Los delitos cibernéticos dentro del T-MEC ¿Cumplimiento del Estado Mexicano?

Carrasco Palacios, Bogarth Alexander

2023-06-06

UNIVERSIDAD IBEROAMERICANA PUEBLA

Estudios con Reconocimiento de Validez Oficial

Por Decreto Presidencial del 3 de abril de 1981

PROYECTO JURÍDICO

"LOS DELITOS CIBERNÉTICOS DENTRO DEL T-MEC, ¿CUMPLIMIENTO DEL ESTADO MEXICANO?

Que para obtener el título de Licenciado en

DERECHO

Presenta

Bogarth Alexander Carrasco Palacios

Andrea Ramírez Ordaz

Sofia Sánchez Arenas

Gabriela Sumano Rodriguez

Directora del Trabajo de Titulación:

Mtra. Ana María Estela Ramírez Santibañez

San Andrés Cholula, Puebla

Primavera 2023

AGRADECIMIENTOS

A mi mamá, siempre me enseñaste que hay luchar y vivir cada día con bondad.

A mi papá, por siempre apoyarme en todas mis ideas.

A mi familia, por a lo largo de la vida mostrarme el significado de unidad.

A la Doctora Isabel Grañén y el C.P Alfredo Harp, por creer en mí y en los Oaxaqueños.

A mis compañeras de proyecto, por aguantarme y apoyarme en la realización de este trabajo.

A mis amigos, por ser la familia que escogí, por festejar la vida, por sobrepasar los baches y sobre todo por mostrarme que la vida de disfrutarse y se logra haciendo lo que nos gusta y rodeado de la gente que nos motiva.

Indivisa Manent

-Bogarth Alexander Carrasco Palacios

Agradezco a Dios por dejarme permitir llegar hasta este punto de mi carrera con altas y bajas pero siempre con su compañía.

A mi familia por apoyarme en cada momento, festejar mis logros como si fueran de ellos y por siempre estar para mi en esta ruleta de emociones que hemos vivido los últimos meses.

A mis compañeros y profesores por compartir este camino conmigo, lleno de enseñanzas, risas, enojos e inclusive llanto, sin ustedes no hubiera sido igual.

Le agradezco a mi abuelita que hasta el último momento estuvo pendiente de mi, sin ella y sin su amor incondicional no hubiera llegado hasta donde hoy estoy, físicamente ya no juntas pero siempre en mi mente y corazón.

Pero en especial agradecimiento y admiración a mi madre, que sin su esfuerzo, dedicación y amor nada de esto hubiera sido posible, es el primer paso para todo lo grande que viene y que haré en tu nombre.

-Andrea Ramírez Ordaz

Con profundo amor y agradecimiento:

A mi mamá, por enseñarme que el amor trasciende la vida, por acompañarme en todo momento del tiempo que estuvimos juntas y por su amor incondicional.

A mi papá, por brindarme su apoyo en todo momento y motivarme a seguir mis sueños.

A mi compañero de vida, mi hermano, por ser mi ejemplo a seguir e impulsarme todos los días a ser una mejor profesionista.

-Sofía Sánchez Arenas

Papá, gracias por impulsarme y motivarme, eres mi ejemplo a seguir y mi mayor inspiración, gracias por el amor incondicional que me das, por esas pláticas y los consejos que he puesto en práctica, gracias por siempre mostrarme el camino correcto y sobre todo, gracias por darme las alas y lanzarme al mundo a volar.

Mamá, mi mejor amiga, gracias por siempre creer en mí, por apoyarme en los momentos en los que me quería rendir, por nunca soltar mi mano y por amarme tanto, espero poder llegar a convertirme en la gran mujer que eres tú.

Joaco, mi compañero de vida, mi mejor amigo y cómplice, gracias por aconsejarme e inspirarme a convertirme en el abogado que eres tú.

Los ama…

-Gabriela Sumano Rodríguez

ÍNDICE

INTRODUCCIÓN

La presente investigación se realizó con la finalidad de visibilizar la falta de regulación jurídica y de organismos para poder combatir los delitos cibernéticos, ya que en los últimos años, debido al desarrollo de las tecnologías de la información han generado vacíos legales, de los cuales algunos sujetos se han apropiado para realizar una afectación al sujeto pasivo.

El primer capítulo, se enfocó principalmente en definiciones de elementos relacionados a los delitos informáticos, como: ciberseguridad, clasificación de algunos ciberdelitos, efectos que provoca su materialización, entre otros, para poder entender el objetivo del trabajo.

El segundo capítulo, se planteó lo solicitado en el T-MEC en cuestión de ciberseguridad, de igual forma se establecieron algunos aspectos que deben de realizar los Estados firmantes del tratado, para prevenir estas conductas antijurídicas.

De igual forma, se establecieron los cuerpos normativos de Estados Unidos de América y Canadá en los cuales se encuentran regulados estos delitos.

Posteriormente, en el capítulo tercero se realizó una exhaustiva investigación respecto a los ajustes en el marco mexicano en cuanto a la materia correspondiente, así como los distintos organismos y leyes creados para prevenir y sancionar los delitos informáticos desde la firma del T-MEC, siendo ésta en 2018.

Finalmente se plantearon distintas soluciones para la disminución de los ciberdelitos en un porcentaje considerable, así como para llevar un adecuado seguimiento de las medidas propuestas.

CAPÍTULO I. Importancia de la ciberseguridad

Los delitos cibernéticos han tenido una notable evolución e importancia en la vida diaria a través del paso de los años. Gracias a las Tecnologías de la Información y Comunicación y a su desmesurado uso han ocasionado la existencia de ataques a la sociedad de distintas formas, las cuales serán analizadas posteriormente.

Por lo consiguiente, optamos por investigar acerca del tema, dada su relevancia en los últimos años y la afectación que ha implicado en distintos sectores sociales de los múltiples países. Para efectos del presente texto, el estudio se enfocará específicamente en los Estados Unidos Mexicanos, Canadá y Estados Unidos de América, ya que son los Estados firmantes del T-MEC.

1.1 Definición de delitos cibernéticos y ciberseguridad

Es por ello que el tema ha sido estudiado por distintos autores e investigadores con mayor frecuencia y profundidad, existiendo distintas definiciones acerca del tema; sin embargo, expondremos las que a nuestro criterio tienen mayor relevancia por su contenido:

Donn B. Parker define a los delitos informáticos como “Todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”[1]

Mientras que Julio Téllez Valdés lo define como:

> Los delitos informáticos son aquéllas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables, establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el

[1] PARKER, Donn, cit pos.ROMEO CASABONA, Carlos Maria, *Poder Informático y Seguridad Jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información,* Madrid, FUNDESCO, Colección Impactos,1987, p.11

universo de funciones y organizaciones de un sistema tecnológico y económico.[2]

Por otra parte Luis Losa Camacho estima como delito informático: “Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas”[3]

Después de analizar diversos conceptos de delitos cibernéticos nos podemos percatar de la existencia de características en común, las cuales identificamos en una tabla para su mayor comprensión:

TABLA COMPARATIVA[4]

AUTORES	FORMA	MEDIO O INSTRUMENTO	OBJETO
DONN B. PARKER	ACTO INTENCIONAL (DOLOSO)	COMPUTADORAS	VÍCTIMA PUEDE SUFRIR UNA PÉRDIDA Y EL AUTOR PUEDE OBTENER UN BENEFICIO
JULIO TÉLLEZ VALDÉS	ACTITUDES CONTRARIAS A LOS INTERESES DE LAS PERSONAS (DOLOSA)	COMPUTADORAS	-
LUIS LOSA CAMACHO	ACCIÓN DOLOSA	DISPOSITIVOS UTILIZADOS EN LAS ACTIVIDADES INFORMÁTICAS	PROVOCA UN PERJUICIO A PERSONAS, SIN NECESARIAMENTE UN BENEFICIO MATERIAL PARA EL AUTOR

[2] TÉLLEZ VALDÉS, Julio, *Los Delitos Informáticos: Situación en México*, Extremadura, Mérida, UNED, 1996, p.461

[3] CAMACHO, Luis Losa, cit pos.LOREDO GONZÁLEZ, Jesús Alberto y RAMÍREZ GRANADOS, *Delitos Informaticos: su clasificación y una visión general de las medidas de acción para combatirlo*, México, UANL, Facultad de ciencias fisico matematicas, 2013, p.45

[4] TABLA COMPARATIVA: De realización propia, obteniendo la información de las definiciones y citas previas.

Seleccionamos los conceptos de los autores anteriormente mencionados, ya que consideramos son completos y claros. Como se puede identificar, los autores coinciden la mayor parte de las características que se deben de tener para considerarse como delito cibernético, por ejemplo: el hecho de que esta conducta antijurídica debe ser realizada por medio de un servidor, siendo este el principal recurso para cometer el delito, por otra parte, nos podemos percatar que los autores coinciden en que es una conducta de tipo dolosa ya que se deben de tener conocimientos informáticos para poder materializar estos delitos.

A partir de la información recuperada, podemos definir al delito cibernético como: Todo comportamiento intencional que se realiza por medio de un ordenador, en el cual se busca la afectación patrimonial, física, psicológica u afín por medio de engaños o de la materialización de un ataque informático al ordenador del sujeto pasivo, teniendo como resultado la búsqueda de un beneficio económico, social, cultural, entre otros para el sujeto activo.

Por otra parte, se analizará el concepto de ciberseguridad, también conocido como seguridad informática, que con base en la Unión Internacional de Telecomunicaciones (UIT), podemos establecerlo como este conjunto de herramientas, de acciones, de formación tecnológica e inclusive políticas las cuales que pueden ser utilizadas en un fin común, como es el de proteger la información de organizaciones y de usuarios en los ciber espacios. De igual forma, podríamos agregar a la ciberseguridad que se implementa para proteger la información, la cual es generada o procesada desde computadoras, servidores, así como dispositivos móviles y de igual forma las redes y sistemas electrónicos".

Como observamos de las definiciones previamente citadas, podemos percatarnos de que la ciberseguridad sirve como un método de prevención, un conjunto de medidas e instrumentos que se realizan e implementan con la finalidad de promover un espacio seguro para usuarios y consumidores de los distintos medios de telecomunicación. Conforme a lo que pudimos analizar al momento de estudiar las distintas ideas planteadas, la ciberseguridad es la medida de protección y previsión para evitar los delitos cibernéticos, de esta forma se busca salvaguardar el patrimonio y la integridad de las personas físicas y morales que son consumidores de los distintos medios; por lo tanto, concluimos que los delitos cibernéticos y la

ciberseguridad se encuentran relacionados con la finalidad de que a través de la ciberseguridad se puedan evitar ataques que tienen como medio algún dispositivo electrónico contra los diversos bienes jurídicos tutelados de terceros.

Consideramos que es una herramienta fundamental y viable ya que se propicia un consumo seguro, porque se tiene cierta certeza de que la información e integridad está siendo protegida de los delincuentes cibernéticos y del uso inadecuado de aquellos datos privados que se almacenan en el entorno digital.

1.2 Clasificación de delitos cibernéticos más comunes.

La evolución de la tecnología ha traído consigo muchos beneficios; sin embargo, al tratarse de campos nuevos de exploración, los delincuentes han hecho uso de esas anomias, con la finalidad de realizar acciones no autorizadas con repercusión en los bienes jurídicos tutelados del sujeto pasivo.

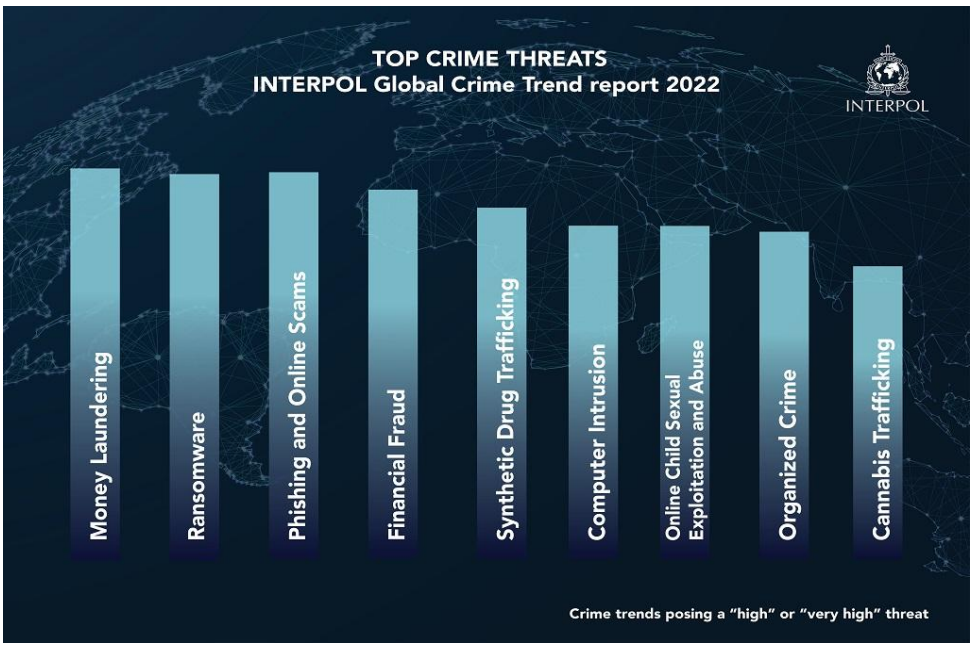
Después de tener una noción clara del significado de delitos cibernéticos y ciberseguridad, nos enfocaremos en explicar los distintos tipos, ya que existe una extensa lista de estas conductas antijurídicas. Para efectos de mayor comprensión e importancia de estudio, en el presente texto se analizarán los delitos cibernéticos más recurrentes.

Es importante mencionar que estos actos son efectuados en su mayoría en momentos construidos, además, realizadas de forma virtual, ya que no es necesario una interacción física de los sujetos del delito. Es por eso que es sustancial la implementación y desarrollo de una adecuada regulación de estos crímenes.

De acuerdo a información emitida por la Organización Internacional de Policía Criminal (INTERPOL) en el año 2022, la ciberdelincuencia se encontró en los primeros lugares, posicionando esta conducta delictiva como una representación de amenaza, incluso se menciona que son crímenes en incremento, para ejemplificar lo anteriormente expuesto, la INTERPOL emitió una gráfica de las amenazas de delitos más relevantes del año 2022:[5]

[5] TABLA QUE MUESTRA EL PORCENTAJES DE DELITOS A NIVEL MUNDIAL, *Los delitos financieros y los cometidos por internet son los que más preocupan a la policía de todo el mundo*, INTERPOL, Información visible en:https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Los-delitos-financieros-y-los-cometidos-por-Internet-son-los-que-mas-preocupan-a-la-policia-de-todo-el-mundo-segun-un-nuevo-informe-de-INTERPOL (fecha de consulta: marzon 2023)

TABLA QUE MUESTRA EL TOP DE PORCENTAJES DE DELITOS A NIVEL MUNDIAL[6]



Como se mencionó previamente, existen múltiples delitos informáticos, Donn B. Parker los clasifica de la siguiente forma[7]:

1.- **Fraudes**

1.1 Datos falsos o engañosos

1.2 Manipulación de programas

1.3 Falsificaciones informáticas

1.4 Manipulación de los datos de salida

1.5 Phishing

2.- Sabotaje informático

2.1 Bombas lógicas

---

[6]TABLA QUE MUESTRA EL PORCENTAJES DE DELITOS A NIVEL MUNDIAL, *Los delitos financieros y los cometidos por internet son los que más preocupan a la policía de todo el mundo*, INTERPOL, Información visible en:https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Los-delitos-financieros-y-los-cometidos-por-Internet-son-los-que-mas-preocupan-a-la-policia-de-todo-el-mundo-segun-un-nuevo-informe-de-INTERPOL (fecha de consulta: marzon 2023)

[7] Parker, D.B, citado en ROMEO CASABONA, op. cit. pp. 22-29

2.2 Gusanos

2.3 Gusanos

2.4 Virus informáticos y malware

2.5 Ciberterrorismo

3.- Espionaje informático y el robo o hurto de software

3.1 Fuga de datos

4.- Robo de servicios

4.1 Hurto del tiempo del computador

4.2. Paratismo informático y suplantación de personalidad

5.- Acceso no autorizado a servicios informáticos

5.1 La llave maestra

5.2 Pinchado de líneas

5.3 Piratas informáticos o hackers

En diversas instituciones y organizaciones se han enlistado los ciberdelitos más frecuentes en los últimos años. Con la finalidad de tener una mejor comprensión, mencionaremos los que a nuestro parecer tienen mayor relevancia[8]:

- Phishing
- Pharming
- Robo de identidad
- Spam
- Intrusión en servicios financieros en línea
- Acceso a material inadecuado (ilícito, violento, pornográfico, etc.)
- Ciberbullying
- Grooming

[8] CAMACHO, Luis Losa, citado en LOREDO GONZÁLEZ, op. cit. p 45.

A continuación se definirán los delitos cibernéticos cometidos con más regularidad en los últimos años, siendo importante tener conocimiento de cómo se realizan estas conductas antijurídicas.

El **Phishing.-** Es un delito en el cual el sujeto activo "phisher" se hace pasar como un contacto común a través de un correo electrónico, algún sistema de mensajería instantánea e incluso haciendo llamadas telefónicas para obtener la información requerida[9].

El **Pharming.-** Este delito se propicia por la vulnerabilidad de los equipos de los propios usuarios y consiste en que un tercero redirija un nombre de dominio a una máquina distinta.[10]

Robo de identidad.- Situación en la cual una persona obtiene, transfiere, utiliza o se apropia de manera indebida, de los datos personales de otra sin la autorización de ésta última, usualmente para cometer un fraude o delito.[11]

Spam.- También conocido como correo basura, se trata de un mensaje enviado a varios destinatarios que usualmente no lo solicitaron, con fines publicitarios o comerciales. La información de dicho correo te invita a visitar una página o descargar algún archivo que por lo general es un virus que roba la información de tu dispositivo.[12]

Ciberbullying.- Término que se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de comunicación como teléfonos móviles o tablets.[13]

---

[9] VIÑAMATA PASCHKES, Carlos, *La propiedad intelectual,* 7a ed, México, Trillas, 2017, p. 154.
[10] Ibidem
[11] Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, *¿Sabes qué es el Robo de Identidad?,* Informacion visible en: https://www.gob.mx/condusef/articulos/recomendaciones-para-prevenir-el-robo-de-identidad (fecha de consulta: marzo, 2023)
[12]Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, *Tipos de Fraude,* https://www.condusef.gob.mx/?p=tipos-de-fraude (fecha de consulta: marzo, 2023)
[13] CORONA, Pablo., "*Asociación de Internet, Mx", ¿Qué es el ciberbullying?,* 2017, Información visible en: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying (fecha de consulta: marzo, 2023).

Grooming.- Forma delictiva de acoso que implica a un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarse en una actividad sexual.[14]

Para efectos de una mejor comprensión de las estadísticas, se realizó una tabla comparativa de los Estados contratantes del T-MEC, tomando en cuenta tres ámbitos: el incremento de estas conductas, los delitos que se cometieron con mayor frecuencia y en este caso, se analizará únicamente la pérdida económica, tomando como parámetro cifras del año 2017 a la actualidad (siguiente página):

TABLA COMPARATIVA ENTRE PARTES DEL T-MEC[15]

PAÍS	DELITOS MÁS RECURRENTES	¿EXISTIÓ ALGÚN INCREMENTO?	AFECTACIÓN ECONÓMICA, RESULTADO DE ESTOS CRÍMENES
ESTADOS UNIDOS DE AMÉRICA[16]	Robo de identidad, fraudes de soporte técnico, phishing.	791,790 denuncias por delitos cibernéticos en 2020. Existió un aumento del 69% en comparación con el año 2019	Más de 4,200 millones de dólares en pérdidas
CANADÁ[17]	Delitos que van desde el fraude de banco o de tarjetas de crédito al robo de identidad.	El costo de los delitos informáticos en Canadá ha aumentado en los últimos 12 meses a 3 mil millones de dólares estadounidenses.	El costo directo promedio de delitos informáticos por víctima en Canadá es de aproximadamente 372 dólares
ESTADOS UNIDOS MEXICANOS[18]	Phishing, Robo de identidad, Pharming, Spam	En el 2019 los fraudes cibernéticos crecieron un 35% con respecto de 2018	El monto reclamado de los fraudes ascendió a 5,908 millones de pesos.

[14] *Grooming: ¿qué es, cómo detectarlo y cómo prevenirlo?,* Save the Children, 2019, Información visible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo (fecha de consulta: marzo, 2023)

[15] TABLA COMPARATIVA: De realización propia

[16] OWAIDA, Amer, *Denuncias de víctimas de delitos informáticos: aumentó de 69% en 2020*, WeLiveSecurity, ESET, 2021. Información visible en: https://www.welivesecurity.com/la-es/2021/03/19/denuncias-victimas-delitos-informaticos-aumentaron-2020/ (fecha de consulta: marzo, 2023).

[17] CHAPAMAN, Leonora, *7 millones de canadiense víctimas de Fraude en Línea*, Canadá, Política y Sociedad, RCI, 2017. Información visible en: https://www.rcinet.ca/es/2013/10/03/7-millones-de-canadienses-victimas-de-fraude-en-linea/#:~:text=El%20informe%20estima%20que%20siete,cr%C3%A9dito%20al%20robo%20de%20identidad.&text=%C2%ABEl%20cibercrimen%20este%20a%C3%B1o%20se%20ha%20duplicado%20desde%20el%20a%C3%B1o%20pasado%E2%80%A6 (fecha de consulta: marzo de 2023).

[18] MEDINA GÓMEZ, Diana, *Los Delitos Cibernéticos y los Problemas a Enfrentar*, México, UNAM, 2020.

Como se señaló, los Estados contratantes del T-MEC han contado con incrementos notorios en la comisión de ciberdelitos, los cuales han ocasionado pérdidas económicas evidentes, además, las conductas realizadas en su mayoría han sido las mismas en los tres Estados; por lo tanto, la creación y puesta en práctica de medidas de seguridad es urgente para poder brindar un ciber entorno seguro para la sociedad.

1.3. Efectos que genera esta conducta antijurídica

Tal como se expuso en los temas previamente estudiados, la ciberdelincuencia es una conducta que tiene como resultado una afectación para el sujeto pasivo, ya sea en personas físicas o jurídicas, independientemente si estas últimas son privadas o públicas; sin embargo, es importante saber que tipo de efectos produce, ya que se interfiere en una diversidad de bienes jurídicos tutelados.

Para los autores Claudio Magliona y Macarena López, los delitos informáticos tienen el carácter de pluriofensivos, esto quiere decir "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo"[19]

Lo anteriormente expuesto quiere decir que no solo afectan sectores económicos, sino que influye en ámbitos como:

- La intimidad.
- Integridad de las personas.
- Datos personales (confidencialidad).
- Repercusión social.
- Reputación.
- Oportunidades de negocio/ pérdida de percepción de futuros ingresos.
- Pérdida de clientes y proveedores.
- Aspectos culturales.
- Seguridad.
- Democracia

[19] MAGLIONA MARKOVICTH, Claudio y LÓPEZ MEDEL, Macarena, D*elincuencia y Fraude Informático*, Chile, Editorial Jurídica de Chile, 1999, p.211.

Los Estados contratantes del T-MEC han implementado políticas y destinado millones de pesos, a la lucha contra los delitos informáticos con la finalidad de fortalecer su ciberseguridad. Canadá destinó más de 14 billones de dólares para prevenir, detectar y recuperarse de los incidentes que fueron ocasionados en el año 2017[20]; por otra parte, México dispuso más de mil 100 millones de dólares en el año 2021[21] y finalmente, Estados Unidos de América asignó 18.78 billones para gastos de ciberseguridad en 2021[22].

La Unión Internacional de las Telecomunicaciones (UIT) es un organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación, el cual emitió gráficas en el año 2020 acerca de un cuestionario el cual tenía como objetivo comprender las bases de seguridad cibernética que han adoptado los distintos países. Se realizaron alrededor de 82 preguntas, tomando en consideración cinco medidas:

•Legales.- Legislación y regulación del cibercrimen y la ciberseguridad.

•Técnicas.- Implementación de técnicas y herramientas, así como de mecanismos de protección.

•Organizativas.- Estrategias, agencias e iniciativas implementadas.

•Desarrollo de capacidades.- Campañas de concientización, capacitación cibernética.

•De cooperación.- Alianzas y colaboraciones entre agencias, empresas y países.

A continuación se muestran los resultados obtenidos por los países contratantes del T-MEC obtuvieron los siguientes resultados:

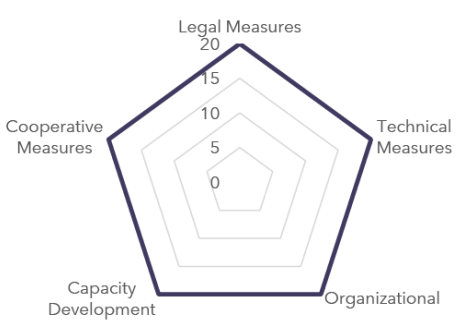
---

[20] STASTICS CANADA, Impact of cybercrime on Canadian buisinesess 2017, información visible en: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm (fecha de consulta: marzo, 2023)

[21] SERRANO, Alex, “México aumenta inversión en ciberseguridad”, *DPL News*; México, serie 2, 2021, Julio-Diciembre 2021.

[22] AUTOR, f, “Gobierno de Estados Unidos gastará más de 18 millones en ciberseguridad”, *El Mundo*, Seattle, Washington, nueva serie, número 23, Enero-Junio 2020.

Gráfica UIT Estados Unidos de América[23]



Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative, Capacity Development Measures

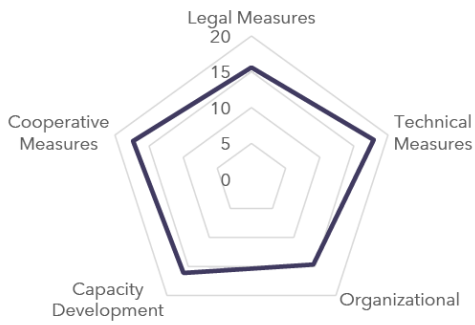
Area(s) of Potential Growth
N/A

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
100.00	20.00	20.00	20.00	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2020

Como se puede observar, Estados Unidos de América cuenta con una calificación sobresaliente, obteniendo el máximo, siendo considerado un país desarrollado, además sin ningún área débil, ya que en todas demostró solidez.

Gráfica UIT Estados Unidos Mexicanos[24]



Development Level:
Developing Country

Area(s) of Relative Strength
Technical, Cooperative Measures

Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.68	15.61	17.90	14.70	16.13	17.34

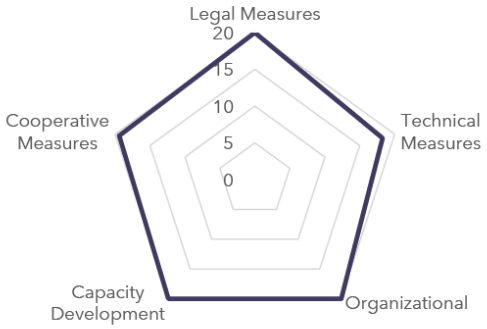
Source: ITU Global Cybersecurity Index v4, 2020

[23] Gráfica UIT Estados Unidos, Global Cybersecurity Index 2020: Country Profiles, American Region, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: marzo, 2023)

[24] Gráfica UIT Estados Unidos Mexicanos, Global Cybersecurity Index 2020: Country Profiles, American Region, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: marzo, 2023)

México obtuvo un puntaje bueno, a pesar de ser considerado un país en desarrollo; sin embargo, cuenta con áreas las cuales puede perfeccionar.

Gráfica UIT Canadá[25]



Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Organizational, Capacity Development Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.67	20.00	18.27	20.00	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2020

Finalmente, Canadá alcanzó un puntaje óptimo, siendo un país desarrollado, empero existen áreas débiles como las técnicas en las cuales puede progresar.

Como se puede notar los daños ocasionados por los delitos cibernéticos pueden llegar a ser extremos, es por eso, que empresas, instituciones y personas físicas deben de contar con la cultura de la prevención, para así evitar los ciberataques y posterior a esto contar con un seguimiento y sanción de esas conductas antijurídicas. De igual forma formar alianzas internacionales y ampararse conjuntamente.

[25] Gráfica UIT Canada, Global Cybersecurity Index 2020: Country Profiles, American Region, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: marzo, 2023)

Capítulo II. Regulación de la ciberseguridad en el T-MEC

En el capítulo anterior se plantearon las bases del enorme mundo que abarca la ciberseguridad y los delitos cibernéticos o informáticos, como se pudo observar existe una gran variedad de enfoques, delitos, opiniones y vías de acción. Por lo que un solo plan o lineamiento que seguir en general sería muy extenso, es por eso que los países han fomentado estrategias y cuerpos normativos de acuerdo al contexto de sus propias necesidades. Sin embargo en un mundo tan globalizado, las interacciones entre naciones y diferentes países es algo diario y sumamente común; por lo que entre los mismos socios comerciales deberá existir una concordancia y consistencia en los medios de protección para generar entre ellos mismo la seguridad jurídica y el fomento de colaboración.

Por ende el 30 de noviembre de 2018 se firmó el Tratado entre México, Estados Unidos y Canadá (T-MEC), el cual entró en vigor el 1 julio de 2020 y tomando el lugar del previo Tratado de Libre Comercio de América del Norte firmado por la mismas naciones en 1994; el T-MEC tiene un vigencia de 16 años y una revisión cada 6 años. Este acuerdo trae varias nuevas disposiciones y beneficios en diferentes materias, pero para este trabajo se mencionan únicamente las relativas al tema del mismo.

2.1 Lo solicitado en el T-MEC

En su capítulo 19 el T-MEC desglosa el tema de Comercio Digital y dentro nos menciona los temas relativos como son la ciberseguridad, las pautas y acciones que deberá seguir cada nación partes para generar una seguridad jurídica en el contexto de los delitos informáticos. Los objetivos que se pueden esgrimir del mismo, son, impulsar el desarrollo de este tipo de comercio, brindando seguridad dentro de los diferentes medios electrónicos, así como promover e innovar las cuestiones de los servicios digitales y prevenir el riesgo a través de procedimientos y mecanismos.

Dentro de este capítulo y precisamente en el artículo 19.15 el T-MEC hace referencia concreta a la ciberseguridad y establece el reconocimiento de las Partes del tratado a visualizar las amenazas cibernéticas que pueden causar problemas

dentro del comercio digital y otras áreas. El artículo establece, en su primer numeral, 2 puntos importantes que los Estados deberán procurar:[26]

1. *desarrollar las capacidades de sus entidades nacionales responsables de la respuesta a incidentes de ciberseguridad.*
2. *fortalecer los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones maliciosas o la diseminación de códigos maliciosos que afecten a las redes electrónicas y utilizar esos mecanismos para tratar rápidamente los incidentes de ciberseguridad, así como el intercambio de información para el conocimiento y las mejores prácticas.*

Mientras que en su segundo numeral, el mismo artículo, hace mencion de integrar a las empresas dentro de cada jurisdicción como una forma de respuesta a los riesgos de ciberseguridad existentes “emplear y alentar a las empresas dentro de su jurisdicción a utilizar enfoques basados en riesgo que dependan de normas consensuadas y mejores prácticas de gestión de riesgos para identificar y proteger contra los riesgos de ciberseguridad y detectar, responder y recuperar de eventos de ciberseguridad.”

Como se pude observar es un artículo demasiado corto el dedicado al tema de seguridad contra los ciberdelitos, no establecen medidas de conducció, de legislación o de algún elemento jurisdiccional concreto; se compone de directrices que las Partes deberán seguir y hacer de manera prioritaria, como son la prevención, el fortalecimiento, la colaboración y la respuesta rápida a incidentes. Sin embargo, cuestiones de ciberseguridad y relativas a los delitos informáticos se desglosan durante más artículos del capítulo 19, los cuales establecen pautas procesales e inclusive legislativas obligatorias para los Estados Parte.

En un primer momento el capítulo en cuestión, establece en su artículo 19.2 Ámbitos de Aplicación y Disposiciones Generales, la importancia de marcos que promuevan la seguridad y eviten los incidentes que obstaculicen el desarrollo, así como las medidas existentes o promovidas que no prevengan la seguridad de los individuos respecto a estos delitos[27]. Es hasta el artículo 19.5 Marco Nacional de las Transacciones Electrónicas, donde se establece un cuerpo jurídico al que los

[26] Vid. artículo 19.15 del Tratado entre México, Estados Unidos y Canadá
[27] Cfr. artículo 19.2 del Tratado entre México, Estados Unidos y Canadá

Estados deberán apegarse, en su numeral primero se menciona “Cada Parte mantendrá un marco legal que rija las transacciones electrónicas y que sea compatible con los principios de la *Ley Modelo de la CNUDMI sobre Comercio Electrónico 1996”.* El texto legislativo mencionado fue preparado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), redactada en 1985 y enmendada en 2006, consta de 36 artículos y 8 enmiendas; es por la cual el T-MEC se decanta para apegarse y establecer un proceso, en este caso de arbitraje, en el que se puedan resolver las controversias en comercio electrónico y de donde se desprenden delitos previamente mencionados en este trabajo como son las operaciones fraudulentas[28].

El tratado menciona por primera vez en este capítulo, protección al consumidor, hasta su artículo 19.7 Protección al Consumidor en Línea, donde establece varios puntos:[29]

- Las partes reconocen la importancia de adoptar y mantener medidas transparentes y efectivas para proteger a los consumidores.
- El adoptar y mantener leyes de protección al consumidor para prohibir prácticas fraudulentas y engañosas
- La importancia de la cooperación entre sus respectivas agencias u otros organismos nacionales pertinentes para la protección del consumidor.

Dentro del mismo artículo se establece una correlación con el capítulo 21 “Competencia”, en su enunciado de “Protección al consumidor”, del cual haremos mención más adelante.

De las conductas jurídicas más frecuentes y previamente mencionadas en el primer capítulo, subtema 1.2 de este trabajo; podemos encontrar con especificidad 2 conductas: Robo de Identidad y SPAM. La primera el Robo de Identidad reflejado en el artículo 19.8 Protección de la Información Personal. Reconociendo los beneficios, la protección y sobre todo la confianza generada por la seguridad jurídica, el T-MEC insta a los Estados parte a mantener o desarrollar un marco legal funcional para la salvaguardar la información personal de las personas, el tratado menciona que dicho marco legal deberá: “considerar las directrices y principios de organismos

[28] Vid. Ley Modelo de la CNUDMI sobre Comercio Electrónico 1996
[29] Cfr. artículo 19.7 del Tratado entre México, Estados Unidos y Canadá

internacionales pertinentes, tales como el Marco de Privacidad de APEC y la Recomendación del Consejo de la OCDE relativa a las directrices para la Protección de la Privacidad y Flujo Transfronterizo de Datos Personales (2013)"[30]. El primer organismo mencionado del Foro de Cooperación Económica Asía Pacifico (APEC), a lo largo de cuatro partes desarrolla puntos importantes para los Estados Parte, como lo son, el alcance, los principios y dentro de estos podemos dar observancia a disposiciones como lo son la prevención, las medidas, la corrección, entre otras; y la última parte referente a su implementación[31]. Por su parte el segundo organismo mencionado realizado por la Organización para la cooperación y el Desarrollo Económico (OCDE), a lo largo de 5 partes nos brinda directrices por las cuales los Estados deben guiarse; entre dichas partes vemos las generalidades, principios básicos nacionales, principios básicos internacionales, la implantación nacional y la última es la cooperación internacional[32]. De lo anterior y dentro del mismo artículo el Tratado desprende los siguientes principios: [33]

- Limitación de la recolección
- Elección
- Calidad de datos
- Especificación de propósito
- Limitación de uso
- Salvaguardias de seguridad
- Transparencia
- Participación individual
- Responsabilidad

Guiados por los principios mencionados deberán ser las medidas garantizadas por las Partes, para que el flujo de datos y el aseguramiento de estos sean necesarios y las anteriores sean proporcionales al riesgo[34]. El apego de las medidas y el marco aplicable por cada Estado deberá partir debera ademas seguir 2 días principales, sobre todo el tiempo dichas medidas no deberán discriminatorias; la segunda idea es que dichas medidas o procesos realizados deberan cumpli con transparencia,

[30] Cfr. artículo 19.8 del Tratado entre México, Estados Unidos y Canadá
[31] Vid. Marco de Privacidad del Foro de Cooperación Económica Asía Pacifico (APEC)
[32] Vid. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales
[33]Vid. artículo 19.8 del Tratado entre México, Estados Unidos y Canadá
[34] Cfr. artículo 19.8 del Tratado entre México, Estados Unidos y Canadá

informado a los individuos sobre dichas maneras de protección, ejercer recursos y cumplir los requisitos. El artículo cierra dando libertad de enfoque a cada Parte, sin despegarse de los principios y directrices mencionados, lo que sí establece es una cooperación como el intercambio de información[35].

La segunda conducta establecida es el Spam, dentro del artículo 19.13 Comunicaciones no solicitadas, el T-MEC aborda de manera concreta, que los Estados Parte deberán adoptar medidas para prevenir este delito y establece 2 puntos fundamentales a saber [36]:

> *Cada Parte adoptará o mantendrá medidas relativas a las comunicaciones electrónicas comerciales no solicitadas enviadas a una dirección de correo electrónico que:*
>
> *(a) requiera a los proveedores de mensajes electrónicos comerciales no solicitados facilitar la capacidad de los receptores para impedir la recepción continua de aquellos mensajes;*
>
> *(b) requieran el consentimiento de los receptores, según se especifique de acuerdo con las leyes y regulaciones de cada Parte, para recibir mensajes electrónicos comerciales*.

Derivado de lo anterior en el numeral segundo, del artículo mencionado, las Partes de igual manera adoptarán medidas las cuales puedan permitir a los mismos individuos de manera preferente evitar dichas comunicaciones electrónicas no deseadas, aunque una primera meta es la reducción de esto. Al igual que con la conducta de protección de datos personales, los Estados manejan un estado de cooperación; algo importante que mencionar es lo establecido en el numeral cuarto "Cada Parte proporcionará recursos contra los proveedores de comunicaciones electrónicas comerciales no solicitadas"[37].

Cerramos el capítulo 19 del T-MEC, sin embargo no terminamos de ver lo solicitado con respecto a nuestro tema. Como previamente lo mencionamos el capítulo 21 Política de Competencia y precisamente en su artículo 21.4 Protección al

[35] Cfr. artículo 19.8 del Tratado entre México, Estados Unidos y Canadá
[36] Vid. artículo 19.13 del Tratado entre México, Estados Unidos y Canadá
[37] Vid. artículo 19.13 del Tratado entre México, Estados Unidos y Canadá

Consumidor, el mismo tratado reitera la importancia de medidas de protección al individuo y el cumplimiento de las disposiciones. De manera sumamente importante mencionado en el numeral segundo[38]:

> *Cada Parte adoptará o mantendrá leyes nacionales de protección al consumidor u otras leyes o regulaciones que prohíban actividades comerciales fraudulentas y engañosas, reconociendo que el cumplimiento de esas leyes y regulaciones sean del interés público. Las leyes y regulaciones que una Parte adopte o mantenga para prohibir estas actividades podrán ser de naturaleza civil o penal*.

De este texto podemos observar como el mismo tratado faculta a los Estados para generar sus marcos nacionales, bajo la idea de interés público; así mismo menciona la naturaleza de los actos de ser de manera civil o penal, dándole naturaleza y vía de conducción a cada delito o conducta antijurídica.

Dentro de sus siguientes y últimos tres numeral se plantea el reconocimiento por los mismo Estados Partes sobre el crecimiento transfronterizo de las actividades, además de la idea de una cooperación y coordinación fundamental.

Estas son las ideas que establece el T-MEC conforme a nuestro tema, lo solicitado, lo recomendado y la obligación a las que adhirieron los Estados Parte. Debido a la dificultad de hablar de 2 conductas antijurídicas, engloba en una generalidad los puntos de acción y profundiza en 2 de manera precisa. A lo largo del Tratado se han hecho referencias a estos apartados u otros puntos de interés, sin embargo esto es lo principal y lo que se ajusta a nuestro trabajo de investigación.

2.2 La ciberseguridad en los cuerpos normativos de Estados Unidos y Canadá

Los Estados Parte que trataremos en este subtema, tienen ya un antecedente importante en la regulación de los delitos informáticos, por lo que se decidió además de separarlos de México, darle un enfoque menor al nuestro; esto también permite un enfoque del estudio e individualiza a nuestra nación. Aunque dentro del tratado identificamos una obligación compartida, al terminar este subtema podremos darnos

[38] Vid. artículo 21.4 del Tratado entre México, Estados Unidos y Canadá

cuenta que en su mayoría comparte semejanzas con las directrices y estrategias de estos Estados Parte.

Al realizar esta investigación llegamos a cuestionar un caso, pareciera que lo relativo a los delitos cibernéticos lo dictaron estas 2 naciones y México solo lo firmó. Este subtema se enfoca en dar una perspectiva general de los delitos cibernéticos en ambas naciones, sin embargo se enfoca más en lo estipulado dentro del T-MEC

Canadá

De acuerdo con el Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), en su apartado “Desarrollos por País”, esta nación cuenta en su derecho sustantivo con una legislación de delitos cibernéticos dentro de su propio Código Penal, dentro de sus artículos 163, 184, 342, y 430; sobre crímenes relacionados cuenta con el Declaración c-15a, Protección para información personal y documentos electrónicos, el Acta de Radio Comunicación en sus artículos 9 y 9.1, además de otros artículos de su código penal como el 318,319 y 322[39]. Respecto a su derecho procesal, el mismo portal nos menciona su código procesal en los artículos 164.1, 185, 186, 487 2.1, 487 2.2 y el 492.2[40], en manera de apoyo la legislación candiense de acuerdo al portal de la OEA cuenta también con artículos dentro de su propio código penal como 487.01, 487.02, 487.03, 492.1 y 492.2, así como las enmiendas realizadas en 2016 a la legislación anterior y el Acta de Competencias artículos 15 y 16[41].

[39] Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), *Desarrollos por País: Canadá.* Información visible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Canada (fecha de consulta: abril, 2023)
[40] Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), *Desarrollos por País: Canadá.* Información visible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Canada (fecha de consulta: abril, 2023)
[41] Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), *Desarrollos por País: Canadá.* Información visible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Canada (fecha de consulta: abril, 2023)

TABLA DEMOSTRATIVA[42]

-	Derecho Sustantivo	Derecho Procesal
Precisamente sobre delitos cibernéticos	Código Penal, artículos 163, 184, 342, y 430	Código Procesal artículos 164.1, 185, 186, 487 2.1, 487 2.2 y el 492.2
Crímenes relacionados / Adicionales	Crímenes Relacionados: -Declaración c-15a -Protección para información personal y documentos electrónicos, -Acta de Radio Comunicación en sus artículos 9 y 9.1 -Código Penal artículos 318,319 y 322	Adicionales: -Código Penal artículos 487.01, 487.02, 487.03, 492.1 y 492.2 -Enmiendas realizadas en 2016 a la legislación anterior -Acta de Competencias artículos 15 y 16

Es de observancia, ver como la legislación candiense no establece una ley, declaración, acta o hasta capítulo, donde se puedan encontrar todo lo relacionado en cuestión de estos temas. Dentro de los artículos previamente enunciados, podemos destacar conductas jurídicas como el Pharming, Phishing, Fraude, Robo de identidad y sabotaje informático; en relación con el T-MEC por parte de la legislación Canadiense, en estos artículos mencionados, vemos una mayor atención a la protección de datos personales, a través de su enunciado en su Código Penal Ofensas semejantes al Robo (Offence Resembling Theft)[43], donde hace mención del robo, duplicado o falsificación de tarjetas de créditos, así como de datos a través de programas computacionales.Sin embargo lo más importante a tomar en cuenta de esta Nación en su combate contra los delitos cibernéticos es la estrategia que han

[42] TABLA DEMOSTRATIVA: De realización propia, obteniendo la información de las definiciones y citas previas.
[43] Cfr. artículo 335, 342 del Código Penal de Canadá (Criminal Code)

realizado desde 2010, como preámbulo, pero renovada y actualizada durante el mandato de Justin Trudeau[44].

Dicha estrategia se enfocado en el dinamismo de las conductas y en la cooperación de los ciudadanos; pues el Gobierno Federal Canadiense busca una colaboración intensa con los diferentes niveles de gobierno, destacando con las provincias y territorios, externa con los organismos internacionales, pero además el apoyo como mencionamos de los ciudadanos, en especial de la Academia y del Sector Privado. Con el fin de establecer una infraestructura de seguridad, colaboración, privacidad y uso personal[45]. Estrategia a través de la cual se han realizado financiamientos para en su momento desarrollar y actualmente mantener el Centro Canadiense de Seguridad Cibernética, así como la Unidad Nacional de Coordinación de Ciberdelito[46]. Organismos que complementan los planes de acción de ciberseguridad en Canadá y apoyan en la investigación de delitos, financiamiento e innovación del ámbito digital en este país.

El Centro Canadiense de Seguridad Cibernética, como lo establece en su portal gubernamental, forma parte del Establecimiento de Seguridad de las Comunicaciones y además de ser establecida como la "única fuente unificada de asesoramiento, orientación, servicios y apoyo de expertos en seguridad cibernética para los canadiense"[47]; dentro del centro podrás realizar un reporte de incidente cibernético, consultar información especializada para individuos, pequeñas y medianas empresas, grandes organizaciones e inclusive instituciones gubernamentales y de academia. Por su parte la Unidad Nacional de Coordinación de Ciberdelito adjunta la Real Policía Montada de Canadá, es la unidad especializada para la prevención, investigación y asesoramiento sobre delitos cibernéticos; cuenta con una colaboración de oficiales y socios del sector civil que apoyan a cumplir sus tareas, en este año (2023) están lanzando el nuevo sistema nacional de denuncia de ciberdelitos[48].

---

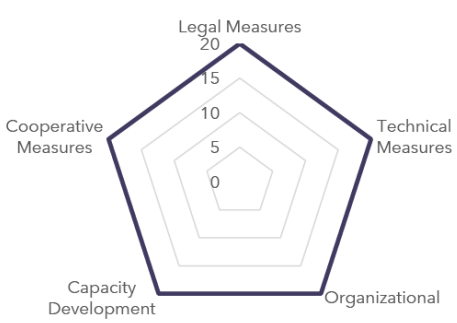
[44] MACUARAN OCHOA, Maria Fernanda, *La evolución de la política de ciberseguridad de Canadá entre 2010 y 2018*, Barcelona, Universitat Autónoma de Barcelona, 2019, pp. 6-8
[45] Idem p.10
[46] Idem p. 9
[47] Government of Canada, Canada Center of Cybersecurity, información visible en: https://www.cyber.gc.ca/en (fecha de consulta: abril, 2023)
[48] Royal Canadian Mounted Police, The National Cybercrime Coordination Center, información visible en: https://www.rcmp-grc.gc.ca/en/nc3 (fecha de consulta: abril, 2023)

Por último dentro de esta estrategia Canadá creó una campaña denominada “GetCyberSafe.CA”, dentro de su página web podemos observar que se trata de “campaña nacional de concientización pública creada para informar a los canadienses sobre la seguridad cibernética y los pasos simples que pueden tomar para protegerse en línea.”, página gubernamental en la que distinguen diversos recursos sobre distintos delitos cibernéticos para fomentar una cultura preventiva y de conocimiento dentro de su misma sociedad[49].

Estados Unidos

Este Estado Parte del T-MEC es el mejor calificado de los tres por parte de La Unión Internacional de las Telecomunicaciones (UIT)

Gráfica UIT Estados Unidos de América[50]



Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative, Capacity Development Measures

Area(s) of Potential Growth
N/A

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
100.00	20.00	20.00	20.00	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2020

Cumpliendo todos los aspectos de calificación, catalogado como desarrollado y sin áreas de potencial desarrollo, además de ser rankeado por la misma UIT como el mejor país a nivel global en tema de ciberseguridad

[49] Government of Canada, GetCyberSafe.CA, información visible en: https://www.getcybersafe.gc.ca/en (fecha de consulta: abril, 2023)
[50] Gráfica UIT Estados Unidos, Global Cybersecurity Index 2020: Country Profiles, American Region, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: marzo, 2023)

Ranking Global UIT[51]

3.1 Global scores and ranking of countries

The following table sets out the score and rank for each country that took part in the questionnaire.

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5

Estos resultados son debido a que Estados Unidos tiene bastante tiempo de haber promulgado leyes, que aunque en ese momento no se vislumbraba como ciberseguridad, daban los primeros matices de importancia. Tal es el caso de la Ley Gramm-Leach Billey de 1999, en la cual "se reformó la industria de servicios financieros, permitiendo que los bancos comerciales y de inversión, las empresas de valores y las compañías de seguros se consolidaran y abordaban las preocupaciones sobre la protección de la privacidad de los consumidores"[52]; previo al inicio de este milenio Estados Unidos ya promulgaba una ley para la protección de información personal, como los datos confidenciales de cada consumidor.

Hablemos de su actualidad, de acuerdo con el portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), en su apartado "Desarrollos por País", esta nación cuenta en su derecho sustantivo con su Código Penal Federal, que es el Título 18 del "U.S CODE" que refiere a "Crímenes y Procedimientos Criminales"[53]; involucrando actos precisos como el fraude, la intercepción de comunicación, la pornografia, falsificación de datos, robo de datos y

[51]Rankin Global UIT, GCI Results: Score and Rankings, Global scores and rankings of countries, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: abril, 2023)
[52] Microsoft Build, Ley Gramm-Leach Billey de 1999, visible en: https://learn.microsoft.com/es-es/compliance/regulatory/offering-glba (fecha de consulta: abril, 2023)
[53] Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), *Desarrollos por País: Estados Unidos.* Información visible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Estados%20Unidos (fecha de consulta: abril, 2023)

desvío de documentos. Con base a lista establecida en el capítulo 1 y en relación al T-MEC atendemos de lo anterior conductas como, el fraude, fuga de datos, robo de servicios, comunicaciones no deseadas (spam), phishing y pharming. En cuanto al derecho procesal cuenta con una ley procesal de delitos informáticos que parte del Título 18 del "U.S CODE" que refiere a "Crímenes y Procedimientos Criminales", de los artículos 2510 a 2522 y 2701 a 2712[54].

Además de mencionar cuenta con una agencia parecida a la observada en Canadá, encargada de varias funciones la cual es la Agencia de Seguridad en Ciberseguridad e Infraestructura (CISA), la cual se refiere a sí misma como "Como agencia de defensa cibernética de la nación, CISA está lista para ayudar a las organizaciones a prepararse, responder y mitigar el impacto de los ataques cibernéticos"[55]. Dentro de su página web podemos ver el apoyo a familias, pequeñas y medianas empresas, grandes corporaciones y directores ejecutivos, así como acciones de respuestas, guías e información básica para la concientización de temas. También esta agencia contempla la colaboración organizacional y la transparencia hacia la sociedad con las medidas que elaboran para su protección, recordar que este es otro de los puntos importantes establecidos por el T-MEC. Siendo una agencia muy parecida al Centro Canadiense de Seguridad Cibernética; con la diferencia de acción en este y de exclusión de la Academia.

En marzo de 2021, tras 2 meses de que el presidente Joe Biden asumiera el cargo como el 46o presidente de los Estados Unidos, el secretario Mayorkas del departamento de Seguridad Nacional de los Estados Unidos, mencionó lo siguiente "El presidente Biden ha hecho de la seguridad cibernética una prioridad principal para la Administración Biden-Harris en todos los niveles de gobierno.". 2 años después, marzo de 2023, la Casa Blanca publicó la "Estrategia Nacional de Ciberseguridad", para seguir actualizando sus marcos legales, sus campañas y sus instituciones, ante una creciente marcha de la era digital y sus delitos.

---

[54]Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), *Desarrollos por País: Estados Unidos.* Información visible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Estados%20Unidos (fecha de consulta: abril, 2023)

[55]Homeland Security, Cybersecurity, Información visible en: https://www.dhs.gov/topics/cybersecurity (fecha de consulta: abril, 2023)

A lo largo de 39 páginas, desarrolla dicha estrategia, partiendo de 5 pilares fundamentales[56]:

1. La defensa de infraestructura crítica
2. Interrupción y desmantelamiento de los actores delictivos
3. modificación de fuerzas del mercado para influenciar a la seguridad y resiliencia
4. Inversión en el futuro
5. forjar relaciones internacionales en busca de un objetivo común

Además de buscar la mejor manera de implementación en nuestra sociedad y su futuro. Su estrategia pretende siempre tener en cuenta los fenómenos emergentes, los actos y actores maliciosos, así como ellos se cargan con la responsabilidad de defender el ciberespacio, de brindar incentivos que promuevan la inversión y de todo la anterior construirlo desde sus ya funcionales políticas[57].

Como pudimos observar los puntos que se esgrimen en el T-MEC, buscan más el cumplimiento de México, pues parten de las estrategias que tienen estos dos países respecto al tema. A lo largo de sus leyes, artículos, campañas y agencias, se visualizan los puntos directrices del tratado y como fueron de ahí emanados para constituir una homologación de criterios ajustándose a sus marcos legales.

[56] Cfr. National Cybersecurity Strategy, 2023
[57] Cfr. National Cybersecurity Strategy, 2023

Capítulo III. Ajustes al marco legal mexicano en materia de ciberseguridad

Una vez realizada la investigación previamente expuesta en el capítulo anterior, podemos observar, que, tanto Canadá como Estados Unidos, cuentan con mecanismos y una extensa normatividad para la detección, regulación y sanción de los delitos informáticos. Sin embargo, para efectos de la presente investigación debemos conocer la manera en la que México está actuando para enfrentar estas actuaciones cibernéticas que afectan a miles de personas.

Es por lo que, en este capítulo se realizará un extenso estudio que nos permita conocer los diferentes ordenamientos jurídicos con los que cuenta la nación para la reglamentación y condenación de los delitos cibernéticos; si se ha cumplido con lo establecido en materia de ciberseguridad de acuerdo a lo contemplado en el Tratado entre Estados Unidos de América, Canadá y México, también conocido como T-MEC; su aplicación y por último si se ha llegado a promover algún medio de defensa extraordinaria por parte de la sociedad.

3.1 ¿Qué marcos jurídicos han sido creados desde la creación del TMEC?

Los delitos cibernéticos constituyen un gran problema social que impactan directamente a la intimidad, comunicación, derecho a la propia imagen, reputación, seguridad, entre muchos otros más. Es por lo que uno de los objetivos que contiene el T-MEC como lo vimos en el capítulo anterior es, reforzar los mecanismos existentes para identificar y combatir los incidentes que se susciten por estos delitos, sin embargo una interrogante que resolveremos en este apartado es reconocer la normatividad en materia de ciberseguridad que tiene México para refutar estas actividades que se llevan cotidianamente.

La Unión Internacional de Telecomunicaciones (UIT)[58], es un organismo especializado en las tecnologías de la información y comunicación de las Naciones Unidas, que tiene a su cargo regular las telecomunicaciones a nivel internacional. Este organismo realiza de forma periódica el *Índice de Ciberseguridad Global*, la cual tiene por objeto realizar un estudio sobre los compromisos, evolución y avances

[58] Unión Internacional de Telecomunicaciones (UIT), *Sobre la Unión Internacional de Telecomunicaciones (UIT)*, acerca de la UIT. Información visible en: https://www.itu.int/es/about/Pages/default.aspx (fecha de consulta: abril, 2023)

en el tema de ciberseguridad, el cual arrojó que en el año 2020 México se encontraba en el lugar número 52 de 182 países evaluados. Como podemos observar la ciberseguridad es aún un desafío que tiene temas pendientes para su regulación, ya que nuestro país es uno de los que recibe mayor cantidad de ataques cibernéticos en el mundo, tan solo en el año 2022 un informe realizado por *Fortinet*, señaló que se sufrieron 187,000 millones de ataques, un 20% más de los que se obtuvieron en 2021[59]. Los delitos cibernéticos son un problema que han ido en aumento conforme pasan los años, la tecnología va evolucionando y a su vez las formas para la configuración de un ataque, es por lo que los países deben estar más preparados para que exista una prevención y medidas eficientes para su sanción.

La ciberseguridad es un tema que debido a su constante transformación involucra un desafío en materia de seguridad pública, de modo que Amber Chamber México presentó los siguientes desafíos con los que nuestro país se enfrenta día con día[60]:

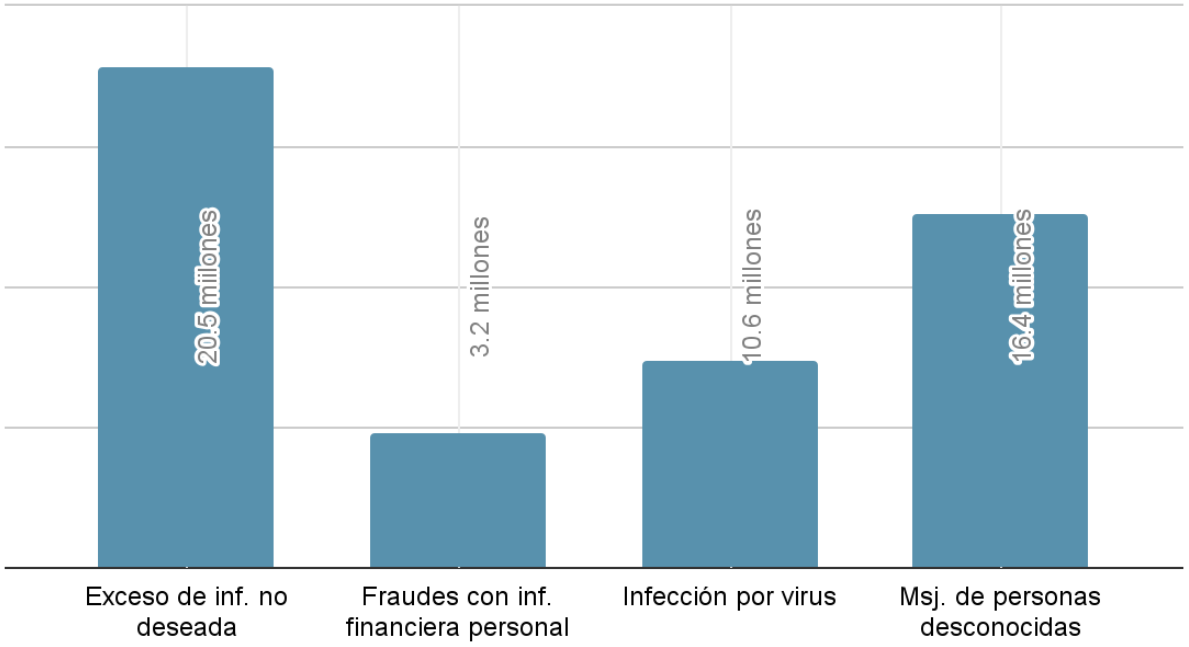
- Exceso de información no deseada
- Fraudes con información financiera personal
- Infección por virus
- Mensajes de personas desconocidas

A continuación, de modo que sea más ilustrativo y ejemplificador, se presenta la estadística del número de personas que han sido afectadas de acuerdo a los desafíos presentados previamente:

[59] Rankin Global UIT, GCI Results: Score and Rankings, Global scores and rankings of countries, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: abril, 2023)

[60] AGUIRRE QUEZADA, Juan Pablo, *Ciberseguridad, desafío para México y trabajo legislativo*, Cuaderno de Investigación No. 87, Instituto Belisario Dominguez, Senado de la Republica, Ciudad de México, p.8, en biblioteca digital información visible en: http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de%20Investigaci%C3%B3n%2087.pdf?sequence=1&isAllowed=y (fecha de consulta: abril, 2023)

GRÁFICA DEMOSTRATIVA[61]



Como podemos observar, el exceso de información no deseada es el principal reto que se debe de atacar a fin de conseguir una disminución y sanción, ya que como las cifras lo muestran, más de 20 millones de usuarios han sido perjudicados.

Ahora bien, la situación de ciberseguridad en México a partir de la firma del T-MEC con los otros dos países contratantes es distinta, si bien en Canadá y Estados Unidos existen programas, mayor reglamentación y protección para un control del ciberataque, en nuestro país no cuenta con una legislación en materia de ciberseguridad, por lo que existe un vacío legal dejando a los ciudadanos en un plano de desprotección. No obstante, desde el 2018 se han presentado once iniciativas de ley en el Senado de la República como en la Cámara de Diputados, en las cuales a nuestra consideración destacan las siguientes:

[61] Gráfica DEMOSTRATIVA: De realización propia, obteniendo la información de las definiciones y citas previas.

TABLA DE INICIATIVAS DE LEY EN MATERIA DE CIBERSEGURIDAD[62]

INICIATIVA Y FECHA DE PRESENTACIÓN	OBJETIVO	PRESENTADA POR	ESTATUS
Iniciativa con Proyecto de Decreto que declara el mes de octubre como: "El Mes Nacional de Ciberseguridad" Presentada: 23 de octubre 2018	Su objeto es que en el mes de octubre de cada año sea el "Mes Nacional de Ciberseguridad"	Senadora Alejandra Lagunes Soto Ruíz	Pendiente en comisión cámara revisora. 5 de noviembre de 2019
Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad. Presentada: 6 de abril de 2020	Tiene por objeto regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad	Senador Jesus Lucia Trasviña Waldenrath	Pendiente en comisión de cámara de origen. 6 de abril de 2021
Iniciativa con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal, en materia de delitos cibernéticos Presentada: 25 de marzo 2021	Esta iniciativa tiene por objeto prevenir y sancionar los delitos cibernéticos	Senador Gustavo Enrique Madero Muñoz	Pendiente en comisión de cámara de origen. 25 de marzo de 2021
Iniciativa que adiciona los artículos 5º y 6º de la Ley de Seguridad Nacional 8 de enero de 2020	Tiene como finalidad instaurar mecanismos legales en materia de ciberseguridad.	Diputada María Eugenia Hernandez Perez	Pendiente en comisión de origen. 8 de enero de 2020

Como podemos observar únicamente la iniciativa presentada por la Senadora Alejandra Lagunes Soto Ruíz fue trasladada a Cámara Revisora y no se enfoca

[62]AGUIRRE QUEZADA, Juan Pablo, *Ciberseguridad, desafío para México y trabajo legislativo*, op.cit. pp. 10-12, en biblioteca digital información visible en: http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de%20Investigaci%C3%B3n%2087.pdf?sequence=1&isAllowed=y (fecha de consulta: abril, 2023)

como tal en la promulgación de un orden normativo. Debemos recordar que una iniciativa con proyecto de ley o decreto la conoce primeramente la Cámara de Origen, la cual tiene como función aprobar y/o hacer modificaciones, para esta a su vez, remitir a la Cámara Revisora en donde como su nombre lo dice, se revisa el proyecto en donde se pueden dar algunos supuestos conforme lo dispuesto por el artículo 72 de la Constitución Política de los Estados Unidos Mexicanos, que nos señala que se puede[63]:

- Aprobar el proyecto de acuerdo a lo establecido por la Cámara de Origen y expedirlo al Poder Ejecutivo para su promulgación y publicación en el Diario Oficial de la Federación
- Desechar en su totalidad el proyecto, regresando a la Cámara de Origen con sus observaciones
- Desechar, modificar o adicionar puntos al proyecto

Dicho lo anterior, la Senadora Alejandra Lagunes en su exposición de motivos hizo una intervención en donde estableció las razones para que se aprobara *"El Mes Nacional de Ciberseguridad*", dando como argumentos lo siguiente[64]:

> *"Hoy damos un paso adelante para que México se sume a este diálogo importantísimo de la comunidad internacional. Y es que, así como las tecnologías de la información y la comunicación han evolucionado, también han hecho las formas y técnicas para delinquir en el ciberespacio, las cuales son cada día más sofisticadas. Lo anterior, ha derivado en el surgimiento de amenazas y riesgos a la dignidad humana, a la integridad de las personas, a la credibilidad, a la reputación y al patrimonio de los individuos, empresas e instituciones públicas…*
>
> *…este dictamen es también un exhorto a las instituciones de gobierno, organizaciones privadas, sociedad civil y comunidades académicas y técnicas para sumarse a la campaña de sensibilización y de reconocimiento al impacto de la ciberseguridad en el desarrollo social, político, humano y económico de nuestro país, así como la responsabilidad compartida de todos los actores en la construcción de un ciberespacio libre, diverso y seguro"*

[63] Vid. artículo 72 de la Constitución Política de los Estados Unidos Mexicanos
[64] Cfr. con Intervención de la Senadora Alejandra Lagunes Soto Ruíz el día 24 de octubre de 2019, información visible en: https://www.senado.gob.mx/65/intervenciones/1267/20647 (fecha de consulta: abril de 2023)

La propuesta que nos explica la senadora es un paso para visibilizar y generar conciencia de un problema que ha ido creciendo conforme evoluciona la tecnología, sin embargo, como se mencionó hace un momento, esta iniciativa fue la única que logró avanzar más que las demás, posicionándose en la cámara revisora, no obstante quedó detenido en el proceso para su aprobación.

Por consiguiente, México pasó por un suceso que marcó como precedente siendo conocido como el mayor ciberataque en la historia del país, en donde un grupo internacional de activistas conocidos como los "*Guacamaya*", se infiltraron al sistema de cómputo de la Secretaría de la Defensa Nacional o como sus siglas se muestran también conocido como SEDENA. En este ciberataque se dio a conocer información y documentos confidenciales que contenían datos desde el año 2016 hasta el 2022, por lo que debido a este suceso se puso en marcha la creación la Ley Federal de Ciberseguridad, en donde los Senadores, junto con la Comisión de Ciencia y Tecnología e Innovación trabajaron en conjunto para su elaboración. Esta propuesta contenía once títulos, distribuidos en setenta y un artículos, dentro de los cuales se tenían cuatro enfoques principales[65]:

1. Garantizar la seguridad nacional mediante la defensa del espacio digital.
2. Crear un marco legal que permita sancionar o tipificar los ciberataques.
3. La realización de *pruebas de penetración o pentesting* anualmente a las instituciones públicas y privadas.
    a. Este tipo de prueba tiene como objetivo que las empresas puedan detectar y prevenir posibles fallos o ataques, a través de un análisis de vulnerabilidades y debilidades en su sistema informático[66].
4. Crear una Agencia Nacional de Ciberseguridad controlada por el Ejecutivo.

Esta ley estaba prevista para su publicación en el mes de diciembre de 2022, sin embargo aún no está disponible. Pese a no contar con una ley específica en la materia, México cuenta con algunas leyes que mencionan la seguridad de la tecnología de la información, siendo estas las subsecuentes:

---

[65]SANTOS CHAVEZ, Juan Jose, *Ley de Ciberseguridad en México*, DELTA PROTECT, 2023. Información visible en: https://www.deltaprotect.com (fecha de consulta: abril, 2023)
[66]SANTOS CHAVEZ, Juan Jose, *Pentesting*, DELTA PROTECT, 2023. Información visible en: https://www.deltaprotect.com/blog/que-es-pentesting (fecha de consulta: abril, 2023)

- **Constitución Política de los Estados Unidos Mexicanos[67]:** en su artículo 28 párrafo décimo quinto, se establece que el Instituto Nacional de Telecomunicaciones tiene a su cargo las siguientes funciones:
    - Desarrollo eficiente de la radiodifusión y telecomunicaciones.
    - Regula y supervisa el uso, aprovechamiento y explotación de las redes y la prestación de servicios de radiodifusión y telecomunicaciones.

- **Código Penal Federal:** En 1999 se reformó el Código Penal Federal en donde se añadió el capítulo II titulado “Acceso ilícito a sistemas y equipos de informática”, en donde se desglosan siete artículos, siendo alguno de ellos:
    - 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[68].
    - 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[69].

- **Ley Federal de Protección de Datos Personales en Posesión de Particulares[70]:**
    - Artículo 19. Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

[67] Vid. artículo 28 de la Constitución Política de los Estados Unidos Mexicanos
[68] Cfr. artículo 211 bis 1 de la Código Penal Federal
[69] Cfr. artículo 211 bis 2 de la Código Penal Federal
[70] Cfr. artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares

- **Ley General de Títulos y Operaciones de Crédito[71]:**
    - Artículo 432 fracción I. la persona que produzca, fabrique, reproduzca, copie, imprima, venda, intercambie o altere cualquier tarjeta de crédito y/o débito o cualquier otro instrumento de pago, incluidos los dispositivos electrónicos, emitido por las entidades de crédito, sin autorización del titular, recibirá una pena de prisión de tres a nueve años, por parte de la autoridad competente, así como una multa.

- **Ley Federal del Derecho de Autor**: a raíz de la firma del T-MEC esta ley se reformó añadiendo el Capítulo V titulado "*De las Medidas Tecnológicas de Protección, la Información sobre Gestión de Derechos y los Proveedores de Servicios de Internet"*
    - Artículo 114 septies[72]: Se consideran Proveedores de Servicios de Internet:
        - Proveedor de acceso a internet es aquella persona que transmite, enruta o suministra conexiones para comunicaciones digitales en línea, sin modificación de contenido, entre los puntos especificados por un usuario, del material seleccionado por el usuario, o que realiza el almacenamiento intermedio y transitorio de ese material hecho de forma automática en el curso de la transmisión, enrutamiento o suministro de conexiones para comunicaciones digitales en línea.
    - De igual forma en el artículo 130 se hizo una modificación quedando de esta manera[73]:
        - Productor de fonogramas es la persona física o moral que fija por primera vez los sonidos de una interpretación o ejecución u otros sonidos o la representación digital de los mismos y es responsable de la edición, reproducción y publicación de fonogramas.

Esto fue un gran cambio a partir de la firma del Tratado, ya que la Ley Federal del Derecho de Autor únicamente contemplaba los medios tradicionales como la radio y

[71] Vid. artículo 432 fracción I, de la Ley General Títulos y Operación de Crédito
[72] Cfr. artículo 114 septies, de la Ley Federal del Derecho de Autor
[73] Cfr. artículo 130, de la Ley Federal del Derecho de Autor

televisión, y con la reforma que se hizo el 1 de julio de 2020 proporciona mayor salvaguarda a los titulares de derecho de autor o derechos conexos en el entorno digital, a través de la implementación de medidas tecnológicas de protección y la responsabilidad de los proveedores de servicios de internet.

3.2 Aplicación del T-MEC en México

Como pudimos observar en el subtema anterior, México tiene una falta de legislación en materia de ciberseguridad, contando únicamente con algunas leyes supletorias que, generan un gran vacío legal, ya que, no especifican de manera concreta las causas, consecuencias o requisitos que deben existir para que haya un encuadramiento de este delito, .

Es por lo que el objetivo de este subtema es conocer la manera en la que el país lleva a cabo acciones y estrategias para combatir los delitos cibernéticos, así como, averiguar qué organismos son los encargados de la ciberseguridad en México.

En primer lugar, contamos con una Estrategia Nacional de Ciberseguridad, que estaba contemplada en el Plan Nacional de Desarrollo de 2013-2018, creada por el Poder Ejecutivo, a través de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. La cual tiene como finalidad identificar y establecer acciones y mecanismos para combatir los delitos cibernéticos en el ámbito económico, político y social, para que la tecnología se use de manera responsable y eficaz, garantizando un bienestar a la sociedad, por lo cual, para lograr su cometido se cuenta con cinco objetivos principales para proteger[74]:

1. La Sociedad y sus derechos→ generar condiciones para que las personas puedan navegar de forma segura y libre en el ciberespacio.
    a. Acciones realizadas:
        i. El 19 de mayo de 2018 se implementaron mesas de trabajo en el Instituto Federal de Telecomunicaciones en donde se discutió el fortalecimiento de políticas públicas, gestión de riesgos y una actualización al marco jurídico.

[74] Cfr. Estrategia Nacional de Ciberseguridad (ENC)

2. La Economía e Innovación→ proteger la economía de los diferentes sectores del país y motivar a la innovación tecnológica, impulsando la industria nacional en materia de ciberseguridad.
    a. Acciones realizadas:
        i. Se llevaron a cabo reuniones entre la Secretaría de Economía y la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información, para analizar tanto el objetivo como las acciones implementadas por la Estrategia Nacional de Ciberseguridad.

3. Las Instituciones Públicas→ brindar un servicio óptimo y la continuidad de los servicios y trámites a la población.
    a. Acciones realizadas:
        i. En febrero de 2018 se reunieron los integrantes del Grupo de Trabajo *"Instituciones Públicas"* integrada por la Secretaría de Gobernación, Secretaría de Hacienda y Crédito Público, Servicio de Administración Tributaria y la Secretaría de Economía, en donde se definió su objetivo *"promover acciones que permitan fortalecer los mecanismos de protección en materia de ciberseguridad con los servidores públicos de la Administración Pública y las Entidades Federativas"*. De igual forma se ajustaron las líneas de acción, sobre las cuales versan la regulación del cumplimiento en las acciones de identificación, detección ante incidentes de ciberseguridad.

4. La Seguridad Pública→ dar una mayor capacitación para dar mejor atención en la investigación de conductas delictivas en el ciberespacio.
    a. Acciones realizadas:
        i. La Policía Federal llevó a cabo sesiones donde se evaluó la cadena de custodia digital y se presentó la Propuesta del Modelo de Madurez de Ciberseguridad para evaluar a las Instituciones Públicas.

5. La Seguridad Nacional→ este objetivo está dirigido para prevenir riesgos y amenazas en el ciberespacio que puedan atentar contra la independencia y soberanía nacional.
    a. Acciones realizadas:
        i. Concientización para funcionarios de alto nivel en materia de ciberseguridad y se hizo una actualización del Manual Administrativo de Aplicación general en materia de tecnologías de la Información y Comunicaciones.

Acorde con las acciones realizadas mencionadas anteriormente, la Estrategia Nacional de Ciberseguridad también ha implementado diferentes foros y talleres en donde se comparten ideas, inquietudes y propuestas en materia de ciberseguridad, en donde su principal motor es generar que la estrategia esté adecuada a las necesidades de la sociedad para poder brindar mejor atención y seguridad cuando se utilizan los programas informáticos, redes y así como los medios[75].

De igual modo, la Organización de los Estados Americanos o también conocido como la OEA, entregó al Estado Mexicano una serie de recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad, con el objeto de mejorar las capacidades de ciberespacio en el país[76]:

- Remite a México consideraciones de gestión de riesgos, la cual implica generar diálogo e incentivar a la población en el uso responsable de las TIC, es decir, las Tecnologías de Información y Comunicación.
- Recomienda incentivar a las empresas a invertir en seguridad cibernética y la modernización de su infraestructura.
- Incluir normas de seguridad de la información para los productos vinculados a internet u otros sistemas digitales.

Pese a la existencia de la Estrategia Nacional de Ciberseguridad y las recomendaciones hechas por la OEA, el país cuenta con algunas Secretarías y mecanismos donde brindan apoyo en la respuesta de incidentes cibernéticos, la primera de ellas siendo:

[75] Cfr. Estrategia Nacional de Ciberseguridad (ENC)
[76] Cfr. Plan de Acciones en Materia de Ciberseguridad, Instituto Federal de Telecomunicaciones

1. MARINA

La Secretaría de Marina en el año 2021 asistió a la *Secretaría Pro-Tempore* 2021-2022 del Foro Iberoamericano de Ciberdefensa, compuesto por las Fuerzas Armadas de Perú, Brasil, Chile, México, Argentina, España, Colombia, Portugal, Uruguay y Paraguay. El cual tiene como objetivo promover estrategias y plan de acción en materia de ciberdefensa.

En el año 2021 esta Secretaría publicó su "Estrategia Institucional para el ciberespacio 2021-2024", que propone fortalecer las capacidades de ciberdefensa, ciberseguridad y seguridad de la información. Algunas acciones que aspira a realizar son[77]:

- Impulsar la investigación y el desarrollo tecnológico
- Crear el cargo de Oficial de Seguridad de la Información
- Incluir las Operaciones en el Ciberespacio dentro del Esquema General de Operaciones Navales de la Armada de México
- Incentivar a que se realicen reformas legales para que la Secretaría de Marina pueda efectuar acciones en el ciberespacio.

2. GUARDIA NACIONAL Y CERT-MX

El Centro de Respuestas a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-MX) se basa en la identificación de amenazas, mediante la gestión de incidentes de seguridad informática, siendo el único punto de contacto dentro y fuera del territorio nacional, a la vez actuando de la mano con el Ministerio Público en la investigación forense digital y el análisis técnico policial. Por otro lado, el equipo que trabaja en la Guardia Nacional cuenta con más de 4 mil colaboraciones establecidas a nivel internacional, de las cuales ochenta por ciento son con Estados Unidos, ya que permiten emitir alertas en materia de ciberseguridad, así como avisos a la población.

Durante el año 2022, el CERT-MX realizó distintos foros y encuentros para fomentar la seguridad en línea y prevenir delitos, de igual forma, se realizó junto al Instituto Federal de Telecomunicaciones la Segunda Edición del ciclo de *"Conferencias de Ciberseguridad 2022"*; y en el marco de la Campaña Nacional Anti Fraude

[77]DPL Ciberseguridad, *Políticas de Ciberseguridad en México: Un compendio para la toma de decisiones, la colaboración y la confianza digital*, DPL Intelligence. Información Visible en: https://dplnews.com/wp-content/uploads/2023/04/DPL-Ciberseguridad-Politicas-de-ciberseguridad-en-Mexico.pdf (fecha de consulta: mayo, 2023)

Cibernético realizó pláticas sobre ciberseguridad junto con otras dependencias como[78]:

- Profeco
- Asociación de Bancos de México
- Condusef

3. SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA

La Secretaría de Seguridad y Protección Ciudadana publicó en octubre de 2021 un Protocolo Homologado de Incidentes Cibernéticos, que tiene como objetivo generar un sólo instrumento para hacer denuncias que involucren nuevas amenazas y delitos cibernéticos, con el fin de facilitar la actuación de las policías, el Ministerio Público y el Poder Judicial. Con este protocolo se busca fortalecer la ciberseguridad en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país, con la finalidad de mantener el orden constitucional[79].

4. INAI

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, es un órgano constitucional autónomo de México encargado del cumplimiento de dos derechos fundamentales:

I. el acceso a la información pública y
II. la protección de datos personales.

El INAI monitorea los ataques cibernéticos a la Plataforma Nacional de Transparencia (PNT), conocida como una de las más hackeadas del país, también enseña al gobierno para dar a conocer información, y realiza recomendaciones

[78]DPL Ciberseguridad, *Políticas de Ciberseguridad en México: Un compendio para la toma de decisiones, la colaboración y la confianza digital*, DPL Intelligence p.31. Información Visible en: https://dplnews.com/wp-content/uploads/2023/04/DPL-Ciberseguridad-Politicas-de-ciberseguridad-en-Mexico.pdf (fecha de consulta: mayo, 2023)
[79]DPL Ciberseguridad, *Políticas de Ciberseguridad en México: Un compendio para la toma de decisiones, la colaboración y la confianza digital*, DPL Intelligence p.32. Información Visible en: https://dplnews.com/wp-content/uploads/2023/04/DPL-Ciberseguridad-Politicas-de-ciberseguridad-en-Mexico.pdf (fecha de consulta: mayo, 2023)

sobre seguridad en línea, con el propósito de generar conciencia a la ciudadanía del uso responsable de internet[80].

La Estrategia Nacional de Ciberseguridad así como las Secretarías ya antes mencionadas, trabajan en conjunto para llevar una adecuada regulación de los delitos cibernéticos, sin embargo, es necesario y fundamental que el Estado Mexicano cuente con una Ley propia en materia de ciberseguridad, para dar mayor protección a los derechos de las personas, para que estas a su vez tengan conocimiento de qué hacer en caso de que se presenten ante un delito que se hace más común día con día.

3.3 Amparos promovidos por la sociedad

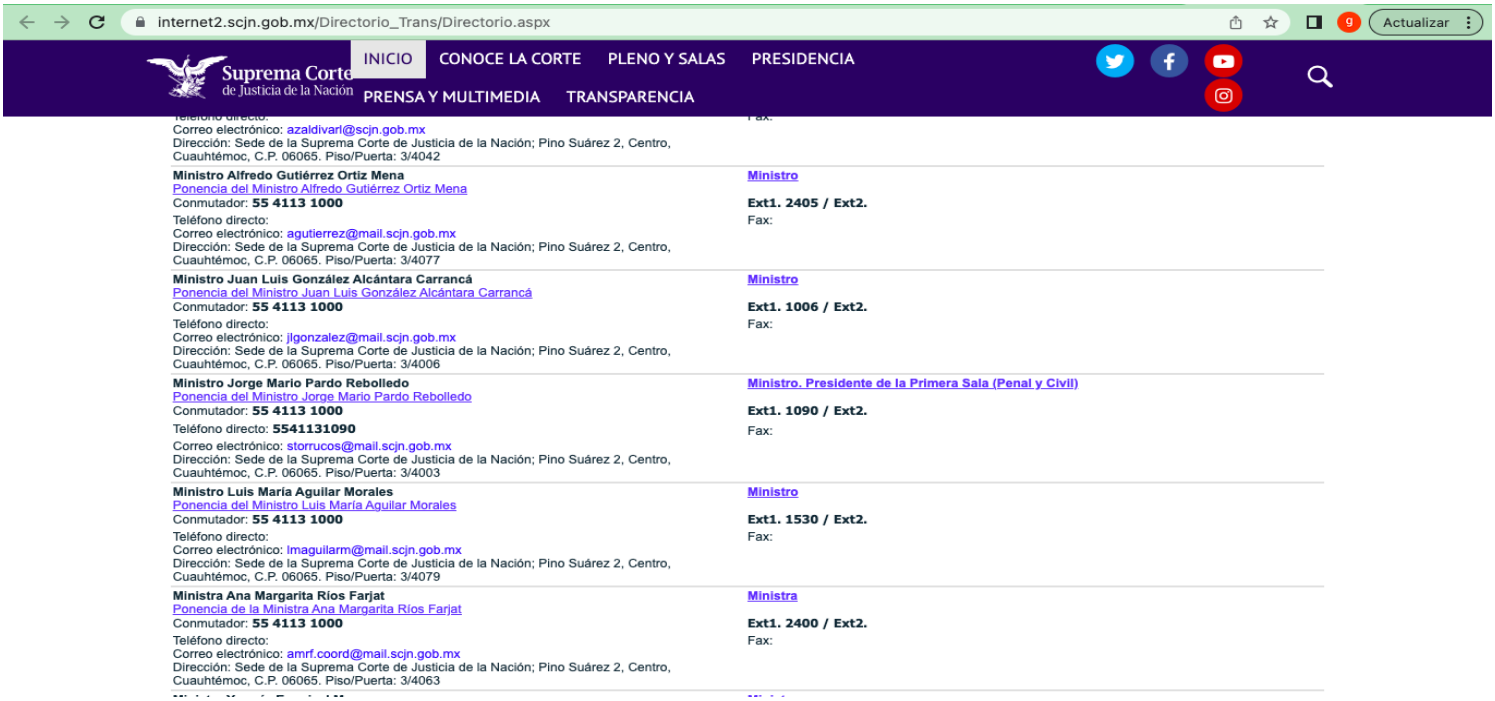
En este subtema buscamos mostrar los amparos promovidos por la sociedad en torno a la protección de sus derechos en materia de ciberseguridad, ya que a través de la investigación realizada pudimos observar, que al no cumplirse en la totalidad con lo que establece el T-MEC específicamente en el capítulo 19.15, pudiesen existir situaciones donde la ciudadanía acuda a un medio extraordinario como lo es el juicio de amparo para que se le otorgue una defensa.

Es por lo que, como ciudadanos y el derecho que tenemos al acceso a la información, decidimos solicitar que se nos proporcione datos sobre lo que versa este subtema. En razón de lo cual, mediante el portal de la Suprema Corte de Justicia de la Nación, en su apartado "*directorio*" se nos remitió a la lista de los ministros, donde encontramos la siguiente información:

- Nombre del (a) ministro (a)
- Correo electrónico
- Dirección
- Número de Extensión para comunicarse directamente a la ponencia.

[80] DPL Ciberseguridad, *Políticas de Ciberseguridad en México: Un compendio para la toma de decisiones, la colaboración y la confianza digital*, DPL Intelligence p.35. Información Visible en: https://dplnews.com/wp-content/uploads/2023/04/DPL-Ciberseguridad-Politicas-de-ciberseguridad-en-Mexico.pdf (fecha de consulta: mayo, 2023)

FOTO DEMOSTRATIVA DE LA PÁGINA DE CONTACTO[81]



Posteriormente elegimos uno de ellos, muy amablemente nos atendieron y nos contactaron con la Secretaría General de Acuerdos con número de extensión 11892295, ya que nos comentaron que ahí podríamos recibir información de lo que estábamos solicitando, una vez que nos pusieron en contacto, se nos informó que no había antecedentes ni algún consecuente del mismo.

Como conclusión de la investigación ejecutada, nos resulta un poco decepcionante que, no solo los legisladores deben de actuar para que haya una regulación de ciberseguridad, sino que la población también debe de involucrarse y exigir que se cumpla con lo establecido en los Tratados Internacionales con los que México es parte, porque en conjunto con las Leyes Federales generan un bloque de constitucionalidad, lo que los pone en un plano de igualdad.

[81] FOTO DEMOSTRATIVA DE LA PÁGINA DE CONTACTO, información visible en: https://www.internet2.scjn.gob.mx/Directorio_Trans/Directorio.aspx (Fecha de consulta: abril, 2023)

CAPÍTULO IV. Propuestas de solución para mitigar los delitos cibernéticos

En relación con los capítulos anteriormente expuesto en el presente nos enfocaremos en dar propuestas de solución para contrarrestar los delitos cibernéticos y en relación con eso México cumpla con mayor eficiencia lo dispuesto en el T-MEC. Como hemos observado, las legislaciones de los demás Estados Parte llevan un mayor avance que el de nuestro país, debido al trabajo temprano que han realizado en la materia.

Mientras que en México si bien existen ciertas normativas, las leyes en materia de protección de datos y las demás disposiciones esparcidas en diversas áreas del sistema jurídico mexicano se quedan cortas en cuanto al funcionamiento y la aplicabilidad que podamos darle. Se cuentan con algunos organismos o con áreas especializadas en organismos específicos, que se ven con facultades y áreas de acción muy limitadas. Debido a esto es que este capítulo se expresa más como una reflexión de lo investigado y a forma de critical personal (del equipo), dar propuestas o vías de acción que le faciliten a nuestro País un fortalecimiento en el área de los ciberdelitos y la ciberseguridad, guiado por lo estipulado en el T-MEC.

4.1 Adecuaciones necesarias al sistema mexicano

Como primer punto nos enfocaremos en la que consideramos lo más alejada del cumplimiento y es la materia legislativa. Mencionar las necesidades que pudiera tener, las escasez en asuntos y el fortalecimiento de las bases establecidas.

Lo primero y más obvio es considerar crear un espacio legal espécificamente enfocado en dicha materia, la cual pudiera cumplir los aspectos teoricos y sustantivos como el de definir, delimitar y establecer facultades, derechos, obligaciones y responsabilidades tanto de los sectores público, privado y social; donde de igual manera se tenga como objetivos el validar los términos como el ciberespacio, cibergobierno, ciberpolicía, ciberempresa, ciberservicio, ciberdelincuencia organizada, ciberdelincuente y ciberseguridad. En una analogía explicativa, buscar en este espacio a crear, el poder trasladar las reglas de la sociedad al ámbito ciberespacial, que es donde varios de los movimientos bursátiles, mercantiles, fiscales y más, se realicen en la actualidad. Mencionamos espacio legal por la forma que el sistema mexicano pueda otorgarle, entre las formas que insinuamos se encuentran las siguientes:

- La creación de una Ley General, la cual dirige y ordena la materia del ciberespacio y por subsecuente la ciberseguridad. Dentro de esta se podrá regular los requisitos y vías procedimentales.
- La estipulación de una apartado propio dentro del Código Penal Federal
- La modificación en las distintas leyes de la materia, para estipular un apartado preciso de observancia del tema.

Como pudimos observar en el capítulo anterior e hilando lo mencionado anteriormente. Podemos establecer que México cuenta con algunas disposiciones legales, pero dispersas, por lo que con las propuesta anterior, podría unificar la materia en un mismo cuerpo normativo.

Ante el Congreso de la Unión como ya lo hemos mencionado se presentó una iniciativa de Ley de Ciberseguridad, a reformar el Código Penal Nacional y la Ley de Seguridad Nacional. Actualmente parece ser que dichas iniciativas se encuentran archivadas en el olvido del Congreso, no saliendo de su misma cámara de origen. Por lo que la posibilidad de establecer una base jurídica para perseguir ciberdelitos e incrementar el cumpliento de ciberseguridad respecto a los objetivos del T-MEC, parecen no ser una a corto plazo, y de tal manera mejorar la jurisdicción.

En un segundo punto y tomando como referencia el subtema 2.2 y 3.2 del presente proyecto, mencionar las organizaciones, las agencias, políticas o estrategias gubernamentales. Si bien México cuenta con una mayor acción en este tema como se dispone en el subtema 3.2 de la investigación, se deberán fortalecer y diversificar las vías de acción.

Para estas propuestas establecimos dos áreas, gobierno nacional y institucional-gubernamental. Lo primero, lo que proponemos es

- Se contemple dentro del presupuesto nacional una cantidad destinada a la ciberseguridad para aspectos como
    - Implementar mayor seguridad en los datos
    - Protección a la infraestructura cibernética del País
    - Posibilidad de cumplimiento de requisitos legales
    - Establecer un control de riesgo sobre pérdidas financieras
    - Establecer un orden de control.

- Establecer y actualizar la Estrategia Nacional de Ciberseguridad. Así como priorizar dentro de los Planes Nacionales de Desarrollo
    - Llevando a cabo un protocolo nacional que tiene como finalidad establecer esquemas de colaboración entre autoridades, organizaciones, empresas y usuarios.
- La implementación de un Organismo de preferencia autónomo, especializado en la materia, con facultades
    - En distintos áreas del derecho
    - Multinível gubernamental
    - La creación de un portal de acceso a la sociedad
    - Órgano investigador y de recomendaciones
    - Requerimiento de informes a las instancias públicas y de gobierno
    - Un boletín público, periódico e informativo, sobre las acciones realizadas e información necesaria del tema.

Estás son las 3 principales propuestas para poder dar cumplimiento efectivo a los pactado dentro del Tratado en cuestión.

En el caso de la segunda área, las propuestas se centran en la coacción de las instituciones de gobierno con la seguridad cibernética y centradas en las áreas principalmente afectadas por estos conductas antijurídicas previamente expuestas, las siguientes son las propuestas:

- Contar con simulacros en ciberseguridad
- Planes de acción sobre el tema
- Capacitaciones
- Designación de un oficial de ciberseguridad
- Realizar informes trimestrales sobre aspectos de ciberseguridad
    - Cumplimento de los demas puntos
    - Acciones realizadas
    - Acciones resueltas
    - Promulgación de información

Son las propuestas primordiales que se han considerado, comparando con lo que ya cuentan los otros Estados Partes del tratado.

En un tercer punto, coincidimos que no solo es necesario un cambio legal y burocrático para lograr el cumplimiento ya referido. Por lo que se han realizado propuestas de impacto y colaboración directa del Gobierno con la Sociedad. Tomando en cuenta acciones realizadas en Canadá y Estados Unidos y referidas previamente en la investigación. Dichas propuestas radican en:

- Materia educativa
    - Programas con reconocimiento de validez que generen más profesionales enfocados en ciberseguridad
    - Incluir en la educación básica y media superior asignaturas destinadas a dar a conocer el ciberespacio junto con la ciberseguridad
    - Programas de capacitación
- Información
    - Impulsar acciones de difusión pública para fortalecer la cultura de ciberseguridad
    - Portal electrónico para obtener veracidad, pertinencia, asesoramiento sobre el tema y vías de conexión.
    - Campañas de concientización

En este último aspecto se busca que México promueva el conocimiento de la materia y mantengan un espacio de transparencia y accesibilidad para la sociedad.

Son los 3 puntos o niveles de cambio que tras realizar la investigación de los anteriores capítulos, consideramos son mayormente necesarias. Dichas propuestas no deben realizarse de manera individual, sino grupal; pues todas conllevan una conexión y un modelo multidisciplinario, el cual permitirá el objetivo en cuestión, el cumplimiento del T-MEC. Representan un modelo de coordinación, que como se ha mencionado a lo largo del proyecto y se establece en el desarrollo de los artículos del Tratado expuestos, la coordinación, la cooperación y la cooperatividad son necesarias para la realización de un ciberespacio más seguro.

4.2 Planeación y desarrollo de las propuestas mencionadas

Para llevar una planeación y un buen desarrollo es primordial que tanto como las organizaciones gubernamentales, empresas privadas y la población sepa darle un buen manejo al ciberespacio. Establecer propuestas claramente es sencillo, llevarlas a cabo y desarrollar un espacio jurídico apto para su establecimiento no lo es. Como se mencionó previamente, la posibilidad cercana de un cambio necesario y eficiente, no se ve; al mencionar una posibilidad a corto plazo no referimos a una inmediatez, lo cual sería lo ideal, sino, a unos posibles años. En estos momentos, la posibilidad de cambio más cercana es la creación de un comisión destinada a planear todas las modificaciones sustantivas necesarias para el establecimiento de las propuestas necesarias.

Pero que seguiría después para dicha comisión, nosotros en un ejercicio demostrativo nos investimos como dicha comisión y mencionamos una línea de acción general para poder desarrollar las propuestas mencionadas de una manera simplificada pero realista.

En un primer momento, deberá darse la creación de dicha comisión, por los medios correspondientes y facultada. La línea que deberá seguir, promover con los órganos respectivos todas las iniciativas de ley y reformas necesarias para el establecimiento de una ley, de modificaciones, de organizaciones. Dentro de los cambios en marcos normativos, consideramos los siguientes como los principales:

1. Constitución Política de los Estados Unidos Mexicanos
2. Ley Federal de Telecomunicación
3. Código Penal Nacional
4. Código de Comercio
5. Ley General de Títulos y Operaciones de Crédito
6. Ley Federal de Protección de Datos Personales en Posesión de Particulares
7. Ley Federal del Derecho de Autor
8. Ley de Seguridad Nacional
9. Ley General de Educación
10. Ley de Acceso a la Información

El cambio en todo este aspecto normativo, permitirá el avance de varias de las propuestas. Reformar para otorgar facultades, para armonizar el aspecto jurídico de la ciberseguridad, para la creación de los organismos, para fortalecimiento de los ya establecidos y sobre todo para continuar con el cambio. En un siguiente momento, ya se podrán entablar los cambios gobierno-nacionales e institucionales-gubernamentales; pudiéndose establecer las modificaciones burocráticas propuestas en el subtema anterior. Por último, una vez establecidos los marcos jurídicos, los sujetos que accionan y el orden burocrático, se podrá enfatizar un cambio con la sociedad, brindándole la información y educación necesarias, resolviendo las propuestas del tercer punto.

El T-MEC se ha firmado ya hace casi 5 años y solo ha producido iniciativas estancadas. Será un proceso largo, sí, sin embargo es uno que debe iniciarse con urgencia pues la sociedad sigue avanzando hacia la tecnología. Para la realización de lo anteriormente mencionado es importante que se involucre al ESTADO MEXICANO, nuestros poderes constitucionales y así mismo la sociedad.

CONCLUSIONES

Como ya se determinó a lo largo de la investigación previa, se considera que el Estado Mexicano no ha cumplido con las obligaciones en cuestión de ciberseguridad, pactadas en el Tratado entre México, Estados Unidos y Canadá. Solo generando cambios ínfimos dentro de las disposiciones a las que se obligaron.

Tras establecer las vías de acción realizadas por los estados parte, Estados Unidos y Canadá, se pudo aclararse los artículos tantos sustantivos, como procesales y de igual forma las campañas tanto internas en sus gobiernos, como de los mismos con la sociedad. Bajo las mismas directrices y en un ámbito más desglosado se lo realizado por el Estado Méxicicano, demostrando las normativas difusas, mínimas y sobre todo establecidas en una diversidad de marcos jurídicos. De lo anterior y mediante una comparación se concluye el atraso en una regulación jurídica y burocrática sobre ciberseguridad por parte del Estado Mexicano en comparación con los demás estados contratantes.

El Tratado establece varios puntos obligatorios los cuales regulan dicha conducta y sobre todo generan una seguridad jurídica para sociedad; donde se busca la claridad normativa, la transparencia de acciones de prevención, sanción o reposición. Puntos generales, que no se han cumplidos, ni se han buscado los medios para su cumplimiento, como se ha expresado en la investigación las iniciativas de cambio que se han intentado, han sido olvidadas en un archivo o en una discusión inconclusa. Si bien México cuenta con disposiciones legales en distintas organizaciones y en distintas leyes, la regulación unificada es necesaria para dar certeza a los medios judiciales y en gran sentido.

Una conclusión a mencionar es que el Estado Mexicano tiene un camino extenso para recorrer, con la necesidad de realizar cambios a nivel legislativo, burocrático y social. Además de modificar a nivel constitucional y también particular, para establecer vías de acción adecuadas al cumplimiento del Tratado. Ya casi a 5 años de su firma y solo ha visto el intento de crear, se considera tras la investigación que no hay posibilidad de cambio a corto plazo, viniendo la elecciones presidenciales en 2024, se estima la idea de un inicio de cambio posterior a dichas fechas.

REFERENCIAS

Libros

- CAMACHO, Luis Losa, cit pos.LOREDO GONZÁLEZ, Jesús Alberto y RAMÍREZ GRANADOS, Delitos Informaticos: su clasificación y una visión general de las medidas de acción para combatirlo, México, UANL, Facultad de ciencias fisico matematicas, 2013.
- MACUARAN OCHOA, Maria Fernanda, *La evolución de la política de ciberseguridad de Canadá entre 2010 y 2018*, Barcelona, Universitat Autónoma de Barcelona, 2019, pp. 6-8
- MAGLIONA MARKOVICTH, Claudio y LÓPEZ MEDEL, Macarena, D*elincuencia y Fraude Informático*, Chile, Editorial Jurídica de Chile, 1999, p.211.
- MEDINA GÓMEZ, Diana, *Los Delitos Cibernéticos y los Problemas a Enfrentar*, México, UNAM, 2020.
- PARKER, D.B, cit pos. .ROMEO CASABONA, Carlos Maria, *Poder Informático y Seguridad Jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información,* Madrid, FUNDESCO, Colección Impactos,1987.
- TÉLLEZ VALDÉS, Julio, *Los Delitos Informáticos: Situación en México*, Extremadura, Mérida, UNED, 1996.
- VIÑAMATA PASCHKES, Carlos, *La propiedad intelectual,* 7a ed, México, Trillas, 2017, p. 154.

Publicaciones periódicas

- AUTOR, f, “Gobierno de Estados Unidos gastará más de 18 millones en ciberseguridad”, *El Mundo*, Seattle, Washington, nueva serie, número 23, Enero-Junio 2020.
- SERRANO, Alex, “México aumenta inversión en ciberseguridad”, *DPL News*; México, serie 2, 2021, Julio-Diciembre 2021.

Documentos

- Canada, National Cybersecurity Strategy, 2023
- Estrategia Nacional de Ciberseguridad (ENC)
- Plan de Acciones Nacional

Legislación Internacional

- Código Penal de Canadá (Criminal Code)

- Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales
- Ley Modelo de la CNUDMI sobre Comercio Electrónico 1996
- Marco de Privacidad del Foro de Cooperación Económica Asía Pacifico (APEC)
- Tratado entre México, Estados Unidos y Canadá (T-MEC)

Legislación Nacional

- Código Penal Federal
- Constitución Política de los Estados Unidos Mexicanos
- Ley General Títulos y Operación de Crédito
- Ley Federal del Derecho de Autor
- Ley Federal de Protección de Datos Personales en Posesión de Particulares

Fuentes electrónicas

- AGUIRRE QUEZADA, Juan Pablo, *Ciberseguridad, desafío para México y trabajo legislativo*, Cuaderno de Investigación No. 87, Instituto Belisario Dominguez, Senado de la Republica, Ciudad de México, en biblioteca digital información visible en: http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de%20Investigaci%C3%B3n%2087.pdf?sequence=1&isAllowed=y (fecha de consulta: abril, 2023)
- CHAPAMAN, Leonora, 7 millones de canadiense víctimas de Fraude en Línea, Política y Sociedad, RCI, 2017. Información visible en: https://www.rcinet.ca/es/2013/10/03/7-millones-de-canadienses-victimas-de-fraude-en-linea/#:~:text=El%20informe%20estima%20que%20siete,cr%C3%A9dito%20al%20robo%20de%20identidad.&text=%C2%ABEl%20cibercrimen%20este%20a%C3%B1o%20se%20ha%20duplicado%20desde%20el%20a%C3%B1o%20pasado%E2%80%A6 (fecha de consulta: marzo, 2023)
- Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, *Tipos de Fraude.* Información visible en: https://www.condusef.gob.mx/?p=tipos-de-fraude (fecha de consutla: marzo, 2023)
- Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, *¿Sabes qué es el Robo de Identidad?.* Información visible en: https://www.gob.mx/condusef/articulos/recomendaciones-para-prevenir-el-robo-de-identidad (fecha de consulta: marzo, 2023)
- CORONA, Pablo., "Asociación de Internet, Mx", *¿Qué es el ciberbullying?.* Información visible

en:https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying (fecha de consulta: marzo, 2023)

- DPL Ciberseguridad, *Políticas de Ciberseguridad en México: Un compendio para la toma de decisiones, la colaboración y la confianza digital*, DPL Intelligence. Información Visible en: https://dplnews.com/wp-content/uploads/2023/04/DPL-Ciberseguridad-Politicas-de-ciberseguridad-en-Mexico.pdf (fecha de consulta: mayo, 2023)
- FOTO DEMOSTRATIVA DE LA PÁGINA DE CONTACTO, información visible en: https://www.internet2.scjn.gob.mx/Directorio_Trans/Directorio.aspx (Fecha de consulta: abril, 2023)
- Government of Canada, Canada Center of Cybersecurity, información visible en: https://www.cyber.gc.ca/en (fecha de consulta: abril, 2023)
- Government of Canada, GetCyberSafe.CA, información visible en: https://www.getcybersafe.gc.ca/en (fecha de consulta: abril, 2023)
- Gráfica UIT Canada, Global Cybersecurity Index 2020: Country Profiles, American Region, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: marzo, 2023)
- Gráfica UIT Estados Unidos, Global Cybersecurity Index 2020: Country Profiles, American Region, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: marzo, 2023)
- Gráfica UIT Estados Unidos Mexicanos, Global Cybersecurity Index 2020: Country Profiles, American Region, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: marzo, 2023)
- *Grooming: ¿qué es, cómo detectarlo y cómo prevenirlo?,* Save the Children, 2019. Información visible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo (fecha de consulta: marzo, 2023)
- Homeland Security, Cybersecurity, Información visible en: https://www.dhs.gov/topics/cybersecurity (fecha de consulta: abril, 2023)
- Intervención de la Senadora Alejandra Lagunes Soto Ruíz el día 24 de octubre de 2019, información visible en: https://www.senado.gob.mx/65/intervenciones/1267/20647 (fecha de consulta: abril de 2023)

- Microsoft Build, Ley Gramm-Leach Billey de 1999, visible en: https://learn.microsoft.com/es-es/compliance/regulatory/offering-glba (fecha de consulta: abril, 2023)
- OWAIDA, Amer, Denuncias de víctimas de delitos informáticos: aumento de 69% en 2020, WeLiveSecurity, ESET, 2021. Información visible en: https://www.welivesecurity.com/la-es/2021/03/19/denuncias-victimas-delitos-informaticos-aumentaron-2020/ (fecha de consulta: marzo, 2023)
- Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), *Desarrollos por País: Canadá.* Información visible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Canada (fecha de consulta: abril, 2023)
- Portal Interamericano de Delitos Cibernéticos de la Organización de Estados Americanos (OEA), *Desarrollos por País: Estados Unidos.* Información visible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Estados%20Unidos (fecha de consulta: abril, 2023)
- Rankin Global UIT, GCI Results: Score and Rankings, Global scores and rankings of countries, ITU Publications, Información visible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (fecha de consulta: abril, 2023)
- Royal Canadian Mounted Police, The National Cybercrime Coordination Center, información visible en: https://www.rcmp-grc.gc.ca/en/nc3 (fecha de consulta: abril, 2023)
- SANTOS CHAVEZ, Juan Jose, *Ley de Ciberseguridad en México*, DELTA PROTECT, 2023. Información visible en: https://www.deltaprotect.com (fecha de consulta: abril, 2023)
- SANTOS CHAVEZ, Juan Jose, *Pentesting*, DELTA PROTECT, 2023. Información visible en: https://www.deltaprotect.com/blog/que-es-pentesting (fecha de consulta: abril, 2023)
- STASTICS CANADA, Impact of cybercrime on Canadian buisinesess 2017, información visible en: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm (fecha de consulta: marzo, 2023)
- TABLA QUE MUESTRA EL PORCENTAJE DE DELITOS A NIVEL MUNDIAL, *Los delitos financieros y los cometidos por internet son los que más preocupan a la policía de todo el mundo*, INTERPOL, Información visible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Los-delitos-finan

cieros-y-los-cometidos-por-Internet-son-los-que-mas-preocupan-a-la-policia-de-todo-el-mundo-segun-un-nuevo-informe-de-INTERPOL (fecha de consulta: marzon 2023)

- Unión Internacional de Telecomunicaciones (UIT), *Sobre la Unión Internacional de Telecomunicaciones (UIT)*, acerca de la UIT. Información visible en: https://www.itu.int/es/about/Pages/default.aspx (fecha de consulta: abril, 2023)

ANEXOS

ANEXO 1: Protocolo de Investigación

Universidad Iberoamericana Puebla

Departamento de Ciencias Sociales

Protocolo de Investigación

Bogarth Alexander Carrasco Palacios

Andrea Ramírez Ordaz

Sofía Sánchez Arenas

Gabriela Sumano Rodríguez

Área de Síntesis y Evaluación Académica: Proyectos Jurídicos e Innovación

Dra. Ana Maria Estela Ramirez Santibañez

9 de febrero de 2023

EL PROTOCOLO DE INVESTIGACIÓN

TEMA

Los delitos cibernéticos dentro del T-MEC, ¿cumplimiento del Estado Mexicano?

OBJETIVO

Establecer→ La importancia de la seguridad cibernética en los ámbitos actuales

Analizar→ Si el Estado mexicano ha implementado leyes para la prevención, regulación y sanción de los delitos cibernéticos

Proponer → En su caso soluciones para una mayor eficiencia en el cumplimiento, en ciberseguridad del TMEC implementación del TMEC

HIPÓTESIS

México, uno de los países contratantes del T-MEC, no ha obtenido un progreso similares a los demás Estado Contratantes en la adaptación de su sistema jurídico a lo pactado en el Tratado entre México, Estados Unidos y Canadá (T-MEC), en cuestión de delitos cibernéticos

JUSTIFICACIÓN DE LA INVESTIGACIÓN

Esta investigación tiene como finalidad demostrar si México ha cumplido con lo establecido en materia de ciberseguridad adecuadamente, de acuerdo a lo contemplado el Tratado entre los Estados Unidos de América, los Estados Unidos Mexicanos y Canadá; dar conocer las medidas implementadas en temas de ciberseguridad y analizar si estas estrategias han tenido una evolución para la protección del patrimonio, datos e integridad de los usuarios y consumidores.

Consideramos que es un tema de estudio relevante, la tecnología se ha transformado a través del paso del tiempo y se encuentra en constante cambio; por lo tanto, los marcos jurídicos deben de evolucionar a la par, para así contar con una adecuada prevención y sanción de los delitos cibernéticos.

Decidimos enfocarnos en el T-MEC por ser una normativa que los países contratantes deben aplicar ante un acto. Es de suma importancia la cooperación entre países para la prevención de los delitos cibernéticos.

Es pertinente realizar un profundo estudio acerca del tema, ya que como sociedad los delitos cibernéticos influyen en nuestro día a día por los alcances económicos, políticos, culturales, sociales que pueden llegar a tener entre otros. Esta influencia puede ser para fines políticos, como el hecho de beneficiar a algún candidato o la intervención de datos privados con la finalidad de obtener un resultado favorable para dichos partidos u obtener información privada de usuarios como cuentas de banco o con fines de acoso y similares, es por eso que es fundamental contar y cumplir con un marco jurídico que satisfaga todas estas necesidades para la protección de personas, instituciones, empresas.

Algunas de las consecuencias de estas conductas son: la recepción de información no deseada, virus, pérdidas económicas, vulnerando la privacidad de personas jurídicas y físicas; por ello, se deben de fortalecer las medidas implementadas en tema de seguridad y observar su cumplimiento.

Los países contratantes deben de brindar una adecuada protección a la información de carácter privado que tanto personas físicas, como instituciones privadas y de gobierno emplean en los medios electrónicos. El Código Penal Federal contempla como delitos informáticos los siguientes: Revelación de secretos y acceso ilícito a

sistemas y equipos de informática, Acoso sexual, Alteración o manipulación de medios de identificación electrónica, Delitos contra la indemnidad de privacidad de la información sexual, Delitos en materia de derechos de autor, Engaño telefónico, Pornografía, Delito equiparado al robo, entre otros.

METODOLOGÍA

En este apartado mencionaremos de forma resumida cómo se desarrollará la investigación, el proceso que seguiremos para darle respuesta a la hipótesis previamente planteada y brindar los argumentos necesarios para su defensa. Con la recopilación de información, su filtración y las conclusiones que se abordaron de dichos procesos. A través del método deductivo, por el cual se procede lógicamente de lo universal a lo particular, partiendo de una premisa general para obtener conclusiones de un caso particular.

De tal forma por el modo y finalidad del trabajo se realizará el uso de la técnica de investigación documental consistente en la búsqueda de fuentes bibliográficas, para poder analizar la figura de los derechos cibernéticos, determinar lo establecido en el Tratado entre México, Estados Unidos y Canadá y ver el progreso o estancamiento por parte del Estado Mexicano para la adaptación a lo convencionalmente dispuesto. La búsqueda se realizó a través de cuerpos jurídicos nacionales e internacionales, así como plataformas, revistas y trabajos de análisis académicos y legales. De igual manera se realizó un filtro de temporalidad, de lo establecido y ocurrido previo al Tratado, como pueden ser causas que ocasionaron las disposiciones del mismo, y de lo sucedido con posterioridad al Tratado, sus consecuencias y cumplimiento. Al inicio de la investigación y del planteamiento hipotético, se estableció delimitar las fuentes de información a fuentes de sistema

jurídico, plataformas gubernamentales, repositorios académicos y revistas de análisis y crítica académica y pública. Debido a la necesidad de enfoques públicos, privados y lo publicitado por parte del gobierno, necesarios para el trabajo.

Haciendo uso del método analítico, el cual Mario Bunge lo establece como el método que aborda problemas circunscriptos uno a uno, y trata de descomponerlo todo en elementos, tratando de entender una situación total en término de sus componentes. Por lo que dividiremos la investigación en enfoques respectivos, relacionados a los capítulos que desarrollaremos a lo largo de la investigación. Durante la realización del trabajo se posibilita la anexión de trabajos que fortalezcan lo realizado, otorguen nuevas perspectivas o actualicen supuestos comentados en el trabajo; de esta forma mantener la actualidad de lo realizado hasta el momento de su entrega.

Con la información recabada y la que se adhiera al trabajo, se fortalecerán conceptos, se aclaran las causas y se puntualiza, de ser así, la falla del sistema jurídico y político Mexicano de adaptar lo propuesto en el Tratado entre México, Estados Unidos y Canadá sus cuerpos legales. Con el fin de obtener el resultado planteado en la hipótesis y poder establecer las variables de acción siguientes a realizarse.

Tras esto haremos uso del método sintético, recopilando la información y reuniendo los capítulos desarrollados con el fin de establecer un orden de entendimiento y análisis apto para la resolución del problema. Concluyendo el método de investigación, con la redacción de los apartados del trabajo, contextualizando los precedentes, estableciendo los realizado hasta el momento y resolviendo la problemática planteada; de tal manera proceder a indicar direcciones

de trabajo y señalar las posibles soluciones al incumplimiento de México, como se plantea en nuestra hipótesis.

MARCO TEÓRICO CONCEPTUAL

Revelación de secretos: Consiste en descubrir secretos o vulnerar la intimidad de una persona a través del apoderamiento o interceptación de documentos sin su consentimiento.

https://www.dexiaabogados.com/blog/delito-revelacion-secretos/

Acceso ilícito a sistemas y equipos de informática: Consiste en que sin la autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Art.211 bis 1 código penal federal

https://www.gob.mx/cms/uploads/attachment/file/235549/Co_digo_Penal_Federal_22_06_2017.pdf

Acoso sexual: Insinuaciones no deseadas, peticiones de favores sexuales, conductas físicas o verbales que sean percibidos como ofensivos.

https://www.conceptosjuridicos.com/mx/acoso-sexual/

Alteración o manipulación de medios de identificación electrónica: Consiste en el hecho de que una persona altere o manipule un mecanismo o sistema de identificación electrónico, magnético, electromagnético, computacional o telemático, de tarjetas de crédito, de débito, de títulos, u otros documentos.

Preguntas y Respuestas Sobre Delitos Informáticos. (2020, August 26). Justia. https://mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/

Delitos contra la indemnidad de privacidad de la información sexual: El que, sin violencia o intimidación y sin que medie consentimiento, realizare actos que atenten contra la libertad o indemnidad sexual de otra persona, será castigado, como responsable de abuso sexual.

https://www.oas.org/dil/esp/Articulos_178_a_183_185_a_196_Codigo_Penal_Espana.pdf

Delitos en materia de derechos de autor: Este tipo de delitos contemplan entre otras conductas la producción, reproducción, distribución y venta, de manera ilícita, de artículos como música, películas y libros sin la autorización del autor.

de la República, F. G. (n.d.). *¿Sabes qué es un delito contra la propiedad intelectual?* Gob.Mx. Retrieved February 15, 2023, from https://www.gob.mx/fgr/es/articulos/sabes-que-es-un-delito-contra-la-propiedad-intelectual?idiom=es

Delito equiparado al robo: Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley.

Código Penal Federal

Engaño telefónico: Es cualquier tipo de engaño en el que un criminal se comunica con una posible víctima a través del teléfono.

Wex: Spanish. (n.d.). LII / Legal Information Institute. Retrieved February 15, 2023, from https://www.law.cornell.edu/wex/es/fraude_telefónico_y_por_telemarketing

Ciberseguridad: La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos, de igual manera se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

¿Qué es la ciberseguridad? (2023, enero 19) latam.kaspersky.com.

https://*latam.kaspersky.com/resource-center/definitions/what-is-cyber-security*

Código de Comercio: Es la norma jurídica encargada de regular las operaciones mercantiles. Esta legislación se aplica en la práctica empresarial para así garantizar el cumplimiento de dichos estándares de carácter legal. La Suprema Corte de Justicia de la Nación, a través del Diccionario Jurídico Mexicano, establece que el Código de Comercio mexicano refleja la idea y el contenido de la codificación en

general. Se trata de un ordenamiento único sobre la materia, que comprende todas las instituciones jurídico-mercantiles existentes.

Código de Comercio.

Código Penal: El Código Penal es un conjunto de normas jurídicas punitivas de un Estado. Es decir, es un código que recoge las penas aplicables a toda persona que cometa algún delito; en él se definen los actos que están tipificados como delitos y se determinan las penas que corresponden.

Código Penal Federal.

Convencionalidad: Es la herramienta que permite a los Estados concretar la obligación de garantía de los derechos humanos en el ámbito interno, a través de la verificación de la conformidad de las normas y prácticas nacionales, con la Convención Americana de los Derechos Humanos y su jurisprudencia.

(S/f). Org.mx. Recuperado el 8 de febrero de 2023, de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S 1405-91932016000200277

Delito Cibernéticos: Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

Paredes, R. (2020, octubre 23). *¿Qué son los delitos cibernéticos?* Rigoberto Paredes Abogados Bolivia – Law Firm; Rigoberto Paredes Law Firm. https://www.rigobertoparedes.com/es/que-son-los-delitos-ciberneticos/

Datos personales: Los datos personales son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Nos dan identidad, nos describen y precisan: edad, domicilio, número telefónico, correo electrónico, patrimonio, trayectoria laboral, académica, profesional, CURP, entre otros.

(S/f). Org.mx. Recuperado el 8 de febrero de 2023, de https://www.infocdmx.org.mx/index.php/protege-tus-datos-personales/¿qué-son-los-datos-personales.html

Internet: El concepto *Internet* tiene sus raíces en el idioma inglés y se encuentra conformado por el vocablo *inter* (que significa *entre*) y *net* (proveniente de *network* que quiere decir *red electrónica*).

Internet. (s/f). Concepto. Recuperado el 8 de febrero de 2023, de https://concepto.de/internet/

Pornografía: Es la filmación, fotografiado y exposición de manera explícita de relaciones sexuales. Es por lo tanto un fenómeno que se hizo extensivo en el siglo XX, momento en el que se desarrollan las tecnologías relacionadas a la misma.

Definición de Pornografía. (n.d.). Enciclopedia.net. Retrieved February 15, 2023, from https://enciclopedia.net/pornografia/

Sistema Jurídico: El conjunto de normas jurídicas objetivas que están en vigor en determinado lugar y época, y que el Estado estableció o creó con el objeto de regular la conducta humana o el comportamiento humano. Integran el conjunto de leyes, costumbres, razones y jurisprudencia de derecho positivo que rigen en los diversos países del mundo. Cada país tiene su propio sistema jurídico y su peculiar manera de considerar las leyes, las costumbres y la jurisprudencia.

Picand, Y., & Dutoit, D. (s/f). *Sistema jurídico*. sensagent. Recuperado el 8 de febrero de 2023, de http://diccionario.sensagent.com/Sistema%20jur%C3%ADdico/es-es/

T-MEC: El Tratado comercial entre México, Estados Unidos y Canadá (T-MEC, o USMCA/CUSMA por sus siglas en inglés), el cual entró en vigor el 1° de julio y sustituye al Tratado de Libre Comercio de América del Norte (TLCAN).

T-MEC. (s/f). Gob.mx. Recuperado el 8 de febrero de 2023, de https://mipymes.economia.gob.mx/exportar-2/t-mec-2/

CAPÍTULOS

CAPÍTULO I: Importancia de la ciberseguridad

1.1 Definición de delitos cibernéticos y ciberseguridad.

1.2 Tipos de delitos cibernéticos más comunes.

1.3 Efectos que genera esta conducta antijurídica.

CAPÍTULO II: Regulación de la ciberseguridad en el T-MEC

2.1 Lo solicitado en el TMEC

2.2 La ciberseguridad en los cuerpos Normativos de Estados Unidos y Canadá

CAPÍTULO III: Ajustes al Marco legal mexicano en materia de ciberseguridad

3.1 Marcos jurídicos han sido creados desde la firma de TMEC

3.2 Aplicación del TMEC en México

3.3 Amparos promovidos por la sociedad

Capítulo IV: Propuestas de solución para mitigar los delitos cibernéticos.

4.1 Adecuamientos necesarios al sistema Mexicano

4.2 Planeación y desarrollo de las propuestas mencionadas

BIBLIOGRAFÍA

Gobierno, E. (n.d.). *Texto sujeto a revisión legal para asegurar su precisión, claridad y congruencia Texto sujeto a autenticación de idiomas TRATADO ENTRE MÉXICO, ESTADOS UNIDOS Y CANADÁ PREÁMBULO*. Gob.Mx. Retrieved February 9, 2023, from https://centrogilbertobosques.senado.gob.mx/docs/T-MEC.pdf

(N.d.). Unodc.org. Retrieved February 9, 2023, from https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf (definición, legislación, aplicación, cooperación, prevención, etc)

Lozano, L. F. (2020, July 1). *¿Qué es el T-MEC y por qué es importante para México?* Forbes México. https://www.forbes.com.mx/economia-que-es-el-t-mec-y-por-que-es-importante-para-mexico/ (beneficios para méxico, diferencia entre T-Mec y TLCAN)

(N.d.-b). Org.Mx. Retrieved February 9, 2023, from https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20México%20(1).pdf

CÓDIGO PENAL FEDERAL

(N.d.). Org.Mx. Retrieved February 9, 2023, from https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20México%20(1).pdf (foro de ciberseguridad entre MEX y USA)

(N.d.-b). Org.Mx. Retrieved February 9, 2023, from https://ciberseguridad.ift.org.mx/files/guias_y_estudios/5_upr_planaccionesciberseguridad.pdf

Quezada, J. P. A. (n.d.). *Ciberseguridad, desafío para México y trabajo legislativo*. Gob.Mx. Retrieved February 9, 2023, from http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de%20Investigaci%C3%B3n%2087.pdf?sequence=1&isAllowed=y (ciberseguridad, desafío para México y trabajo legislativo)

Rivera, M. (2020, December 2). *Los pasos que México debe seguir para fortalecer su ciberseguridad*. Business Insider México | Noticias pensadas para ti. https://businessinsider.mx/pasos-mexico-ciberseguridad-tmec-2020/ (soluciones para reforzar la ciberseguridad en México)

de Grau, T. de F. (n.d.). *Facultat de Ciències Polítiques i Sociologia*. Uab.Cat. Retrieved February 9, 2023, from https://ddd.uab.cat/pub/tfg/2019/tfg_182627/TFG_Maria_Fernanda_Macuaran.pdf (El avance de ciberseguridad entre 2010 y 2018 en canda, nos sirve para el ultimo capitulo)

(N.d.). Revistatransregiones.com. Retrieved February 9, 2023, from https://revistatransregiones.com/web/index.php/tr/article/view/18/15 (delitos ciberneticos, se enfoca en mexico y es de 2021)

Aponte, R., & Thanayri, E. J. (n.d.). *Análisis de los delitos cibernéticos en el estado de Puebla a la luz del derecho nacional e internacional*. Iberopuebla.Mx. Retrieved February 9, 2023, from http://repositorio.iberopuebla.mx/bitstream/handle/20.500.11777/4802/TESINA%20MARIFER%20ORTIZ%20ELBA%20ROMERO%20IVANA%20VÁSQUEZ.pdf?sequence=1&isAllowed=y (delitos cibernéticos, ase 3, ibero)

Paredes, R. (2020, October 23). *¿Qué son los delitos cibernéticos?* Rigoberto Paredes Abogados Bolivia – Law Firm; Rigoberto Paredes Law Firm. https://www.rigobertoparedes.com/es/que-son-los-delitos-ciberneticos/ (cuando se comete un delito cibernetico)

De información, T. y. R. (n.d.). *Capítulo cuarto*. Unam.Mx. Retrieved February 9, 2023, from https://archivos.juridicas.unam.mx/www/bjv/libros/9/4301/6.pdf

CRONOGRAMA

Cosas por realizar	Fecha
· Entrega de Cronograma · Borrador del árbol de problemas · Elección del tema de la investigación	24 de enero de 2023
· Realización del protocolo	24 de enero al 6 de febrero de 2023
· Revisión final del protocolo, correcciones y adhesiones	7 de febrero de 2023
· Entrega del protocolo	**9 de febrero de 2023**
· Definir estructura y posibles subtemas del capítulo 1 · Establecer la forma en que el equipo trabajara el capítulo 1	14 de febrero de 2023
· Desarrollo del primer capítulo	16 de febrero al 2 marzo de 2023

· Revisión final del capítulo, correcciones y adhesiones · Definir estructura y posibles subtemas del capítulo 2 · Establecer la forma en que el equipo trabajara el capítulo 2	14 de marzo de 2023
· Empezar el desarrollo del segundo capítulo	16 de marzo de 2023
· **Entrega del primer capítulo y los avances realizado al segundo capítulo**	**21 de marzo de 2023**
· Desarrollo de lo faltante del capítulo 2	23 de marzo al 6 de abril de 2023
· Revisión final del capítulo, correcciones y adhesiones · Definir estructura y posibles subtemas del capítulo 3 · Establecer la forma en que el equipo trabajara el capítulo 3	11 de abril de 2023

· Empezar el desarrollo del tercer capítulo	13 de abril de 2023
· Entrega del segundo capítulo y los avances realizado al tercer capítulo	**18 de abril de 2023**
· Desarrollo de lo faltante del capítulo 2 · De lo hecho hasta el momento, comenzar la presentación para la entrega final	20 de abril al 2 de mayo de 2023
· Revisión final del capítulo, correcciones y adhesiones · Revisión en su totalidad del proyecto · Realizar infografía para presentación final	4 de mayo de 2023
· Entrega final del proyecto jurídico **· Concluir la presentación e infografía**	**9 de mayo de 2023**

· Ensayo en equipo de la presentación a exponer	10 de mayo de 2023 *En caso de no exponer la primer a fecha, el 15 de mayo se hará un segundo ensayo
· Presentación final del proyecto, mediante la presentación e infografía realizada	11 de mayo (primera fecha) o 16 de mayo de 2023 (segunda fecha)

ANEXO 2: Infografía

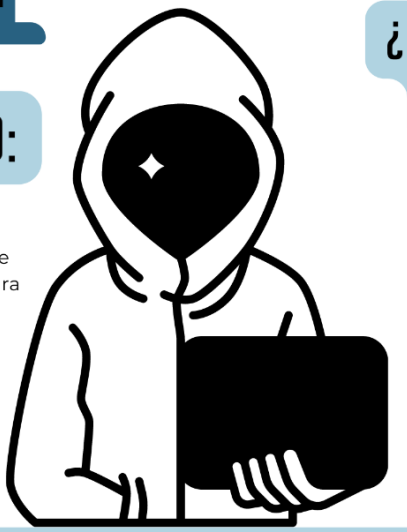
IBERO PUEBLA

LOS DELITOS CIBERNÉTICOS DENTRO DEL T-MEC

¿CUMPLIMIENTO DEL ESTADO MEXICANO?

CIBERSEGURIDAD:

Conjunto de medidas e instrumentos que se realizan e implementan con la finalidad de promover un espacio seguro para usuarios y consumidores de los distintos medios de telecomunicación.



¿QUÉ SON LOS DELITOS INFORMÁTICOS?

Todo comportamiento intencional que se realiza por medio de un ordenador.
Se busca la afectación patrimonial, física, psicológica u afín por medio de engaños o de la materialización de un ataque informático al ordenador del sujeto pasivo

TIPOS MÁS COMUNES

- Phishing
- Pharming
- Robo de identidad
- Spam
- Intrusión en servicios financieros en línea
- Acceso a material inadecuado (ilícito, violento, pornográfico, etc.)
- Ciberbullying
- Grooming

¿QUÉ FUE SOLICITADO EN EL T-MEC?

*Fortalecer los mecanismos para identificar y mitigar las intrusiones maliciosas y desarrollar las capacidades de respuesta a incidentes.

CIBERSEGURIDAD EN E.U.A Y CANADÁ

Canadá-> Cuenta con una legislación de delitos cibernéticos dentro de su propio Código Penal.
E.U.A->En su Código Penal Federal, en el Título 18 del "U.S CODE" que refiere a "Crímenes y Procedimientos Criminales".

AJUSTES AL MARCO LEGAL MEXICANO

México no cuenta con una legislación en materia de ciberseguridad, por lo que existe un vacío legal dejando a los ciudadanos en un plano de desprotección.

Desde el 2018 se han presentado once iniciativas de ley.

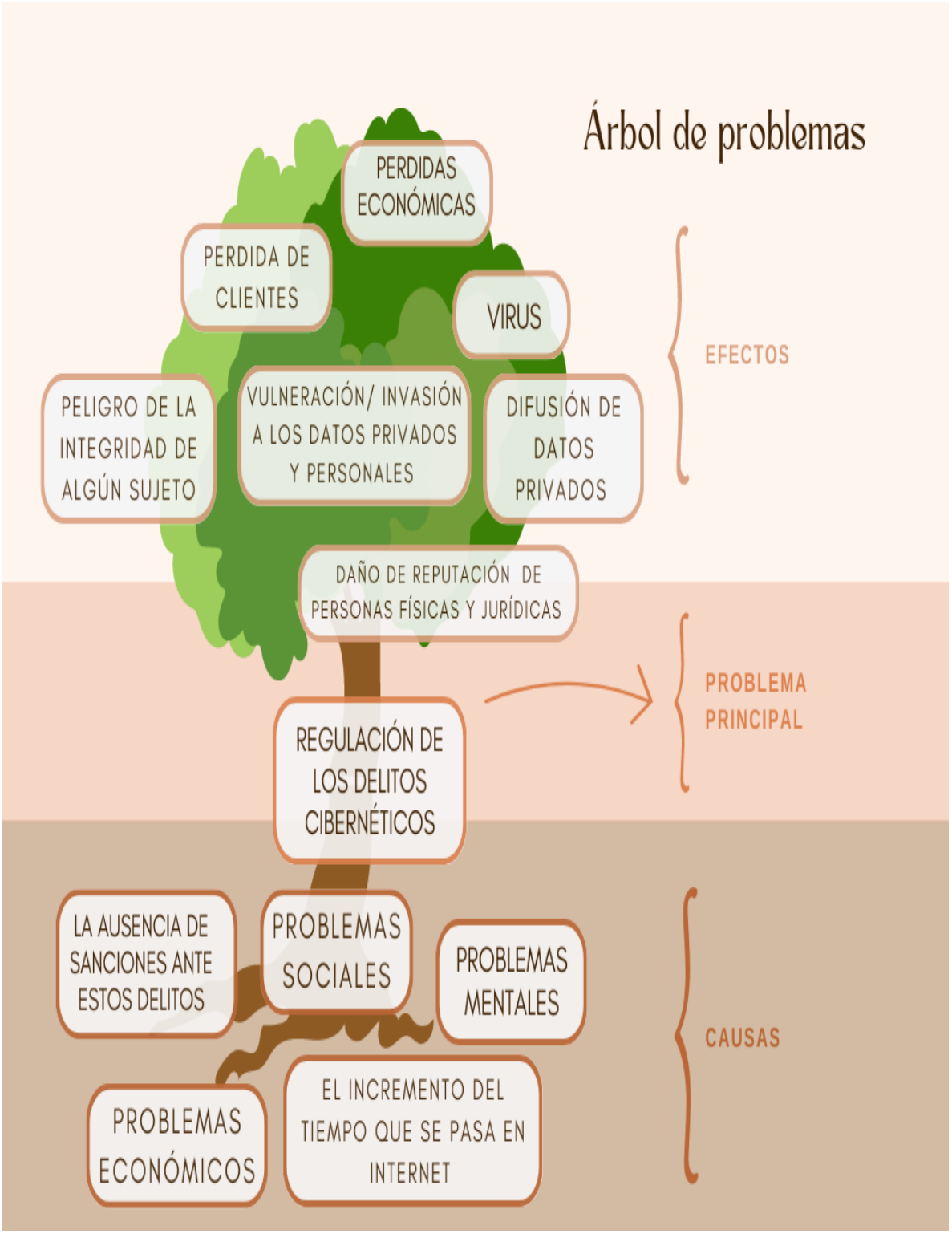
PROPUESTAS DE SOLUCIÓN

- Mantener el software actualizado e instalación de parches de seguridad.
- Programas cortafuego.
- Creación de Ley especializada en delitos cibernéticos

TRABAJO EN EQUIPO ELABORADO POR: Bogarth Alexander Carrasco Palacios, Andrea Ramírez Ordaz, Sofía Sánchez Arenas y Gabriela Sumano Rodríguez.

MATERIA Y LICENCIATURA: Proyectos Jurídicos e Innovación (ASE III) DERECHO

ANEXO 3: Árbol de problemas


Árbol de problemas
PERDIDAS ECONÓMICAS
PERDIDA DE CLIENTES
VIRUS
PELIGRO DE LA INTEGRIDAD DE ALGÚN SUJETO
VULNERACIÓN/ INVASIÓN A LOS DATOS PRIVADOS Y PERSONALES
DIFUSIÓN DE DATOS PRIVADOS
EFECTOS
DAÑO DE REPUTACIÓN DE PERSONAS FÍSICAS Y JURÍDICAS
PROBLEMA PRINCIPAL
REGULACIÓN DE LOS DELITOS CIBERNÉTICOS
LA AUSENCIA DE SANCIONES ANTE ESTOS DELITOS
PROBLEMAS SOCIALES
PROBLEMAS MENTALES
PROBLEMAS ECONÓMICOS
EL INCREMENTO DEL TIEMPO QUE SE PASA EN INTERNET
CAUSAS

ANEXO 4: Sinopsis

Los delitos cibernéticos constituyen un gran problema que ha ido evolucionando conforme el desarrollo de las Tecnologías de la Información y Comunicación, es por lo que, los países deben trabajar arduamente por establecer mecanismos de prevención, detección y sanción ante esta conducta antijurídica.

El T-MEC es un Tratado Internacional firmado en el 2018 por los países contratantes, estos siendo México, Estados Unidos y Canadá, de ahí en su capítulo 19.15 se establecieron las bases para regular la ciberseguridad, el cual para efecto del presente proyecto jurídico será el sustento para su estudio. Así mismo se desarrollará de manera más amplia y extensa , a fin de conocer la manera en la que los Estados contratantes han hecho el cumplimiento de esta normatividad.