El suscrito **OMAR FAYAD MENESES**, Senador del Grupo Parlamentario del Partido Revolucionario Institucional de la LXIII Legislatura del Congreso de las Unión, en ejercicio de la facultad conferida en la fracción II del artículo 71 de la Constitución Política de los Estados Unidos Mexicanos, y de los artículos 8, numeral 1, fracción I, 164 y 169 numerales 1, 2 y 4 del Reglamento del Senado de la República, someto a consideración del pleno de la Cámara de Senadores **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL PARA PREVENIR Y SANCIONAR LOS DELITOS INFORMÁTICOS,** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

Internet ha propiciado que muchos sectores de la economía y gobiernos basen su operación en esta red mundial, en el cual millones de personas lo utilizan como parte de su modo de vida actual para la comunicación, consulta de información e incluso para realizar compra venta de artículos y operaciones financieras. La evolución de tecnologías como el Internet ha contribuido al desarrollo de las sociedades que han sabido incorporarlas y aprovecharlas en sus actividades cotidianas. Empresas, gobiernos y países enteros tienen cantidades exorbitantes de información por lo que actualmente controlar la integridad, disponibilidad y confidencialidad del Internet se vuelve un tema fundamental en lo económico y político de las naciones.

Así mismo, con el desarrollo de las tecnologías de información y comunicación (TIC) y el aumento del uso de Internet en los sectores económico, cultural, académico, recreativo y social, se generan circunstancias propicias para aquellos que buscan un beneficio personal en detrimento de otros. Las afectaciones derivadas comparten un origen y una serie de características comunes de la actividad delictiva como el bajo grado de riesgo para el delincuente y el alto grado de efectividad y gran impacto, así como la facilidad de ejecución y el anonimato. En muchos casos, no es imprescindible grandes conocimientos por parte del delincuente para efectuar algún delito cibernético.

Las nuevas tecnologías y la creciente demanda del internet, resultan un campo fértil para la delincuencia, que ha encontrado nuevas formas para consumar delitos a través de medios electrónicos y tecnológicos, los cuales son aprovechados para afectar a la ciudadanía, las empresas y el gobierno.

La tecnología está presente en todos los ámbitos de nuestra vida cotidiana y ha transformado nuestra forma de pensar, de actuar, de relacionarnos, comunicarnos y en general, las herramientas con las que llevamos a cabo nuestras actividades sociales, políticas y económicas.

El uso de internet ha revolucionado nuestro tiempo, es un espacio virtual donde hay una enorme fuente de información, ya que permite acumular el conocimiento humano de múltiples ámbitos en un solo lugar. Ha cambiado la forma de aprender, de estudiar y de hacer investigaciones.

Un signo distintivo ha sido la potenciación de su capacidad como medio de comunicación, ya que pasamos de las páginas web a los sitios interactivos, a la web 2.0, donde existe una interacción en doble vía, entre usuarios con medios como el correo electrónico, los chats, los servicios de mensajería instantánea y las redes sociales.

Esto obliga a transformar también nuestro marco jurídico ya que a través de estos medios se realizan conductas humanas, que tienen efectos en el mundo real, y afectan la esfera jurídica de las personas.

Actividades como el comercio electrónico, el periodismo digital, la publicidad y las opiniones, mensajes o elementos vertidos en redes sociales pueden derivar en menoscabos del patrimonio, la reputación, el honor o la actividad profesional de alguien.

Acciones como el acoso y el contacto en redes sociales con fines de trata de personas, los fraudes, la suplantación de identidad, entre otros son conductas nocivas que están presentes cada vez más.

El incremento de los incidentes va en estricta relación con el incremento del número de usuarios de internet, redes sociales y medios informáticos.

De acuerdo con las cifras de la Unión Internacional de Telecomunicaciones (UIT), en el mundo existen alrededor de **3,000 millones de cibernautas (40% de la población mundial)**[1] con una tasa de crecimiento anual aproximada de 14%. Un estudio realizado por la firma de software Symantec señala que la cifra de víctimas es de aproximadamente **12 víctimas por segundo: 1 millón diarias y 378 millones al año**. El reporte indica que las pérdidas económicas anuales oscilan entre los **375 y 575 mil millones de dólares** (MDD)[2].

Un dato relevante del panorama mundial, es que el Foro Económico Mundial considera las fallas de la infraestructura crítica y los ciberataques como parte de los principales riesgos globales, incluso entre los primeros diez lugares[3].

El uso y abuso de las tecnologías de la información, la incorporación del Internet al mundo real fue avasallador. De tal manera, que los sistemas jurídicos de las naciones no se encontraban preparadas con los mecanismos legales necesarios para afrontar dicha problemática. México, no fue la excepción.

En Latinoamérica, y conforme al estudio realizado por la Organización de Estados Americanos (OEA) en colaboración con la firma de software Trend Micro[4], se presentó un incremento entre el 8% y el 40% en ataques durante 2012, siendo México el mercado más problemático. Dicho aumento se generó en ciberataques y acciones "hacktivistas", lavado de dinero y ataques a infraestructuras críticas.

El robo de la banca en línea ha sido ampliamente reportado en América Latina. Esta actividad presentó características distintivas entre los países, dependiendo del banco o país de destino y la naturaleza de las medidas de autenticación y seguridad que protegen los datos financieros.

De acuerdo al decreto publicado en el diario oficial de la Federación el 11 de junio de 2013, el Estado Mexicano 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.

El escenario en México, de acuerdo con datos de la Asociación Mexicana de Internet (AMIPCI), es el notable incremento en la cifra de cibernautas, pasando de 34.9 millones en 2010 a 53.9 millones en 2014, 43% de la población nacional. Es uno de los países con más actividad en la red según el reporte de la OEA y se espera una cobertura de hasta un 98% con la implementación del proyecto México conectado a cargo de la Secretaría de Comunicaciones y Transportes.

---

[1] Unión Internacional de Telecomunicaciones (2014).
[2] "Reporte Global de Cibercrimen" de Norton (2013).
[3] http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf
[4] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.

La actividad de programas de cómputo maliciosos (malware) también fue una de las principales afecciones, registrándose un incremento del 40% en incidentes cibernéticos en 2012[5]. Se estima que en 2013 la pérdida económica anual en México fue alrededor de los 3 mil MDD según los datos del Reporte Norton de 2013. En países como Alemania la afectación del cibercrimen representa una afectación del 1.6% del PIB, en Estados Unidos del 0.64% y en Brasil del 0.36%, según el estudio publicado por la Unión Internacional en Telecomunicaciones denominado "Comprensión del Ciberdelito, Fenómenos, Dificultades y Respuesta Jurídica".

El Estudio sobre los hábitos del Internet en México realizado por la AMIPCI (2014) indica que 18.4 millones (36%) de cibernautas son personas menores de edad, un gran número de posibles víctimas de delitos contra menores.

El estudio arrojó que el promedio en el tiempo de conexión a Internet de los cibernautas en México es de más de cinco horas al día y que el uso es principalmente para el correo electrónico, redes sociales (9 de cada 10 lo utilizan) y búsqueda de información, en ese orden.

La AMIPCI identificó que en México se incrementó el comercio electrónico en 2014, llegando a movilizar más de 10 mil MDD, lo que representa un 34% más que en el año anterior.

Otro dato relevante de México es la importancia que tienen las micro, pequeñas y medianas empresas (MIPYMES) en el desarrollo económico y social de la nación, ya que datos de Promexico refieren que existen cerca de 4.2 millones de MIPYMES que generan el 52% del Producto Interno Bruto (PIB) y el 72% de los empleos formales. El 95% de ellas son particularmente Pequeñas y Medianas e impulsan de manera relevante el crecimiento económico digital del país con el fortalecimiento de sus infraestructuras tecnológicas[6].

Otro ejemplo, según datos del último Reporte Global de Cibercrimen Norton (2013), en 12 meses, al menos 556 millones de usuarios web en todo el mundo, fueron víctimas de acciones como la recepción de virus o malware, robo de identidad, ciberbullying, hackeo de cuentas, fraude financiero difamación a través de fotografías y filtración de videos íntimos. Esto significó un incremento de 118% respecto de los 255 millones de personas en 2011[7]

Por obvias razones, el estudio señala que el mercado virtual al que se accede mediante teléfonos móviles es el medio donde más crece el cibercrimen. El 48% de usuarios de Smartphone no utiliza medidas de protección básicas como contraseñas de acceso y un 57 % desconoce la existencia de software de protección para dispositivos móviles.

De igual manera, existe el uso de conexiones WiFi inseguras para acceder a cuentas personales (bancarias, correo electrónico o redes sociales), un escenario extremadamente fácil para que quienes cometen cibercrímenes ganen acceso a la información de las personas.

Existen muchas voces que en diversos escenarios ponen en la agenda el incremento de los delitos informáticos, también conocidos como cibernéticos perpetuados tanto por la delincuencia común,

---

[5] Latin American and Caribbean Cybersecurity Trends & Government Responses" (2012).

[6] ProMéxico es el organismo del Gobierno Federal encargado de coordinar las estrategias dirigidas al fortalecimiento de la participación de México en la economía internacional, apoyando el proceso exportador de empresas establecidas en nuestro país y coordinando acciones encaminadas a la atracción de inversión extranjera. Sitio web https://www.promexico.gob.mx/es/mx/home.

[7] El Reporte Norton, ahora en su cuarta edición, es un estudio anual comisionado por la empresa Symantec, que examina los comportamientos, hábitos y peligros de los usuarios digitales, así como los costos del cibercrimen al que están sujetos. En 2013, el estudio recopiló información de 13 mil 22 adultos entre las edades de 18 y 64, a lo largo de 24 países.

como por la organizada, entre ellos, lavado de dinero, fraude, trata de personas, pornografía infantil, entre otros, que no conocen fronteras, e incluso, algunos actos que si bien pudieran considerarse como delitos o medios preparativos para la comisión de un delito, no pueden ser perseguidos y mucho menos sancionados, ya que hasta el momento y por la falta de regulación de la ley, no cuentan con algún tipo penal.

Las contravenciones, conductas nocivas en el ámbito informático han sido definidas tanto por organizaciones internacionales como es el caso de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), estableció en el año de 1983, que el "Computer Crime" es "todo comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos." Desde la academia Gabriel Andrés Campoli los conceptualiza a los delitos informáticos como "aquellos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos" y agrega que "delitos electrónicos o informáticos electrónicos, son una especie del género delitos informáticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios ."[8]

Varios autores han clasificado los delitos informáticos, entre ellos, Irving J. Sloan, Ulrich Sieber, Olivier Hance, Pablo Andrés Palazzi, Gabriela Barrios, Esther Morón Lerma, Antonio-Enrique Pérez Luño y Miguel Ángel Davara Rodríguez, rescatamos aquí la lista hecha por Hiram Piña Libien:

Hacking.- Conducta criminógena por acceso no autorizado a un equipo o sistema informático. Se considera debe ser punible el acceso no autorizado simple y de forma agravada la conducta que además tiene por objeto la producción de daños, que la intrusión tenga un fin específico, que a consecuencia de ello se tenga un resultado específico y, que la conducta tenga por objeto la violación de derechos intelectuales.

Cracking.- Se limita a la vulneración del software comercial acometiendo conductas de piratería informática.

Phishing.- Se trata de correos electrónicos y portales aparentemente enviados por instituciones conocidas como un banco, para que en realidad son falsos, son de una red organizada de delincuentes informáticos en el que piden al usuario que actualice sus datos, pero en realidad se los estará proporcionando para cometer ilícitos.

Evil twins.- Son redes inalámbricas Wi-Fi que aparentan ofrecer conexiones a internet pero solo son una fachada que sirve para robar cualquier número de tarjeta de crédito y contraseñas que se digite usando la conexión.

Pharming.- Se presenta cuando un criminal informático desvía a un consumidor hacía una página electrónica apócrifa, a pesar de que el usuario haya escrito correctamente la dirección electrónica que quiere consultar.

Spamming.- Consiste en el envío masivo de información no solicitada por medio del correo electrónico, generalmente con fines publicitarios.

[8] Cfr. En Delitos informáticos en México de Jorge Esteban Cassou Ruiz [en línea], disponible en: http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_informáticos.pdf

Robo de identidad.- Opera no sólo contra personas físicas, pues también contra personas jurídicas y de derecho público, para ofrecer por ejemplo trámites y pedir pagos por ellos.

Ciberterrorismo.- Se trata de la posibilidad de que sean atacados tanto los sistemas de información como las redes de datos o que estos sean utilizados por y para perpetrar actos terroristas.

Propagación de Malware.- Proveniente de los términos MALicious softWARE, se constituye por programas, documentos o mensajes que pueden causar daños a los equipos de los usuarios a través de las redes de datos

Empleo de tecnologías Pop-Up Ads y Adware.-Son programas que se instalan con o sin el consentimiento de los usuarios informáticos para desplegar en intervalos de tiempo anuncios y mensajes publicitarios que se sobreponen a la aplicación informática en uso.

Instalación de sniffers.- Son analizadores de protocolos que capturan tráfico en una red de cómputo y que pueden ser utilizados para espiar y obtener la información de un usuario u organización.

Spyware o programas espía en las computadoras personales para conocer los hábitos y actividades de familiares o empleados.- Aplicaciones informáticas cuyo objetivo es la recopilación de información personal sin consentimiento del usuario, ya sea para transmitirla a terceros o para vigilar conductas, actividades e información, obtener passwords, estados de cuenta bancarios, conocimiento de su correspondencia electrónica.

Durante la presente administración, diciembre de 2012 a agosto de 2015, la Policía Federal ha emitido más de mil 400 alertas de seguridad dirigidas a las áreas de informática de los tres órdenes de gobierno e instituciones privadas, que fortalecen la tarea de prevención y mitigación de incidentes cibernéticos. Así mismo, mediante la colaboración internacional, la Policía Federal ha podido atender un total de **80 mil 938 incidentes relacionados con ataques cibernéticos**.

- 57% Infección por código malicioso.
- 14% Phishing.
- 13% Vulnerabilidades en infraestructura TIC.
- 11% Acceso lógico no autorizado.
- 4% correo SPAM.
- 0.36% Denegación de servicio.
- 0.34% Ataques de fuerza bruta.
- 0.30% Divulgación de información no autorizada.

A través del Centro Nacional de Atención Ciudadana (088) se han atendido aproximadamente más de **33 mil reportes telefónicos** relacionados con delitos informáticos en el mismo periodo,

- 56.38% delitos por medios electrónicos.
    - Fraude y extorsión (31.07%).
    - Agravio contra personas (21.77%).
    - Denuncia de ilícitos a través de la red (3.54%).
- 36.75% delitos contra la seguridad informática.
    - Phishing (12.86%).
    - Robo de contraseñas (8.82%).
    - Código malicioso (8.09%).
    - Criptolocker (5.51%).
    - Otros (1.47%)
- 6.87% delitos contra menores a nivel nacional.
    - Amenazas contra menores (1.51%).

- Difamación (1.03%).
- Pornografía infantil (0.96%).
- Otros delitos (3.37%).

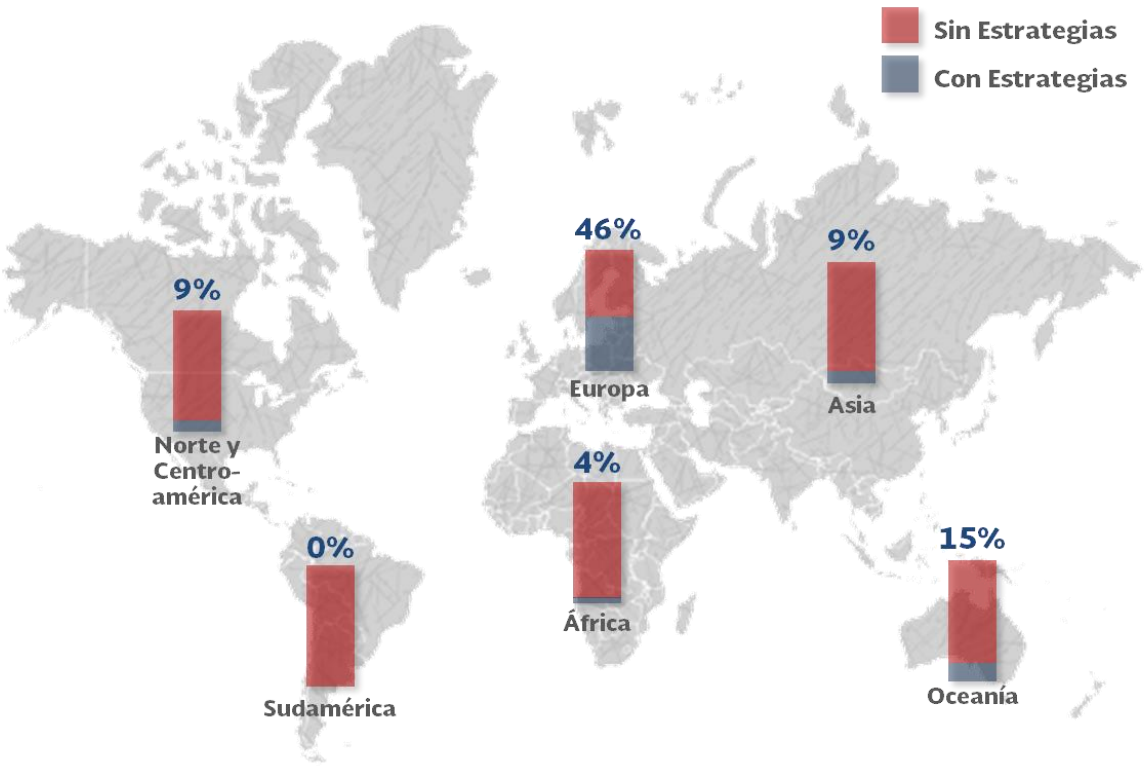
Países que cuentan con Estrategias de Ciberseguridad.

El 16% de los países a nivel mundial, entre los que se encuentran Estados Unidos de América, Canadá y Reino Unido como ejemplo, si cuentan con Estrategias de Ciberseguridad. En México, la Policía Federal, a través de la División Científica, alineado al Plan Nacional de Desarrollo y al Programa Nacional de Seguridad Pública 2013 – 2018, desarrollo la Estrategia de Ciberseguridad a fin de hacer frente a la ciberdelincuencia basada en tres ejes principales. 1) Dirigir acciones de prevención y atención de los delitos cibernéticos, 2) Detección y atención oportuna de amenazas y ataques cibernéticos y 3) Fortalecer las capacidades técnico-científicas para la investigación de delitos cibernéticos.

Prevención y Atención Ciudadana, que busca principalmente fortalecer las capacidades enfocadas a informar y crear una cultura del uso responsable del Internet, atendiendo a los sectores de la población más vulnerables como lo es la niñez mexicana; dando confianza a la ciudadanía fortaleciendo el comercio electrónico y concientizando a los diferentes sectores de la población de los riesgos que podrían presentarse en el Internet si no se toman las medidas preventivas adecuadas, así también se considera el proponer un modelo de policías cibernéticas para el país y la generación de estadísticas de delitos informáticos para el diseño de políticas públicas.

Reducción y mitigación de riesgos y ataques cibernéticos, enfocada principalmente a coordinar a través del Centro Especializado en Respuesta Tecnológica (CERT-MX) de la Policía Federal las acciones de seguridad cibernética para las instalaciones estratégicas informáticas del país, desarrollar y adquirir herramientas especializadas para automatizar y eficientar los procesos de identificación y mitigación de amenazas y ataques cibernéticos, fortalecer grupos de especialización en la detección y atención de incidentes cibernéticos, fortalecer las capacidades de inteligencia del CERT-MX en la prevención e investigación de delitos informáticos, consolidar el intercambio de información y colaboración con policías cibernéticas extranjeras.

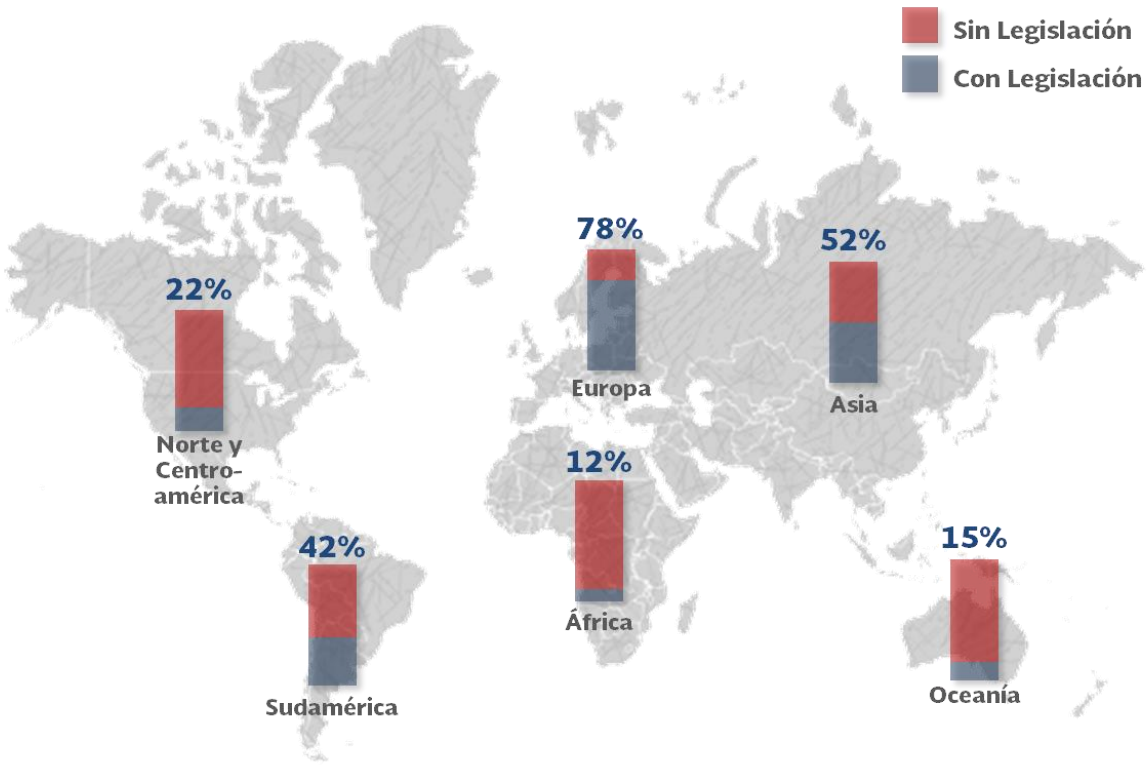
La Estrategia de Ciberseguridad de la Policía Federal considera la colaboración de diferentes sectores del país como son las dependencias gubernamentales (Secretaría de Educación Pública, Secretaría de Economía, Petróleos Mexicanos, Comisión Federal de Electricidad, entre otras), asociaciones y cámaras (Asociación de Bancos de México, Asociación Mexicana de Internet, cámaras de comercio) y asociaciones civiles. Dicha colaboración se realizará en el marco de atribuciones de cada uno de los diferentes actores, lo que permitirá sumar esfuerzos, haciendo compatibles las iniciativas actuales y las que llegaran proponerse en un tema tan relevante en lo económico, social y la seguridad como es el Internet y las tecnologías de la información.



Fuente: http://www.thiber.org/estrategias-nacionales-de-ciberseguridad-en-el-mundo/

Avances de Legislación Nacional en contra el Cibercrimen.

Actualmente el 41% de los países a nivel mundial si cuentan con Legislación contra el Cibercrimen, donde aparte de los mencionados, se ubica aAlemania, Austria, Holanda, Francia y España y Chile. En México se ha incluido el acceso ilícito a sistemas y equipos de informática en el Artículo 211 bis 1 a 211 bis 7 del Código Penal Federal.



Fuente: cybercrimelaw.net/Cybercrimelaw.html

En este contexto, se han hecho esfuerzos institucionales para atender la alta incidencia de estos delitos y uno de ellos, la adecuación al marco legal para poder sancionar muchos de estas conductas, clasificándolas como delitos e imponiéndoles sanciones dentro de las normas penales.

La regulación de los delitos informáticos ha tenido diversas orientaciones, siendo la relevante la relacionada a la protección de datos personales.

El párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos señala que: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos..."

A su vez, la Ley de Protección de Datos Personales en Posesión de Particulares que entró en vigor el 5 de Julio del 2010 en su capítulo XI artículos 168, 169 y 170, habla sobre "los Delitos en Materia del Tratamiento Indebido de Datos Personales".

La Ley Federal de Instituciones de Crédito en el artículo 112 bis fracción IV tipifica la alteración, copia o reproducción de la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero. También el artículo 113 Bis habla de utilizar, obtener, transferir o de cualquier otra forma, se disponga de recursos o valores de los clientes de las instituciones de crédito.

El artículo 194 del Código Federal de Procedimientos Penales habla de la pornografía con menores de edad, pero nunca lo hace desde el punto de vista de las tecnologías de la información. Se puede

tratar de adivinar en la fracción 13 del mismo artículo, escrito que esta copiado en la Ley Federal de Delincuencia Organizada pero en el artículo 2 fracción V.

En el artículo 201 fracción f se habla de "Realizar actos de exhibicionismo corporal o sexuales simulados o no, con fin lascivo o sexual"..." que sean contenidas o reproducidas en medios magnéticos, electrónicos o de otro tipo y que constituyan recuerdos familiares.

El artículo 202 del mismo Código Penal Federal habla de "Pornografía de Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo" y su "publicación, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos"

Otros delitos que están tipificados son sobre el acceso ilícito a sistemas y equipos de informática, propiedad del gobierno, particulares y bancarios, contenidos en el Título Noveno Capítulo II, artículos del 211 Bis 1 al 211 Bis 7, a saber:

TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

CAPITULO I

Revelación de secretos

Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capitulo II

Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos

por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Por otra parte, para las violaciones al derecho de autor, el Código Penal Federal en el artículo 424 bis fracción I, señala "producir, reproducir, introducir al país, almacenar, transportar, distribuir, vender o arrendar copias de obras, fonogramas, videogramas o libros, protegidos..." pero nunca menciona programas de cómputo o bases de datos como la Ley Federal del mismo nombre en el Titulo IV, Capitulo IV que si habla de los Programas de Computación y las Bases de Datos desde el artículo 101 al artículo 114.

Del mismo modo, para la interrupción en un servicio electrónico de conmutación, una red pública de telecomunicaciones por medio de la destrucción física se prevé en el artículo 167 fracción II y en el mismo sentido pero en una red o instalación privada es el artículo 177 del Código Penal Federal.

Como vemos, existen desde el 17 de Mayo del 1999, en que se publicaron en el Diario Oficial de la Federación por primera vez, figuras relacionadas con los delitos informáticos.

No obstante lo anterior, diversos juristas señalan que existe en la norma jurídica mexicana un rezago sobre el tema de los delitos informáticos.

Más allá de tales análisis jurídicos, las estadísticas señalan que los delitos informáticos no han dejado de presentarse, por el contrario van en aumento, tal como lo señalábamos anteriormente.

Por todas estas circunstancias, es importante seguir avanzando en el diseño de nuevas leyes que puedan regular de manera más amplia y contundente las sanciones a aplicarse en la comisión de

estos delitos, y del mismo modo, actualizar el catálogo de conductas a sancionar según la evolución de los mismos,

El Modelo de Policía Cibernética en México.

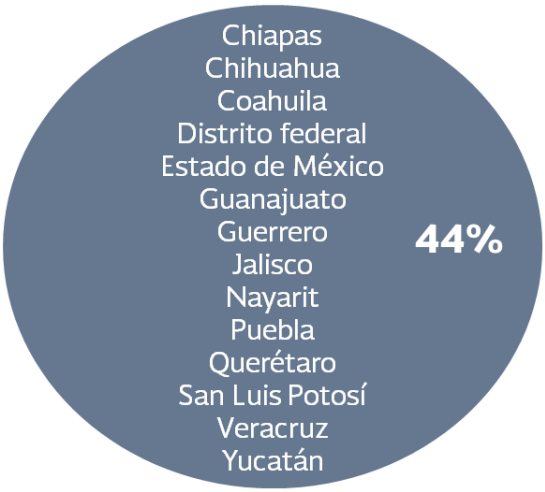
Ante este panorama, no se puede dejar al azar la prevención, investigación y persecución de estos delitos, por lo que se requiere de cuerpos especializados dentro de las instituciones de seguridad pública que puedan hacer frente con eficacia a las actividades delictivas que se están cometiendo con dispositivos informáticos y el uso de Internet, respuesta que va surgiendo con la instauración de policías cibernéticas en el país.

El Programa Nacional de Seguridad Pública (PNSP) ha establecido en su estrategia 2.7.6 el desarrollo de un Modelo de Policía Cibernética para las Entidades Federativas que sentará las bases de coordinación entre la Policía Federal y las Policías Estatales para especialización de las Policías actuales en materia de Ciberseguridad y/o mejora de las Policías Cibernéticas, con el objetivo de Prevenir, Atender e Investigar Delitos Cibernéticos que afectan a la ciudadanía y la infraestructura crítica del Estado Mexicano

La implementación del Modelo de Policía Cibernética en el estado mexicano tiene el objetivo de especializar policías activos con el fin de incrementar la capacidad en la prevención y atención de Delitos Cibernéticos, proponiendo un modelo de operación y los canales de comunicación que sirvan como marco de implementación para la creación y fortalecimiento de las Policías Cibernéticas del País.

El Modelo de la Policía Cibernética Estatal establece la organización y procedimientos para la creación, conformación de la estructura orgánica, capacitación y aplicación de herramientas tecnológicas de la Policía Cibernética Estatal, así también dar la asesoría en la integración del Manual General de Operación que contenga los procesos operativos.

Actualmente 14 entidades federativas cuentan con una unidad cibernética estatal o similar, sin embargo requieren de fortalecimiento, su capacidad de actuación en la prevención, atención e investigación de delitos cibernéticos es limitada.



Consideración de Herramientas Jurídicas para la Investigación y Sanción de Delitos Informáticos.

El delito cibernético es de naturaleza global, ya que se pueden originar desde cualquier parte del mundo donde se tenga acceso a internet, por ello se requiere la colaboración público-privada para prevenir, investigar y sancionar este tipo de delitos, por ello, es necesario considerar, en el proyecto de ley, lo siguiente:

- Herramientas jurídicas a las instituciones encargadas de prevenir, investigar y sancionar los delitos cibernéticos, de tal forma que los operadores de telecomunicaciones y proveedores de servicios de internet, así como los proveedores de servicios y de contenidos en la red tengan la obligación de colaborar con las autoridades para prevenir u obtener información que puede identificar a los presuntos responsables o que permita generar nuevas líneas de investigación (Considerar la Ley Federal de Telecomunicaciones y otros ordenamientos).

- Establecer mecanismos de colaboración internacional, que permita prevenir, identificar, detener o neutralizar un ataque originado desde el extranjero o bien que permita obtener información de prueba o evidencia de tal forma que se pueda identificar a los presuntos responsables o generar nuevas líneas de investigación (Considerar los tratados de asistencia legal mutua).

Mecanismos Internacionales de Colaboración

Se requiere contar con instrumentos jurídicos que permitan un margen de actuación dinámico a las autoridades y que brinden obligatoriedad a los proveedores de servicios de comunicación electrónicas, al igual que con operadores y proveedores de servicios de internet en México, a proporcionar información a petición de la autoridad sobre la cuenta y contenido de las comunicaciones, para atención de investigaciones cibernéticas.

Actualmente, México cuenta con los siguientes:

a) Alianza Global contra el abuso sexual de niños en internet.

México forma parte a través de la Procuraduría General de República. (Promovido por E.U y la Unión Europea; conformado por más de 50 países). Colaboración de diversos países e interpol que tie**ne como finalidad el intercambio de información y mejores prácticas** para identificar y proteger a las víctimas de estos delitos y castigar a quienes los cometan.

Para fortalecer el trabajo de la Alianza se ha creado un espacio de intercambio de información de diversas fuentes para identificar a las redes de delincuencia cibernética. También se está trabajando en una plataforma para desarrollar posiciones comunes entre las autoridades de los Estados miembros, y se creará una página virtual que incorpore las iniciativas internacionales destinadas a frenar la delincuencia, en colaboración con la INTERPOL**. La instancia encargada es la PGR.**

b) Centro Nacional para Menores desaparecidos y Explotados (por sus siglas en ingles NECMEC).

Se cuenta con diferentes **mecanismos de denuncia, e intercambio de información**, Se resalta el CyberTipLine que brinda un mecanismo centralizado para que el público y los proveedores de servicios en internet denuncien sospechas de explotación sexual de menores.

Desde agosto de 2011, el CENADEM de la PF colabora con el NCMEC.

c) Coalición Regional contra el Tráfico de Mujeres y Niñas en América Latina y el Caribe.

Trabaja a nivel local, nacional, regional e internacional para promover el derecho de las mujeres y las niñas a una vida libre de violencia y explotación sexual. Cuenta con una Base de datos con información para identificar niñas, niños y adolescentes reportados en el turismo sexual.

d) Convenio Iberoamericano de Cooperación Sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia.

Se firmó en España en la sede de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB).

México recientemente a través del Procuraduría General de la Republica firma este convenio que tiene como objeto **reforzar la cooperación para la adopción de medidas de aseguramiento y obtención de pruebas para lucha contra la ciberdelincuencia**. La COMJIB está formada por 21 miembros.

e) Tratado para la asistencia Legal Mutua y Ley de Privacidad de las Comunicaciones Electrónicas.

Este tratado suscrito con Estados Unidos de Norte América, brinda facilidades a nuestro país para contar con asistencia legal para el tratamiento d los casos internacionales del cibercrimen que sean presentados ante la autoridad de procuración e impartición de justicia en

El convenio de Budapest.

Es imprescindible la celebración de tratados internacionales que fortalezcan la colaboración con Policías Cibernéticas de otros países, y el Convenio de Budapest resulta conveniente para México en virtud de lo siguiente:

- Es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes:

1) La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.
2) La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.
3) Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Los siguientes delitos están definidos por el Convenio: acceso ilícito, interceptación ilegal, la interferencia de datos, la interferencia del sistema, mal uso de los dispositivos, la falsificación informática, el fraude relacionado con la informática, los delitos relacionados con la pornografía infantil y los delitos relacionados con los derechos de autor y derechos conexos.

Asimismo, se exponen cuestiones de derecho procesal como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. Además, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua (con consentimiento o disponibles al público) y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras.

El Convenio es el resultado de cuatro años de trabajo de expertos europeos e internacionales. Se complementa con un Protocolo Adicional que realiza cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del Convenio.[9] México sería el tercer país en Latinoamérica en adherirse al Convenio después de República Dominicana y Panamá.

Otros de los puntos a considerar, son las conductas que si bien no están al momento consideradas como delito, si se observa el incremento como medios de preparación para la comisión de algunos de los delitos relacionados, como se observa en el acercamiento a través de las redes sociales que realizan adultos con menores de edad, simulando a su vez ser menos de edad, quienes al ganarse la confianza de los menores, generan acciones como el envío de imágenes con poca o nada de ropa, en simulaciones sexuales, u otras de ese tipo, con las que posteriormente los extorsionan o presionan para que el contacto se realice de manera presencial abusando de ellos o incluso llegando al asesinato, por lo que es indispensable tipificar las conductas como delito y que con ello la autoridad pueda intervenir antes de que se dé una situación grave.

Es conveniente hacer énfasis que ante la especialidad de los delitos, el incremento de los hechos constitutivos de delitos y la variedad de actores en los delitos informáticos, serían insuficientes señalar las conductas delictivas en reformas al Código Penal, que permitiría que estas se diluyeran entre todos los tipos penales plasmados, que hubiera incidido en una reducción en el impacto buscado, por lo que lo conveniente es plasmarlos en una ley especial, que asegure el nivel jerárquico y la correcta aplicación de la norma hipotética una vez que el sujeto se coloca en el supuesto, lo que incidirá en acciones de prevención del delito, y de castigo.

Por lo que respecta a las sanciones consistentes en multa, se mantienen los salarios mínimos contra los días multa que establece el Código Penal Federal como unidad de medida, para las sanciones pecuniarias de la iniciativa en virtud de:

1. Los días salario mínimo, siguen vigentes en el ámbito federal

2. La propuesta de reforma constitucional en materia de desindexación del salario mínimo, la contempla como “unidad de medida actualizada” y no como “días multa”.

[9] Fuentes: http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm
http://es.wikipedia.org/wiki/Convenio_sobre_cibercriminalidad

3. Apenas fue aprobada en la Cámara de Diputados y se encuentra en el Senado pendiente de aprobación, por lo que no se encuentra vigente.
4. Una vez aprobada por el Congreso, queda pendiente la aprobación de la mayoría de las legislaturas de los estados

5. En caso de ser aprobada, el transitorio cuarto del dictamen de la iniciativa de reforma constitucional en materia de desindexación del salario mínimo, señala un plazo máximo de un año para adecuar la legislación federal, una vez publicada, lo que conllevara en su momento la reforma a esta Ley.

Días multa

Pese a la ya próxima desaparición de las diferentes unidades de medida que se han venido utilizando en los distintos ordenamientos, los días multa se encuentran regulados como una de las varias unidades de medidasplasmada en el Código Penal Federal, ubicando en el artículo 29 para la sanción pecuniaria, establece que es “”la percepción neta diaria del sentenciado en el momento de consumar el delito, tomando en cuenta todos sus ingresos.”

Bajo este criterio, una persona con percepciones antes deducciones y sumando todos sus ingresos, de mil pesos diarios, en los casos demultas de 5,000 DSMV, ascendería a 5 millones de pesos.

EL Código Penal Federal en el mismo artículo 25, contempla la sustitución de la multa por la prestación de trabajos favor de la comunidad, en la que cada jornada de trabajo saldará un día de multa.

Bajo este mismo criterio, en caso de sustitución de penas, se estaría que ante el caso de los 5,000 días multa como sanción menor, equivalen a más de 13 años de jornadas de trabajo, superando los 200 años de estas jornadas.

Situación que independientemente de superar cualquier criterio lógico, caería en el supuesto de penas inusitadas o trascendentales, prohibidas en el mismo artículo 22 constitucional

Un punto adicional a resaltar en relación con la iniciativa, es que con esta no se pretende imponer ningún tipo de censura al uso de Internet y de los dispositivos electrónicos, ya que el único objetivo, es clarificar, catalogar, sistematizar y fijar penas a conductas ya establecidas como delitos en protección de los usuarios, cuando estas son cometidas con o por el uso de Internet o de medios informáticos, con lo que más que un acto de censura, se privilegia con esta iniciativa, la posibilidad de usar Internet de manera libre y razonada a los gustos y necesidades de cada persona, garantizándola la privacidad sin que se incurra en algún riesgo, ante la impunidad con la que los delincuentes se han asentado en Internet.

Por lo antes expuesto, me permito someter a la consideración de ésta H. Cámara de Senadores, el siguiente proyecto de:

DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL PARA PREVENIR Y SANCIONAR LOS DELITOS INFORMÁTICOS:

Artículo único. Se expide la Ley Federal para Prevenir y Sancionar los Delitos Informáticos, para quedar como sigue:

LEY FEDERAL PARA PREVENIR Y SANCIONAR LOS DELITOS INFORMÁTICOS

TÍTULO PRIMERO
DISPOSICIONES GENERALES

Capítulo Único
Ámbito de aplicación y definiciones

Artículo 1. La presente Leytiene por objeto prevenir, investigar, perseguir y sancionar los delitos informáticos, que por su naturaleza, origen, destino e impacto tengan repercusiones jurídicas en el territorio nacional.

Artículo 2. En los casos no previstos en esta Ley serán aplicables los tratados internacionales, el Código Penal Federal, el Código Nacional de Procedimientos Penales, la Ley Federal Contra la Delincuencia Organizada y demás disposiciones relativas y aplicables.

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

I. **Arma Informática:** Cualquier programa informático, sistema informático, o en general cualquier dispositivo o material creado o diseñado con el propósito de cometer algún delito informático.

II. **Ataque Cibernético:**Acción organizada y deliberada de una o más personas con el fin de vulnerar la seguridad, afectar disponibilidad o generar degradación de sistemas computacionales o redes, mediante el uso de armas informática o código maliciosos.

III. **Ciberespionaje:** Acto con el cual se obtienen información secreta en cualquiera de sus modalidades (voz, datos, imágenes) sin el permiso de aquél quien es dueño de la información. Los métodos por los cuales se consigue esta información son exclusivamente informáticos, haciendo uso de armas informáticas, redes de computadoras locales, Internet y/o mediante cualquier técnica informática.

IV. **Cibernética:**Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología.

V. **Código malicioso:**Programa o código de sistema informático creado específicamente para dañar, interrumpir o afectar un sistema informático, así como obtener información o realizar ciberespionaje sobre el equipo o sistema afectado.

VI. **Dispositivo informático:** Conjunto de componentes electrónicos y programas de cómputo que relacionados entre sí ordenadamente permiten el procesamiento, almacenamiento, transmisión y/o visualización de datos o información.

VII. **Delitos informáticos:**Los delitos previstos en esta Ley.

VIII. **Información Sensible de Usuarios:**Toda información que posea un proveedor de servicios y que esté relacionada con el usuario, que permita determinar datos personales, ubicación geográfica, información relacionada con medios de pago o facturación.

IX. **Infraestructura Informática:** Conjunto de sistemas informáticos, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar las tecnologías de la información.

X. **Infraestructura Crítica Nacional:** Infraestructura informática o de control industrial que soporta los procesos sustantivos de los sectores producticos, cuya afectación o vulneración ponen en riesgo la estabilidad de la Nación.

XI. **Instituciones de Seguridad Pública federales:** Las Instituciones Policiales, de Procuración de Justicia, del Sistema Penitenciario y dependencias encargadas de la Seguridad Pública a nivel federal.

XII. **Internet:** Sistema de redes ligadas entre sí por un protocolo común especial de comunicación de alcance mundial, que facilita servicios de comunicación de datos, voz y video.

XIII. **Medios informáticos:** Conjunto de procesos y productos derivados de las nuevas herramientas, soportes de la información y canales de comunicación, relacionados con el almacenamiento, procesamiento y transmisión de archivos electrónicos digitalizados.

XIV. **Programa informático:** Conjunto de instrucciones lógicas y reglas informáticas que integran componentes lógicos necesarios para que una computadora realice una o varias específicas.

XV. **Proveedor de servicios:** Persona física o moral que ofrece servicios de comunicación a través de cualquier sistema informático, o bien, que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

XVI. **Red pública:**Red de computadoras o sistemas informáticos interconectados, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica y sin restricciones de acceso.

XVII. **Seguridad informática:**Prácticas aplicadas en sistemas y dispositivos informáticos a fin de proteger y resguardar su funcionamiento y la información en él contenida.

XVIII. **Sello digital:** Serie de caracteres derivada de la encriptación de la información de la Cadena Original del Comprobante , para evitar su falsificación

XIX. **Sistema Informático:**Conjunto de partes interrelacionadas, hardware y software que permite almacenar, procesar y transmitir datos o información.

XX. **Terrorismo informático:**Es el uso de las tecnologías de información, comunicación e Internet con fines terroristas, como son, la afectación a la infraestructura crítica nacional, realizar acciones de capacitación, entrenamiento, reclutamiento y financiamiento de actividades terroristas, así como la difusión de información con el objetivo de causar pánico y desestabilización de la paz pública.

XXI. **Usuario:**Persona física o jurídica que use o adquiera bienes o servicios de un proveedor de servicios de tecnologías de la información e Internet.

TÍTULO SEGUNDO
DE LA ATENCIÓN A LA SEGURIDAD INFORMÁTICA

Capítulo I
De la Prevención y Coordinación

Artículo 4. Los delitos previstos en esta Ley se prevendrán, investigarán, perseguirán y sancionarán por la Federación, con la colaboración de autoridades correspondientes a todos los órdenes de gobierno, de conformidad con la Ley General del Sistema Nacional de Seguridad Pública y demás disposiciones aplicables.

Artículo 5. Las acciones de prevención de los delitos informáticos tienen por objeto fomentar la cultura de prevención, proximidad y difusión de dichas conductas con el objeto de reducir la incidencia delictiva y las vulnerabilidades informáticas.

Artículo 6. La prevención se efectuará a través de los siguientes mecanismos:

I. Implementación de políticas y procedimientos para la difusión de acciones preventivas respecto a la identificación y denuncia de los delitos informáticos.

II. Vigilancia de la seguridad y los derechos de las personas en la red pública de Internet. .

III. Promociónde las denuncias por la probable comisión de los delitos informáticos ante la autoridad ministerial correspondiente.

Artículo 7. Las Instituciones de Seguridad Pública federal se coordinarán para:

I. Realizar estudios sobre las causas estructurales, distribución geodelictiva, estadísticas, tendencias históricas y patrones de comportamiento que permitan la investigación para la prevención de los delitos sancionados en esta Ley, para lo cual contarán con el apoyo de las entidades federativas, en términos de la Ley General del Sistema Nacional de Seguridad Pública.

II. Obtener, procesar e interpretar la información geodelictiva por medio del análisis de los factores que generan las conductas delictivas previstas en esta Ley.

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

IV. Llevar a cabo campañas nacionales orientadas a prevenir y evitar los factores y causas que originan el fenómeno delictivo sancionado en esta Ley, así como difundir su contenido.

V. Establecer relaciones de colaboración con las autoridades competentes, así como con la sociedad civil,para orientar medidas tendentes a la prevención de los delitos informáticos.

VI. Observar las demás obligaciones establecidas en otros ordenamientos.

Capítulo II
De lasunidades especializadas en la prevención e investigación de los delitos informáticos

Artículo 8. Las Instituciones de Seguridad Pública federal contarán con unidades especializadas en la prevención e investigación de los delitos informáticos, de acuerdo al ámbito de sus competencias. La Federación apoyará y promoverá la creación de unidades cibernéticas en las Entidades Federativas así como su coordinación en términos de los artículos 75 y 76 de la Ley General del Sistema Nacional de Seguridad Pública.

El personal de dichas unidades deberá contar con la capacitación especializada en el campo de las tecnologías de la información y comunicación, áreas afines y demás necesarias, para la adecuada atención de los delitos informáticos.

Artículo 9. La unidad especializada encargada de atender los temas de prevención en la Policía Federal realizará investigación para la prevención de los delitos contenidos en la presente ley, para tal efecto, contará con las siguientes atribuciones:

I. Establecer mecanismos de coordinación y cooperación con gobiernos e instituciones nacionales y extranjeras para prevenir y reducir la comisión de delitos en el país, en coordinación con las autoridades competentes.

II. Salvaguardar la seguridad y los derechos de las personas en la red pública de Internet.

III. Proponerpolíticas y estrategias para la prevención de los delitos informáticos.

IV. Promover la celebración de tratados internacionales y acuerdos interinstitucionales en materia de prevención e intercambio de información para la prevención, relacionada con delitos informáticos y vigilar su cumplimento.

V. Establecer mecanismos para la cooperación de diversos organismos públicos, sociales y privados, tanto nacionales como internacionales para el intercambio de información.

VI. Establecer mecanismosde cooperación con organismos y autoridades nacionales e internacionales relacionados con la prevención de delitos electrónicos.

VII. Operar laboratorios de código maliciosos, electrónica forense, nuevas tecnologías y demás que resulten necesarias para prevenir la comisión de delitos señalados en la fracción II de este artículo;

VIII. Supervisar las acciones necesarias para la investigación de los delitos electrónicos cometidos, requeridas por la autoridad competente;

IX. Gestionar, conforme a las disposiciones aplicables, la cooperación con empresas proveedoras del servicio de Internet para suspendersitios, páginas electrónicas y cualquier contenido que atenten contra la seguridad pública, así como para prevenir y combatir los delitos en los que se utilizan medios electrónicos para su comisión;

X. Promover la cultura de la prevención de los delitos en los que se utilizan medios electrónicos para su comisión, así como la difusión del marco legal que sanciona los mismos;

XI. Generar estadísticas de los delitos informáticos y sistemas de medición tendentes a la generación de mapas geodelictivos y georeferenciados de las conductas previstos en esta Ley.

Artículo 10. La unidad especializada encargada de la investigación y persecución de los delitosinformáticos en la Procuraduría General de la República, tendrá las siguientes atribuciones:

I. Investigar las denuncias relacionadas con los delitos informáticos.

II. La coordinación y cooperación con autoridades federales, en sus esfuerzos comunes para mejorar y dar cabal cumplimiento a las disposiciones de la presente ley.

III. Coordinar la representación de la Federación ante organismos internacionales en materia de investigación y persecución de los delitos informáticos.

TÍTULO TECERO
DE LA COORDINACIÓN

Capítulo I
De la Colaboración con otras Instituciones y con Particulares

Artículo 11. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedoresde servicios de aplicaciones y contenidos, a que hace referencia el artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión, colaborarán en la investigación de los delitos informáticos, por lo que deberán:

I. Proporcionar oportunamente asistencia técnica y la información que requieran las autoridades federales competentes para la investigación de los Delitos Informáticos.

II. Colaborar con las autoridades competentes en las acciones que permitan investigar y perseguir los delitos previstos en esta Ley.

III. Realizar las demás acciones que prevea la legislación aplicable.

Artículo 12. Las Instituciones que integran el sistema financiero colaborarán con la Unidad especializada de la Procuraduría General de la República, en la investigación de los delitos previstos en esta Ley, de conformidad con la Ley de Instituciones de Crédito y demás disposiciones legales aplicables.

Artículo 13. Cuando la comisión de un delito informático se efectúe a través de una infraestructura tecnológica pública, las autoridades estarán obligadas a colaborar con las instituciones de seguridad pública en la investigación correspondiente.

Artículo 14. Los Proveedores de Servicios y en general, toda aquella institución privada que mantenga infraestructura informática para la proveeduría de servicios de telecomunicaciones y de aplicaciones en internet, deberán conservar los datos de tráfico de origen y destino de la comunicación, o cualquier otra información que pueda ser de utilidad a la investigación, en los términos que establece el artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, y las disposiciones reglamentarias que al efecto se emitan.

Capítulo II
De la Coordinación con otros países

Artículo 15. Las Instituciones de Seguridad Pública federal, en el ámbito de sus respectivas competencias promoverán la celebración de tratados internacionales, acuerdos interinstitucionales y demás acciones conjuntas con instituciones de otros países para la prevención, investigación y persecución de los delitos informáticos.

TÍTULO CUARTO
DE LOS DELITOS INFORMÁTICOS

Capítulo I
De los Delitos Contra Sistemas Informáticos

Artículo 16. A toda persona que, sin la autorización correspondiente o excediendo la que le haya sido conferida, acceda, intercepte, interfiera o use un sistema informático, se le impondrá una sanción de uno a ocho años de prisión y multa de ochocientos a mil días de salario mínimo vigente.

Artículo 17. A todo aquel que dolosamente destruya, inutilice, dañe o realice cualquier acto que altere el funcionamiento de un sistema informático o alguno de sus componentes, se le impondrá una sanción de cinco a quince años de prisión y multa de hasta mil días de salario mínimo vigente.

Se sancionará con la misma pena a quien,sin estar autorizado para ello, destruya, dañe, modifique, difunda, transfiera o inutilicela información contenida en cualquier Sistema Informático o en alguno de sus componentes.

La pena será de diez a veinte años de prisión y multa hasta de mildías de salario mínimo vigente, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión dolosa, por cualquier medio, de un arma informática o código malicioso.

Capítulo II
De las Armas Informáticas

Artículo 18. A quien utilice armas informáticas o códigos maliciosos se le impondrán de dos a seis años de prisión y multa de doscientos a quinientosdías de salario mínimo vigente.

Artículo 19. A quien fabrique, distribuya, comercie armas informáticas o códigos maliciososse le impondrán detres a siete años de prisión y multa de doscientos a quinientosdías de salario mínimo vigente.

Capítulo III
Depredador Sexual

Artículo 20. A quien fingiendo una identidad o usando la real, realice el acercamiento entre éste o incluso un tercero, con un menor de edad, a través de redes sociales o cualquier otro medio vía internet, con el propósito de facilitar un encuentro sexual, comete el delito de depredación sexual.

A quien cometa este delito con personas mayores de 15 años y menores de 18 años de edad, se le impondrá una pena de siete a quince años de prisión y multa de quinientos a mil días de salario mínimo vigente.

A quien cometa este delito con personas menores de 15 años de edad, se le impondrá una pena de quince a veintiocho años de prisión y multa de mil a diez mil días de salario mínimo vigente.

Capítulo IV
Intimidación

Artículo 21. A quien, a través de medios informáticos, acose, hostigue, intimide, agreda o profieracualquier forma de maltrato físico, verbal o psicológico en contra de usuarios de Internet, de forma reiterada y sistemática, se le impondrá una pena de seis meses a dos años de prisión y multa de cincuentaa ochenta días de salario mínimo vigente.

Si la conducta descrita en el párrafo anterior es cometida por un servidor público o medie una relación de superioridad laboral o derivada de la influencia que la persona ejerza sobre la víctima, se le aumentará en una mitad de las penas previstas en el primer párrafo.

Capítulo V
De los Delitos contra la Divulgación Indebida de Información de Carácter Personal

Artículo 22.A quien, sin la autorización correspondiente, revele, difunda o ceda, en todo o en parte, información privada referente a imágenes, audio, video o la informaciónsensible de usuarios,obtenidos por cualquier medio, se le impondrán deseis a doce años de prisión y multa de ciento cincuenta a doscientos días de salario mínimo vigente.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para el usuario o para un tercero, la pena se aumentará de un tercio a la mitad.

Artículo 23.A quien, sin la autorización correspondiente, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, contenidos en un Sistema Informático, se le impondrán de seisa doce años de prisión y multa de ciento cincuenta a doscientos días de salario mínimo vigente.

Artículo 24.A quien dolosamente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la información personal de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un ordenador o Sistema Informático, se le impondrán de cinco a diez años de prisión y multa de cien a ciento cincuentadías de salario mínimo vigente.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la información o para un tercero.

Artículo 25.A quien ofrezca o preste servicios destinados a cumplir los mismos fines previstos en este capítulo, se le impondrán de cinco a diez años de prisión y multa de hasta cuarenta días de salario mínimo vigente.

Capítulo VI
De los Delitos Contra el Patrimonio

Artículo 26. A quien, sin estar debidamente autorizado, adquiera, comercialice, posea o distribuya información de tarjetas de crédito, débito o instrumentos financieros o mercantiles de particulares, se le impondrán de dos a seis años de prisión y multa de doscientos a quinientos días de salario mínimo vigente.

Artículo 27. A quien, sin estar la debida autorización, emita, fabrique o distribuya tarjetas de crédito, débito o instrumentos financieros o mercantiles análogos, se le impondrán de veinte a treinta años de prisión y multa de ochocientos a mil quinientos días de salario mínimo vigente.

Artículo 28. A quien, sin estar debidamente autorizado, adquiera, posea, transfiera, comercialice, distribuya, controle o custodie cualquier equipo de fabricación de tarjetas de crédito, débito o de instrumentos financieros o mercantiles, se le impondrán de veinte a treinta años de prisión y multa de ochocientos a mil quinientos días de salario mínimo vigente.

Artículo 29. A quien, sin estar debidamente autorizado, adquiera, posea, transfiera, comercialice, o utilice cualquier equipo o componente que capture, grabe, copie o transmita la información de dichas tarjetas o instrumentos, se le impondrán de veinte a treinta años de prisión y multa de ochocientos a mil quinientos días de salario mínimo vigente.

Artículo 30.A quien, sin autorización para portarla, utilice una tarjeta de crédito o débito o instrumento financiero o mercantil, o el que utilice indebidamente algún medio informático para requerir la obtención de dinero, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, se le impondrán de seis a doce años de prisión y multa de ciento cincuenta a doscientos días de salario mínimo vigente.

Artículo 31.A quien, por cualquier medio cree, capture, grabe, copie, altere, duplique, clone o elimine la información contenida en una tarjeta de crédito o débito, o cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier medio informático, cree, capture, duplique o altere la información en un sistema informático, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, se le impondrán deocho a catorce años de prisión y multa detrescientos a quinientos días de salario mínimo vigente.

Se aplicará la misma pena a quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas de crédito, débito o cualquier instrumento destinado al mismo fin, o de la información contenida en estos o en un sistema.

Artículo 32.A quien se apropie de una tarjeta de crédito, débito o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, se le impondrán decinco a diez años de prisión y multa de ochenta a ciento sesenta días de salario mínimo vigente.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Capítulo VII
Suplantación

Artículo 33. Comete el delito de suplantación de dominio aquel que, mediante el uso de Armas Informáticas falsifica o suplanta un sitio web de un proveedor de servicios, con el objeto de redireccionar al usuario a otro sitio web apócrifo, para obtener información sensible del usuario, siempre que de dicha conducta resulta algún daño o perjuicio, o bien, para cualquier otro fin delictivo.

Al que cometa la conducta prevista en el párrafo anterior, se le impondrán deseis a doce años de prisión y multa de ciento cincuenta a doscientos días de salario mínimo vigente.

A quien publique, replique, comercialice, almacene o distribuyasitios web apócrifos, en el territorio nacional o cualquier otro lugar fuera de él, se le impondrán de cinco a diez años de prisión y multa de cien a ciento cincuentadías de salario mínimo vigente.

Artículo 34. Comete el delito de suplantación de identidad aquel que, mediante el uso de Armas Informáticas suplantela identidad de cualquier persona física o moral, para obtener, capturar, grabar, digitalizar o escuchar información sensible de otros usuarios.

Al que cometa la conducta prevista en el párrafo anterior, se le impondrán deseis a doce años de prisión y multa de ciento cincuenta a doscientos días de salario mínimo vigente.

Las penas se incrementarán en una mitad a quien utilice, comercialice, almacene o distribuya, con fines personales, de lucro o para cualquier otro fin delictivo, la información obtenida en términos del párrafo anterior.

Capítulo VIII
Ataque Cibernético

Artículo 35. Al que convoque, organice, participe o ejecute un Ataque Cibernético,se le impondrán de veinte a treinta años de prisión y multade cien hasta de mil días de salario mínimo vigente.

Capítulo IX
Terrorismo informático

Artículo 35. Se impondrá pena de prisión de veinte a cincuenta y cinco años y multa de dos mil a diez mil días de salario mínimo vigente, sin perjuicio de las penas que correspondan por otros delitos que resulten:

I. A quien utilizando armas cibernéticas, ejecute ataques Infraestructuras Informáticas o infraestructuras Críticas Nacionales, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad o a un particular, u obligar a este para que tome una determinación.

II. A quien lleve a cabo actividades de capacitación, entrenamiento, reclutamiento y financiamiento de actividades terroristas.

III. Al que acuerde o prepare un acto de terrorismo cibernético que se pretenda cometer, se esté cometiendo o se haya cometido en territorio nacional.

Las sanciones a que se refiere el primer párrafo de este artículo se aumentarán en una mitad, cuando además:

a. El delito sea cometido afectando gravemente una Infraestructura Crítica Nacional.

b. Se genere un daño o perjuicio a la economía nacional.

IV. Al que con sus actos afecte cualquier sistema cibernético de información o medios informáticos de la Nación, o

V. En la comisión del delito se tenga en calidad de rehén a una persona o se mantengan el control ilícito parcial o total de un medio informático destinado a la prestación de un servicio público.

Artículo 36. Se impondrá pena de seis a quince años de prisión y multa de quinientos a mil días de salario mínimo vigente, a quien encubra a un terrorista informático, teniendo conocimiento de sus actividades o de su identidad.

Artículo 37. Se impondrá pena de quince a veintiocho años de prisión y multa de mil a diez mil días de salario mínimo vigente al que amenace o publique por cualquier medio impreso, audiovisual o de Internet, con cometer el delito de terrorismo informático a que se refiere el artículo 14 de esta Ley.

Capítulo X
Ciberespionaje

Artículo 38. Se impondrá pena de prisión de seis años a quince años y multa de quinientos a mil días de salario mínimo vigente a la persona que en tiempo de paz, con objeto de guiar a una posible invasión del territorio nacional o de alterar la paz interior, tenga relación o inteligencia a través de medios informáticos, bases de datos digitales militares, o información relacionada con la seguridad nacional, obtenida por medios digitales con persona, grupo o gobierno extranjeros o le dé instrucciones, información o consejos.

La misma pena se impondrá al extranjero o mexicano por nacimiento o naturalización que en tiempo de paz proporcione, sin autorización a persona, grupo o gobierno extranjero, documentos digitales, instrucciones, o cualquier dato de establecimientos o de posibles actividades y bases de datos digitales militares obtenidos por medios digitales.

Se impondrá pena de prisión de quince a veinte años y multa de mil a diez mil días salario mínimo vigente al extranjero o mexicano por nacimiento o naturalización que, declarada la guerra o rotas las hostilidades contra México, tenga relación o inteligencia con el enemigo o le proporcione información o documentos digitales o cualquier ayuda por medios informáticos que en alguna forma perjudique o pueda perjudicar a la Nación Mexicana.La misma pena se impondrá al extranjero o mexicano por nacimiento o naturalización que en tiempo de paz proporcione, sin autorización a persona, grupo o gobierno extranjero, documentos digitales, instrucciones, o cualquier dato de establecimientos o de posibles actividades y bases de datos digitales militares obtenidos por medios digitales.

Se impondrá pena de prisión de quince a veinte años y multa de mil a diez mil días salario mínimo vigente al extranjero o mexicano por nacimiento o naturalización que, declarada la guerra o rotas las hostilidades contra México, tenga relación o inteligencia con el enemigo o le proporcione información o documentos digitales o cualquier ayuda por medios informáticos que en alguna forma perjudique o pueda perjudicar a la Nación Mexicana.

Artículo 39. Se impondrá pena de prisión de seis a quince años y multa de quinientos a mil días de salario mínimo vigente, al mexicano que, teniendo en su poder documentos digitales o informaciones confidenciales de sistemas electrónicos de un gobierno extranjero, los revele a otro gobierno, si con ello perjudica a la Nación Mexicana.

Capítulo XI
Manipulación y Violación de Sellos Digitales

Artículo 37. Al que manipule los sellos digitales usados por orden de la autoridad pública se le aplicarán de cuarenta a doscientos cuarenta jornadas de trabajo en favor de la comunidad.

Capítulo XII
Intromisión Abusiva de la Privacidad

Artículo 38. A quien, sin consentimiento del afectado, difunda, publique, copie, reproduzca, comparta, exhiba a través de Internet o cualquier otro medio electrónico imágenes, audio o videos de contenido sexual o erótico, tomadas por la misma víctima o por un tercero, que se hayan obtenido en el ámbito de la privacidad con o sin el consentimiento del afectado, se le aplicarán sanciones de seis a quince años de prisión y multa de quinientos a mil días de salario mínimo vigente.

Los administradores de sitios de Internet que no bajen estas imágenes de manera inmediata a solicitud del afectado, serán sancionados con las mismas penas del inciso anterior.

Capítulo XIII
Violación de correspondencia o mensajería electrónica

Artículo 39. Se aplicará de uno a cinco años y multa de cien a doscientos salarios mínimos:

I.- Al que abra indebidamente una comunicación escrita electrónica que no esté dirigida a él, y

II.- Al que indebidamente intercepte una comunicación escrita electrónica que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido.

No aplicará lo previsto en este artículo, cuando los padres abran o intercepten las comunicaciones escritas electrónicamente dirigidas a sus hijos menores de edad o inimputables y los tutores respecto de las personas que se hallen bajo su dependencia.

Artículo 40. Al empleado de una red pública que conscientemente dejare de transmitir la señal de Internet, un mensaje que se le entregue con ese objeto, o de comunicar al destinatario el que recibiere de otra oficina, si causare daño, se le impondrá adicionalmente una pena de seis meses a tres años de prisión y multa de cincuenta a cien días de salario mínimo vigente.

Capítulo XIV
Reglas comunes para los delitos Informáticos

Artículo 41. Los delitos previstos en esta Ley se perseguirán por querella, salvo el caso de los delitos cometidos contra los sistemas informáticos o contra infraestructuras informáticas críticas, pertenecientes a instituciones de los tres órdenes de gobierno, en cuyo caso se perseguirán de oficio.

Artículo 42. Para la determinación delas penas previstas en esta Ley, el juez requerirá del auxilio de peritos y expertos en las materias a que hace referencia esta Ley.

Artículo 43. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

I. Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

II. Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función.

Artículo 44. Toda pena que se imponga en términos de esta Ley llevará consigo la pérdida de los efectos que de él provengan y de los bienes, medios o instrumentos con que se haya preparado o ejecutado, así como de las ganancias provenientes del delito, cualesquiera que sean las transformaciones que hubieren podido experimentar.

Artículo 45. Sin perjuicio de las penas contenidas en esta Ley, se impondrán, en términos del Código Penal Federal las penas accesorias siguientes:

I. El decomiso de instrumentos, objetos o productos del delito.

II. El trabajo comunitario por el término de hasta un año.

III. La destitución e inhabilitación para el ejercicio de un empleo o cargo públicos; para el ejercicio de la profesión, arte o industria, hasta tres años después de cumplida la pena principal, cuando el delito se haya cometido con abuso de la posición de acceso a información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un empleo o cargo públicos, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada, respectivamente.

Artículo 46. En los casos de condena por cualquiera de los delitos previstos en el capítulo V, el juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado.

TITULO QUINTO
DEL RESARCIMIENTO Y REPARACIÓN DEL DAÑO

Capítulo I
De los Mecanismos Alternativos de Solución de Conflictos

Artículo 47. Salvo disposición legal en contrario, en la substanciación de la acción penal promovida por particulares, se observarán en todo lo que resulte aplicable las disposiciones relativas al procedimiento, previstas en la Ley Nacional de Mecanismos Alternativos de Solución de Controversias en Materia Penal, en el Código Nacional de Procedimientos Penales y otros ordenamientos que contemplen mecanismos alternativos de solución de controversias.

Capítulo II
De la Reparación del daño

Artículo 48. Para la reparación del daño a favor de la víctima o del ofendido del delito, se estará a lo dispuesto en el, Código Nacional de Procedimientos Penales, en la Ley General de Víctimas y demás disposiciones aplicables.

TRANSITORIOS

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

SEGUNDO. Lo estipulado en el Título Quinto, capítulo I en lo relacionado De los Mecanismos Alternativos de Solución de Conflictos aplicará lo relativo al Código Nacional de Procedimientos Penales y la Ley Nacional de Mecanismos Alternativos de Solución de Controversias, en los mismos términos y plazos en que entrarán en vigor el Código Nacional de Procedimientos Penales, de conformidad con lo previsto en el artículo segundo transitorio del Decreto por el que se expide el Código Nacional de Procedimientos Penales y el artículo primero transitorio del Decreto por el que se expide la Ley Nacional de Mecanismos Alternativos de Solución de Controversias en Materia Penal, se reforman diversas disposiciones del Código Nacional de Procedimientos Penales y se reforman y adicionan diversas disposiciones del Código Federal de Procedimientos Penales

TERCERO. Lo estipulado en el Título Quinto, capítulo I en lo relacionado De los Mecanismos Alternativos de Solución de Conflictos, lo relativo al Código Federal de Procedimientos Penales, quedará derogado de conformidad con lo señalado en el artículo tercero transitorio Decreto por el que se expide el Código Nacional de Procedimientos Penales.

CUARTO. Para la jurisdicción en donde no haya entrado en vigor el Código Nacional de Procedimientos Penales se entenderá que se utilizará en su lugar el Código Federal de Procedimientos Penales.

Dado en el salón de sesiones del Senado de la República, en la ciudad de México Distrito Federal, a los veintidós días del mes de octubredel año de dos mil quince.

SENADOR OMAR FAYAD MENESES