ACUSE

Ciudad de México, 22 de febrero de 2022
CCM/IIL/IIL/018/2022

DIP. NAZARIO NORBERTO SÁNCHEZ
PRESIDENTE DE LA COMISIÓN DE SEGURIDAD CIUDADANA DEL CONGRESO DE LA CIUDAD DE MÉXICO II LEGISLATURA
PRESENTE

DIP. NAZARIO NORBERTO SÁNCHEZ
II LEGISLATURA
23 FEB 2022
Recibió:
Hora: 12:47

Por este conducto, y en atención a su oficio CCDMX/IIL/CSC/075/2022 de fecha 27 de enero del año en curso, por el cual solicita a este Instituto a mi cargo la realización de una investigación y/o estudio respecto al tema de "ciberseguridad" y "la Legislación en materia de derecho Informático, ciberseguridad y ciberdelitos", así como "si existe legislación internacional, nacional y de las entidades federativas respecto a estos temas, así como las políticas públicas y leyes al respecto en la Ciudad de México"

Sobre el particular le envío la investigación solicitada en forma impresa y digital para los efectos de que cuente con información que abone a la elaboración del proyecto de dictamen del que hace mención.

Sin más por el momento le envío un cordial saludo.

ATENTAMENTE

LIC. GERMÁN TORRES SERRANO
ENCARGADO DE DESPACHO

Paola 24/02/22
RECIBIDO
12.19 pm.

C.c.p. Asistencia Técnica, para su conocimiento.
c.c.p. lic. Lizeth Bonilla Mendoza.- Subdirectora de Estudios Legislativo Comparados, Practicas Parlamentarias y Capacitación Legislativa del IIL.

"CIBERSEGURIDAD"

INTRODUCCIÓN

La Constitución Política de los Estados Unidos Mexicanos garantiza la protección de la persona, la familia y las propiedades. El vigor de nuestra ley suprema es brindar a todos los mexicanos el derecho a vivir bajo el amparo de las leyes y la protección legítima de las autoridades. Esto lo encontramos en las llamadas "garantías de seguridad", mismas que se derivan de lo que estipulan los artículos 14, 16, 21 y 73 constitucional, los cuales velan porque los derechos de los ciudadanos no resulten afectados debido a procedimientos ilícitos. Nos encontramos en una época digital en la que las y los ciudadanos se comunican e interactúan aprovechando las tecnologías de la información, sino que también aumenta el número de operaciones comerciales en el ámbito digital, lo cual expande las oportunidades de servicios a nivel global. Esto se traduce en un crecimiento constante en el flujo de información personal, económica, política y social.

La pandemia de coronavirus (COVID-19) provocada por el virus SARS-CoV-2 favorecieron al aumento de los ciberataques a las tecnologías de la Información y Comunicación (TICs), debido al incremento en su uso a nivel mundial; sin embargo, en el caso particular de México, la ciberseguridad se convirtió en un tema particularmente complejo durante este tiempo, más aún por no contar con un marco regulatorio que ayude a mitigar los efectos de dichos ataques.

ANTECEDENTES

Las redes y plataformas digitales se han convertido en parte fundamental para la operatividad de la vida diaria en hogares, empleos, educación, instituciones y gobiernos, conectando a grandes comunidades en la sociedad de la información por medio de conexión a internet, sabemos que es una herramienta que en algunos casos exige sus propios instrumentos y estrategias de protección en conectividad, esto con el fin de salvaguardar la integridad de las personas y de sus derechos fundamentales, por ejemplo para proteger el trabajo y la información en manos de las instituciones públicas y por supuesto proteger también las infraestructuras críticas como son los Sistemas Tecnológicos para el control y automatización de redes de energía, de distribución de agua, de Medios de Transporte, entre otros.

En general, a la ciberseguridad se le pueden dar diversas definiciones, esto será de acuerdo al contexto en el que se utilice, pero al final se busca que principalmente se quieren prevenir, y su caso, sancionar alteraciones malintencionadas, robo, fraude, sabotajes, ataques y daños a los sistemas informáticos. Sin duda el principal objetivo de la ciberseguridad, es brindar seguridad de tecnología de la información o seguridad de la información electrónica.

En algunos casos, la ciberseguridad, se subdivide en tratar de garantizar:

- La seguridad de red, entendiendo esta como la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.
- La seguridad de las aplicaciones, esta se enfoca básicamente en mantener el software y los dispositivos libres de amenazas.
- La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.
- La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Incluye aquellos permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- La recuperación ante desastres y la continuidad del negocio definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres serían determinadas por la propia organización de que se trate.

- La capacitación del usuario final es el elemento más impredecible. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.[1]

INTERNACIONAL

En mayo de 2021, Estados Unidos declaró el estado de emergencia tras un ciberataque a la mayor red de oleoductos del país. Un grupo de hackers desconectó por completo y robó más de 100 GB de información del Oleoducto Colonial, que transportaba más de 2,5 millones de barriles por día, el 45% del suministro de diésel, gasolina y combustible que consumen los aviones de la costa este.[2]

De acuerdo a una publicación virtual de CIO, México, de fecha 14 de septiembre del 2021, aproximadamente en un plazo de 5 minutos se producen más de 150 mil ciberataques en el mundo, el promedio al día de ataques online es de 45 millones.[3]

El informe de la Organización de los Estados Americanos (OEA) y el Bando Internacional de Desarrollo (BID) analiza la madurez de la ciberseguridad en los 32 países que integran la región de América Latina y el Caribe, bajo 5 dimensiones:

1. Política y Estrategia de Ciberseguridad
2. Cultura Cibernética y Sociedad
3. Educación, Capacitación y Habilidades en Ciberseguridad
4. Marcos legales y regulatorios
5. Estándares, Organizaciones y tecnologías

Dependiendo de las acciones que tomen los países respecto de estas dimensiones, la

[1] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] https://www.bbc.com/mundo/noticias-internacional-57033536#:~:text=El%20ciberataque%20afect%C3%B3%20a%20una,El%20gobierno%20de%20EE.&text=declar%C3%B3%20este%20domingo%20un%20estado,desde%20la%20noche%20del%20viernes.

[3] https://cio.com.mx/el-paradigma-de-una-cultura-global-de-ciberseguridad-en-el-mundo-empresarial/

medición establece un nivel de madurez de la capacidad de ciberseguridad que va de la etapa inicial, pasando por la formativa, la consolidada, la estratégica hasta llegar a la dinámica.[4]

Según el Reporte de ciberseguridad 2020, en la sección de Perspectiva de la Unión Europea (UE) para afrontar las amenazas del ciberespacio, desde el 2013, la UE ha liderado la creación de capacidades internacionales de seguridad Cibernéticas debido a la naturaleza global de las amenazas; construir y preservar alianzas y asociaciones solidas con terceros países es fundamental para prevenir ataques cibernéticos que atentan contra la estabilidad y seguridad internacional, y continua promoviendo un modelo de creación para suscitar la estabilidad cibernética global basado en derechos y valores como el derecho a la privacidad y protección de datos personales, además de promover el espacio abierto, libre y seguro. Cabe destacar que todo esto son parte de las prioridades en la Agenda 2030 para el Desarrollo Sostenible y los esfuerzos para su puesta en marcha.

La Unión Europea sugiere que una resiliencia cibernética fuerte, requiere necesariamente de abordajes colectivos amplios y estructuras eficaces que promuevan la ciberseguridad y se pueda responder a los ciberataques en los Estados Miembros de la Unión Europea;

Se debe contar con enfoques de políticas transversales con autonomía estratégica para avances en la tecnología, esto realizado con expertos cada vez más calificados; sin duda se debe acompañar de normas, reglas y principios de manera voluntaria de los Estados que han sido articulados por el Grupo de Expertos Gubernamentales de Naciones Unidas, es de mencionar que la preparación cibernética es fundamental tanto para el Mercado Único Digital como para la Seguridad y Defensa de la Unión.

De acuerdo a las experiencias en esta materia, se ha señalado qué para establecer el nivel de ciberseguridad de un país, se toman en cuenta 5 criterios:

1) La capacidad de prevención de ciberataques,

2) Legislación en materia de ciberseguridad,

[4] https://ciapem.org/la-estrategia-nacional-de-ciberseguridad-de-mexico-debe-trascender-del-papel-oea-y-bid/

3) Cooperación con otros países,

4) El nivel de preparación de las organizaciones no gubernamentales y

5) La eficacia del ente regulador a nivel nacional.

Dentro de los países que lideran las listas de los estudios encargados de evaluar la **ciberseguridad a nivel mundial** tenemos Estados Unidos, Canadá, Francia, Australia, Malasia, Singapur y Japón.

Si bien los países señalados, son los más avanzados en este rubro, aun no tienen cubierto totalmente cada una de los 5 criterios tomados en cuenta.

La Unión Europea cuenta actualmente con **la Ley de Seguridad Cibernética** aprobada en junio del 2019, con el fin de fortalecer las medidas de ciberseguridad de los productos, servicios y procesos digitales en toda la UE.

En Estados Unidos se creó **la Directiva de Política Nacional, cuya tarea principal es** evaluar el impacto de los ciberataques y lograr la cooperación entre el gobierno y el sector privado.

Rusia ha estado dispuesta a firmar un acuerdo de cooperación con EEUU en materia de ciberseguridad.

CIBERSEGURIDAD EN AMÉRICA LATINA

De acuerdo a diversos reportes, lamentablemente los países de América Latina están poco preparados contra los ciberataques, los gobiernos y las empresas privadas en general invierten pocos recursos en este rubro.

No obstante lo anterior, los países de Latinoamérica más avanzados son Colombia, Argentina y México, aún falta mucho por recorrer.

Pese que los países de América Latina no son países desarrollados, éstos cuentan con una alta tasa de conectividad, en especial en zonas urbanas, de acuerdo al estudio por el IICA, el BID y Microsoft, el 71% de la población ya cuenta con acceso a internet, en tanto que en las zonas rurales existe un rezago del 37%

En general la conectividad alcanza un 68%, lo que nos coloca por encima de África quien cuenta con sólo un 18% de población conectada a internet.

Desde los años noventa, los gobiernos latinoamericanos han sido fundamentales en la masificación de la conectividad o la red por medio de diseño e implementación de políticas que ampliaron las infraestructuras y facilitaron el acceso a dispositivos.

En marzo de 2016 el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) se concentraron en ofrecer a los países de la región de América Latina y Caribe, un estado de ciberseguridad y la manera de fortalecer las capacidades nacionales en esa materia; lamentablemente, los ciberataques se han incrementado, dejando clara la vulnerabilidad que se presenta en esta región del mundo, no obstante, esto trajo como consecuencia la implementación del nuevo Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), con el fin de medir el crecimiento y desarrollo de los Estados Miembros y poder defenderse de las constantes amenazas al espacio cibernético y generar oportunidades para que los profesionales en la rama se actualicen. De igual manera resalta que derivado de los constantes ataques cibernéticos, se incrementó el interés en usuarios por la seguridad cibernética y la búsqueda de capacitación cada vez más sofisticada.

Aunque América Latina y Caribe mejoro sus capacidades de ciberseguridad, específicamente el Caribe comenzó a formular iniciativas de seguridad cibernética incluyendo medidas de creación de capacidad que fueron implementadas de manera adecuada pero sin coordinación entre actores clave.

Uruguay ha sido el país calificado en la región con la más alta madurez en estrategias de ciberseguridad [5], Colombia fue el de mayor desarrollo de dicha seguridad en dimensiones de "Política y estrategia" y "Cultura y Sociedad", para el caso de Centro América y México presentaron un nivel superior en las dimensiones de "Cultura y Sociedad" y en "Educación, capacitación y habilidades" mientras que el puntaje ha sido inferior en las dimensiones de "Política y Estrategia" y "Estándares, organizaciones y tecnologías", México en particular presento la mejor posición de la región con madurez en todas las dimensiones, pero el reporte sugiere que debería centrarse en mejorar el despliegue de estándares de seguridad cibernética y controles técnicos, así como fomentar el desarrollo de un mercado de ciberseguridad.

---

5 https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/ciberseguridad-uruguay-lidera-america-latina-caribe#:~:text=As%C3%AD%20lo%20indica%20el%20reporte,modelo%20de%20madurez%20en%20ciberseguridad.

NACIONAL

Jonathan López Torres, autor de *Ciberespacio & Ciberseguridad* resume que la ciberseguridad, es una política pública que debe garantizar la seguridad informática de las instituciones gubernamentales, proteger la información en poder de las autoridades, asegurar la disponibilidad y la continuidad de los servicios y procesos públicos (como trámites para la obtención de licencias municipales o juicios jurídicos) y salvaguardar la confidencialidad, la integridad y la disponibilidad de la información.[6]

De acuerdo con el Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT), México ocupa el lugar 63 de 175 países en materia de preparación de seguridad cibernética.[7]

En los temas que destaca México son protección de activos digitales, con la Ley Federal de Protección de Datos Personales. No obstante México tiene un alarmante el rezago en cuanto a regulación sobre ciberseguridad; no solo respecto al resto de los países, sino a los desafíos en la materia.

Es importante señalar, que México representa un mercado enorme con gran potencial de ganancias económicas para cibercriminales, ejemplo de ellos son:

- Algunos de los ataques más recientes a instituciones mexicanas, que fueron llevados a cabo contra la Condusef, el SAT y Banxico en julio de 2020
- Los ataques a la Secretaría de la Función Pública en julio de 2020; que expuso la información sobre declaraciones patrimoniales de 830 mil funcionarios públicos
- Uno contra el ISSSTE, que expuso en internet durante un lapso indeterminado de tiempo la información de 551 asegurados del ISSSTE sin protección.
- El ataque de ransomware a la Lotería Nacional en junio de 2021, donde se encriptó información crítica, financiera, interna y de empleados, y como rescate se pidió casi un millón de pesos a cambio de las claves para descifrar esta información y que no se publicara.[8]

[6] https://www.eleconomista.com.mx/amp/opinion/Los-estados-necesitan-una-ley-de-ciberseguridad-20210124-0004.html
[7] https://businessinsider.mx/importancia-marco-regulatorio-ciberseguridad-mexico/
[8] https://businessinsider.mx/importancia-marco-regulatorio-ciberseguridad-mexico/

A efecto de combatir casos como los anteriores, el Gobierno Federal cuenta con una Estrategia Nacional de Ciberseguridad, una guía rectora con cuatro ejes: sociedad, seguridad nacional, economía y gobierno, pero que según la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) no ha salido del papel y tampoco se ha convertido en una política de Estado.

Cabe destacar, que las empresas mexicanas con una vulnerabilidad mayor son quienes sufren más de ciberataques; sin embargo, la gran mayoría de estas son pymes.

De acuerdo al Reporte de Ciberseguridad 2020 del BID, un tercio de los países en América Latina no cuenta con un marco legal sobre delitos informáticos; desafortunadamente, México es parte de ellos.

En nuestro país, existe una Estrategia Nacional de Ciberseguridad, presentada en el Gobierno de Enrique Peña Nieto, esta cuenta o se basa en 4 ejes rectores:

1. Sociedad
2. Seguridad nacional
3. Economía y
4. Gobierno

En 2020 el Congreso estatal de San Luis Potosí puso a discusión legislativa una iniciativa de Ley de Ciberseguridad local, pocas semanas después lo hizo el Congreso de la Ciudad de México, éste último desde entonces han presentado diversas iniciativas, sin que a la fecha se cuente con una ley en la materia.

La Ley Modelo de Ciberseguridad tiene como bases sólidas: las investigaciones de López Torres, ya que la fue construyendo mientras realizaba la investigación de *Ciberespacio & Ciberseguridad*. Esta Ley contempla la creación de oficinas estatales de ciberseguridad, en coordinación con fiscalías especializadas, además de obligaciones y responsabilidades de los servidores públicos que deben ejecutarla y hacer valer su cumplimiento. Integrada con

definiciones de ciberdelitos, con sus respectivas sanciones físicas y monetarias, un catálogo disperso en distintos órdenes jurídicos.[9]

En 1999 se reformó el Código Penal Federal donde se añadió el capítulo "Acceso ilícito a sistemas y equipos de informática" que contenía un catálogo de delitos informáticos que en la actualidad se encuentran en el título noveno, denominado: "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.- 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.

[9] https://www.eleconomista.com.mx/amp/opinion/Los-estados-necesitan-una-ley-de-ciberseguridad-20210124-0004.html

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.

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.

Debido a este antecedente, se suscitaron diversos avances legislativos en materia de ciberseguridad, siendo algunos de estos:

- **12 de abril de 2005:** se presentó una Iniciativa que reformaba el Código Penal Federal, el Código Federal de Procedimientos Penales, la Ley Federal contra la delincuencia organizada, y la Ley de la Policía Federal Preventiva, en materia de delitos cibernéticos y de delitos contra menores.
- **28 de marzo de 2012:** Una iniciativa que reformaba el Código Penal Federal en materia de delitos en contra de medios o sistemas informáticos.
- **22 de octubre de 2015:** Iniciativa por la que se expedía la Ley Federal para prevenir y sancionar los delitos informáticos.
- **17 Abril 2018:** Iniciativa que expedía la Ley General de Seguridad Privada, reformaba la Ley General del Sistema Nacional de Seguridad Pública y abrogaba la Ley Federal de Seguridad Privada.
- **19 de marzo de 2019:** Iniciativa que expedía la Ley de Seguridad Informática.
- **10 Septiembre 2019:** Iniciativa para reformar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- **1 de Septiembre de 2020:** Iniciativa que la Ley General de Ciberseguridad.[10]

La iniciativa para que se emitiera la Ley General de Ciberseguridad, fue presentada por el senador Miguel Ángel Mancera, también incluía modificaciones de los siguientes

[10] https://contactaabogado.com/noticias-juridicas/derecho-informatico/en-que--consiste-la-ley-general-de-ciberseguridad-en-me-xico-320b/

ordenamientos: Código Penal Federal; Ley General del Sistema Nacional de Seguridad Pública; Ley General del Sistema Nacional de Seguridad, y Ley de Seguridad Nacional. Todo ello con el objeto de crear ordenamientos legales tendientes a prevenir, erradicar y combatir los delitos cibernéticos.

Entre los temas a resaltar en dicha iniciativa:

- La creación del Centro Nacional de Ciberseguridad.
- La creación de una comisión permanente de ciberseguridad en el interior del Consejo Nacional de Seguridad Pública, que se encargará de darle seguimiento al cumplimiento de las acciones del Centro Nacional de Ciberseguridad.
- La actualización del catálogo de cibercrímenes y sus penas.

Es de comentar que este instrumento legislativo, no fue bien recibido por todo el sector social, algunas organizaciones no gubernamentales se pronunciaron en contra, por considerar que algunas de las propuestas atentan contra la libertad de expresión y privacidad de los usuarios de internet en nuestro país, se criminaliza a las expresiones en internet, así como el uso legítimo de tecnologías, entre otros temas.

La monitorización del servicio de internet por parte de los proveedores del mismo, se contempla en el artículo 30 de dicha propuesta de ley, y abarca la vigilancia del tráfico y la difusión de información considerada prohibida, sin que se defina lo que se entenderá por "información prohibida" sabiendo que la seguridad informática es de gran importancia para el Estado, la sociedad y las empresas; sin embargo; si bien con la Ley de Ciberseguridad se pretende brindar más seguridad a usuarios de internet y las transacciones electrónicas, enfocándose con especial atención en la libertad de expresión y el uso libre de las tecnologías de la información.[11]

Entra las múltiples consecuencias derivadas del confinamiento por el Covid-19, es que se produjo un aumento de los ciberataques a las tecnologías de la Información y Comunicación (TICs), esto por el incremento en su uso a nivel mundial; sin embargo, en el caso particular de México, la ciberseguridad se convirtió en un tema particularmente complejo durante este

[11] https://contactaabogado.com/noticias-juridicas/derecho-informatico/en-que--consiste-la-ley-general-de-ciberseguridad-en-me-xico-320b/

periodo, por no contar con un marco regulatorio que ayude a mitigar los efectos de dichos ataques.

En la presentación del estudio "El Estado de la Ciberseguridad en México" de Metabase Q, diversos expertos en el ámbito de las TICs hablaron de la importancia de que nuestro país no solo cuente con un marco regulatorio en torno a la ciberseguridad, sino también de cómo debe integrarse este concepto en la cultura de la sociedad mexicana.[12]

En nuestro país, quienes desafortunadamente sufren más ciberataques son (pymes), esto es porque por sí solas representan un pilar importante en la economía mexicana, ya que generan alrededor del 70% del empleo formal y representan 52% del PIB nacional, según datos oficiales. El 79% de los ataques de ciberseguridad que sucedieron el año pasado fueron a pymes; hubo más de 4,000 millones de intentos por atacarlas.

De ahí la imperiosa necesidad de que en México exista un organismo de coordinación que integre al sector privado, al educativo y a gobierno para saber de forma coordinada el cómo prevenir, investigar, accionar y sancionar los temas de ciberseguridad.

Ante las posibles causas del porqué México es blanco para ataques cibernéticos se contemplan:

- La falta de un marco regulatorio sólido e innovador.
- La falta de programas en ciberseguridad efectivos (defensa y resiliencia cibernética).
- Una baja cultura de concientización sobre la importancia de la ciberseguridad.

Algunos de los ataques más recientes a instituciones mexicanas fueron los llevados a cabo contra la Condusef, el SAT y Banxico en julio de 2020.

En ese mismo año la Secretaría de la Función Pública también sufrió un ciberataque exponiendo información sobre declaraciones patrimoniales de 830 mil funcionarios públicos.

[12] https://businessinsider.mx/importancia-marco-regulatorio-ciberseguridad-mexico/

Posteriormente sucedió uno contra el ISSSTE, que expuso en internet durante un lapso indeterminado de tiempo la información de 551 asegurados del ISSSTE sin protección.

El caso más reciente fue el ataque de ransomware a la Lotería Nacional en junio de 2021, donde se encriptó información crítica, financiera, interna y de empleados, pidiendo un rescate a cambio de las claves para descifrar esta información y que no se publicara.

A pesar de los constantes ciberataques, en México existen esfuerzos para contar con un marco normativo que propicie la seguridad y confianza digital y como evidencia de esto, según el estudio, es la importancia otorgada a entidades como el INAI.

En 2017 el gobierno mexicano lanzó la Estrategia Nacional de Ciberseguridad (ENC) que precisa los objetivos, ejes transversales y actores involucrados para definir las acciones encaminadas al uso, aprovechamiento y seguridad de las TIC.

Con la publicación del 6 de septiembre de 2021 de la Estrategia Nacional Digital. Se promovía la implementación del Protocolo Homologado para la Gestión de Incidentes Cibernéticos entre Instituciones, buscando fortalecer la coordinación entre autoridades para mejorar la prevención de incidencias cibernéticas también se publicó el acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

No obstante contar con este tipo de legislación no es suficiente; se debe observar la infraestructura institucional necesaria para implementarla eficazmente, fomentar cultura y concientización de los ciudadanos mexicanos.[13]

No obstante lo señalado en "México y su posición en ciberseguridad" (publicado en 2019 por CIO México reporta que a pesar de que México en el Índice de Ciberseguridad Global (ICG) de La Unión Internacional de Telecomunicaciones (UIT) se posiciona en el número 28 de 193 países, en términos de preparación en seguridad cibernética, se coloca entre los tres primeros países de la región de las Américas, precedido sólo por los Estados Unidos y Canadá. Las mejores calificaciones de México son en materia legal y técnica, esto se comprueba con la Ley de Protección de Datos Personales en Posesión de los Particulares ya que se enfoca en una

[13] https://businessinsider.mx/importancia-marco-regulatorio-ciberseguridad-mexico/

mejor protección de los activos digitales, además México presenta continuos planes para desarrollar e implementar regulaciones mayores.

Por otro lado menciona que las compañías mexicanas podrían mejorar la distribución de los recursos asignados a ciberseguridad. Y de acuerdo con el *Reporte PwC, durante el 2015, la mayor parte de las empresas locales, solamente invirtieron 3.87% o alrededor de 5 millones de dólares norteamericanos en seguridad cibernética del total de su presupuesto para TI.*

Según el reporte *Ciberseguridad y privacidad: de la percepción a la realidad de PwC México, reveló que "las empresas mexicanas participantes están planeando incrementar exponencialmente -hasta en un 68%- su inversión en infraestructura de seguridad y hasta un 70.2% en detección de malware y medidas de prevención."* Aunque México está entre los países de América Latina más preparados y conscientes en seguridad cibernética, las empresas mexicanas deben lograr asegurar a sus empresas de manera interna e invertir en medidas de ciberseguridad apropiadas para los señalados riesgos cibernéticos.

Igual de importante es resaltar que derivado de la pandemia en el año 2020 en México se potenciaron los daños a infraestructuras críticas, fraudes, suplantación de identidad, ataques de *ransonware* y otros delitos cibernéticos. Tan sólo entre el 18 de septiembre y el 20 de octubre, se reportaron 2 mil 218 ciberataques contra ciudadanos, y 7 mil 964 contra instituciones privadas y públicas.

En los primeros 9 meses de 2020, se reportó que México ha sido el país más atacado en Latinoamérica, al recibir el 22.57 por ciento de 1 millón 319 mil 260 ataques de *ransonware* (secuestro de datos para pedir rescate), en agravio de 297 mil empresas, alerta Javier Juárez Mojica, comisionado del Instituto Federal de Telecomunicaciones (IFT).

Sólo entre el 18 de septiembre y el 20 de octubre de este 2020, la policía cibernética de la Guardia Nacional recibió 2 mil 218 reportes de ciberataques de ciudadanos, y 7 mil 964 incidentes de seguridad de instituciones privadas, públicas del país, como Nextel, CFE, Universidad de las Américas y el ITAM.

Aunado a ello, se investigaron 78 casos de trata de personas, pornografía infantil, secuestro, amenazas, desaparición forzada y extorsión, y se inhabilitaron 437 sitios web apócrifos que usurpaban instancias como gobierno de la Ciudad de México y del Instituto para Devolver al Pueblo lo Robado.[14]

El 25 de marzo 2021, la senadora Jesús Lucía Trasviña Waldenrath propuso la creación de la Ley General de Ciberseguridad y la derogación de diversas disposiciones del Código Penal Federal que lo convertiría en un instrumento de persecución contra discursos protegidos por el derechos a la libertad de expresión y de criminalización de personas usuarias de las Tecnologías de la Información y la Comunicación (TIC). Regular la ciberseguridad es uno de

[14] https://contralinea.com.mx/mexico-10-mil-ciberataques-al-mes/

los objetivos de la senadora desde 2020, en aquél momento propuso la creación de la "Ley de Seguridad Informática" que buscó sancionar de 4 a 8 años de prisión al que "ejecute un programa" que "altere el funcionamiento" de un "sistema informático", con lo cual hubiere criminalizado a toda persona usuaria de una computadora o dispositivo móvil.

Entre los puntos más importantes de dicha iniciativa están:

- La definición de ciberdelincuencia es sumamente vaga y amplia: "*Actividades que llevan a cabo individuo(s) realiza(n) en el que utilizan como medio o como fin a las Tecnologías de la Información y Comunicación*". Con esta definición toda actividad en internet podría considerarse como "ciberdelincuencia", lo cual genera confusión e inseguridad jurídica.
- En el entorno digital resulta complejo determinar quiénes son los sujetos de una obligación porque debe darse un análisis de todas las situaciones que se desarrollan ahí. Es decir, interactúan una multiplicidad de relaciones secundarias (por ejemplo, entre el sistema de hardware y software) además de una diversidad de proveedores que operan en las diferentes capas que configuran el espacio digital. Esta iniciativa no atiende esta complejidad lo que impide un acceso pleno a la justicia.
- Las acciones y conductas consideradas "ilícitas" ejercidas a través del uso desproporcionado de las TIC comienzan su creación, planificación y ejecución en el espacio físico por personas físicas e incluso morales. Por lo tanto, resulta compleja la imputación de responsabilidad a los sujeto(s) de la conducta ilícita, además de lo complicado para recaudar evidencias, presentación de peritajes, informes y todo lo relacionado para integrar la carpeta de investigación realizada por parte de las autoridades correspondientes.
- Existen otras definiciones que ponen en gran riesgo la protección de personas a su derecho a la libertad de expresión. El artículo 32 contempla la *Incitación a la Violencia y Alteración del Orden Social,* y establece que cualquier actividad a través de las TIC que ocasione "daño" a la "imagen o reputación" será penalizada con 2-10 años de prisión. Aunque la iniciativa de ley prevé excepciones a "expresiones que se realicen en apego a la libertad de expresión", también incluye limitaciones bajo términos amplios como "hostilidad" o "discriminación" lo cual permitiría una aplicación arbitraria en el sistema jurídico.
- No hay protección para las personas alertadoras (*whistleblowers*), puesto que el artículo 24 establece que cualquier persona que, "sin autorización" obtiene y usa información confidencial, enfrentaría una pena de 4 a 10 años en prisión, y más aún si se trata de propiedades del Estado. Lo anterior dejaría de incentivar a las personas que alerten sobre temas de corrupción, violaciones a los derechos humanos, delitos ambientales, alertas sobre redes de prostitución infantil entre otros hechos.

- La iniciativa no pasa la prueba tripartita de proporcionalidad en sentido amplio de idoneidad, necesidad y proporcionalidad en sentido estricto. Las penas son altas por crímenes que no están claramente formulados y existen sanciones severas que conducirán a la autocensura. Además la iniciativa alude a perseguir un fin constitucionalmente legítimo como es la libertad de expresión e información, sin embargo está justificada bajo todos los preceptos, sin antes evaluar si realmente tal restricción es idónea y proporcional, o si existen otras medidas menos lesivas para los derechos humanos y que logren el mismo fin.
- Se debe considerar que existe un marco legal que contempla varios delitos mencionados en la iniciativa como son el caso de abuso sexual y acoso, que son aplicables en el ámbito físico así como en el ámbito digital. Este tipo de iniciativas son redundantes y no significan mayor acceso a la justicia. [15]

LOCAL

Dentro del marco legal de la Ciudad de México, no se contempla ninguna Ley específica en materia de ciberseguridad, el código penal del Distrito Federal vigente, tampoco contempla ningún tipo penal por delitos cibernéticos, como ya señalamos que si lo hace el Código Penal Federal.

[15] https://articulo19.org/propuesta-de-ley-general-de-ciberseguridad-criminaliza-el-uso-cotidiano-de-internet-y-tiene-capacidad-de-censurar-la-critica/#:~:text=%E2%80%93%20El%2025%20de%20marzo%202021,libertad%20de%20expresi%C3%B3n%20y%20de

CONCLUSIONES

La importancia de crear la Ley de Ciberseguridad para así proteger al individuo y sus intereses, pero, cuando los problemas de afectación que llegan a surgir son nuevos, tal como pasa con la web y las redes sociales, es necesario que se elaboren nuevas leyes que garanticen la defensa de los ciudadanos.
La perplejidad de CIBERSEGURIDAD es un fenómeno social de naturaleza multifactorial. No requiere carta de presentación: es conocida por todos y padecida por cada uno de los sectores de nuestra sociedad, sin distinción de raza, sexo, edad, condición social o económica. Es sin duda uno de los mayores retos que habrá de enfrentar la Ciudad de México.

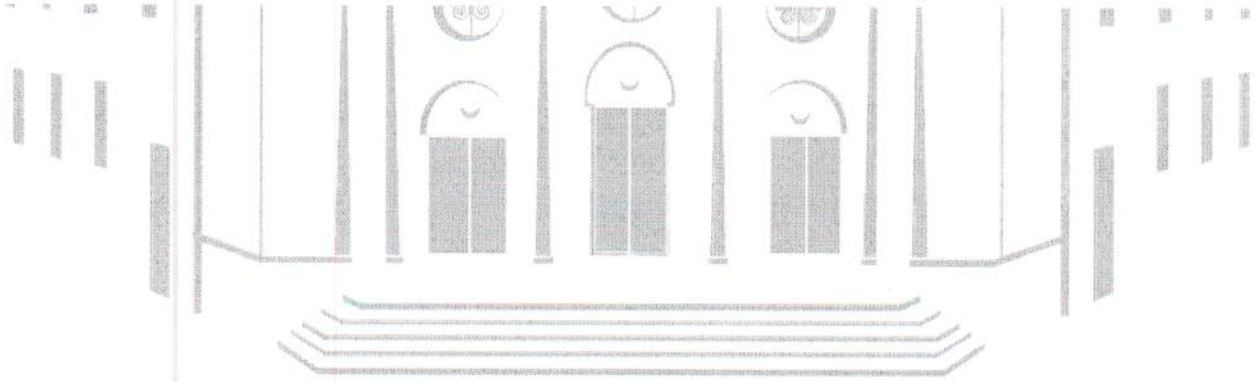
Por ello se plantea las necesidades de construir una nueva LEY entablado institucional que sitúe la seguridad y prevenir; esta propuesta es la expresión de varias vías para lograr sentar las bases de la convivencia armónica entre los ciudadanos. Además es importante avanzar en esta dirección, implica aceptar que se necesita edificar alianzas transversales e integrales, es decir, que se fortalezca una correlación de fuerzas, en la escuela, la familia, la comunidad y en los poderes del Gobierno de la Ciudad de México.

Debemos hacer frente a la raíz de la delincuencia cibernética, por lo cual es una propuesta programática para llenar el vacío de la asignatura pendiente y ausente, que es la ciberseguridad y delito.

Las carencias de políticas públicas en materia de ciberseguridad y el silencio a la actualización de una Estrategia Nacional de Ciberseguridad, ya cimentada y con buena participación de todos los niveles que la desarrollaron, es un punto vulnerable que requiere atención para estas nuevas amenazas digitales enunciadas a lo largo de este documento. Los pronunciamientos por parte de la autoridad pertinente son necesarios para poder colaborar y seguir trabajando cada uno desde su propia trinchera, pues son temas que no pueden ser minorizados o dejados a la deriva, ya que la población usuaria de tic crece día a día.

A nivel de seguridad nacional se entiende la confidencialidad de las autoridades para mantener información a resguardo; sin embargo, el ciberespacio es un medio propicio para que esta se vea filtrada. Lo ideal en un escenario de concientización de parte de la autoridad correspondiente es sumar esfuerzos con los usuarios de manera generalizada y abierta para su correcta participación como eslabones de esta cadena.

Finalmente, para aprovechar los beneficios que nos ofrece las tecnologías, es fundamental que existan reformas y marcos regulatorios, para contar con una normatividad en la gestión de seguridad de la información, que incorporen estrategias de ciberseguridad para la prevención, detección y respuesta a incidentes cibernéticos.



SISTEMA DE PORTALES DE OBLIGACIONES DE TRANSPARENCIA

COMPROBANTE DE PROCESAMIENTO

Fecha de emisión: 20/04/2022 18:13:45 Folio: 165049642149409

Organismo Garante:	Ciudad de México
Sujeto Obligado:	Congreso de la Ciudad de México
Fecha de registro:	20/04/2022 18:13:41
Nombre de archivo:	A125Fr18_Estudios-realizados-.xlsx
Tipo de operación:	Alta
Estatus:	INICIADO
Fecha Término:	
Registros Cargados Principal:	0
Registros Cargados Secundarios:	No Aplica

Estructura de la Normatividad

Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de
ARTICULO 125 FRACCION XVIII

Formato	Usuario
A125Fr18_Estudios-realizados-por-órganos-legislati	instituto.
Estudios realizados por órganos legislativos	