciente importancia de la ciberseguridad obliga a las empresas a realizar cambios fundamentales en sus planes estratégicos, sus modelos operativos y su estructura organizacional.

> *"Las empresas, la sociedad y el gobierno en México necesitan trabajar en conjunto para combinar recursos y facilitar el intercambio de información para garantizar su seguridad futura en este mundo cada vez más digital"*, aseguró[9].

Actualmente las personas son identificables a nivel digital por sus comportamientos a través de los diferentes dispositivos móviles.

En el país, no hay una legislación clara para algunos fraudes como la suplantación de identidad.

> "*La suplantación de identidad conlleva una multiplicidad de ilícitos; por lo tanto, debe ser analizado de manera global*", comentó Cynthia Solís, investigadora del Centro de Estudios e Investigación de Derecho Inmaterial de la Universidad de París Saclay.

---

[8] Retomado de *"Ciberdelitos se duplican en un año en México"* https://www.elsiglodedurango.com.mx/noticia/1020608.ciberdelitos-se-duplican-en-un-ano-en-mexico.html

[9] Retomado de "Crece el acceso a Internet en México...y el cibercrimen también", consultado en: https://idconline.mx/corporativo/2018/06/14/crece-el-acceso-de-internet-en-mexicoy-el-ciberdelito

Durante el *"Foro de Usurpación de identidad en internet, problemática, prevención y solución"*, organizado por la Barra Mexicana del Colegio de Abogados, la especialista explicó que actualmente las personas son identificables a nivel digital por sus comportamientos a través de los diferentes dispositivos móviles.

> "*Si alguien ingresa a nuestro celular, tiene acceso total a nuestra información personal, que va desde conocer domicilio, contactos personales e incluso monitorear estado nuestro de salud*", dijo la especialista. Señaló que la sociedad mexicana es muy vulnerable ya que los usuarios no toman las medidas necesarias para evitar un ataque de suplantación de identidad.

También mencionó que legalmente se carece de una uniformidad en los tipos penales del fuero común y no existe un tipo penal en el Código Penal Federal que lo sancione.

La investigadora dijo que la policía cibernética está muy limitada para actuar contra este tipo de delitos, porque no existe una cultura de denuncia de parte de los usuarios. Sin embargo, en caso de ser víctima de estos ataques, es necesario denunciar los hechos ante el Ministerio Público y colaborar con las instituciones financieras y comerciales para recabar la mayor información acerca del incidente.

A manera de consejo, Cynthia Solís señaló que los usuarios tienen la opción de suscribirse a las notificaciones del sitio de internet del buró de crédito para que reciban una alerta cuando algún intruso consulte sus datos financieros. De esta manera estarán monitoreando datos relevantes en tiempo real.

El exceso de confianza y mala gestión de nuestra identidad digital en las distintas plataformas tecnológicas son algunas de las causas por las cuales podemos convertirnos en víctimas potenciales de suplantación de identidad en México.

> "*Pese a no ser un delito nuevo en nuestro país, la suplantación de identidad en internet se ha propagado mucho más fácil por las plataformas tecnológicas que existen. Comúnmente, un ataque cibernético lleva entre seis y ocho meses de planeación. Sin embargo, se ejecuta en muy poco tiempo y a afecta a millones de usuarios*", dijo.

Señaló que este ciberdelito requiere mayor atención en México, lugar en donde no existen mediciones precisas. Sin embargo, ejemplificó diciendo que en EU casi el 50% de los internautas ha sufrido estos ataques[10].

Por lo tanto, como se les ha venido narrando parte de la gran problemática que engloba los delitos en el ciberespacio, es necesario que tomemos acciones que puedan solucionar estos y futuros problemas suscitados.

---

[10] Extracto retomado de "¿Sabías que los ataques informáticos no son castigados en México?", consultado en: https://vanguardia.com.mx/articulo/sabias-que-los-ataques-informaticos-no-son-castigados-en-mexico

No solo porque pueden afectar a los particulares, sino que también afecta al estado mismo, ante las nuevas tecnologías de interconexión que tenemos como son las páginas de nuestras Secretarias de Estado y toda la red informática que hay de cada una de ellas en su actuar, es necesario que vayamos pensando en la creación de una legislación especial en la materia, además de que resulta evidente poder dotar de las herramientas suficientes para la persecución delictiva a través cometida en la Tecnologías de la Información y Comunicación.

Pues a decir de la Perspectiva de ciberseguridad en México, de junio de 2018, el avance tecnológico que beneficia a la población se encuentra habilitado por una infraestructura invisible de sistemas digitales que permiten la transmisión y manejo de datos, así como complejos procesos computacionales.

Esta red también afecta nuestras interacciones con negocios físicos (*brick and mortar*), y aunque realicemos actividades fuera de la red dependemos de la conectividad y de las TI.

Se estima que la carga computacional2 de centros de datos crezca 19% anualmente en los próximos 7 años. Si la tasa se mantiene, el crecimiento de dispositivos para el 2025 necesitará más de 300% del poder computacional de centros de datos. Por lo menos 94% de este poder estará distribuido de forma global y descentralizada en la nube (*Cloud computing*).

Las operaciones de las empresas y organismos que empleen procesamiento en la nube dependen de la integridad de centros de datos distribuidos alrededor del mundo.

Si bien hoy en día contamos con el Centro Nacional de Investigación (CNI), el establecimiento de la Dirección de Ciberseguridad en el Banco de México y la creación del CERT-MX dentro de la Policía Federal, y son una clara muestra de los avances en los mecanismos de respuesta nacional.

Resulta necesaria la creación de una agencia nacional dedicada a este objetivo y que la misma pueda coadyuvar con los tres niveles de gobierno y que para reforzar el marco normativo esta legislación que como todas las legislaciones pueden ser perfectibles, sea una muestra más clara de tipificación del ciberdelito, la cual hoy se encuentra fragmentada en códigos locales y federales y dejan en ambigüedad su relevancia jurídica, por ello, esta Ley representa un paso más en la búsqueda de soluciones pertinentes a la necesidad creciente en materia de ciberdelitos..

Aunado a lo anterior, con esta Legislación podrían replicarse a profundidad estas experiencias tanto a nivel estatal y en otras dependencias clave para asegurar que las entidades disponen de capacitación adecuada y puedan colaborar efectivamente entre ellas y mejor aún, se podrían celebrar convenios de intercambios de experiencias y colaboraciones con otras agencias internacionales en la materia.

Sin duda alguna las medidas de fomento de la confianza a esta Iniciativa, constituyen un reto para todos los estados que han intentado regular el uso de las Tecnologías de la Información y Comunicación, por ello hoy vengo a presentarles la siguiente legislación, no como un mecanismo de control social sino como la necesidad de regular las conductas antijuridicas que tiene lugar dentro del ciber espacio a fin de erradicar lo que comencemos coloquialmente como ciberdelitos que hoy por hoy perjudican a más y más personas.

Esta iniciativa surge como la necesidad de salvaguardar a nosotros mismos, familiares, hijas e hijos y cualquier persona que tenga acceso a estas herramientas tecnológicas, que nacieron con el fin de facilitar nuestra vida diaria, y que sin duda así ha sido, pero que lamentablemente personas mal habidas han desfigurado su uso y se han aprovechado del hueco legal existen para llevar a cabo la comisión delictiva en el ciberespacio y en general en las Tecnologías de la Información y Comunicación.

Por lo anteriormente expuesto, someto a consideración de esta honorable Asamblea el siguiente:

**Decreto por el que se reforman y derogan diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se Expide la Ley de Seguridad Informática.**

**PRIMERO.** Se Reforman y Derogan Diversas Disposiciones del Título Noveno, Libro Segundo del Código Penal Federal, para quedar como sigue:

**CÓDIGO PENAL FEDERAL.**

**LIBRO SEGUNDO**

**TITULO NOVENO**

**De las amenazas y delitos cometidos en contra de la Seguridad Informática y las Tecnologías de la Información y Comunicación**

**Artículo 210**.- Los delitos en contra de la Seguridad Informática, Internet o Tecnologías de la Información y Comunicación; así como los delitos vinculados, deben ser perseguidos, investigados, procesados y sancionados conforme a las reglas de autoría, participación y concurso previstas en la legislación especial en la materia, y las reglas de acumulación de procesos previstas en el Código Nacional de Procedimientos Penales.

**Artículo 211**.- Para efectos de delitos cometidos en contra de las instituciones que integran el sistema financiero a través de las Tecnologías de la Información y Comunicación, se sancionaran de conformidad con lo previsto en la legislación especial en la materia.

**Artículo 211 Bis**. - Derogado

**Artículo 211 bis 1**.- Derogado

**Artículo 211 bis 2**.- Derogado

**Artículo 211 bis 3**.- Derogado

**Artículo 211 bis 4**.- Derogado

**Artículo 211 bis 5**.- Derogado

**Artículo 211 bis 6**.- Derogado

**Artículo 211 bis 7**.- Derogado

**SEGUNDO.** Se expide la Ley de Seguridad Informática, para quedar como sigue:

## LEY DE SEGURIDAD INFORMÁTICA

### TÍTULO I

### Disposiciones Preliminares

**Artículo 1.-** La presente Ley es de orden público, interés social y observancia general en todo el territorio nacional. Tiene por objeto establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la Seguridad Informática, en sus respectivos ámbitos de competencia; así como establecer los tipos penales en materia de Seguridad Informática en armonía con lo previsto en la Ley penal vigente, así como integrar la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea; a fin de regular los instrumentos legítimos para fortalecer los controles aplicables a la materia.

**Artículo 2.-** Los delitos en contra de la Seguridad Informática, Internet o Tecnologías de la Información y Comunicación; así como los delitos vinculados, deben ser perseguidos, investigados, procesados y sancionados conforme a las reglas de autoría, participación y concurso previstas en la legislación penal aplicable, y las reglas de acumulación de procesos previstas en el Código Nacional de Procedimientos Penales.

**Artículo 3.-** Corresponde a la Secretaría de Seguridad y Protección Ciudadana, a través de la Agencia de Nacional de Seguridad Informática, el coordinar y determinar la política en la materia de Seguridad Informática, así como dictar lo lineamientos que permitan articular las acciones aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las Tecnologías de la Información y Comunicación de manera segura y responsable para el desarrollo sostenible del Estado Mexicano.

La Agencia Nacional de Seguridad Informática (ANSI) es un órgano especializado dependiente de la Secretaría de Seguridad y Protección Ciudadana, cuyo objetivo central será emitir lineamientos y acciones de prevención e investigación de conductas ilícitas a través de medios informáticos, monitoreo de la red pública de Internet para identificar conductas constitutivas de delito, efectuando actividades de investigación en la red de Internet, así como de ciberseguridad para la reducción, mitigación de riesgos de vulnerabilidades, amenazas y ataques cibernéticos que permitan salvaguardar la Seguridad Informática nacional.

Los procedimientos y acciones destinadas para dichos fines respetaran plenamente los derechos humanos en todo el territorio nacional, prestando auxilio y protección a las entidades federativas y los municipios, frente a riesgos y amenazas que comprometan o afecten la seguridad informática en los términos de la presente Ley.

Dicha agencia contara con un órgano de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá la obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

**Artículo 4.-** Para los efectos de la presente Ley, se entenderá por:

I. **Activo de información.** Es toda aquella información y medio que la contiene, que por su importancia y el valor que representa para cualquier dependencia o entidad de la Administración Pública Federal, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y Alcaldías, así como los particulares, debiendo ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

II. **Activos de las Tecnologías de la Información y Comunicación (TIC)**. Son los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, componentes, bases de datos o archivos electrónicos y la información contenida en éstos.

III. **Agencia Nacional de Seguridad Informática (ANSI)**: Es un órgano especializado y dependiente de la Secretaría de Seguridad y Protección Ciudadana, cuyo objetivo central será emitir lineamientos y acciones de prevención e investigación de conductas ilícitas a través de medios informáticos, monitoreo de la red pública de Internet para identificar conductas constitutivas de delito, efectuando actividades de ciber-investigaciones, así como de ciberseguridad en la reducción, mitigación de riesgos de vulnerabilidades, amenazas y ataques cibernéticos que permitan salvaguardar la Seguridad Informática en territorio nacional.

IV. **Amenaza.** Cualquier posible acto que pueda causar algún tipo de daño a los activos de información de las dependencias o entidades de la Administración Pública Federal, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y las Alcaldías de la Ciudad de México, así como los particulares.

V. **Catálogo Nacional de Infraestructuras Críticas de Información.** Relación de las Infraestructuras Críticas de Información de los diferentes sectores del país.

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

VII. **Ciber-ataque.** Acción realizada a través de las redes de telecomunicaciones con el objetivo de dañar las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas.

VIII. **Ciberdefensa**. Conjunto de acciones, recursos y mecanismos del estado en materia de seguridad nacional para prevenir, identificar y neutralizar toda ciber-amenaza o ciber-ataque que afecte a la infraestructura crítica nacional.

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

X. **Ciberespacio.** Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas

y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico.

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

XII. **Datos Informáticos.** Es toda aquella representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

XIII. **Datos Personales.** Cualquier información concerniente a una persona física identificada o identificable.

XIV. **Datos Relativos al Tráfico.** Se entenderá como los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que un elemento del sistema de comunicación, y que indique el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

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

XVI. **Proveedor de servicios:** será toda entidad pública o privada que ofrezca servicios de comunicación a través de un sistema informático.

XVII. **Redes Sociales:** es la estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación, mediante el intercambio de información.

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

XIX. **Sistema Informático:** todo dispositivo o conjunto de dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa informático.

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

XXI. **Tecnologías de Operación (TO).** Hardware o software que detecta o genera un cambio a través del control y/o monitoreo de dispositivos físicos, procesos y eventos en las instituciones.

XXII. **Unidad de Medida y Actualización (UMA).** Es la unidad de cuenta, índice, medida o referencia económica en pesos sirve para determinar la cuantía del pago de las obligaciones y supuestos previstos en las leyes federales, de las entidades federativas, así como de las disposiciones jurídicas que emanen de todas ellas.

XXIII. **Vulnerabilidades.** Las debilidades identificadas en la ciberseguridad dentro de las dependencias o entidades de la APF, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y Delegacionales, así como los particulares que potencialmente permiten que una amenaza afecte los activos de TIC, a la Infraestructura Información Esencial, así como a los Activos de Información.

**Artículo 5.-** La Seguridad Informática se rige por los principios de legalidad, responsabilidad, respeto a los derechos humanos y garantías individuales y sociales, confidencialidad, lealtad, transparencia, eficiencia, coordinación y cooperación.

## TÍTULO II

## De las Amenazas contra la Seguridad Informática

**Artículo 6.-** Para los efectos de la presente Ley, se entenderá como amenazas contra la Seguridad Informática:

I. Cuando se tenga acceso deliberado e ilegitimo dentro de un sistema informático, con la intención de obtener datos personales.

II. La interceptación deliberada e ilegítima a través de medios técnicos de datos informáticos en transmisiones no publicas dirigidas a un sistema informático, originadas y un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informáticos que sirva comedio de transporte de dichos datos informáticos.

III. Actos tendientes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, a través del ciberespacio;

IV. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación a los activos de información, así como a los activos de las Tecnologías de Información y la Comunicación;

V. Actos que impidan a las autoridades actuar contra la ciberdelincuencia;

VI. Actos que tiendan a dar usos indebidos a los datos informáticos y personales, así como los relativos al tráfico en un sistema informático o dentro del internet;

VII. Actos tendientes para obstaculizar o bloquear actividades de inteligencia o contrainteligencia dentro de la ciberdefensa, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos;

VIII. Actos tendientes para destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos a través de internet.

IX. Actos deliberados e ilegítimos que dañen, borren, deterioren, alteren o supriman datos informáticos, contenidos dentro de los sistemas informáticos del Estado y particulares.

X. La producción, venta, obtención para su utilización, importación, difusión u otra forma de las Tecnologías de Operación, en atención a los derechos de autor vigentes en la materia.

## TÍTULO III

## CAPITULO PRIMERO

### De los Delitos y Vulnerabilidades de los Sistemas Tecnológicos de Información

**Artículo 7.-** Se entenderá como acceso deliberado o ilegitimo a las Tecnologías de Operación, al que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático y utilice las Tecnologías de la Información o la Comunicación, por lo que se le impondrá una pena de cuatro a ocho años de prisión y una multa de cuatrocientos a ochocientos UMA.

En igual circunstancia se castigará al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, contra sistemas bancario, entidades financieras o cuando el autor sea el encargado de administrar, dar mantenimiento o soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 8.-** Se entenderá como acceso deliberado o ilegitimo a los Datos Informáticos y demás Activos de Información, al que, con la intención de usar cualquier dispositivo de la Tecnología de la Información y Comunicación, accediera parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, se impondrá una pena de seis a diez años de prisión y una multa de quinientos a novecientos UMA.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 9.-** Se entiende como interferencia al Sistema Informático, al que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático, de forma temporal o permanente, se le impondrá una pena de ocho a catorce años de prisión y una multa de novecientos a mil seiscientas UMA.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 10.-** Causa daños a sistemas informáticos el que destruye, daña, modifica, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice activos de las TIC o cualquiera de los componentes que conforman las TO, se le impondrá una pena de cuatro a ocho años de prisión y una multa de cuatrocientos a ochocientos UMA.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 11.-** Se cometen delitos y vulnerabilidades contra los sistemas tecnológicos de información cuando utilizando las Tecnologías de la Información y Comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o

preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, por lo que se le impondrá una pena de cuatro a ocho años de prisión y una multa de cuatrocientos a ochocientos UMA.

La comisión de este delito se considerará agravada cuando en la comisión del delito descrito sea funcionario público, aumentando la pena hasta en dos terceras partes.

## CAPÍTULO SEGUNDO

## De los Delitos Informáticos

**Artículo 12.-** La violación de la Seguridad al Sistema Informático, se efectúa cuando sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, ameritando una sanción que va de los cuatro a ocho años de prisión y una multa de cuatrocientos a ochocientos UMA.

En igual supuesto incurrirá quien induzca a un tercero para que de forma involuntaria, ejecute un programa, mensaje, instrucciones o secuencias para violar medidas de seguridad.

No incurrirá en sanción alguna quien ejecute las conductas descritas en los Arts. 8 y 9 de la presente Ley, cuando con autorización de la persona facultada se realicen acciones con el objeto de conducir pruebas técnicas o auditorías de funcionamiento de equipos, procesos o programas.

**Artículo 13.-** Se entenderá dentro de los delitos informáticos que se comete estafa informática cuando se manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para interpósita persona, se le impondrá de seis a doce años de prisión y una multa de quinientos a novecientos UMA.

En igual circunstancia se castigará al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, contra sistemas bancario, entidades financieras o cuando el autor sea el encargado de administrar, dar mantenimiento o soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 14.-** Se entiende por fraude informático, al que, por medio del uso indebido de las Tecnologías de la Información y Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, se le impondrán de dos a ocho años de prisión y de trescientos a novecientas UMA.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 15.-** Para efectos de la presente Ley se entiende que realiza espionaje informático, al que con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y Comunicación o en cualquiera de sus componentes, se le impondrá de cinco a diez años y una multa de seiscientos a mil doscientos UMA.

Si alguna de las conductas descritas en el párrafo anterior se comete con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, se le impondrá una pena de diez a veinte años y multa de novecientos a dos mil UMA.

En misma concordancia con las penas establecidas en el presente artículo se castigará todo ciber-ataque que se dé contra Infraestructuras Críticas de Información.

## CAPÍTULO TERCERO

### De los Delitos Informáticos Relacionados con el Contenido De Datos

**Artículo 16.-** Se entiende que existe manipulación indebida de registros informáticos cuando se deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro de acceso, se le impondrá una pena de cuatro a ocho años de prisión y una multa de cuatrocientos a ochocientos UMA.

De igual manera se da una manipulación de Tecnologías de Información y Comunicación en materia financiera, cuando intencionalmente y sin la debida autorización por cualquier medio cree, capture, grabe, copie, altere, duplique, clone o elimine datos informáticos contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; con el objeto de incorporar, modificar usuarios, cuentas, registros, consumos no reconocidos, la configuración actual de éstos o de los datos en el sistema.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 17.-** Se entiende que existe alteración, interferencia o vulnerabilidades a los Datos Relativos al Tráfico, cuando se violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento e interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos e ineficaces, para alterar o destruir los datos de un tercero, se le impondrá una pena de cinco a nueve años de prisión y una multa de quinientos a mil UMA.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

**Artículo 18.-** Se puede hurtar la identidad de las personas a través de sus datos dentro de las Redes Sociales y las Tecnologías de Operación de un sistema Informático en el Ciberespacio cuando se suplante, se apoderare de la identidad de una persona natural o jurídica, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, por medio de las Tecnologías de la Información y Comunicación se le impondrá una pena de cuatro a ocho años de prisión y una multa de cuatrocientos a ochocientos UMA.

Esta acción deberá considerarse agravada cuando las conductas descritas en el párrafo anterior se cometan en perjuicio de propiedades del Estado, aumentando la penalidad antes mencionada, hasta en dos terceras partes.

## CAPITULO CUARTO

## De la Propiedad Intelectual en los Sistemas Informáticos

**Artículo 19.-** Se castigará con prisión de cinco a nueve años de prisión y una multa de quinientos a cinco mil UMA, a quien deliberadamente, a escala comercial por medio de un sistema informático o a través del uso de las Tecnologías de la Información y Comunicación, copie, manipule o reproduzca sin consentimiento previo de conformidad a la legislación aplicable, en materia derechos de autor.

## CAPITULO QUINTO

## Del Acoso Sexual, la Trata de Personas y la Pornografía Infantil en el Ciberespacio

**Artículo 20.-** Para efectos de la presente Ley, se entiende como Acoso Sexual a través de las Redes Sociales y las Tecnologías de la Información y Comunicación, al que realice alguna conducta sexual indeseada por quien la recibe, que implique

frases, señas u otra conducta inequívoca de naturaleza o contenido sexual, por medio del uso de los Activos de las Tecnologías de Información y Comunicación, por lo que se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil UMA.

**Artículo 21.** Comete el delito de chantaje sexual por medio del uso de los Activos de las Tecnologías de Información y Comunicación, quien amenaza de difamación pública o daño semejante para obtener algún provecho pecuniario o material de alguien y lo obliga a actuar de una determinada con la finalidad de obtener dicho beneficio propio o de un tercero en perjuicio de la víctima, por lo que se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil UMA.

De igual manera, castigará a quien difunda, revele, publique, ceda o comercializa imágenes, materiales audiovisuales o audios con contenido sexual de cualquier persona, que obtuvo con su anuencia, se le impondrá una pena de cinco a nueve años de prisión y multa de quinientos a mil doscientas UMA.

**Artículo 22.-** Se entiende como delitos relacionados con la pornografía infantil en el Internet y las Redes Sociales cuando se fabrique, transfiriera, difunda, distribuya, alquile, importe, exporte, ofrezca, financie, comercie, ejecute, exhiba o muestre material pornográfico a través de un sistema informático. Que se entenderá como todo material que contenga la representación visual de un menor adoptando un comportamiento sexualmente explicito; o simule ser un menor adoptando un comportamiento sexual explicito. Para efectos del presente artículo, se entenderá como menor a toda persona que sea menor a los 18 años; por lo que al autor de este delito se le impondrá pena de siete a catorce años de prisión y de ochocientos a dos mil UMA.

**Artículo 23.-** Se da la utilización de niñas, niños, adolescentes o personas con discapacidad en pornografía a través del uso de las Redes sociales y las Tecnologías de la Información y Comunicación, cuando por cualquier medio que involucre el uso de las Tecnologías de la Información y Comunicación produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda de cualquier forma, imágenes, videos o exhiba en actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, o utilice la voz de niñas, niños, adolescentes o personas con discapacidad, se le impondrá la pena de siete a catorce años de prisión y de ochocientos a dos mil UMA, así como el decomiso de los objetos, instrumentos y productos del delito.

**Articulo 24.-** Dentro del ciberespacio se pueden cometer los delitos de Lenocinio y Trata de Personas a través de las Tecnologías de la Información y Comunicación, mismos que se castigarán y perseguirán de conformidad a lo establecido tanto en el Código Penal Federal como en la Ley para Prevenir y Sancionar la Trata de Personas.

## CAPITULO SEXTO

### Delitos Financieros a través de las Tecnologías de la Información y Comunicación

**Artículo 25.-** Los delitos financieros cometidos a través de las Redes Sociales y las Tecnologías de la Información y Comunicación a través del Ciberespacio, es aquel que se realiza sin autorización y a nombre de un tercero, mediante el uso de las Tecnologías de Operación, venda o comercialice bienes o servicios, suplantando la identidad del productor, proveedor o distribuidor autorizado.

Motivo por el cual, se castigará la comisión delictiva en materia de delitos financieros en el ciberespacio, de conformidad con lo establecido en la Ley para Regular las Instituciones de Tecnología Financiera

## TÍTULO IV

### De la Estrategia Nacional de Ciberseguridad y la Agencia Nacional de Seguridad Informática

**Artículo 26.-** Dentro del Plan Nacional de Desarrollo y en el programa que de él se derive, se definirán los temas de Seguridad Informática, de conformidad con lo establecido en materia de Seguridad Nacional a partir de la cual se creara una Estrategia Nacional de Ciberseguridad.

La Estrategia Nacional de Ciberseguridad será un plan integral, transversal capaz de adaptarse y mejorar continuamente de conformidad a los retos, riesgos, amenazas y vulnerabilidades inherentes a las TIC.

**Artículo 27.-** Dentro de la Estrategia Nacional de Ciberseguridad se emitirán los lineamientos que permitan articular las acciones aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las Tecnologías de la Información y Comunicación de manera segura y responsable para el desarrollo sostenible del Estado Mexicano en sus tres ámbitos de gobierno.

**Artículo 28.-** Los procedimientos y acciones de la Estrategia Nacional de Ciberseguridad respetaran plenamente los derechos humanos en todo el territorio nacional.

**Artículo 29.-** Corresponde a la Agencia Nacional de Seguridad Informática (ANSI), el coordinar y determinar la política en la materia de Seguridad Informática, así como dictar lo lineamientos que permitan articular las acciones aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las Tecnologías de la Información y Comunicación de manera segura y responsable. Así como crear el Catálogo Nacional de Infraestructuras Críticas de Información.

La actuación de la Agencia Nacional de Seguridad Informática deberá sujetarse a los efectos de investigación o de procedimientos penales contemplados en el Código Nacional de Procedimientos Penales, y de ser necesario podrá reservarse el derecho de actuación en las restricciones a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios.

La Agencia Nacional de Seguridad Informática, podrá en todo momento obtener o grabar con medios técnicos propios la obtención en tiempo real de datos relativos al tráfico, y es obligación de los proveedores de servicios colaborar en todo momento con dicha agencia.

**Artículo 30.-** Es obligación de la Agencia Nacional de Seguridad Informática, trabajar en materia de policía cibernética, salvaguardando y garantizando en todo momento una protección adecuada de los derechos humanos y libertadas de manera proporcional, teniendo en cuenta la naturaleza de procedimiento se dictarán las condiciones de supervisión judicial en la aplicación de dichos procedimientos de actuación, la restricción anterior queda sin efectos cuando se traten de temas de interés o de seguridad nacional.

Quedará bajo resguardo de la Agencia Nacional de Seguridad Informática la conservación de datos informáticos almacenados incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o modificación a fin de tener dichas bases de datos para cuando sean requeridas por las autoridades competentes.

Así como prestar auxilio y protección a las entidades federativas y los municipios, frente a riesgos y amenazas que comprometan o afecten la seguridad informática en los términos de la presente Ley.

**Artículo 31.-** Corresponde a gobiernos de las entidades federativas, en el ejercicio de las atribuciones que les correspondan por virtud de lo previsto en el presente Capitulo, cooperar en todo momento con la Agencia Nacional de Seguridad Informática.

Los proveedores de servicios, en todo momento, están obligados a cooperar con la Agencia Nacional de Seguridad Informática en los requerimientos que sean solicitados, para determinar los datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático, dispositivo de almacenamiento informático, así como un listado de los servicios que brindan en el territorio nacional.

Para efectos del párrafo anterior se deberá constar con un listado de proveedores de servicios que contemple, el tipo de servicio de comunicación brindado o utilizado, las técnicas utilizadas al respecto, periodo de servicio, identidad, dirección IPS, situación geográfica, puntos de acceso y de interconexión y cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación.

El incumplimiento de los dos párrafos anteriores será motivo de suspensión permanente de las concesiones y permisos otorgados a los proveedores de servicios además de una multa de mil a treinta mil UMA.

**Artículo 32.-** Para efectos de la presente Ley, se garantizará la cooperación de los poderes y órganos de gobierno de las entidades federativas en la función de garantizar la Seguridad Informática, por lo cual se establecerá la obligación de aportar cualquier información del orden local a la Agencia de Nacional de Seguridad Informática (ANSI), así como colaborar con las autoridades a fin de lograr una coordinación efectiva y oportuna de políticas, acciones y programas previstos en la Estrategia Nacional de Ciberseguridad, con la finalidad de promover la participación de las Entidades y los Municipios en las políticas, acciones y programas en materia de Seguridad Informática.

## TÍTULO V

## Disposiciones Finales y de Cooperación Internacional

**Artículo 33.-** Lo previsto en la presente Ley serán aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas en que se incurra. Para la deducción de la responsabilidad civil se estará a lo dispuesto en la normativa aplicable.

**Artículo 34.-** A falta de previsión expresa en la presente Ley, se estará a las siguientes reglas de supletoriedad:

**I.** Respecto del apoyo que deban prestar las Instancias se estará a lo dispuesto en la Ley General del Sistema Nacional de Seguridad Pública;

**II.** En lo relativo al régimen disciplinario de los servidores públicos que integran la Agencia de Nacional de Seguridad Informática (ANSI), se aplicará la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos;

**III.** Con referencia al control judicial de la inteligencia para la Seguridad Informática, será aplicable en lo conducente el Código Federal de Procedimientos Civiles y Penales vigentes, así como lo establecido en la Ley Orgánica del Poder Judicial de la Federación;

**IV.** En materia de coadyuvancia y de intervención de comunicaciones privadas, será aplicable el Código Federal de Procedimientos Penales y la Ley Federal contra la Delincuencia Organizada;

**V.** Por cuanto hace a la información de Seguridad Nacional, se estará a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y

**VI.** Para el resto de los aspectos, se aplicarán los principios generales del derecho.

**Artículo 35.-** El Estado podrá celebrar convenios de colaboración generales y específicos que deriven de la presente Ley, con otros Estados para lograr solicitudes de asistencia mutua de carácter internacional en materia de Seguridad Informática.

En materia de prevención, la ANSI podrá intercambiar información con agencias internacionales sobre nuevas amenazas cibernéticas descubiertas en Tecnologías de Operación y Tecnologías de la Información y Comunicación.

## TRANSITORIOS

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

**SEGUNDO. -** El Ejecutivo Federal emitirá el Reglamento de la ley dentro de los 90 días siguientes a la entrada en vigor del presente Decreto.

**TERCERO. –** La Agencia Nacional de Seguridad Informática a que se refiere esta ley, se integrará dentro de los 120 días siguientes a la entrada en vigor del presente Decreto.

**CUARTO. -** El Reglamento de la Agencia Nacional de Seguridad Informática deberá expedirse dentro de los 90 días siguientes a la entrada en vigor del presente Decreto.

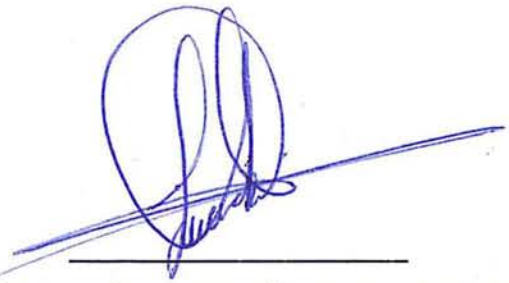
**QUINTO. –** La Estrategia Nacional de Ciberseguridad a que se refiere el Capitulo Octavo de la presente ley deberá realizarse dentro de los 90 días siguientes a la entrada en vigor del presente decreto, tomando en cuenta lo previamente establecido en los lineamientos de acción del antiguo Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT- MX), misma que tendrá que revisarse y actualizarse a los 365 días siguientes a la integración de esta.

**SEXTO. -** Los recursos para llevar a cabo los programas y la implementación de las acciones que se deriven de la presente ley, se cubrirán con cargo al presupuesto autorizado a la Secretaria de Seguridad y Protección Ciudadana, para el presente ejercicio fiscal y los subsecuentes, asimismo, no requerirán de estructuras orgánicas adicionales por virtud de los efectos de esta; de conformidad con lo ya previsto para el funcionamiento Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), referente a las instalaciones, personal y requerimientos utilizados por el antiguo Centro que será de utilidad para la naciente Agencia Nacional de Seguridad Informática.

**SÉPTIMO. -** En un marco de coordinación, las Legislaturas de los Estados, promoverán las reformas necesarias en la Legislación Local, con la finalidad de

armonizar el presente decreto con su legislación vigente, dentro de un término de 6 meses, contados a partir de la entrada en vigor de la presente Ley.

**SUSCRIBE**



**JESÚS LUCÍA TRASVIÑA WALDENRATH**
**Salón de Sesiones, a los 19 días del mes de marzo de 2019**