SENADO DE LA REPÚBLICA
LXIV LEGISLATURA
P R E S E N T E

La suscrita, **Senadora Alejandra Lagunes Soto Ruiz**, integrante del Grupo Parlamentario del Partido Verde Ecologista de México en la LXIV Legislatura de la Cámara de Senadores, de conformidad con lo establecido en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos; los artículos 8, numeral 1, fracción I, 164, numeral 1 y 169 del Reglamento del Senado de la República, someto a la consideración de esta Honorable Asamblea la presente **INICIATIVA CON PROYECTO DE DECRETO PARA REFORMAR Y ADICIONAR DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL EN MATERIA DE CIBERDELITO,** con base en las siguientes consideraciones:

I) CONSIDERACIONES

El desarrollo de las tecnologías de la información y la comunicación (TIC) ha transformado la forma en que entendemos el mundo y cómo nos vinculamos unos con otros, expandiendo de manera considerable el crecimiento y oportunidades económicas y sociales, la mejora en la prestación y capacidad de servicios. Además, se han generado enormes oportunidades para construir instituciones públicas más abiertas, transparentes y eficientes; para el desarrollo de la economía digital y la construcción de sociedades más justas, democráticas e informadas. Por otro lado, también se debe reconocer que han surgido también, nuevos retos en materia de riesgos y amenazas a los derechos humanos, la protección de datos personales, el patrimonio de las personas e instituciones, e incluso peligros latentes para la seguridad nacional e infraestructuras críticas del país.

La incorporación de las TIC en las economías globales ha tenido un crecimiento considerable, en los últimos años se han duplicado los usuarios de internet en todo el mundo, que en 2014 alcanzaban el 50.1% de la población[1]. México no ha sido ajeno a este crecimiento, de acuerdo al 15° Estudio sobre los Hábitos de los Usuarios de Internet en México (2019), nuestro país alcanza un 71% de penetración entre la población de personas de 6 años en adelante, con 82.7 millones de usuarios conectados[2].

[1] ITU. "World Telecommunications, ICT Indicators Database 2015". https://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx.

[2] Asociación Mexicana de Internet. "Estudio sobre los Hábitos de los Usuarios de Internet en México 2018".

La expansión tan rápida de internet y de las tecnologías de la información, ha multiplicado el número de ciudadanos digitales. El internauta mexicano pasa conectado a internet diariamente en promedio 8 horas con 20 minutos; desgraciadamente, esta expansión no se ha visto acompañada por un aumento proporcional en los protocolos y políticas públicas para proteger la seguridad de las personas en línea.

De acuerdo con datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) del 2017 elaborada por el Instituto Nacional de Estadística, Geografía e Informática (INEGI), 17.4 millones de hogares (50.9% del total nacional) disponen de conexión a Internet.

De acuerdo con estas estadísticas, 71.3 millones de personas declararon usar Internet. Esto equivale a un 63.9% de la población.[3]

En México, como resultado de las acciones y programas impulsados por la reforma constitucional en materia de telecomunicaciones, entre 2012 y 2017 el número de usuarios de Internet aumentó en más de 30 millones, pasando de 40.9 a 71.3 millones de usuarios.[4] El enfoque de conectividad, penetración y acceso a Internet que ha premiado en el diseño programático y legislativo del país necesita acompañarse de la creación y articulación de definiciones sobre las prácticas y conductas maliciosas y delictivas en Internet.

La Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC) en su *"Estudio Exhaustivo Sobre el Delito Cibernético, 2013"*[5] señala que las definiciones de delito cibernético dependen en gran medida del propósito para el que se use el término. Un número limitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos representan el núcleo del delito cibernético; los actos informáticos realizados para beneficio, daño personal o financiero, que incluyen formas delincuenciales relacionadas con la identidad y actos relacionados con contenidos informáticos, no se prestan fácilmente para los esfuerzos de generar definiciones legales del término compuesto. Asimismo, el término delito cibernético debe ser considerado como un conjunto de actos o conductas que pueden organizarse en categorías basadas en el objeto del delito material y el *modus operandi*.

[3] http://www.beta.inegi.org.mx/programas/dutih/2017/

[4] Sexto informe de Gobierno. 1 de septiembre de 2018. http://cdn.presidencia.gob.mx/sextoinforme/informe/6_IG_INFORME_COMPLETO.pdf p. 504

[5] https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

La *National Crime Agency* (Agencia Nacional Criminal de Reino Unido) divide al delito cibernético en dos categorías amplias:

- Los delitos ciber-dependientes o crímenes cibernéticos "puros", definidos como delitos que solo pueden cometerse utilizando una computadora, redes de computadoras u otras formas de tecnologías de la información y comunicación.
- Los delitos ciber-habilitados (como el fraude, la compra de drogas ilegales o la explotación sexual infantil) que pueden llevarse a cabo en línea o fuera de línea, pero al utilizar Internet llegan a tener una escala y velocidad sin precedentes.[6]

De acuerdo con las definiciones antes valoradas, se pueden identificar distintas tipologías que engloban a las conductas criminales que se realizan con el empleo de tecnologías de la información y digitales, como medio, fin o habilitadores. Mientras que un delito informático, tiene como común denominador el ataque a activos de información, es decir la disponibilidad, confidencialidad e integridad de la información, los ciberdelitos o cibercrímenes se definen por su relación, ataque y/o utilización de medios tecnológicos.

La revolución digital ha traído consigo problemas y retos parcialmente nuevos, a los que el derecho penal y su sistema no pueden ser ajenos. La caracterización, tanto criminológica como dogmática, de los ciberdelitos no es sencilla y plantea problemas jurídico-penales de diversa índole. Las variadas denominaciones que se han utilizado (en primer lugar, “delitos informáticos”, y posteriormente “ciberdelitos” o “cibercrímenes”, entre otras) reflejan una evolución en el conjunto de figuras delictivas agrupadas en diversas clasificaciones pero que, en realidad, no se han traducido en un concepto dogmático de ciberdelito.

La delincuencia organizada ha aprovechado rápidamente las oportunidades que ofrece Internet, en particular el crecimiento del comercio electrónico y la banca en línea. Los grupos delictivos especializados se dirigen a individuos, pequeñas empresas y grandes redes corporativas para sustraer información personal de forma masiva a fin de aprovechar los datos sensibles que tienen a su disposición.

Por lo que se refiere a la legislación en materia de delitos cibernéticos, ésta debe articularse de forma que sea tecnológicamente neutral y flexible para responder a la evolución constante del crimen y la tecnología, para garantizar el estado de

[6]http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved

derecho y los derechos humanos, y estar armonizada con las leyes de otros países con miras a una cooperación internacional.

El Informe 2016 del Observador de la Ciberseguridad en América Latina y el Caribe, desarrolla el Modelo de Madurez de Capacidad de Seguridad Cibernética como punto de referencia para encontrar soluciones que contribuyan en la prevención y mitigación de riesgos de la actividad delictiva o maliciosa en el ciberespacio, a través de cinco dimensiones de capacidad de seguridad cibernética (no necesariamente independientes unas de otras):1) políticas y estrategia nacional de seguridad cibernética; 2) cultura cibernética y sociedad; 3) educación, formación y competencias en seguridad cibernética; 4) marco jurídico y reglamentario; y 5) normas, organización y tecnologías.

El Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), coloca a México en el tercer lugar en el continente americano respecto el cumplimiento de estándares en la materia; sin embargo este reporte también identifica áreas críticas que son necesarias atender, como contar con una agencia responsable de supervisar la implementación de una estrategia integral de ciberseguridad; establecer acuerdos bilaterales y multilaterales; fomentar una industria doméstica; y firmar acuerdos público - privados en la materia[7].

El objetivo principal de la Estrategia Nacional de Ciberseguridad, publicada en conjunto por la Organización de Estados Americanos (OEA) y la Presidencia de la República en 2017 a recomendación internacional, consiste en propiciar que individuos, empresas y entes públicos -de los diferentes poderes y órdenes de gobierno, realicen sus actividades con el uso de tecnologías de información y comunicación de manera libre, confiable, segura y resiliente, y con ello impulsar el desarrollo económico, social y político de México.[8]

Este documento establece la visión del Estado mexicano en la materia y reconoce lo siguiente:

- La importancia de las Tecnologías de la Información y Comunicación (TIC) como un factor de desarrollo 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.

[7] Índice Global de Ciberseguridad 2017. Unión Internacional de Telecomunicaciones. 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[8] https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS%20(1).pdf

- Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.
- La necesidad de una cultura general de ciberseguridad.

De acuerdo con el *National Cyber Security Index* (índice Nacional de Ciberseguridad) preparado por la e-*Governance Academy Foundation* de Estonia, con datos al 7 de abril de 2018[9], nuestro país ocupa la posición 64 de 126. Una de sus referencias en materia de seguridad cibernética a nivel global mide la preparación de los países para prevenir amenazas de ciberseguridad y la gestión de incidentes, centrándose en cuatro aspectos medibles de la ciberseguridad implementados por los gobiernos:

I. Legislación vigente;
II. Unidades establecidas;
III. Formatos de cooperación; y
IV. Políticas

El Foro Económico Mundial, en su Informe Mundial de Riesgos 2018[10], reconoce que: a nivel tecnológico los ciberataques y el fraude o robo masivo de datos constituyen uno de cinco principales riesgos mundiales percibido por los países. Esto se traduce en el crecimiento de los riesgos en materia de ciberseguridad tanto en términos de su prevalencia, como de su potencial disruptivo y en el crecimiento de casi al doble de los ataques en contra de empresas. Otra de las tendencias que refiere el Informe es el crecimiento de los ciberataques a infraestructura esencial y a sectores industriales estratégicos, lo cual podría provocar el colapso de sistemas que mantienen en funcionamiento a sociedades enteras.

La ciberdelincuencia es uno de los delitos transnacionales de mayor riesgo y de más rápido crecimiento a los que se enfrentan los países, personas, instituciones financieras y corporaciones. La naturaleza sin fronteras de estos delitos, así como la inmediatez, asimetría en capacidades técnicas y humanas para prevenirlos, investigarlos, mitigar su impacto, perseguirlos y sancionarlos han representado serios obstáculos para responder eficazmente a estas amenazas.

El empleo de términos como delincuencia informática, cibercriminalidad, delitos informáticos, entre otros, se ha convertido en una constante en nuestra sociedad. El nacimiento y la rápida difusión de las redes informáticas están propiciando que la cibercriminalidad sea uno de los ámbitos delictivos con más rápido crecimiento. La

[9] https://ncsi.ega.ee/country/mx/

[10] http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

rapidez, el anonimato, la comodidad y la amplitud de alcance que facilitan las nuevas tecnologías, hacen que los delincuentes aprovechen las mismas para llevar a cabo diversas actividades delictivas, tanto tradicionales aprovechando los nuevos medios, como otras nuevas modalidades nacidas dentro de este ámbito.

Ataques contra sistemas informáticos, robo y manipulación de datos, usurpación de identidad, actividades pedófilas, estafas comerciales y bancarias mediante distintas técnicas como la suplantación de identidad, difusión de software malicioso, creación de redes de *bots* para distintos fines, entre otros, constituyen parte de estas actividades delictivas cometidas utilizando medios informáticos. El alcance mundial y la rápida difusión de este tipo de actividades han causado que gobiernos de todo el mundo empiecen a implementar en sus legislaciones medidas para combatirlas y tratar de evitar y prevenir los efectos nocivos que puedan causar en sus ciudadanos.[11]

En México, se ha calculado, que la ciberdelincuencia genera pérdidas anuales por 5 mil millones de dólares, sin embargo, también se señala que cerca del 80% de los delitos cibernéticos se pueden prevenir.[12]

Los ciberdelitos se han convertido en una epidemia digital, mundial y silenciosa. La mayoría de los usuarios de Internet en el mundo ha sufrido y sido víctima de actividades delictivas en la red, quedándose indefensos al intentar hacer frente a los ciberdelincuentes cobijados por el anonimato de la Internet.

Por otra parte, la empresa de seguridad en sistemas Norton, ha reportado una cifra mayor, afirmando que en 2017 los ciberdelincuentes robaron a clientes de servicios financieros, bancarios y empresas en México 7 mil 700 millones de dólares. En el mismo año, de acuerdo a esta empresa, México fue el segundo país en el mundo con mayor número de víctimas de fraude cibernético, con poco más de 33 millones de afectados.[13]

Para el primer trimestre de 2018, de acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), los fraudes cibernéticos crecieron 63% respecto del mismo periodo de 2017 y representan cada año una mayor proporción, pasando del 13% en 2013 al 61% en 2018. El monto de los fraudes cibernéticos ascendió a $2,340 millones de pesos; se

---

[11] http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815

[12] El Economista. Ciberdelincuencia deja pérdidas anuales de 5,000 mdd. 13 de noviembre de 2017 https://www.eleconomista.com.mx/tecnologia/Ciberdelincuencia-deja-perdidas-anuales-de-5000-mdd-20171113-0070.html

[13] Televisa News. México es el segundo país con el mayor número de fraudes cibernéticos. 23 de enero de 2018 https://noticieros.televisa.com/ultimas-noticias/mexico-es-segundo-pais-mayor-numero-fraudes-ciberneticos/

bonificó el 60% del monto reclamado y 89 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario.[14] Asimismo, de acuerdo con los últimos datos generados por dicho organismo, al cierre del primer semestre de 2018 se han disparado los fraudes cibernéticos con un promedio mensual de 333 mil casos, destacando el crecimiento en fraudes cibernéticos realizados en operaciones de comercio electrónico y las operaciones con banca móvil[15].

Estas cifras revelan que los ciberdelitos se encuentran al alza, por lo que se requieren mayores esfuerzos para combatirlos efectivamente.

La tendencia internacional de cibercrimen indica que los incidentes y ataques cibernéticos están en aumento tanto en frecuencia, como en grado de afectación y sofisticación. Es urgente fortalecer las medidas de seguridad y las capacidades de la infraestructura digital de nuestro país, así como el marco jurídico que lo regula, para que contribuyan a gestionar y mitigar los riesgos a los nuevos requerimientos, riesgos y amenazas en el ciberespacio, así como a que atiendan la prevención y atención de delitos.

La lucha efectiva contra la ciberdelincuencia requiere de una cooperación internacional reforzada, rápida y eficaz en materia penal, los Estados miembros del Consejo de Europa impulsaron en 2001 la firma del Convenio de Budapest sobre la Ciberdelincuencia, tanto para los Estados Miembros del Consejo de Europa como los Estados no miembros mediante la adhesión a dicho Convenio por invitación del Comité de Ministros del Consejo de Europa. Por lo que se refiere a México, es imperativa la adhesión a este Convenio, y es que de poco sirve tener una legislación penal actualizada como se busca con esta iniciativa, si no existe un marco de coadyuvancia internacional para combatir una forma de delincuencia que no reconoce fronteras físicas.

El artículo 6° de nuestra Constitución reconoce como parte de los derechos fundamentales, el derecho al acceso a las tecnologías de la información y comunicación, a los servicios de banda ancha e internet, así como a la manifestación de ideas y el acceso a la información. El derecho internacional de los derechos humanos es aplicable a las nuevas tecnologías de la comunicación, tal y como es reconocido en la Declaración de Principios de Ginebra con motivo de la Cumbre Mundial sobre la Sociedad de la Información[16].

---

[14] CONDUSEF. Estadísticas (consultado en septiembre de 2018) https://www.condusef.gob.mx/gbmx/?p=estadisticas

[15] https://www.eluniversal.com.mx/cartera/negocios/cada-hora-se-cometen-463-fraudes-ciberneticos-en-mexico-condusef

[16] https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html

Asimismo, como parte de las conclusiones del Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, presentado en Asamblea General de las Naciones Unidas en 2013,[17] se establece que el derecho internacional, y en particular la Carta de las Naciones Unidas, son aplicables y esenciales para mantener la paz y la estabilidad, y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones. También se refieren a la adopción de medidas voluntarias para incrementar la confianza, la transparencia, y la cooperación internacional para construir capacidades en la esfera de la seguridad de las tecnologías de la información y las comunicaciones.

En el entorno nacional, la Suprema Corte de Justicia de la Nación, mediante la tesis emitida por la Segunda Sala bajo el rubro "Flujo de información en red electrónica (Internet). Principio de restricción mínima posible."[18] determinó que el marco del derecho internacional de los derechos humanos sigue siendo pertinente y aplicable a las nuevas tecnologías de la comunicación; afirmando que Internet se ha convertido en un medio fundamental para que las personas ejerzan su derecho a la libertad de opinión y de expresión, atento a sus características singulares, como su velocidad, alcance mundial y relativo anonimato. Por tanto, en atención a ese derecho humano, se reconoce que en el orden jurídico nacional y en el derecho internacional de los derechos humanos, existe el principio relativo a que el flujo de información por Internet debe restringirse lo mínimo posible, esto es, en circunstancias excepcionales y limitadas, previstas en la ley, para proteger otros derechos humanos.

En los próximos años el uso de las TIC se intensificará en todos los ámbitos de la vida pública y privada de las personas y comunidades. Con ello, también incrementará las amenazas digitales, y el número y naturaleza de los ciberdelitos. Ante este escenario, resulta necesario actualizar el marco legal de México en la materia, así como implementar programas permanentes de capacitación para las autoridades encargadas de la impartición y procuración de la justicia.

Por un lado, conforme a lo previsto en el artículo 6° de nuestra Constitución, el Estado mexicano tiene la obligación de garantizar el acceso a las tecnologías de la información y comunicación, a los servicios de internet y de banda ancha, a la

[17] http://undocs.org/es/A/68/98

[18] https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=FLUJO%2520DE%2520INFORMACI%25C3%2593N%2520EN%2520RED%2520ELECTR%25C3%2593NICA%2520(INTERNET).%2520PRINCIPIO%2520DE%2520RESTRICCI%25C3%2593N%2520M%25C3%258DNIMA%2520POSIBLE&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=1&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2014515&Hit=1&IDs=2014515&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema=

manifestación de ideas, así como el acceso a la información. Por otro lado, las cifras de ciberdelitos e incidencia informática que se cometen en nuestro país crecen día con día. Por lo anterior, resulta necesaria la implementación de medidas legislativas para la tipificación de delitos que sancionen severamente el uso indebido de las tecnologías de la información y comunicaciones.

II) ANTECEDENTES

Los antecedentes de esta iniciativa se remontan a una serie de reformas al Código Penal Federal que se han realizado a partir de 1999 con el objetivo de brindar herramientas necesarias para la procuración e impartición de justicia frente al desarrollo de las TIC.

a) Decreto de Reformas publicado en el Diario Oficial de la Federación del 17 de mayo de 1999 del entonces Código Penal Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, en el que entre otros rubros, se adiciona el artículo 168 Bis y el Capítulo II al Título Noveno del Libro Segundo denominado acceso ilícito a sistemas y equipos de informática, y con ello los artículos 211 Bis 1; 211 Bis 2; 211 Bis 3; 211 Bis 4; 211 Bis 5; 211 Bis 6; 211 Bis 7; asimismo, se agregaron los artículo 424 Bis y Ter.

A continuación se presentan las reformas aprobadas en ese entonces - resaltando los cambios para su fácil identificación:

> **"Artículo 167.-** Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:
>
> **VI.** Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de **fibra óptica**, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;
>
> **Artículo 168 bis.-** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:
>
> **I.** Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o
>
> **II.** Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas.

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.

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.

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.

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 424 ter.- Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, videogramas o libros, a que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código."

b) Posteriormente, mediante Decreto publicado en el Diario Oficial de la Federación, el 24 de junio de 2009, se modificaron los artículos 211 bis 2 y bis 3 para quedar de la siguiente forma:

Artículo 211 bis 2.- ... ...

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.- ... ...

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.

c) Finalmente, y de manera más reciente, se publicaron reformas en Diario Oficial de la Federación el 17 de junio de 2016 al artículo 211 Bis 2, para quedar como sigue:

Artículo 211 Bis 2.- ... ...

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

III) CONTENIDO DE LA INICIATIVA

Se espera que para 2025 existan 300 millones de dispositivos conectados en México. El crecimiento del 70% de los dispositivos para dicho año requiere de un crecimiento de más de 300% del poder computacional de centros de datos. Más del 94% de este poder computacional estará en la nube.

En México, más de 33 millones de personas fueron afectadas por el cibercrimen en 2017, esto quiere decir 1 de cada 4 personas. Para 2019 se estiman pérdidas por ciberataques de hasta 2 mil millones de dólares a nivel mundial.[19]

Por estas razones, es necesario actualizar el Código Penal Federal con el objetivo de que refleje las realidades a las que se enfrentan los Estados. Asimismo, resulta necesario robustecer las capacidades de las autoridades encargadas de la seguridad, y de la procuración e impartición de justicia en nuestro país.

A continuación se presenta un desglose de las propuestas atendiendo las categorías (capítulos) correspondientes en el Código Penal Federal vigente:

EN MATERIA DE DELITOS A LAS VÍAS DE COMUNICACIÓN Y CORRESPONDENCIA

En materia de Ciberseguridad, cobran también relevancia aquellos ilícitos con mayor recurrencia en las redes de comunicación y telecomunicación inalámbricas en detrimento de los derechos fundamentales de las personas. Por lo anterior, esta iniciativa propone agregar tres fracciones y dos incisos al Artículo 168 Bis a efecto de integrar al Código Penal Federal tipos penales que sancionen todo tipo de conducta que propicie el uso ilícito de dispositivos que intervengan sin anuencia del o los interesados, señales de comunicaciones privadas, geolocalización o datos de navegación en internet, así como de contraseñas, códigos de acceso o datos informáticos.

[19] Cifras tomadas del estudio Perspectivas de Ciberseguridad en México, Mckinsey&Company, 2018

De igual forma se propone sancionar aquellas conductas que posibiliten el uso indebido de dispositivos, programas de computación especializados en señales, redes y aplicativos de cualquier aparato portátil o casero que atenten contra la privacidad, confidencialidad, integridad, disponibilidad de la información y sistemas informáticos.

EN MATERIA DE DELITOS DE VIOLACIÓN DE CORRESPONDENCIA

Es innegable que una de las formas de correspondencia más comunes en la actualidad, son el uso del correo electrónico, la telefonía y mensajería digital por lo que se torna necesario una actualización del Artículo 177 para sancionar a quien intervenga los datos de tráfico de las telecomunicaciones realizadas por cualquier vía telefónica, medios digitales, o cualquier medio de comunicación de orden público sin mandato de autoridad judicial competente.

Asimismo, se agrega una agravante duplicando la pena de prisión en el caso de que el ilícito sea perpetrado por servidores públicos que en ejercicio de sus funciones o aprovechando el cargo, ordene, permita, autorice o realice las conductas señaladas en este artículo, además de la privación del cargo o inhabilitación para ocupar otro hasta por cinco años.

EN MATERIA DE DELITOS DE CORRUPCIÓN Y DE PORNOGRAFÍA DE MENORES DE 18 AÑOS O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA COMPRENDER EL SIGNIFICADO DEL HECHO O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA RESISTIRLO.

El uso masificado de las TIC ha traído consigo la evolución de las prácticas de delincuencia, particularmente en ámbitos tan sensibles y graves como la pornografía infantil. La pornografía infantil es definida por la UNICEF como la representación material -por vía de película, impresión, foto, audio o video-grabación y representaciones digitales computarizadas- de niños, niñas y adolescentes realizando actos sexuales reales o simulados para la gratificación sexual de los usuarios, incluyendo la producción.[20]

En el contexto actual, a través del uso de herramientas de edición y sobreposición de rostros, el delito de pornografía infantil ha evolucionado a tal grado que se puede manipular con herramientas de edición, ya fotografías o videos como *deep fakes* (videos pornográficos modificados utilizando tecnología de intercambio de caras a

[20] Infancia robada, UNICEF, https://www.unicef.org/mexico/spanish/mx_resources_infancia_robada.pdf

través de inteligencia artificial, por lo que el rostro del protagonista se reemplaza por el de otra persona.)

En función de lo anterior, se propone una modificación al artículo 200, para sancionar a aquellas personas que produzcan, almacenen, difundan o transmitan a menores de dieciocho años, cualquier tipo de material enunciado en el artículo 200 a través también de medios electrónicos, virtuales, digitales o dispositivos de almacenamiento de datos informáticos.

EN MATERIA DE DELITOS DERIVADOS DEL ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

La incidencia de ataques informáticos ha ido en aumento, subrayando con ello la necesidad de su regulación legal. En un mundo actual caracterizado por la interconectividad, donde los servicios están vinculados entre sí en la nube, en el que los asistentes virtuales, los *routers* y demás dispositivos inteligentes pueden ser la puerta de entrada para ilícitos o en el que un sitio web puede ser infectado por un código malicioso para minar criptomonedas, por dar sólo algunos ejemplos actuales.

Como consecuencia, se hace cada vez más necesario un perfil de usuario más atento, con más herramientas para hacer un uso responsable y consciente de la tecnología, que sepa, no solo cómo protegerse, sino además que conozca los riesgos que conlleva subir información a la nube.[21]

México se ha convertido en un referente de ciberataques a nivel mundial. Cifras recientes detallan que en 2018, México sufrió más de 21.000 intentos de descargar o difundir *ransomware* , y que ha sido el punto de origen de más del 60% de los ataques de de este tipo en América Latina.[22]

En México, la usurpación de identidad aumenta día con día, según datos del Banco de México, nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos, se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria. Comúnmente, desemboca en ilícitos tales como abrir cuentas de crédito, contratar

[21] TENDENCIAS 2019: Privacidad e intrusión en la aldea global, ESET, https://www.welivesecurity.com/wp-content/uploads/2018/12/Tendencias-Ciberseguridad-2019-ESET.pdf

[22] FortiGuardLabs Research Center, https://fortiguard.com/, Marzo 2019

líneas telefónicas, seguros de vida, realizar compras e incluso, en el cobro de seguros de salud, vida y pensiones.[23]

En virtud de lo anterior, se propone sancionar a quien sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información o datos informáticos contenidos en equipos, redes, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos por algún mecanismo de seguridad físico y/o digital en los términos del primer párrafo del artículo del artículo 211 bis 1.

Adicionalmente, se propone sancionar a quien sin autorización modifique, cause daño u obstaculice por cualquier medio o método, el funcionamiento de equipos o sistemas informáticos protegidos contra el acceso no autorizado. en los términos del segundo párrafo del referido artículo.

Se propone adicionar un tercer párrafo a dicho artículo 211 bis 1 a fin de sancionar a sin autorización, por cualquier medio o método, modifique, dañe, deteriore, suprima o provoque la pérdida parcial o total de información o datos informáticos contenidos en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos contra el acceso no autorizado, imponiéndose de uno a tres años de prisión y multa de ciento cincuenta a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente.

Respecto al artículo 211 Bis 2 se propone sancionar a quien sin autorización altere, modifique, destruya o provoque por cualquier medio o método, la pérdida, inaccesibilidad, parcial, o total de información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, protegidos por algún mecanismo de seguridad.

Otra adición a este artículo consiste en sancionar a quien sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, infringiendo medidas de seguridad con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático en los términos señalados en dicho precepto.

[23] Robo de identidad un delito en aumento, Condusef, https://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf

Por cuanto concierne al artículo 211 Bis 3, se propone adicionar al tipo penal existente al que, estando autorizado para acceder a equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, del Estado, indebidamente, por cualquier medio o método altere, modifique, extraiga, destruya, dañe, deteriore, suprima o provoque pérdida parcial o total de información contenida en dichos equipos, sistemas o medios de almacenamiento del Estado, se hará acreedor a las sanciones señaladas en el primer párrafo. Respecto al segundo párrafo también se sancionará en los términos señalados, al que estando autorizado, indebidamente copie o reproduzca información contenida en equipos, sistemas o medios de almacenamiento, físicos o virtuales del Estado. Finalmente, en el párrafo tercero se agregan medios de almacenamiento informáticos físicos o virtuales, en donde se extraiga o facilite información indebidamente.

Respecto el Artículo 211 Bis 4 primer párrafo se agrega al que sin autorización cause daño, altere u obstaculicen, por cualquier medio o método, el funcionamiento de sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad físico y/o digital ahí señalados se hará acreedor a la sanción correspondiente. Respecto al segundo párrafo se agrega que al que sin autorización, por cualquier medio o método, modifique, altere, deteriore, suprima, destruya o provoque la pérdida parcial o total de información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán las sanciones ahí señaladas.

Se agrega un tercer párrafo que establece que al que sin autorización acceda, conozca, copie, extraiga, reproduzca, o difunda, para beneficio propio o de un tercero, por cualquier medio o método, información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, 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 multa de cien a seiscientos días.

En el Artículo 211 Bis 5 se agrega que al al que estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero indebidamente altere, modifique, destruya, inhiba, bloquee o provoque pérdida parcial o total de información contenida en sistemas o equipos de informática por cualquier mecanismo o método, se le impondrán las sanciones señaladas en el párrafo primero. Respecto al segundo párrafo se agrega que al quien estando autorizado para acceder sistemas, equipos o medios de almacenamiento informáticos, físicos

o virtuales de las instituciones que integran el sistema financiero, indebidamente copie, extraiga, reproduzca, o difunda información, para beneficio propio o de un tercero, se le impondrán las sanciones ahí señaladas.

Se agrega un nuevo tipo penal en el Artículo 211 Ter referido a la falsificación informática para quedar en los siguientes términos:

> *Se le impondrán de cuatro a ocho años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización introduzca, altere, borre o suprima datos informáticos que generen datos no auténticos con la intención de que sean tomados o utilizados como auténticos para efectos legales, con independencia de que los datos sean directamente legibles e inteligibles.*
>
> *Se impondrá pena de cuatro a diez años de prisión y multa de doscientos a quinientos de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente en los casos siguientes:*
>
> *a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito, lucrar; y,*
>
> *b) Cuando los actos descritos en el inciso anterior se realicen para inducir a usuarios a la provisión de datos confidencial*es, personales y/o financieros, tanto de personas físicas como de personas morales.

También se agrega el Artículo 211 Quáter, el cual es especialmente importante ya que por fin se introduce a nivel federal, luego de haber estado regulado desde hace algunos años en los Códigos Penales locales, el delito de Usurpación de Identidad con la siguiente redacción:

> *Se le impondrán de uno a cuatro años de prisión y multa de cien a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien usurpe la identidad de otra persona, a través de un sistema o medio informático, o infringiendo medidas de seguridad físicas o digitales, con la intención de causar un daño o perjuicio a una persona, u obtener un beneficio indebido, para sí mismo o para otra persona.*
>
> *Las penas señaladas en este artículo se incrementarán hasta en una mitad cuando el ilícito sea cometido por un servidor público*

aprovechándose de sus funciones, o por quien sin serlo, se valga de su formación, profesión o empleo para ello.

EN MATERIA DE DELITOS DE FRAUDE

El delito de fraude es uno de los que más se ha visto robustecido a través del uso ilícito de la informática, incrementando el número de víctimas, de beneficios económicos e impunidad de quienes los cometen. En la Iniciativa se agregan dos fracciones al artículo 387 del Código Penal Federal para quedar de esta forma: *"Las mismas penas señaladas en el artículo anterior, se impondrán:*

I. a XXI. …

***XXII.** Al que causare un perjuicio patrimonial a otro, mediante la introducción, alteración, borrado o supresión de datos informáticos.*

Asimismo, a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.

***XXIII.** A quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.*

EN MATERIA DE DELITOS DE DERECHOS DE AUTOR

Finalmente, y considerando que de acuerdo con la Encuesta Global de Software 2018 elaborada por la Business Software Alliance (BSA) generó pérdidas anuales en 2017 en nuestro país por 760 millones de dólares y que por otro lado arrojó que un 49% del software que se usa en nuestro país carece de licencia legal, es necesario realizar una actualización en materia de delitos autorales proponiendo una adición a la fracción II del Artículo 424 bis para quedar como sigue: "Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. …

II. A quien fabrique con fin de lucro un dispositivo o sistema físico o digital, cuya finalidad sea desactivar, inhibir o alterar los dispositivos electrónicos de protección de un programa de computación.

PROGRAMAS DE CAPACITACIÓN PERMANENTES

Uno de los aspectos más importantes en las acciones para hacer frente a la ciberdelincuencia es el contar con instituciones capaces de investigar, perseguir, asegurar evidencia electrónica y juzgar el cibercrimen.
En ese sentido, organismos como el Consejo de Jueces Europeos han establecido que es esencial que las y los jueces, además de realizar sus estudios en derecho, reciban capacitación detallada y diversa para que puedan realizar sus labores efectivamente.[24] Asimismo, el Índice de Ciberseguridad de la Unión Internacional de Telecomunicaciones integra a la construcción de capacidades como uno de sus 5 pilares. La construcción de capacidades incluye, entre otros elementos, el análisis de la existencia de programas de capacitación en el país[25].

Por ello, se proponen dos transitorios para establecer que:

- La Fiscalía General de la República y la Guardia Nacional, deberán implementar un programa permanente de capacitación especializada en materia de ciberseguridad y ciberdelincuencia dirigido a las autoridades y personal de las entidades gubernamentales federales responsables de la denuncia e investigación de los delitos en la materia; y que

- El Consejo de la Judicatura Federal deberá implementar un programa permanente de capacitación judicial continua y especializada en materia de ciberseguridad y ciberdelincuencia dirigido a las autoridades de los órganos jurisdiccionales federales responsables en sancionar los delitos en la materia.

[24] "Cybercrime training for judges and prosecutors: a concept" Project on Cybercrime and Lisbon Network. Council of Europe. October 8th, 2009. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybercrime%20training%20for%20judges%20and%20prosecutors.pdf
[25] Global Cybersecurity Index. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Para mayor claridad sobre las reformas que se plantean, se presenta el siguiente cuadro comparativo del texto vigente con las disposiciones que se proponen reformar mediante la iniciativa:

Texto vigente	Propuesta de modificación
Artículo 168 bis.- Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho: I. al II. …	**Artículo 168 Bis.-** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien deliberada e ilegítimamente: I. al II. … III. Produzca, venda, obtenga para su utilización, arriende, importe, difunda o que mediante cualquier otra forma ponga a disposición: a) Dispositivos, incluidos programas informáticos diseñados o adaptados principalmente para la intervención de comunicaciones privadas, geolocalización o la interceptación de datos de navegación en internet sin consentimiento; b) Contraseñas, códigos de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático sin consentimiento. IV. Produzca, venda, obtenga para su utilización, arriende, difunda o que mediante cualquier otra forma ponga a disposición dispositivos electrónicos, programas informáticos o tecnologías de comunicación que permitan la obtención encubierta de datos, información confidencial o que atenten contra la privacidad. V. Posea alguno de los elementos contemplados en la fracción anterior, con la intención de ser utilizados para cometer ilícitos relacionados con la violación de confidencialidad, integridad, privacidad y disponibilidad de la información y sistemas informáticos.
Artículo 177.- A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.	**Artículo 177.-** Se impondrán de seis a doce años de prisión y multa de trescientos a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien, sin mandato de autoridad judicial competente, intercepte o

	intervenga comunicaciones privadas o los datos transmitidos a través de las redes o servicios públicos de telecomunicaciones o por cualquier medio o método, datos informáticos en transmisiones dirigidas a un sistema o equipo informático, originadas desde otro sistema o equipo, o realizadas dentro del mismo, incluidas las emisiones electromagnéticas y radiofrecuencias provenientes de un sistema o equipo informático que transporte dichos datos informáticos. La pena prevista en este artículo se duplicará para el caso de servidores públicos que en ejercicio de sus funciones o aprovechando su cargo, ordenen, permitan, autoricen o realicen las conductas señaladas en este artículo, además de la privación del cargo y la inhabilitación para ocupar otro hasta por cinco años.
Artículo 200.- Al que comercie, distribuya, exponga, haga circular u oferte, a menores de dieciocho años de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales o simulados, sea de manera física, o a través de cualquier medio, se le impondrá de seis meses a cinco años de prisión y de trescientos a quinientos días multa. ….	**Artículo 200.-** Se impondrán de seis meses a cinco años de prisión y multa de trescientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, **a quien financie, comercie, distribuya, exponga, ponga en circulación, oferte, difunda o transmita a menores de edad, l**ibros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales, simulados o creados por medios tecnológicos, sea de manera física, o a través de cualquier medio **electrónico, digital o de dispositivos de almacenamiento de datos informáticos.** …
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.	**Artículo 211 Bis 1.-** Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, **a quien** sin autorización **acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método,** información **o datos informáticos contenidos en equipos, redes, sistemas o medios de almacenamiento informáticos, físicos o**

	virtuales, protegidos por algún mecanismo de seguridad **físico y/o digital.**
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.	Se le impondrán de tres meses a un año de prisión y multa de cincuenta a ciento cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **modifique, cause daño u obstaculice por cualquier medio o método, el funcionamiento de equipos o sistemas informáticos protegidos contra el acceso no autorizado.**
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.	**Artículo 211 Bis 2.-** Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **altere,** modifique, destruya o provoque **por cualquier medio o método,** la pérdida, **inaccesibilidad, parcial, o total de** información contenida en equipos, **sistemas o medios de almacenamiento informáticos, físicos o virtuales** del Estado, protegidos por algún mecanismo de seguridad.
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.	Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **acceda,** conozca, copie, **extraiga o reproduzca por cualquier medio o método,** información contenida en **equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales** del Estado, **infringiendo medidas de seguridad con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático,** 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	Se le impondrán de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización **acceda**, conozca, obtenga, copie, **extraiga** o utilice información contenida **en equipos, sistemas o medios de**

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. …	**almacenamiento informáticos, físicos o virtuales** de seguridad pública, protegidos por algún mecanismo de seguridad.Si el responsable es o hubiera sido servidor público en una institución de seguridad pública **o de justicia penal, se le destituirá** y se le impondrá una inhabilitación de cuatro a diez años para desempeñarse **en otro cargo público.** …
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	**Artículo 211 Bis 3.-** Se le impondrán de dos a ocho años de prisión y multa de trescientos a novecientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que, estando autorizado para acceder a equipos, sistemas **o medios de almacenamiento informáticos, físicos o virtuales,** del Estado, indebidamente, **por cualquier medio o método altere,** modifique, **extraiga,** destruya, **dañe, deteriore, suprima o** provoque pérdida **parcial o total** de información **contenida en dichos equipos, sistemas o medios de almacenamiento del Estado.** Se le impondrán de uno a cuatro años de prisión y multa de ciento cincuenta a cuatrocientos cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado, **indebidamente copie o reproduzca información contenida en equipos, sistemas o medios de almacenamiento, físicos o virtuales del Estado.** Se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, **físicos o virtuales,** en materia de seguridad pública, indebidamente obtenga, **extraiga,** copie, **facilite** o utilice información que contengan. 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 establecida, destitución e inhabilitación por un plazo igual al de la pena

en otro empleo, puesto, cargo o comisión pública.	resultante para desempeñarse en **otro cargo público.**
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 4.-** Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización **cause daño, altere u obstaculice, por cualquier medio o método, el funcionamiento de sistemas o equipos de informática** de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad **físico y/o digital.** Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización, **por cualquier medio o método, modifique, altere, deteriore, suprima, destruya o provoque la pérdida parcial o total de información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales,** 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 multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga, reproduzca, o difunda, para beneficio propio o de un tercero, por cualquier medio o método, información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.**
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	**Artículo 211 Bis 5.-** Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder a sistemas, **equipos o**

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. …	**medios de almacenamiento informáticos, físicos o virtuales,** de las instituciones que integran el sistema financiero indebidamente **altere,** modifique, destruya, **inhiba, bloquee** o provoque pérdida **parcial o total** de información **contenida en sistemas o equipos de informática por cualquier mecanismo o método.** Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder sistemas, equipos **o medios de almacenamiento informáticos, físicos o virtuales** de las instituciones que integran el sistema financiero, indebidamente copie, **extraiga, reproduzca, o difunda información, para beneficio propio o de un tercero.** …
	Artículo 211 Ter.- Se le impondrán de cuatro a ocho años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización introduzca, altere, borre o suprima datos informáticos que generen datos no auténticos con la intención de que sean tomados o utilizados como auténticos para efectos legales, con independencia de que los datos sean directamente legibles e inteligibles. **Se impondrá pena de cuatro a diez años de prisión y multa de doscientos a quinientos de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente en los casos siguientes:** **a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito, lucrar; y,** **b) Cuando los actos descritos en el inciso anterior se realicen para inducir a usuarios a la provisión de datos confidenciales, personales y/o financieros, tanto de personas físicas como de personas morales.**

	Artículo 211 Quáter.- Se le impondrán de uno a cuatro años de prisión y multa de cien a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien usurpe la identidad de otra persona, a través de un sistema o medio informático, o infringiendo medidas de seguridad físicas o digitales, con la intención de causar un daño o perjuicio a una persona, u obtener un beneficio indebido, para sí mismo o para otra persona. **Las penas señaladas en este artículo se incrementarán hasta en una mitad cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su formación, profesión o empleo para ello.**
Artículo 387.- Las mismas penas señaladas en el artículo anterior, se impondrán:	**Artículo 387.-** Las mismas penas señaladas en el artículo anterior, se impondrán: I. a XXI. … **XXII. Al que causare un perjuicio patrimonial a otro, mediante la introducción, alteración, borrado o supresión de datos informáticos.** **Asimismo, a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.** **XXIII. A quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.**
Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:	**Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. … II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.	I. … II. A quien fabrique con fin de lucro un dispositivo o sistema **físico o digital,** cuya finalidad sea desactivar, inhibir o alterar los dispositivos electrónicos de protección de un programa de computación.

Conforme a lo anteriormente expuesto y con fundamento en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos y en los artículos 8, numeral 1, fracción I, 164, numeral 1 y 169 del Reglamento del Senado de la República, someto a la consideración de esta Cámara de Senadores la siguiente:

INICIATIVA CON PROYECTO DE DECRETO QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL EN MATERIA DE CIBERSEGURIDAD.

ARTÍCULO ÚNICO.- Se reforman los artículos 168 Bis, 177, 200, 211 Bis 1, 211 Bis 2, 211 Bis 3, 211 Bis 4, 211 Bis 5, y 424 bis y se adicionan los artículos 211 Bis 8, 211 Ter, 211 Quáter y 387 fracción XXII del Código Penal Federal, para quedar como sigue:

INICIATIVA CON PROYECTO DE DECRETO QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL EN MATERIA DE CIBERSEGURIDAD.

ARTÍCULO ÚNICO.- Se reforman los artículos 168 Bis, 177, 200, 202, 202 Bis, 211 Bis 1, 211 Bis 2, 211 Bis 3, 211 Bis 4, 211 Bis 5, 403 y 424 bis y se adicionan los artículos 211 Bis 8, 211 Ter, 211 Quáter, 387 fracciones XXII y XXIII, y 424 bis. fracción II del Código Penal Federal, para quedar como sigue:

TITULO QUINTO
Delitos en Materia de Vías de Comunicación y Correspondencia

CAPÍTULO I
Ataques a las vías de comunicación y violación de correspondencia

Artículos 165 a 168.- …

Artículo 168 Bis.- Se impondrán de seis meses a dos años de prisión y multa de trescientos a tres mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien deliberada e ilegítimamente:

I. a II.

III. Produzca, venda, obtenga para su utilización, arriende, importe, difunda o que mediante cualquier otra forma ponga a disposición:

a) Dispositivos, incluidos programas informáticos diseñados o adaptados principalmente para la intervención de comunicaciones privadas, geolocalización o la interceptación de datos de navegación en internet sin consentimiento;

b) Contraseñas, códigos de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático sin consentimiento.

IV. Produzca, venda, obtenga para su utilización, arriende, difunda o que mediante cualquier otra forma ponga a disposición dispositivos electrónicos, programas informáticos o tecnologías de comunicación que permitan la obtención encubierta de datos, información confidencial o que atenten contra la privacidad.

V. Posea alguno de los elementos contemplados en la fracción anterior, con la intención de ser utilizados para cometer ilícitos relacionados con la violación de confidencialidad, integridad, privacidad y disponibilidad de la información y sistemas informáticos.

Artículos 169 a 176.- …

Artículo 177.- Se impondrán de seis a doce años de prisión y multa de trescientos a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien, sin mandato de autoridad judicial competente, intercepte o intervenga comunicaciones privadas o los datos transmitidos a través de las redes o servicios públicos de telecomunicaciones o por cualquier medio o método, datos informáticos en transmisiones dirigidas a un sistema o equipo informático, originadas desde otro sistema o equipo, o realizadas dentro del mismo, incluidas las emisiones electromagnéticas y radiofrecuencias provenientes de un sistema o equipo informático que transporte dichos datos informáticos.

La pena prevista en este artículo se duplicará para el caso de servidores públicos que en ejercicio de sus funciones o aprovechando su cargo, ordenen, permitan, autoricen o realicen las conductas señaladas en este artículo, además de la privación del cargo y la inhabilitación para ocupar otro hasta por cinco años.

TITULO OCTAVO

DELITOS CONTRA EL LIBRE DESARROLLO DE LA PERSONALIDAD.

CAPÍTULO I
Corrupción de Menores de Edad, de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo.

Artículo 200.- Se impondrán de seis meses a cinco años de prisión y multa de trescientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que financie, comercie, distribuya, exponga, ponga en circulación, oferte, difunda o transmita a menores de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales, simulados o creados por medios tecnológicos, sea de manera física, o a través de cualquier medio electrónico, digital o de dispositivos de almacenamiento de datos informáticos.

…

TITULO NOVENO

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

Capítulo II
Acceso ilícito a sistemas y equipos de informática

Artículo 211 Bis 1.- Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información o datos informáticos contenidos en equipos,

redes, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos por algún mecanismo de seguridad físico y/o digital.

Se le impondrán de tres meses a un año de prisión y multa de cincuenta a ciento cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización modifique, cause daño u obstaculice por cualquier medio o método, el funcionamiento de equipos o sistemas informáticos protegidos contra el acceso no autorizado.

Se le impondrán de uno a tres años de prisión y multa de ciento cincuenta a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización, por cualquier medio o método, modifique, dañe, deteriore, suprima o provoque la pérdida parcial o total de información o datos informáticos contenidos en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, protegidos contra el acceso no autorizado.

Artículo 211 Bis 2.- Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización altere, modifique, destruya o provoque por cualquier medio o método, la pérdida, inaccesibilidad, parcial, o total de información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, protegidos por algún mecanismo de seguridad.

Se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga o reproduzca por cualquier medio o método, información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales del Estado, infringiendo medidas de seguridad con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Se le impondrán de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización acceda, conozca, obtenga, copie, extraiga o utilice información contenida en equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales de seguridad pública, protegidos por algún mecanismo de seguridad.

Si el responsable es o hubiera sido servidor público en una institución de seguridad pública o de justicia penal, se le destituirá y se le impondrá una inhabilitación de cuatro a diez años para desempeñarse en otro cargo público.

…

Artículo 211 Bis 3.- Se le impondrán de dos a ocho años de prisión y multa de trescientos a novecientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que, estando autorizado para acceder a equipos, sistemas o medios de almacenamiento informáticos, físicos o virtuales, del Estado, indebidamente, por cualquier medio o método altere, modifique, extraiga, destruya, dañe, deteriore, suprima o provoque pérdida parcial o total de información contenida en dichos equipos, sistemas o medios de almacenamiento del Estado.

Se le impondrán de uno a cuatro años de prisión y multa de ciento cincuenta a cuatrocientos cincuenta veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado, indebidamente copie o reproduzca información contenida en equipos, sistemas o medios de almacenamiento, físicos o virtuales del Estado.

Se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil veces el valor diario de la Unidad de Medida y Actualización vigente, a quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales, en materia de seguridad pública, indebidamente obtenga, extraiga, copie, facilite o utilice información que contengan. 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 establecida, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro cargo público.

Artículo 211 Bis 4.- Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización cause daño, altere u obstaculice, por cualquier medio o método, el funcionamiento de sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad físico y/o digital.

Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al

que sin autorización, por cualquier medio o método, modifique, altere, deteriore, suprima, destruya o provoque la pérdida parcial o total de información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, 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 multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que sin autorización acceda, conozca, copie, extraiga, reproduzca, o difunda, para beneficio propio o de un tercero, por cualquier medio o método, información contenida en sistemas, redes, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

Artículo 211 Bis 5.- Se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales, de las instituciones que integran el sistema financiero indebidamente altere, modifique, destruya, inhiba, bloquee o provoque pérdida parcial o total de información contenida en sistemas o equipos de informática por cualquier mecanismo o método.

Se le impondrán de tres meses a dos años de prisión y multa de cincuenta a trescientas veces el valor diario de la Unidad de Medida y Actualización vigente, al que estando autorizado para acceder sistemas, equipos o medios de almacenamiento informáticos, físicos o virtuales de las instituciones que integran el sistema financiero, indebidamente copie, extraiga, reproduzca, o difunda información, para beneficio propio o de un tercero.

…

Artículo 211 Ter.- Se le impondrán de cuatro a ocho años de prisión y multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien sin autorización introduzca, altere, borre o suprima datos informáticos que generen datos no auténticos con la intención de que sean tomados o utilizados

como auténticos para efectos legales, con independencia de que los datos sean directamente legibles e inteligibles.

Se impondrá pena de cuatro a diez años de prisión y multa de doscientos a quinientos de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente en los casos siguientes:

a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito, lucrar; y,

b) Cuando los actos descritos en el inciso anterior se realicen para inducir a usuarios a la provisión de datos confidenciales, personales y/o financieros, tanto de personas físicas como de personas morales.

Artículo 211 Quáter.- Se le impondrán de uno a cuatro años de prisión y multa de cien a quinientas veces el valor diario de la Unidad de Medida y Actualización vigente, a quien usurpe la identidad de otra persona, a través de un sistema o medio informático, o infringiendo medidas de seguridad físicas o digitales, con la intención de causar un daño o perjuicio a una persona, u obtener un beneficio indebido, para sí mismo o para otra persona.

Las penas señaladas en este artículo se incrementarán hasta en una mitad cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su formación, profesión o empleo para ello.

TITULO VIGESIMO SEGUNDO
Delitos en Contra de las Personas en su Patrimonio

CAPÍTULO III
Fraude

Artículo 386.- …

Artículo 387.- Las mismas penas señaladas en el artículo anterior, se impondrán:

I a XXI.- …

XXII. Al que causare un perjuicio patrimonial a otro, mediante la introducción, alteración, borrado o supresión de datos informáticos.

Asimismo, a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.

XXIII. A quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.

TITULO VIGESIMO SEXTO
De los Delitos en Materia de Derechos de Autor

Artículo 424.- …

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. …

II. A quien fabrique con fin de lucro un dispositivo o sistema **físico o digital,** cuya finalidad sea desactivar, inhibir o alterar los dispositivos electrónicos de protección de un programa de computación.

TRANSITORIOS

Primero. El presente decreto entrará en vigor a los noventa días de su publicación en el Diario Oficial de la Federación.

Segundo. La Fiscalía General de la República y la Guardia Nacional, deberán implementar un programa permanente de capacitación especializada en materia de ciberseguridad y ciberdelincuencia dirigido a las autoridades y personal de las entidades gubernamentales federales responsables de la denuncia e investigación de los delitos en la materia.

Tercero. El Consejo de la Judicatura Federal deberá implementar un programa permanente de capacitación judicial continua y especializada en materia de

ciberseguridad y ciberdelincuencia dirigido a las autoridades de los órganos jurisdiccionales federales responsables en sancionar los delitos en la materia.

Salón de Sesiones de la Cámara de Senadores del Honorable Congreso de la Unión, a 15 de octubre de 2019.

SENADORA ALEJANDRA LAGUNES SOTO RUIZ
PARTIDO VERDE ECOLOGISTA DE MÉXICO