Facultad de Ciencias Jurídicas y Justicia

Licenciatura en Ciencias Jurídicas, Sociales y de la Justicia

El Delito Informático en Guatemala, México y Costa Rica

(Tesis de Licenciatura)

Andrea María Serrano Del Cid

Guatemala, septiembre 2021

Facultad de Ciencias Jurídicas y Justicia
Licenciatura en Ciencias Jurídicas, Sociales y de la Justicia

El Delito Informático en Guatemala, México y Costa Rica

(Tesis de Licenciatura)

Andrea María Serrano Del Cid

Guatemala, septiembre 2021

Para efectos legales y en cumplimiento a lo dispuesto en el artículo 1°, literal h) del Reglamento de Colegiación del Colegio de Abogados y Notarios de Guatemala, **Andrea María Serrano Del Cid**, elaboró la presente tesis, titulada: **El Delito Informático en Guatemala, México y Costa Rica.**

AUTORIDADES DE UNIVERSIDAD PANAMERICANA

M. Th. Mynor Augusto Herrera Lemus
Rector

Dra. Alba Aracely Rodríguez de González
Vicerrectora Académica

M. A. César Augusto Custodio Cóbar
Vicerrector Administrativo

EMBA. Adolfo Noguera Bosque
Secretario General

FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA

Dr. Enrique Fernando Sánchez Usera

Decano de la Facultad de Ciencias Jurídicas y Justicia

LCDA. GLADYS JEANETH JAVIER DEL CID
Abogada y Notaria

Guatemala, 23 de marzo 2021

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como **tutora** de tesis del (la) estudiante **Andrea Maria Serrano Del Cid** ID **000018872.** Al respecto se manifiesta que:

a) Brindé acompañamiento a la estudiante en referencia durante el proceso de elaboración de la tesis denominada: **El delito informático en Guatemala, México y Costa Rica.**
b) Durante ese proceso le fueron sugeridas correcciones que realizó conforme los lineamientos proporcionados.
c) Habiendo leído la versión final del documento, se establece que el mismo constituye un estudio serio en torno al tema investigado, cumpliendo con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito **DICTAMEN FAVORABLE,** para que se continúe con los trámites de rigor.

Atentamente,

LICENCIADA
Gladys Jeaneth Javier Del Cid
ABOGADA Y NOTARIA

Lcda. Gladys Jeaneth Javier Del Cid
Abogada y Notaria

Email: janyjavier@gmail.com

UNIVERSIDAD PANAMERICANA

"Sabiduría ante todo, adquiere sabiduría"

Guatemala, cinco de junio de dos mil veintiuno

Señores Miembros

Consejo de la Facultad de Ciencias Jurídicas y Justicia

Universidad Panamericana Presente

Estimados Señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como revisor de la tesis del estudiante **Andrea María Serrano Del Cid**, ID **000018872** titulada: **El Delito informático en Guatemala, México y Costa Rica.**

Al respecto me permito manifestarles que, la versión final de la investigación fue objeto de revisión de forma y fondo, estableciendo que la misma constituye un estudio serio que cumple con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica. En virtud de lo anterior, por este medio emito **DICTAMEN FAVORABLE** para que se continúe con los trámites de rigor.

Atentamente

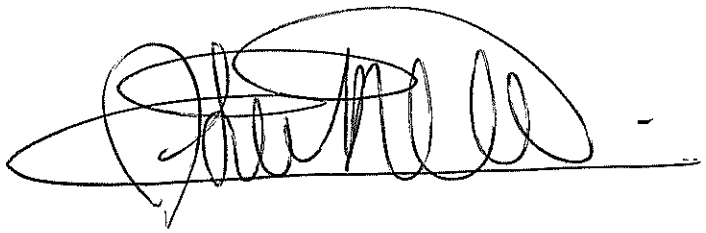
Licda. Valeria Stefanía

Reyna Cifuentes

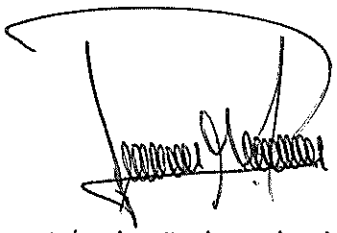
En la ciudad de Guatemala, el día veintitrés de agosto del año dos mil veintiuno, siendo las quince horas horas, yo, **Lilian Magaly González Alvarado**, Notaria, número de colegiado treinta y un mil ochocientos setenta y cinco (31875), me encuentro constituida en casa treinta y cuatro condominio Citadella, Sábana Arriba zona diecisiete, ciudad Guatemala, soy requerida por **Andrea María Serrano Del Cid**, de treinta años de edad, soltera, guatemalteca, estudiante, de este domicilio, quien se identifica con Documento Personal de Identificación (DPI) con Código Único de Identificación (CUI) dos mil cincuenta y uno, espacio cuarenta y ocho mil cuatrocientos nueve espacio cero ciento uno (2051 48409 0101), extendido por el Registro Nacional de las Personas de la República de Guatemala, quien requiere mis servicios profesionales con el objeto de hacer constar a través de la presente **DECLARACIÓN JURADA** lo siguiente: **PRIMERA:** El requirente, **BAJO SOLEMNE JURAMENTO DE LEY** y enterado por el infrascrito notario de las penas relativas al delito de perjurio, DECLARA ser de los datos de identificación personal consignados en la presente y que se encuentra en el libre ejercicio de sus derechos civiles. **SEGUNDA**: Continúa declarando bajo juramento el requirente: i) ser autor del trabajo de tesis titulado: "**El Delito informático en Guatemala, México y Costa Rica**" ii) haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; iii) aceptar la responsabilidad como autor del contenido de la presente tesis de licenciatura. No habiendo nada más que hacer constar, finalizo el presente instrumento en el mismo lugar y fecha de inicio a las quince horas con treinta minutos, la cual consta en una hoja de papel bond tamaño oficio, impresa en ambos lados, que numero, firmo y sello, a la cual le adhiero los timbres para cubrir los impuestos correspondientes que determinan las leyes respectivas: un timbre notarial del

valor de diez quetzales con serie AX guión cero ciento sesenta y tres mil doscientos ocho (AX 0163208) y un timbre fiscal del valor de cincuenta centavos con número de registro dos millones ciento quince mil trescientos cincuenta y seis (2115356). Leo íntegramente lo escrito al requirente, quien enterado de su contenido, objeto, validez y demás efectos legales, la acepta, ratifica y firma con el Notario que autoriza. **DOY FE DE TODO LO EXPUESTO.**

f)



ANTE MÍ:



Licda. Lilian Magaly González Alvarado
ABOGADA Y NOTARIA

UNIVERSIDAD PANAMERICANA
"Sabiduría ante todo; adquiere sabiduría"

Ref. O.I. 30-2021
ID 000018872

ORDEN DE IMPRESIÓN DE TESIS DE LICENCIATURA

Nombre del Estudiante: **ANDREA MARÍA SERRANO DEL CID**
Título de la tesis: **EL DELITO INFORMÁTICO EN GUATEMALA, MÉXICO Y COSTA RICA**

La Vicedecano de la Facultad de Ciencias Jurídicas y Justicia,

Considerando:

Primero: Que previo a otorgársele el grado académico de Licenciada en Ciencias Jurídicas, Sociales y de la Justicia, así como los títulos de Abogada y Notaria, la estudiante ya mencionada, ha desarrollado el proceso de investigación y redacción de su tesis de licenciatura.
Segundo: Que tengo a la vista el dictamen favorable emitido por la tutora, Licenciada Gladys Jeaneth Javier Del Cid, de fecha 23 de marzo de 2021.
Tercero: Que tengo a la vista el dictamen favorable emitido por la revisora, Licenciada Valeria Estefanía Reyna Cifuentes, de fecha 05 de junio de 2021.
Cuarto: Que tengo a la vista el acta notarial autorizada en la ciudad de Guatemala, el día 23 de agosto de 2021 por la notaria Lilian Magaly González Alvarado, que contiene declaración jurada de la estudiante, quien manifestó bajo juramento: *ser autor del trabajo de tesis, haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; y aceptar la responsabilidad como autor del contenido de su tesis de licenciatura.*

Por tanto,

Autoriza la impresión de la tesis elaborada por la estudiante ya identificada en el acápite del presente documento, como requisito previo a la graduación profesional.

Guatemala, 08 de septiembre de 2021.

"Sabiduría ante todo, adquiere sabiduría"

UNIVERSIDAD PANAMERICANA · FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA · M.Sc. Andrea Torres Hidalgo · VICE-DECANO

M.Sc. Andrea Torres Hidalgo
Vicedecano de la Facultad de Ciencias Jurídicas y Justicia

Nota: *Para efectos legales únicamente el sustentante es responsable del contenido del presente trabajo.*

Dedicatoria

A mi madre: Gracias por su apoyo y amor incondicional, por creer en mí y alentarme a desafiar los límites de lo impuesto socialmente a las mujeres. La amo mucho.

A mi padre: Por forjarme el cuestionar todo e inculcarme el pensar lógicamente por sobre todas las formas. Por enseñarme que, si quería ser grande, tenía que leer a los clásicos y escuchar a los clásicos. No estaría donde estoy si no fuera por usted papa, lo amo mucho, gracias por ser tan genial.

A mi hermano: Mi primer mejor amigo, gracias por tu apoyo y tus consejos siempre, te quiero mucho nene.

A Jan: Tu apoyo fue indispensable para mi proceso de cierre, gracias por tu paciencia y tu cariño a lo largo de los años. Espero seguirle dando la vuelta al mundo a tu lado.

A mis amigos: Mis compañeros de la facultad: Carlos, Edgar. Ivonnie, Kevin, Melvin, Osbaldo, Elenita, Lesvia, Karin y Alex: Su compañía lleno la jornada sabatina de momentos especiales, los aprecio mucho.

A Lily: Mi mejor regalo de la facultad, tu guía y apoyo durante la carrera fueron cruciales para mi desarrollo personal y profesional, espero poder seguir aprendiendo mucho de ti. Todo mi cariño.

Índice

Resumen

Este estudio de investigación versó sobre los avances tecnológicos que se ha tenido a lo largo de los últimos años a nivel mundial, el cual ha influido directamente en el desarrollo de la humanidad, ya que, a través de los medios de comunicación se facilita en tiempo real el intercambio de datos e información. Sin embargo, no todo ha resultado de forma positiva, ya que, con ese intercambio de datos e información que hacen las personas a través del Internet, la delincuencia ha encontrado oportunidad y una nueva opción de cometer hechos delictivos, debido a que se han aprovechado de herramientas digitales que no se encontraban reguladas de forma amplia y específica como tipos penales, lo que representó un reto enorme para los gobiernos centrales a nivel global, toda vez, que estos ordenamientos jurídicos no estaban preparados ni respondían para esta nueva modalidad de criminalidad.

Por tal razón, países de América Latina como México, Costa Rica, entre otros, fueron de los primeros países de la región en implementar modificaciones a sus ordenamientos jurídico-penales y procesales que contemplaron los delitos perpetrados a través de la red. En Guatemala, sin embargo, a pesar de que en tres ocasiones se ha intentado crear una ley ordinaria que regule los delitos cibernéticos, a la fecha aún no existe un fundamento legal bajo el cual pueda sancionarse dicho comportamiento,

quedando una mayoría de los delitos de esa naturaleza reportados, impunes.

Fue por ello que resultó en demasía importante realizar un análisis comparativo de los ordenamientos jurídicos y de datos estadísticos sobre delitos informáticos en México, Costa Rica y Guatemala, con el fin de determinar si la existencia y aplicabilidad de una normativa específica que regule lo relativo al Delito Informático, tiene efecto disuasivo en los países que sí cuentan con la misma, y cómo se comparan con Guatemala, país que carece de esta.

Palabras clave

Cibernético. Comunicación. Criminalidad. Tecnología. Información.

Introducción

Guatemala no cuenta con una legislación específica que permita tipificar de forma apropiada los Delitos Informáticos, lo cual ha causado, que cuando ocurren estos delitos, no sean sancionados, vulnerando los derechos humanos. Esto a su vez expone a menores de edad como su población más vulnerable y potencialmente más afectada.

El aumento de la comisión de este tipo penal en los últimos años, demanda la realización de esta investigación, a efecto de impulsar una reforma en la legislación penal guatemalteca que regule los delitos informáticos, para que estos puedan ser tipificados y sancionados.

En la actualidad no existe un estudio analítico y comparativo entre Guatemala, México y Costa Rica que permita determinar la viabilidad de la implementación de una ley especifica que regule el Delito Informático en Guatemala e informe a la población sobre su existencia y la amenaza que representa el crecimiento de la comisión de este tipo penal.

Como parte de los objetivos de investigación, en principio se tendrá el general, lo que se buscará a través de él es comparar las legislaciones e iniciativas existentes de los países objeto de este estudio y la viabilidad de aplicación de los preceptos de ley y su ajuste a la naturaleza evolutiva del

delito informático en Guatemala; en ese contexto, el primer objetivo específico será identificar al delito informático en sus distintas modalidades y los eventos históricos que le dieron notoriedad global, sus antecedentes, los elementos que lo componen y los sujetos que forman parte del mismo, así como, las repercusiones que causan dependiendo el ámbito en el que se lleve a cabo. Como segundo objetivo específico, se realizará un análisis comparativo entre las estadísticas de la comisión de este tipo de hechos delictivos en los países objeto de la presente investigación, a través de esta comparación se identificará las pautas de comisión de delito informático a través del tiempo, así como las diferencias y similitudes que existen en esos países.

Los métodos a utilizar en esta investigación serán el analítico y comparativo. Analítico ya que distingue los elementos de las legislaciones e iniciativas a investigar, y se procede a revisar ordenadamente cada uno de ellos por separado. El método comparativo paralelamente permite el análisis sistemático de información colectada en el método analítico, realizando un contraste entre los elementos de las legislaciones e iniciativas, y mejorando el conocimiento de las diferencias o similitudes encontradas, para estructurar los objetivos tanto general como específicos. Para alcanzar los objetivos, tanto general como específicos, es necesario abordar los siguientes temas: en el primer subtitulo se detallarán los antecedentes del delito informático a nivel general y las conductas y

elementos que componen al mismo, así como su clasificación dependiendo el tipo, lo cual sentará una base de conocimiento claro para el lector conforme avance en la lectura del presente estudio. En el subtítulo segundo, se abarcará la comparación estadística de delitos informáticos reportados entre el periodo 2016-2018 en los países objeto de este estudio de investigación, la identificación de patrones de comisión a lo largo del tiempo y una ilustración gráfica que facilite el análisis comparativo entre países que cuentan con legislaciones reguladoras de la materia y quienes carecen de esta. Por último, en el tercer subtitulo, se desarrollará de forma individual la legislación e iniciativas existentes de cada país sujeto de este estudio.

El Delito Informático

Antecedentes

La globalización ha sido causal de desarrollo, creando una expansión masiva de bienes y servicios para contribuir al crecimiento integral de la sociedad, en la cual las computadoras han tenido un rol clave en la automatización de procesos, específicamente modificando el uso y manejo de información. Las computadoras han pasado de ser herramientas auxiliares para el desarrollo de actividades cotidianas a ser medios eficaces para extraer datos de diversa naturaleza y facilitar su transmisión, lo cual permite clasificarlas como medio de comunicación. Según el diccionario de la Real Academia de la Lengua Española, informática es el "conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales".

Históricamente, la creación de nuevas tecnologías de comunicación entre las personas también ha implicado su aprovechamiento indebido e ilícito. Esto sucedió desde la creación del telégrafo cuando los operarios del mismo filtraban información militar confidencial o bien tergiversaban el mensaje a transmitir a efecto de evitar o promover crisis políticas. Asimismo, con la incorporación del teléfono a la vida cotidiana de las personas, al ser utilizado para reclamar el rescate en casos de secuestro,

extorsión e incluso siendo utilizado en casos de conspiración como el método de comunicación principal.

Con lo anterior queda claro que el auge de las tecnologías ha traído consigo innumerables avances para la humanidad, pero también otra serie de retos para las autoridades, legisladores e investigadores, quienes han tenido que centrarse cada vez más en la persecución y sanción de las conductas antijurídicas que van surgiendo paralelamente al desarrollo tecnológico acelerado. En este contexto surgen los denominados delitos informáticos o cibernéticos.

Sin embargo, a diferencia de las tecnologías mencionadas anteriormente, los delitos informáticos tuvieron un crecimiento más periódico, consecuencia de la comercialización de las computadoras personales e incorporación de internet con pocas o nulas restricciones, lo cual facilitó el entorno para la comisión de hechos ilícitos.

Los orígenes del delito informático pueden rastrearse a inicios de los 60, cuando artículos en revistas y novelas infundían temor sobre las nuevas tecnologías y sus alcances. En ese entonces, el temor consistía mayormente en la creación de maquinaria y tecnología que reemplazara la mano de obra humana. Curiosamente, ya se consideraba como un riesgo potencial lo que el abuso o uso indebido de las nuevas tecnologías podían

causar para el entorno, siendo la invasión a la privacidad uno de los mayores temores de la sociedad conservadora de aquel entonces. La obra de George Orwell titulada “1984” jugó un rol clave en el temor difundido, ilustrando un entorno donde un gran hermano omnipresente controlaba y vigilaba la vida de las personas a través del uso de nuevas tecnologías.

Posteriormente en la década de 1970 se materializó el delito informático como tal, representando pérdidas cuantiosas para los sectores privados y estatales que tenían acceso a la red. A partir del desarrollo de delitos económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión. Los objetivos del delito eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco espionaje industrial.

Esto no era un mal colectivo en aquel entonces, ya que el uso de internet era reservado para grandes empresas que podían costear el uso del mismo, y para uso de inteligencia militar. Con la apertura de internet global a mediados de la década de los años 90, la transición a la red del comercio, banca y la apertura masiva de sitios de interacción social, marcó el inicio de una nueva era para los delitos perpetrados a través de internet.

Definición

El delito informático es definido como “el acto u omisión que sancionan las leyes penales que protegen información en un sistema informático o equipos de informática ya sea modificando la información o dañándolos, o bien obteniendo a través de ellos alguna cosa o lucro indebido” (Montaño Alejandro, 2008 p.140)

En la definición de delito informático, hay que tomar en cuenta que no es compuesto por una conducta antijurídica singular o con un resultado similar. En la actualidad, no hay campo tecnológico con intervención humana que no sea susceptible al alcance informático, lo que causa dificultad al delimitar el delito en sí; lo cual a su vez representa un reto para los legisladores para definir los elementos que constituyen la conducta punible.

Por su parte, Julio Téllez Valdez (2003) conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a “*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin*” y por las segundas “*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin*” (p.35)

A pesar de la complejidad que representa, una definición relativamente simple podría ser la siguiente: Delito informático es el uso de cualquier sistema informático como medio o fin de un delito. De esta manera se abarcan todas las modalidades delictivas de acuerdo al marco legal de cada país; sin embargo, para esto es conveniente también definir qué es un sistema informático.

De acuerdo con el Convenio sobre la Ciberdelincuencia adoptado en Budapest, por los Estados Miembros del Consejo de Europa (2001) indica: “Por sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa" (p.3)

Esta definición abarca no solo a las computadoras, sino a otros tipos de dispositivos como *data centers, módems* y cualquier otro sistema que permita la ejecución de un programa y/o manipulación de datos.

En ese sentido, para poder delimitar el contenido de este fenómeno, se debe optar primero por una denominación genérica y flexible, acerca del mismo como sería delito informático o criminalidad informática, sin limitarse así a términos rígidos.

Elementos del delito informático

Derivada la amplitud de ámbitos y formas en las que puede perpetrarse el delito informático, los elementos que lo componen pueden variar. Sin embargo, a efecto de delimitar los elementos fundamentales se utilizará la clasificación definida por Loredo (2013), que comprende los siguientes elementos: el *iter criminis*, el equipo informático, el internet y el anonimato absoluto y relativo. (p.26)

Iter criminis

El delito no se lleva a cabo *impromptu*. Generalmente obedece a algún tipo de preparación o concepción mental de quien va a cometerlo. De acuerdo a la doctrina penal, Gonzalez (2003) indica lo siguiente: "El *iter criminis* comprende el camino o etapas del delito, tanto internas o mentales (no punibles) como físicas o externas (materialización o consumación del delito)" (p.111). En el caso específico del delito informático, el *iter criminis* se lleva a cabo cuando el autor del delito investiga, planea y selecciona a su víctima. Cabe mencionar que para que esta conducta no sea penada por la ley no debe causar daño o perjuicio a terceros.

El equipo informático

Nidia Callegari (2008) define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas" (p.37). Toda realización de un delito utiliza un medio o herramienta física para consumarse. En el caso preciso del delito informático, la utilización dolosa y sin derecho de cualquier medio tecnológico como fin o medio para materializar una conducta antijurídica, vuelven el equipo informático un elemento fundamental del delito en cuestión.

Anonimato absoluto

El sujeto activo experto de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que puede valerse de sus conocimientos de la red y herramientas tecnológicas para remotamente y sin poder ser rastreado utilizar equipos informáticos ajenos y evitar ser descubierto.

De igual forma, existen programas de enmascaramiento o que no permiten evidenciar la verdadera dirección ya sea de correo electrónico o del número IP. Al no poder ser identificado el sujeto activo, se configura el anonimato absoluto e imposibilita la persecución penal. Lamentablemente la facilidad con la que se puede guardar la identidad en este tipo de delitos

lo vuelve atractivos para la nueva generación de cibercriminales, constituyéndose como el ámbito delictivo con mayor crecimiento según estadísticas presentadas en el reporte consolidado anual de criminalidad de las Naciones Unidas en 2013 otorgado por la Oficina de las Naciones Unidas en su división de drogas y crimen por sus siglas en ingles UNODC.

Anonimato relativo

Según Carlos Montt (1993) "El anonimato relativo se lleva a cabo cuando el autor del delito informático le atribuye sus acciones a alguna organización que oculta su identidad". Sin embargo, únicamente permanece anónimo por un corto periodo de tiempo, antes de ser rastreado y descubierto derivado de su falta de experiencia técnica para cubrir su rastro en la red. Por eso se le denomina relativo, ya que la anonimidad de la que goza el sujeto activo del delito es temporal. (p.55)

Internet

El equipo informático por sí solo no es dañino ni peligroso. Al contrario, fue creado para automatizar procesos administrativos, realizar múltiples operaciones simultáneamente como algunas de sus funciones. Su utilización constituyó un avance significativo para la humanidad y la ciencia. Sin embargo, con la poderosa fusión de equipo informático e internet, permitiendo la conexión inmediata de millones de equipos

informáticos con pocos límites, a lo largo del mundo, se constituye el internet como el medio a través del cual se lleva a cabo el delito informático. En un orden de ideas sucesivo, en el equipo informático se origina el comando dañino, y este comando se transporta a través de internet para consumar el delito informático.

Características del delito informático

El autor, Téllez Valdez (2003), identifica los siguientes:

- Son conductas criminales de cuello blanco o bien de alto nivel, ya que generalmente sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya las bases de datos bancarias e instituciones estatales son blancos frecuentes derivado de los datos sensibles que manejan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho y a la novedad del delito.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar, por lo que la manipulación de información obtenida ilegalmente puede causar tensión política.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Tienden a proliferar cada vez más, con la facilidad de adquirir equipo informático e internet en la actualidad. (p. 52)

Haciendo un análisis de las características descritas anteriormente, cabe señalar que es imperativo para el sector justicia el actuar de la manera más eficaz, para evitar este tipo de delitos y la tasa de impunidad que acarrean. Se debe de legislar atendiendo los aspectos técnicos y sociales que componen el delito, recurriendo a las diferentes áreas que tiene el conocimiento, tanto técnico en materia de informática, como en lo legal (el derecho), ya que, si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular.

Sujetos del Delito Informático

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. Loredo (2003) indica: “Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo” (p.56).

Sujeto activo

De acuerdo al profesor chileno Montt (1993), se entiende por tal “Quien realiza toda o una parte de la acción descrita por el tipo penal” (p. 129).

Derivado de la naturaleza misma del delito informático, las personas que los cometen son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes. Los sujetos activos de este delito en particular tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Sujeto pasivo

De acuerdo a lo establecido por Carlos Montt (1993) “El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo”. En primer lugar, se debe de distinguir que sujeto pasivo ó víctima del delito es el ente o persona sobre la cual recae la conducta de acción u omisión que realiza el sujeto activo, en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros. (p.57)

Clasificación del delito informático

Los delitos informáticos abarcan una gran variedad de modalidades, tal como se mencionan en la página *web* de la Organización Internacional de Policía Criminal, por sus siglas en inglés: INTERPOL y se enlista a continuación:

- Ataques contra sistemas y datos informáticos
- Usurpación de la identidad
- Distribución de imágenes de agresiones sexuales contra menores
- Estafas a través de internet
- Intrusión en servicios financieros en línea
- Difusión de virus
- *Botnets* (redes de equipos infectados controlados por usuarios remotos)
- *Phishing* (adquisición fraudulenta de información personal confidencial)

De la clasificación anterior, se puede notar, que el objetivo final del Delito Informático no difiere demasiado del objetivo de los delitos penales "tradicionales", teniendo como denominador común la conducta antijurídica entre ambos tipos, la nueva modalidad siendo la variante en el caso del Delito Informático, y utilizando el internet como medio de comisión.

Sin embargo, también existen riesgos relacionados con el uso de las redes sociales y acceso a todo tipo de información, tales como:

- Acceso a material inadecuado (ilícito, violento, pornográfico, etc.)
- Adicción - procrastinación (distracciones para los usuarios, juegos de apuesta)
- Problemas de socialización
- Acoso (pérdida de intimidad)
- *Sexting* (manejo de contenido erótico vía mensaje)
- *Ciberbullying* (acoso entre menores por diversos medios: móvil, internet, videojuegos, etc.)
- *Cibergrooming* (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat)

Entre los mencionados anteriormente, no todos pueden ser formalmente tipificados como delitos por sí mismos. No obstante, pueden constituirse como hechos generadores de un potencial delito en el futuro, si no se toman las medidas necesarias a tiempo. La ley al establecer claramente los supuestos de hecho que constituyen la conducta antijurídica, con su respectiva consecuencia, tiene efecto disuasivo para el potencial criminal.

Análisis de estadísticas de Comisión de Delito Informático reportado en Guatemala, México y Costa Rica durante el periodo 2016-2018

Antecedentes

De acuerdo a la revista *Insight Crime* en una publicación de septiembre del año 2016, en los últimos años, el uso de internet en Latinoamérica ha crecido más rápido que en cualquier otra región en el mundo, y paralelo a

ese crecimiento ha aumentado el *cibercrimen*. Según los resultados de una encuesta publicada por Grant Thornton en el 2016, un aproximado de 11% de los negocios en Latinoamérica ha sufrido alguna consecuencia de un ciberataque en los últimos doce meses. Entre los ataques sufridos se encuentran: La filtración de información confidencial, manipulación de banca virtual, software fraudulento en teléfonos móviles entre otros delitos de naturaleza informática.

Según estimaciones del Registro de Internet de América latina y el Caribe, por sus siglas en inglés LACNIC, que es el organismo que maneja el registro de direcciones de internet para la región, el *cibercrimen* le cuesta a la región alrededor de 90,000 millones de dólares al año.

La falta de estadísticas oficiales sobre delito informático en algunos de los países objeto de este estudio representa un aspecto sustancialmente problemático que impide desarrollar un trabajo formal de observación, análisis y elaboración de estrategias o planes a mediano o largo plazo orientados a combatir el *cibercrimen*. Lo anterior se debe en parte a que la comisión masiva de delitos informáticos es relativamente nueva, aunado a que la legislación penal en Latinoamérica no ha avanzado con la rapidez necesaria para ajustarse a esta nueva modalidad de conducta ilícita. Sin embargo, existen organizaciones privadas que se dedican a la recolección y consolidación de estos datos, (en los países donde no existen estadísticas

oficiales) a fin de fomentar el conocimiento entre los usuarios y potencialmente alertar a las autoridades estatales sobre las cifras emergentes del delito informático.

Según el Observatorio de Delitos Informáticos de Latinoamérica, por sus siglas ODILA, las denuncias de delitos que derivada su naturaleza permiten ser catalogados como cibernéticos, se ha triplicado en los últimos 5 años, con prevalencia los delitos perpetrados utilizando sitios de interacción social de forma virtual, denominados redes sociales. A fin de ilustrar con claridad, las redes sociales son sitios de internet formados por comunidades de individuos con intereses o actividades en común (como amistad, parentesco, trabajo entre otros) y que permiten el contacto entre estos, con el objetivo de comunicarse e intercambiar información.

En consecuencia, de lo anterior, la comparación estadística de este estudio se centrará en el periodo comprendido entre el año 2016 al año 2018, ya que marca la transición y evolución del delito informático, al ya no centrarse en corporaciones, organizaciones gubernamentales y bancos, por mencionar algunos de sus objetivos preferentes, y se enfoca en usuarios individuales como nuevas víctimas, al encontrarse estos en una posición más vulnerable.

La selección de los países sujeto de este estudio se deriva de que tanto Guatemala, como Costa Rica y México comparten cifras de acceso a internet de similares proporciones, lo cual de acuerdo a una proporción lógica debería representar estadísticas de comisión similares de delito informático. Para delimitar las variables del delito informático en la comparación estadística, se utilizará la clasificación brindada por la INTERPOL, misma que fue detallada en el capítulo anterior.

El Delito Informático en Guatemala

Antecedentes de la historia del internet en Guatemala

En Guatemala, el internet nace en el año 1992 a través del convenio entre el Consejo Nacional de Ciencia y Tecnología, por sus siglas: CONCYT y la Empresa Guatemalteca de Telecomunicaciones, por sus siglas: GUATEL. El convenio fue denominado "Programa de Información Científica y Tecnológica – Red Maya – MAYAnet". Esta red tenía la finalidad de proveer la interconectividad de alta velocidad entre las universidades nacionales y las instituciones de investigación científica tanto a nivel nacional como panamericano. A través de este acuerdo, tomando en cuenta que MayaNet era un proyecto científico/académico, con mucho potencial para el desarrollo del país, GUATEL brindó una

ayuda sustancial, ofreciendo rebajas en la comunicación vía satélite y dos años de servicio gratuito a los miembros de MayaNet.

La operación de MayaNet dio inició en diciembre del año 1995, ofreciendo todos los servicios de internet. El enlace satelital era de 64 kbps (kilo bits por segundo por sus siglas en inglés) y el costo era de US$ 3,200 mensuales para el enlace internacional, el equivalente aproximadamente a US$4500 actuales según tasas de inflación. En aquel entonces MayaNet se ofrecía únicamente a universidades, instituciones de investigación científica y algunas oficinas del gobierno derivado que era un proyecto fundado en gran proporción con fondos gubernamentales. No fue sino hasta 1998 que surgieron varios proveedores de servicio de internet privado a precios más accesibles para los usuarios locales. Hoy, numerosos proveedores comerciales atienden la creciente demanda guatemalteca por poner su información a disposición del mundo.

Análisis de estadísticas de comisión sobre el delito informático en Guatemala entre el 2016 al 2018

Antecedentes

Según el boletín estadístico correspondiente al segundo semestre del año 2018 de la Superintendencia de Comunicaciones de Guatemala, por sus siglas SIT, indica que la cantidad de teléfonos móviles operando en

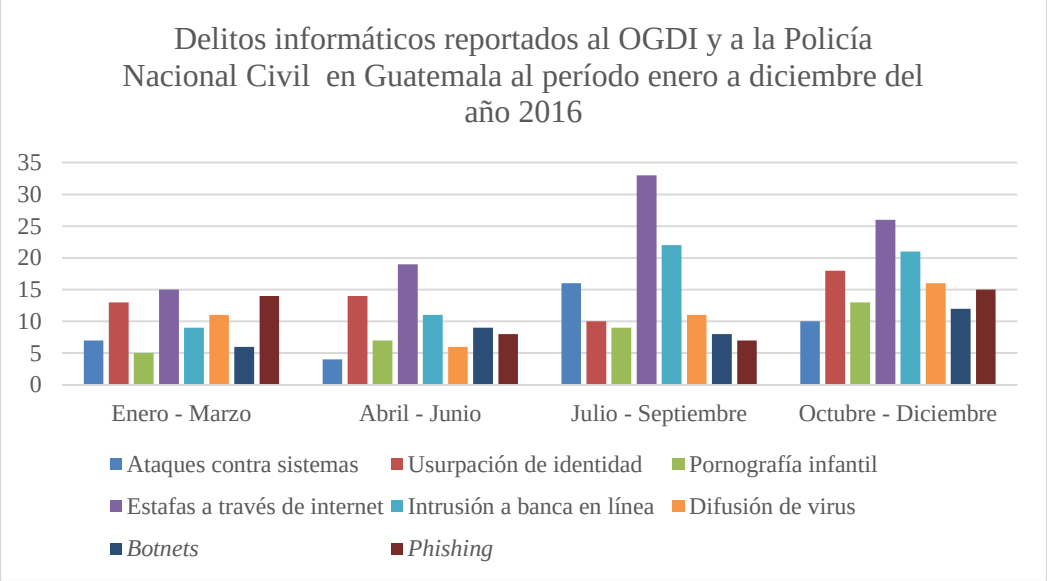
Guatemala alcanza los 20.4 millones de usuarios, es decir, supera la población nacional de acuerdo al último censo efectuado por el Registro Nacional de las Personas, por sus siglas - RENAP en el año 2019. Con este dato es casi seguro asumir que un porcentaje considerable de la población cuenta con al menos un dispositivo o medio informático de comunicación. Este crecimiento masivo ha tenido consecuencias gravosas, pero no siempre perceptibles para el usuario de redes promedio, al facilitar el intercambio malicioso de información, usurpación de identidad, realización de estafas, los ataques a sistemas informáticos tanto públicos como privados, entre otros, configurando el delito informático.

En Guatemala, no existe normativa específica que aborde los delitos informáticos acorde a estándares internacionales; tampoco existe normativa relacionada con la protección de datos personales. Actualmente, desde el año 2015 existe la sección contra delitos informáticos de la Policía Nacional Civil (PNC) la cual fue inaugurada para fortalecer las acciones de prevención, investigación, y atención a las víctimas de delitos informáticos, la cual opera en conjunto con la Unidad Científica de Peritaje Forense del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF). Sin embargo, el Ministerio Público, que es el ente encargado de promover la persecución penal y dirigir la investigación de los delitos de acción pública; aún no cuenta con una unidad de delitos

cibernéticos, la cual deberá ser creada y reforzada para trabajar en conjunto con las demás unidades relacionadas al tema.

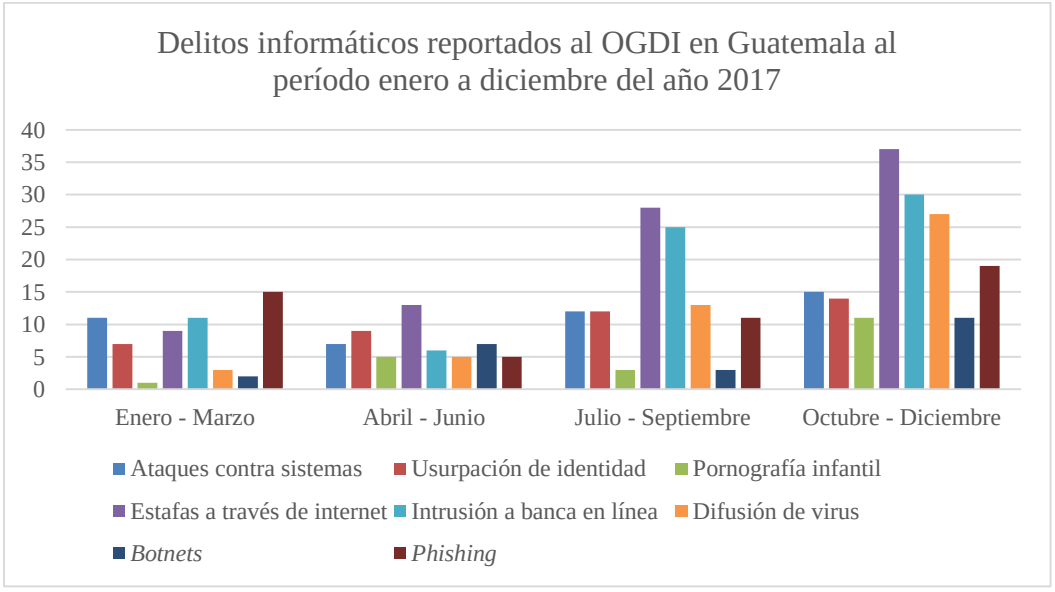
En consecuencia, de lo anterior, no existe un compilado estadístico oficial sobre las cifras reportadas de delito informático en Guatemala. A pesar de esto en agosto del año 2016 nace el Observatorio Guatemalteco de Delitos Informáticos, por sus siglas OGDI, fundado por José R. Leonett, Perito Forense Digital, Gerente de Ciberseguridad en INFO Y MAS Guatemala, y Gerente General de la Red Latinoamericana de Informática Forense, por sus siglas, REDLIF en Guatemala. Generando un aporte al sector empresarial, educativo, universitario y a la población en general, al convertirse en un centro de consulta y estadísticas sobre delitos informáticos en Guatemala, así como un medio para la prevención y educación de la ciudadanía en contra de los delitos informáticos en el país, quien amablemente facilitó los datos despejados en las gráficas a continuación, los cuales fueron tabulados con los datos proporcionados por sección de delitos informáticos de la Policía Nacional Civil.

Estadísticas de delitos informáticos reportados al OGDI y a la Policía Nacional Civil en Guatemala durante el periodo correspondiente de enero a diciembre del año 2016.



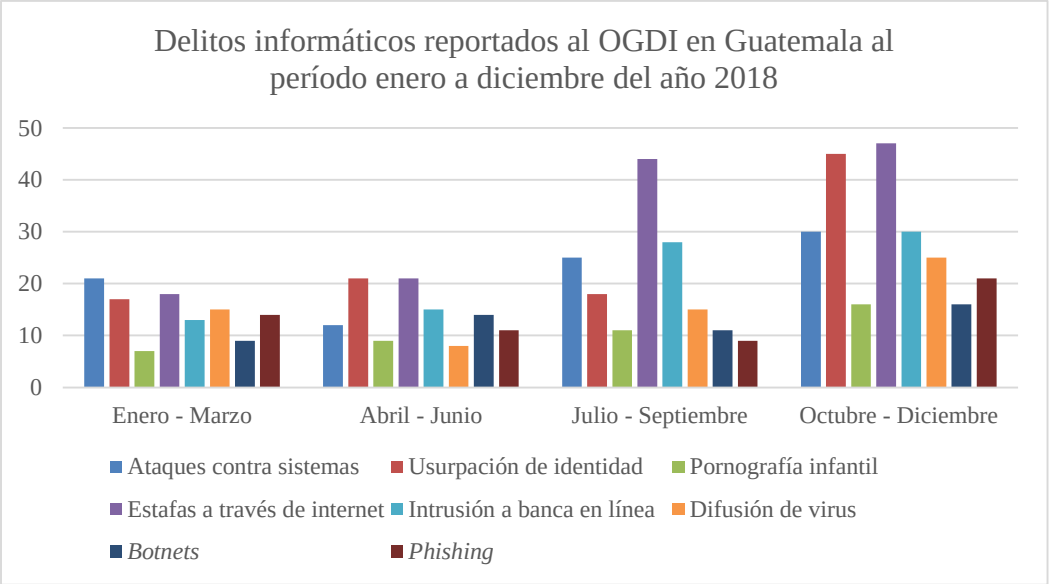
Fuente: Elaboración propia con datos proporcionados por el OGDI y Policía Nacional Civil.

Estadísticas de delitos informáticos reportados al OGDI ya la Policía Nacional Civil en Guatemala durante el periodo correspondiente de enero a diciembre del año 2017.



Fuente: Elaboración propia con datos proporcionados por el OGDI y Policía Nacional Civil

Estadísticas de delitos informáticos reportados al OGDI y a la Policía Nacional Civil en Guatemala durante el periodo correspondiente de enero a diciembre del año 2018.



Fuente: Elaboración propia con datos proporcionados por el OGDI y Policía Nacional Civil

De acuerdo a los datos colectados por el OGDI y la PNC, durante el primer semestre de los años analizados, el número de denuncias presentadas es relativamente constante, manteniéndose a la baja, siendo las estafas a través de internet las instancias que más se reportaron junto con las denuncias de usurpación de identidad.

Sin embargo, en todos los cuadros gráficos, es evidente que el número de denuncias aumenta considerablemente en el segundo semestre del año. En una reunión vía *Skype* con el Ing. José Leonett y la sustentante, en donde

se discutió que la razón por la que se podía acreditar ese aumento era la temporada de pago de bonificación anual para trabajadores del sector público y privado. Dicha bonificación en Guatemala consiste en una remuneración pagadera de forma anual adicional a los sueldos y salarios que generalmente reciben los trabajadores del sector público y privado en el mes de julio de cada año.

La época de pago de la bonificación anual para trabajadores del sector público y privado en Guatemala, desde su sanción en el año 1992 ha representado un alivio financiero a mediados de año que permite a los guatemaltecos que gozan de este beneficio, la adquisición de mercancías, pago de servicios, así como mejorar en términos generales la situación económica y social de quienes lo reciben. Sin embargo, de acuerdo a estadísticas oficiales tanto de la Policía Nacional Civil como del Ministerio Público, es una temporada de alto riesgo para las personas víctimas de estos delitos, puesto que atentan contra la propiedad privada y la integridad de las personas. Los gráficos anteriores demuestran que el delito informático no es la excepción al alza ocasionada por este riesgo temporal, evidenciando que la modalidad de comisión de delitos contra las personas y la propiedad privada ha migrado al medio electrónico.

Un fenómeno similar sucede en el mes de diciembre, cuando se hace efectivo el pago del aguinaldo, con el agravante que en el mes de diciembre existe un alza comercial de hasta el 200% a consecuencia de la temporada navideña. Esto aunado a que el periodo de bonificación navideña coincide con época de vacación escolar, incitando tanto a jóvenes como adultos por igual a hacer uso del internet para satisfacer la necesidad de bienes y artículos a precios más bajos. Los delincuentes han encontrado en las transacciones por internet, una forma de hacer dinero fácil ejecutando estafas.

Según el Ministerio Público, de un análisis de 128 expedientes de estafas cometidas en páginas de internet, se evidenció que las estafas más cometidas son por compra de teléfonos y vehículos. Sin embargo, con el tiempo la gama se ha extendido, siendo estos productos por los cuales se dan más estafas en las páginas electrónicas:

- Teléfonos
- Vehículos
- Consolas de videojuegos
- Electrodomésticos
- Alquiler de inmuebles, casas de playa
- Instrumentos musicales
- Amueblados de sala

Existe preocupación, ya que durante el transcurso del año 2018 se plantearon 1,100 denuncias por delitos de naturaleza informática en el país, con lo cual se supera tres veces más de las que se contabilizaron el año anterior, según el OGDI y datos de la PNC. Entre los hechos más denunciados se encuentran el acoso a personas por parte de grupos criminales, robo de identidad en cuentas de redes sociales y difamación. El Ministerio de Gobernación que tiene a su cargo a la PNC, a través del viceministerio de tecnología, está trabajando fuertemente en impulsar y firmar el convenio de Budapest y así establecer una ley que regule y permita procesar a las personas que cometan delitos informáticos en el país.

El Delito Informático en México

Antecedentes del internet en México

Al igual que en Guatemala, la utilización inicial e implementación de internet tenía como finalidad el facilitar el intercambio de información de carácter académico entre entidades educativas. En aquel entonces era únicamente cuestión de tiempo para que el Estado Mexicano manifestara interés y se uniera al proyecto para su desarrollo. A razón de esto, a inicio de los años 90 fue creado el organismo RED-MEX por sus siglas “Red Mexicana” constituido a su vez por diferentes instituciones académicas

que se dedicaba a discutir políticas, estatutos y procedimientos con el fin de regular el desarrollo de las redes de comunicación electrónica en México. El 20 de enero del año 1992 en la Universidad de Guadalajara y por iniciativa de entidades gubernamentales, así como universidades públicas y privadas, tales como: Universidad de las Américas, Colegio de Postgraduados, Universidad de Guanajuato, Universidad de Veracruz, Instituto de Ecología, Universidad Iberoamericana e Instituto de Mexicali, se crea MEX-net14 el cual se encargaría de decodificar, propiciar y contribuir en el desarrollo de internet en México.

Durante la década entre el año 1983 al año 1993, la red de internet fue de uso privado, el cual incluso podría calificarse como secreto, siendo el uso del mismo reservado para los fines académicos y análisis gubernamental a través de las principales instituciones de educación superior y centros de investigación. En aquel entonces, dichas instituciones eran las únicas que tenían acceso a internet. El 18 de enero del año 1993 el Consejo Nacional de Ciencia y Tecnología, por sus siglas CONACYT, fue la primera institución pública en conseguir un enlace a internet a través del Centro Nacional de Investigación Atmosférica en Estados Unidos, y en este mismo año la Universidad Autónoma Metropolitana y el Instituto Tecnológico Autónomo de México, consiguieron intercambiar información entre dos redes diferentes.

Según datos del Instituto Federal de Telecomunicaciones, en el año de 1994 se logró fusionar las redes de MEX-net y de CONACYT con lo que surgió la Red Tecnológica Nacional que alcanzó un enlace de 2 Mbps y en este mismo año con el surgimiento de la (WWW) iniciaron los usos comerciales de la internet y la creación de los primeros dominios (.mx) y (.edu.mx). Para finales de este mismo año bajo el dominio (.mx) estaban declaradas 44 instituciones académicas, 5 empresas en (.com.mx) y una institución bajo (.gob.mx), y se creó un soporte unificado nacional incorporando varias instituciones educativas y las primeras empresas mexicanas interesadas en internet.

De acuerdo al Centro de Información de Redes en México, por sus siglas NIC – México, en 1995 el número de servidores creció en un 160% desde su inicio en el año 1993, y surgió la segunda etapa de desarrollo de la Internet en México. En octubre del mismo año los dominios bajo (.mx) ascendió a 100 dejando por detrás a los dominios bajo (.edu.mx) con lo que un mes después se anunció la creación del Centro de Información de Redes de México (NIC-México), quien era responsable de administrar y coordinar los recursos de la internet en México.

Actualmente el Instituto de Estudios Superiores de Monterrey, por sus siglas ITESM, y NIC-México son los responsables de asignar y administrar los nombres de los dominios ubicados bajo la designación

(.mx). La Universidad Autónoma de México, por sus siglas UNAM, IPN y el ITESM contribuyen en establecer los fundamentos de una cultura en la red, además de contribuir en la capacitación en el desarrollo de sitios web, y vela por los protocolos de seguridad de computadoras para empresas con el fin de disminuir costos. Además, siete de las principales instituciones educativas del Estado mexicano se han encargado de promover y coordinar una red alternativa denominada INTERNET 2, construida con 202 Universidades en cooperación con las industrias privadas y el gobierno, con fines científicos y tecnológicos en el país donde la UNAM es el centro de operaciones de la red nacional de INTERNET 2 cuya responsabilidad es asegurar la alta disponibilidad de la red y el rápido reconocimiento de fallas y degradación del servicio.

El nivel de secretismo y exclusividad que se manejaba alrededor de esta herramienta impedía que existiera una presión popular que demandara su pronta implementación. En términos generales, una mayoría de la población sabía muy poco o no sabía nada en lo absoluto sobre la existencia de la internet. En un discurso impartido por Jose Angel Curria en el año de 1995, un político y economista mexicano, hizo la declaración sobre la guerra de Chiapas en México siendo una guerra de papel e internet, lo que a su vez provocó el interés masivo de la población sobre lo que era el internet y la web, generando el furor del internet público en México.

Análisis de estadísticas de comisión sobre el delito informático en México entre el año 2016 al año 2018

De acuerdo al censo publicado en el año 2019 por el Instituto Nacional de Estadística y Geografía, por sus siglas INEGI, México tiene alrededor de 126 millones de personas. Es el segundo país con más habitantes de América Latina. Aunado a esto, el uso del internet ha crecido sustancialmente, de acuerdo a datos del Instituto Federal de Telecomunicaciones, desde el año 2013, las líneas de internet móvil crecieron más del 116%, al pasar de 27.4 millones en junio del año 2013 a 76.9 millones en junio del año 2017, mientras que los usuarios de internet residencial registrados ascendían a 65.5 millones de personas, es decir el 59.5% del total de la población.

En México, es esperado que, al ser un país en crecimiento, se tenga consigo unas fallas inocentes respecto al control y gestión de los cibercrímenes en las empresas. Ya sea por desinformación, por no querer gastar en implementación de medidas de seguridad y prevención o por no atenderlo. Los costos generados a consecuencia de la ciberdelincuencia en México ascienden a un estimado de 300 millones de dólares al año, de acuerdo a dato proporcionado por la Fiscalía General de la Justicia de México. De acuerdo a estimaciones realizadas por Nielsen Holdings en un estudio publicado en el año 2016, los principales sectores afectados por

ciberdelincuentes en México durante el año 2015, principalmente fueron el sector privado (25%), el sector educativo (35%) y dependencias de Gobierno (28%).

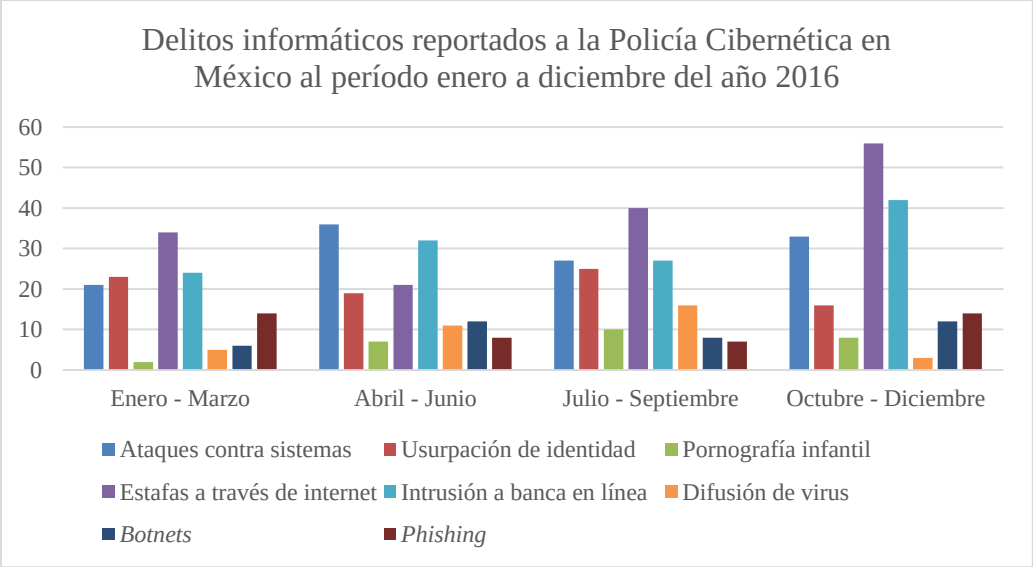
A pesar de lo anterior, México fue de los primeros países en la región latinoamericana en modificar su legislación para que se pudiesen tipificar los delitos perpetrados a través de internet o con la utilización de aparatos de comunicación móvil. El Estado de Sinaloa fue el primero en tipificar el delito informático; y casualmente es el único que lo denomina así.

Establece que comete delito informático, la persona que dolosamente y sin derecho, use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información, así también intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Esta modificación al Código Penal de Sinaloa fue agregada en el año 1992, sin embargo, no fue sino hasta en el año 2005 que el Código Penal Federal fue modificado para incluir las infracciones contempladas en el Código Penal de Sinaloa, y a su vez agregar el marco que permitiría tipificar delitos en materia de pornografía infantil, corrupción de menores, comunicación y correspondencia, revelación de secretos y acceso ilícito a

sistemas y equipos de informática, falsificación de documentos en general, amenazas y revelación de datos personales, así como delitos en contra de las personas en su patrimonio vía electrónica.

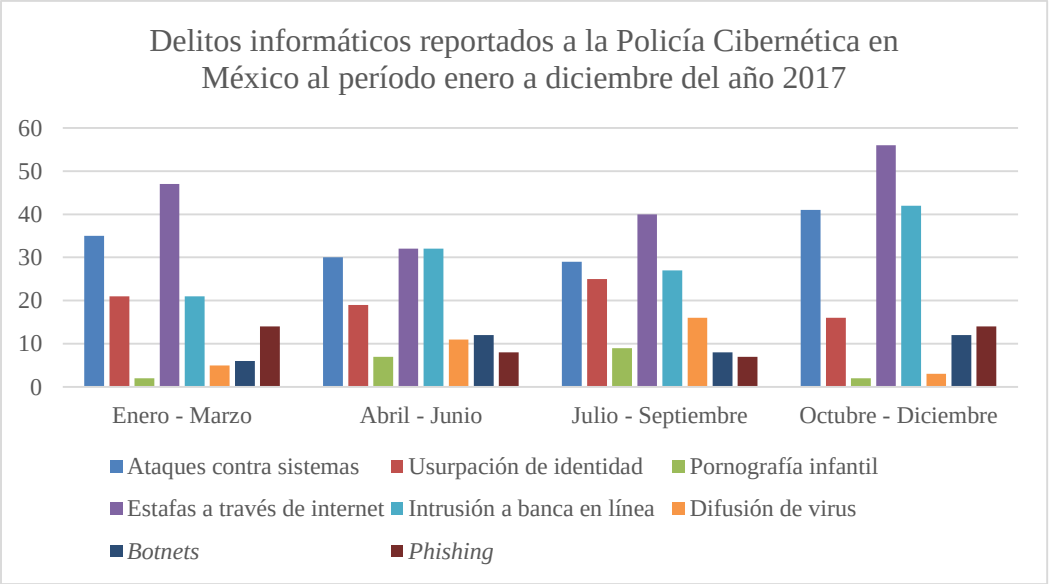
En la actualidad, la entidad encargada de prevenir, monitorear, patrullar y mantener el dato estadístico en términos de delitos informáticos en México, es la Policía Cibernética, formada desde el año 2013 por la Secretaría de Seguridad Ciudadana de México, quienes facilitaron los datos de las gráficas que a continuación se describen.

Estadísticas de delitos informáticos reportados a la Policía Cibernética en México durante el periodo correspondiente de enero a diciembre del año 2016.



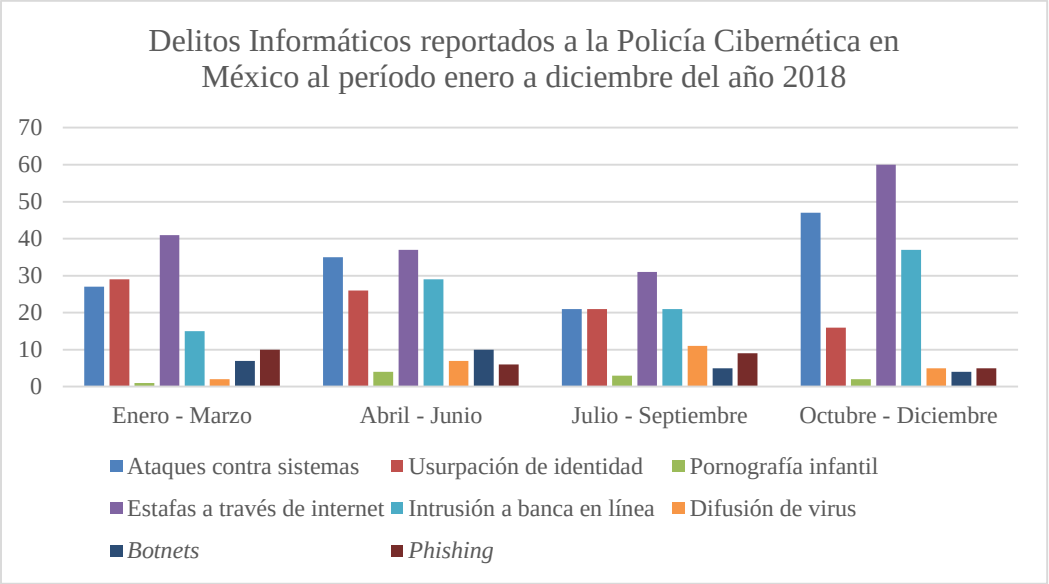
Fuente grafica anterior: Elaboración propia con datos proporcionados por la Policía cibernética de México

Estadísticas de delitos informáticos reportados a la Policía Cibernética en México durante el periodo correspondiente de enero a diciembre del año 2017.



Fuente: Elaboración propia con datos proporcionados por la Policía cibernética de México

Estadísticas de delitos informáticos reportados a la Policía Cibernética en México durante el periodo correspondiente de enero a diciembre del año 2018.



Fuente: Elaboración propia con datos proporcionados por la Policía cibernética de México

A primera vista en términos de cifras reportadas, México cuenta con una mayor cantidad de reportes contabilizados en general, lo cual es resultado de su densidad poblacional. Como se mencionó anteriormente, según datos de INEGI, México es el segundo país más poblado de América Latina con un aproximado de 126 millones de habitantes, de los cuales 79 millones tienen acceso a internet en sus aparatos móviles, y 65 millones de hogares cuentan con servicio de internet residencial.

De acuerdo a las gráficas anteriores, los delitos que encabezan las listas son las estafas a través de internet, la intrusión a banca en línea y los ataques contra sistemas. A diferencia de los datos ilustrados sobre Guatemala, México no tiene un pico tan evidente a partir del segundo semestre del año, y los datos se dispersan a lo largo del año de forma relativamente constante, aunque en una cantidad mucho mayor. Sin embargo, esto no quiere decir que México sea inmune al alza en crimen estacional, ya que, en el último trimestre del año, que cuenta con no menos de tres festividades oficiales que incitan al comercio, a la movilización de personas y al consumo extraordinario de bienes y servicios, siendo estas: el día de muertos, el día de la virgen de Guadalupe, Navidad y año nuevo. En una entrevista vía *Skype* con la agente de la Policía Cibernética Elizabeth Melchor desde la ciudad de México, ella explica que generalmente las festividades de fin de año son tiempos en los cuales los consumidores de bienes y servicios en línea se encuentran particularmente vulnerables, siendo esta la época del año en la que se reciben más reportes. La agente Melchor (2020), explica:

> Con las festividades del último trimestre del año las denuncias se disparan, ya que, en un afán de aprovechar su tiempo de descanso de la mejor forma, o bien buscando artículos de tecnología para entretener a los más pequeños, los usuarios utilizan la internet con el afán de no concurrir a la multitud y obtener lo que buscan de forma rápida. Es de conocimiento público que muchos almacenes y lugares de entretenimiento ofrecen paquetes ofertados o precios promocionales para incentivar el consumo en esa época del año, con lo que los perpetradores de delitos vía informática aprovechan que las personas tienen necesidad y tienen una guardia baja ante sus ataques. Entre lo más común son las estafas al realizar compras por internet, las cuales pueden ser de infinitas formas, entre las más reportadas es

> la venta de artículos y bienes robados por internet, en las cuales se publican fotos genéricas de los artículos, haciéndole creer al comprador que va a obtener un artículo nuevo, cuando en realidad es robado y a veces inutilizable ya que cuenta con reporte de robo, (en el caso de los teléfonos móviles).

Otra modalidad que nos comparte la agente Melchor (2020), que es más refinada, ya que requiere un conocimiento técnico más elevado, consiste en que el perpetrador envía correos con vínculos promocionales que le prometen al comprador que necesita redirigirlo a algún sitio web para acceder a la oferta o bien ingresar datos como correo electrónico entre otros, con los cuales logran accesar a la computadora del usuario sin que este lo note y básicamente espiar todo lo que este hace sin ningún tipo de filtro, con lo que obtiene: usuarios, contraseñas, entre otros datos tipificados como privados que son de extrema utilidad a los malhechores. Lo descrito anteriormente, es una variación del *Phishing* tradicional, en el cual el malhechor busca ganar acceso a computadoras ajenas para pescar información que le sea de utilidad para chantajear al usuario o ingresar sin autorización a su sistema, o bien lo dirige a un sitio que parece legítimo a los ojos del usuario, con la intención de que el usuario ingrese sus credenciales y caiga en la trampa.

Melchor (2020) menciona que es preocupante, ya que, al estar experimentando esta transición al mundo virtual, ella advierte que la prevención es realmente el único medio de protección y defensa, ya que incluso en países con el desarrollo legal y técnico de México, la legislación

existente no es modificada y ajustada con la suficiente rapidez para poder proteger y perseguir y lo más importante condenar a quienes utilicen medios informáticos para sus fines ilícitos.

Asimismo, el director general de la AMIS, Recaredo Arias (2018), manifiesta que en México fueron afectadas por ataques cibernéticos más de 33 millones de personas en el año 2017, una de cada cuatro personas, por lo que es importante estar protegido contra ese tipo de riesgos que van al alza.

En la actualidad, de acuerdo al presupuesto público de Hacienda, el país tiene planeados apenas unos 2.600 millones de pesos (aproximadamente 122 mil dólares) para los servicios de inteligencia de seguridad nacional. Esto podría significar una vulnerabilidad para el país en caso de ser atacado.

Una de las recomendaciones de la Interpol para el gobierno de Andrés Manuel López Obrador es que el país se adhiera al Convenio de Budapest, que trata sobre ciberdelincuencia y al que están integrados varios países sudamericanos como Argentina, Perú y Chile, así como Costa Rica en Centroamérica.

El Delito Informático en Costa Rica

Antecedentes del Internet en Costa Rica

Costa Rica fue el primer país centroamericano en conectarse a Internet. Según el Dr. Ignacio Siles (2008, p.25) La primera iniciativa fue de parte del ex Rector de la Universidad de Costa Rica, por sus siglas UCR, el Dr. Claudio Gutiérrez Carranza, durante su gestión en el año 1974 al año 1981, quien había propuesto la idea de conectar a la universidad a Arpanet, (la predecesora de Internet). Pero en aquel entonces era un proyecto demasiado ambicioso derivado del uso estrictamente militar de Arpanet y en aquel entonces el costo era extremadamente oneroso para la universidad pública, para algo que no tenían realmente claro cuál era su propósito. Está de más decir que no se contó con el aval necesario para llevar a cabo el proyecto.

Luego, llegó al país un grupo de estudiantes, que después de cursar estudios en el exterior se propusieron lograr tal conexión. Uno de ellos, quien lideraría el proyecto de manera exitosa, fue un físico francés-costarricense llamado Guy de Téramond, costarricense a quien suele atribuirse el éxito del proyecto, siendo el mayor impulsador del mismo. De esta forma se reanima la discusión, ahora con el apoyo del ex rector Dr. Gabriel Macaya Trejos (1996-2004), quien ya estaba promoviendo otro proyecto de conexión. De igual manera, durante la gestión del ex

rector Luis Garita Bonilla (1988-1996), se gestaron muchos proyectos relacionados que también dieron impulso al desarrollo de esta herramienta de búsqueda.

Así es como en 1990 la UCR se conecta a la Bitnet, una red creada en el año 1981 en Estados Unidos por la Universidad de Nueva York. Este paso abre aún más las discusiones y la curiosidad por las redes, por lo que solo dos años después ya se estaba en proceso de conexión a Internet. También, el Consejo Superior Universitario Centroamericano crea Huracán: un proyecto fuera de la UCR que permitía una conexión -no directa- a Internet de todos los países centroamericanos. Huracán fue el primer enlace no comercial, estrictamente para comunicación académica que existió de forma abierta en el istmo centroamericano.

Todo estaba listo a finales del año 1992 para realizar tal propósito, sin embargo, el huracán Andrew causó estragos en Estados Unidos y afectó las antenas satelitales receptoras con las que se iba a conectar el país. Una vez resuelto el atraso, el 26 de enero del año 1993 se escuchó en las instalaciones de la UCR: "¡Un paquete, un paquete!", que fue lo primero que gritaron los miembros del equipo de trabajo al recibir un correo; de esta manera Costa Rica se convirtió en el quinto país en Latinoamérica en conectarse a Internet.

Ese mismo año le llega el fin a Bitnet en el país y se establece la CRNet, una asociación sin fines de lucro que buscaba promover la cooperación para una red nacional de conexión a Internet. Así se establece una conexión entre el Instituto Tecnológico Nacional (TEC), la Universidad Estatal a Distancia (UNED) y la Universidad de Costa Rica (UCR), creando la primera red nacional de conexión a Internet.

Análisis de estadísticas de comisión sobre el Delito Informático en Costa Rica entre el año 2016 al año 2018

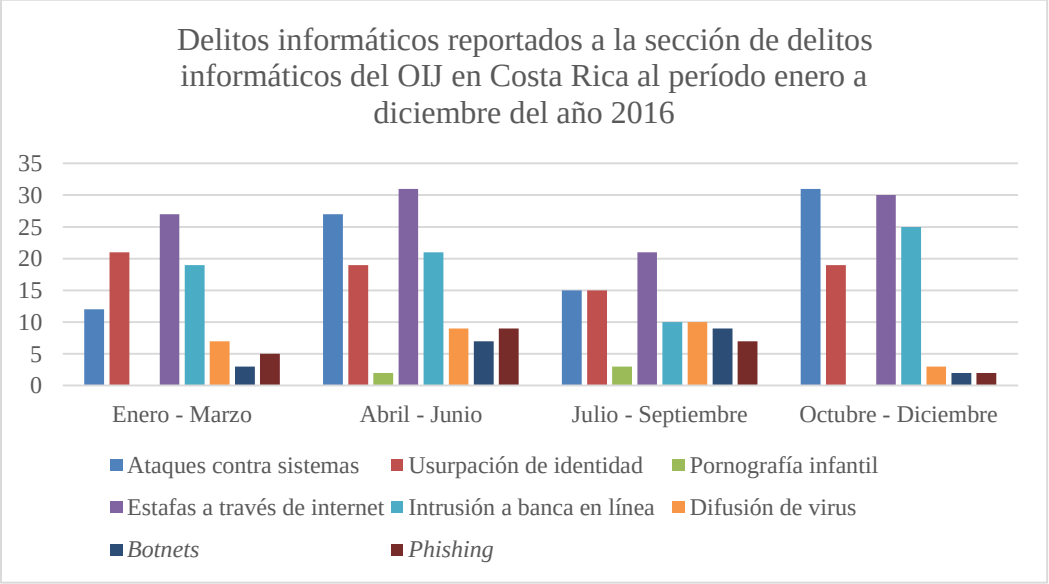
Según datos de la Comisión Económica para América Latina y el Caribe, por sus siglas, CEPAL, entre el año 2010 al año 2015, se registró la etapa con más desarrollo en términos de infraestructura de internet para Costa Rica, aumentando el número de hogares con acceso a internet desde un 24% en el año 2010 a un 60% a finales del año 2015. Registrando con esto el crecimiento más significativo del istmo centroamericano. Esto se debe en parte al programa impulsado por el gobierno costarricense, Hogares Conectados de FONATEL, que subsidia una computadora portátil y conexión a internet a las familias de más escasos recursos; este beneficio al finalizar el año 2017 había beneficiado a un total de 112 mil familias de escasos recursos.

El gobierno costarricense ha tomado como su prioridad el volver accesible el internet para todos, lo cual ha tenido frutos sin precedentes. El acceso a Internet medido por el número de suscriptores creció 440% entre el periodo comprendido entre el año 2010 al año 2015. La modalidad más usada fue la conexión vía teléfono móvil con un crecimiento de 688%. Así la Internet móvil pasó de representar cerca del 60% de las suscripciones en el 2010 a casi 90% en el año 2015, llegando a tener casi cinco millones de suscriptores. Sin olvidar que Costa Rica de acuerdo al último censo publicado en el año 2019, cuenta con casi cinco millones de habitantes. Como dato interesante, se da el mismo fenómeno que en Guatemala, en términos de usuarios de internet móvil, casi sobrepasando el número de conexiones móviles a la cantidad de habitantes. Con lo que se puede afirmar con seguridad, que al año 2020, el número de conexiones móviles registradas superó el 1 per cápita.

Sin embargo, este crecimiento no ha venido sin consecuencias, ya que el otorgar equipo informático a ciudadanos de escasos recursos sin complementar con un programa de capacitación sobre uso y medidas de seguridad, representa un gran riesgo a la población, dejándola vulnerable a ataques y a esquemas de fraude no tradicional para las cuales no están preparados.

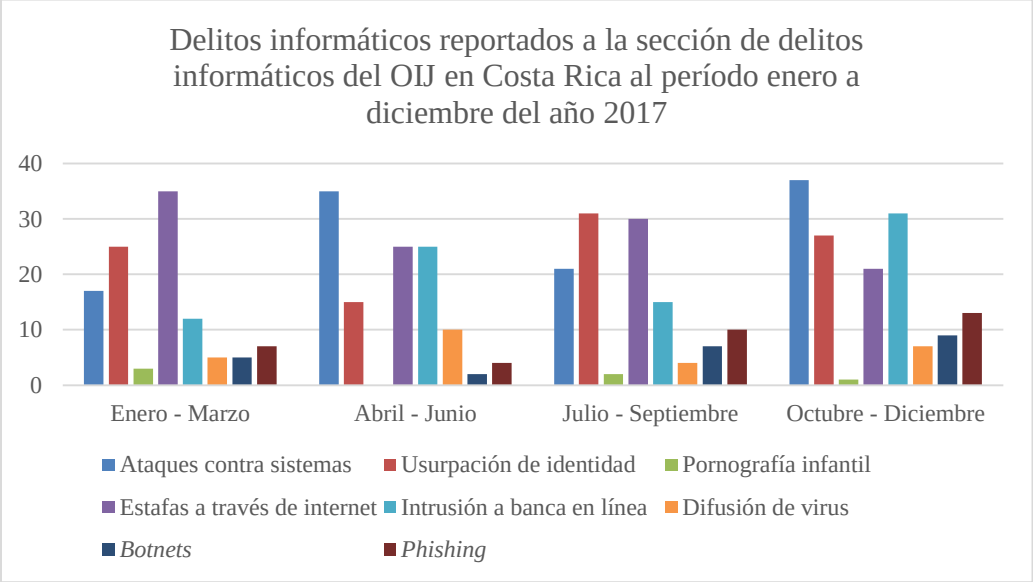
El rango de estudio estadístico de este trabajo es interesante para Costa Rica, ya que se lleva a cabo en una época donde el acceso a internet ya no está limitado a los grupos sociales que pueden costear el servicio mensual, sino que además involucra habitantes de todos los ámbitos sociales.

Estadísticas de delitos informáticos reportados a la sección de delitos informáticos de OIJ en Costa Rica durante el periodo correspondiente de enero a diciembre del año 2016.



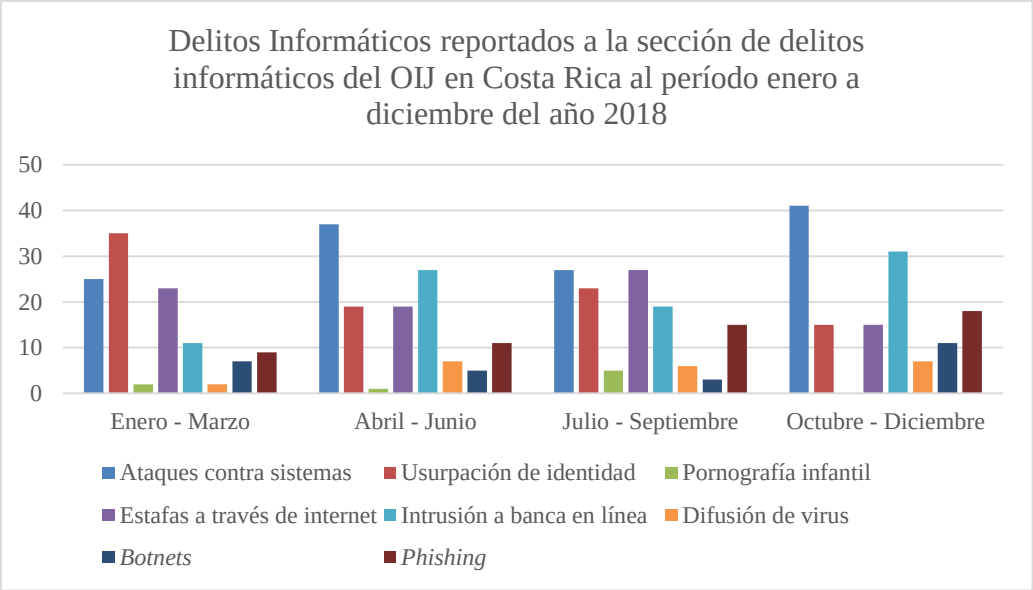
Fuente: Elaboración propia con datos proporcionados por la sección de delitos informáticos de OIJ en Costa Rica

Estadísticas de delitos informáticos reportados a la sección de delitos informáticos de OIJ en Costa Rica durante el periodo correspondiente de enero a diciembre del año 2017.



Fuente: Elaboración propia con datos proporcionados por la sección de delitos informáticos de OIJ en Costa Rica

Estadísticas de delitos informáticos reportados a la sección de delitos informáticos de OIJ en Costa Rica durante el periodo correspondiente de enero a diciembre del año 2018.



Fuente grafica anterior: Elaboración propia con datos proporcionados por la sección de delitos informáticos de OIJ en Costa Rica

Como se puede observar en las gráficas anteriores, se puede decir con certeza que, ha habido cambios en la sociedad costarricense, en términos de acceso y uso de internet, y con esto proporcionalmente ha incrementado la actividad delictiva vía informática.

En Costa Rica, al igual que en México, se puede observar el mismo patrón de comisión del delito informático, dispersado a lo largo del año, sin tener picos en ninguna época en particular. A pesar de cómo en una mayoría de países latinoamericanos, el último trimestre del año es objeto de

festividades y bonificaciones adicionales, y Costa Rica no es la excepción a la regla, a pesar de esto no hay un alza significativa en esas fechas, lo cual a primera vista puede parecer bueno, sin embargo, únicamente quiere decir que el usuario debe mantenerse a la defensiva y alerta en cualquier época del año.

Al realizar un análisis general de los tres principales incidentes: estafas a través de internet, ataques contra sistemas y usurpación de identidad, se puede observar que los tres se encuentran muy relacionados entre sí, siendo éstas tres conductas las más frecuentes y necesarias para ejecutar los fraudes patrimoniales. En comunicación electrónica con la funcionaria de la OIJ Laura Pacheco, ella comunica que la última tendencia de los cibercriminales en Costa Rica ha sido hacerse pasar por entidades y funcionarios de gobierno ya sea vía telefónica o a través de correo electrónico, utilizando software que mimetiza los sitios y números de teléfono de las entidades públicas. Por este medio les comunican a las víctimas que tienen pagos pendientes, o que deben actualizar su información llenando un formulario electrónico, con lo que ganan acceso a medios de pago y otros datos de carácter privado sin sospecharlo la víctima. Los ciudadanos de forma inconsciente no creen que los criminales llegarían a un punto tan serio como hacerse pasar por funcionarios de gobierno, por lo que generalmente no dudan de la

legitimidad de la comunicación, cuando en realidad es fraudulenta en estos casos particulares.

Más allá de las pérdidas financieras que este tipo de fraude pueda ocasionar, la funcionaria Pacheco hace énfasis en que la pérdida de legitimidad y de confianza en los canales de comunicación gubernamentales y el cuestionamiento de parte del pueblo hacia el gobierno central causa un daño incuantificable. Las Secretarías de Comunicación gubernamentales sostienen que los portales ofrecidos a los usuarios para que realicen consultas y efectúen trámites cuentan con todas las medidas de seguridad para protección de los usuarios, pero la confianza ha sido dañada. La funcionaria Pacheco indica que esto le deja una sensación al ciudadano de que no puede confiar en absolutamente nadie, y cuestionan si acudir a demandar justicia realmente servirá de algo, ya que no consideran que el gobierno esté cuidando de ellos.

Ante el alza evidente de delitos de esta naturaleza en Costa Rica, el gobierno costarricense a través del Organismo de Investigación Judicial, han estado gestionando boletines oficiales y capacitaciones en línea para dar a conocer a la población en general las medidas de seguridad recomendadas ante la transición inminente del comercio y transacciones gubernamentales al medio informático, así como ilustrar los modos

conocidos de estafa o bien medios por los que se puede ser vulnerable en línea.

Comparación jurídica de legislaciones e iniciativas que contengan el Delito Informático entre Guatemala, México y Costa Rica

Guatemala: Iniciativa de ley 5601 Ley de Prevención y Protección contra la Ciberdelincuencia

Como se ha mencionado anteriormente en este estudio, Guatemala es de los pocos países en la región latinoamericana que no cuenta con una legislación específica que regule el delito informático, a fin de que el mismo pueda tipificarse propiamente como delito y como tal pueda ser perseguido penalmente para ser posteriormente sometido al debido proceso como la ley establece.

Hasta la fecha se han presentado tres iniciativas de ley que contemplan el delito informático: en el año 2017 la iniciativa 5254 Ley de Ciberdelincuencia, en el año 2018 la iniciativa 5339 Ley Contra Actos Terroristas y en el año 2019 la iniciativa 5601 Ley de Prevención y Protección contra la Ciberdelincuencia. Dichas iniciativas han sido promovidas a instancia de una minoría en el pleno del Congreso de la

República de Guatemala, y lastimosamente solo reciben atención momentánea, ya que a pesar de que una mayoría de congresistas reconocen los riesgos que existen en el ciberespacio, con el tiempo cualquier inquietud al respecto se desvanece a consecuencia de atender otros temas que se consideran de mayor prioridad o que benefician a mayor escala el bien común, por lo que cualquier proyecto al respecto termina engavetado.

La presentación de la última iniciativa de ley con el propósito de combatir la ciberdelincuencia fue anunciada por el diputado José Rodrigo Valladares (2019), quien informó que esta nueva propuesta sustituye a la iniciativa 5254, que presentó con anterioridad con el mismo propósito.

Valladares (2019), argumentó que el proyecto de ley mencionado, fortalecerá el combate a este tipo de actos criminales que se cometen en el ciberespacio, y en su momento fue objeto de análisis en las mesas de trabajo que se instalaron y en las que participaron representantes de diversos sectores involucrados en el tema, entre otros, el Viceministro de Tecnología de la Información y las Comunicaciones, del Ministerio de Gobernación, Gabriel Juárez Lucas y representantes del Consejo Nacional de Seguridad.

Este tipo de legislación es necesaria para el combate a la ciberdelincuencia, actualmente se han suscitado casos relacionados al tema y se les ha dado el tratamiento debido, sin embargo, una ley que combata este tipo de delitos es una herramienta sumamente necesaria, indicó Juárez Lucas.

Delitos como acoso por internet, el *ciberbullying*, la usurpación de identidad en redes sociales, la pornografía infantil, ataques a redes de información, entre otros, serían sancionados de forma más severa con la propuesta, y en palabras del Viceministro Juárez Lucas (2019): "Es necesario abordar diversas problemáticas que se dan en el ciberespacio, estamos elaborando una propuesta lo suficientemente completa para poder contribuir al combate de este tipo de delitos".

El legislador anunció que, en su momento, se sostendrá una reunión con jueces y magistrados con el propósito de establecer las penas y sanciones legales para quienes cometan este tipo de delitos e integrarlos a la propuesta.

Iniciativa 5601: Sobre el Delito Informático

El Estado de Guatemala debe garantizar a los habitantes de la república la libertad, la justicia y el desarrollo integral de la persona entre otros deberes, ello exige que el Estado debe dar garantías para promover la

confianza del usuario de internet en los servicios en línea, el comercio y el gobierno electrónico, imponiendo penas a la Ciberdelincuencia, pero respetando el derecho a la privacidad, el derecho a la libertad de expresión en Internet, el derecho al secreto de las comunicaciones y el derecho a la libertad informática.

En la iniciativa 5601 se establece como objeto de ley, los bienes jurídicos tutelados constitucionalmente. Su objeto abarca todos los delitos que contempla el Código Penal que sean cometidos utilizando como medio los sistemas informáticos o sistemas que empleen TICs; comprende además el ámbito territorial y personal de aplicación de la ley, y para los efectos de la extensión y alcances de los ámbitos espaciales de aplicación, se reconoce el ciberespacio como un medio para la comisión de los delitos tipificados en la iniciativa de ley.

La tipificación actual de los delitos informáticos contenidos en el Código Penal, no responde a las modalidades de los ilícitos que se cometen a través de redes o sistemas informáticos, muchos de ellos ya reconocidos en la legislación internacional como por ejemplo la interceptación ilícita, el abuso de los dispositivos, el fraude o estafa informática e incluso la pornografía infantil, por la utilización de medios informáticos para su comisión.

Los delitos que se incorporarían a la legislación penal guatemalteca de acuerdo a la iniciativa 5601 son: acceso ilícito, interceptación ilícita, ataque a la integridad de los datos, ataque a la integridad del sistema. También regula delitos considerados dentro de los delitos propiamente denominados informáticos siendo éstos: falsificación informática, apropiación de identidad ajena; abuso de dispositivos, fraude informático. También se incorpora el delito de acoso cibernético y engaño pederasta.

Iniciativa de ley 5601: Ciberdelitos contra las personas

Entre los delitos que contempla la iniciativa 5601, y en el ámbito del Delito Informático en general, se puede hacer una diferenciación clara, entre los delitos informáticos cuyo fin es la obtención ilegal de riqueza a través de la intercepción o acceso ilícito a sistemas informáticos, los cuales podrían denominarse delitos informáticos contra el patrimonio, y los delitos informáticos que atacan a las personas directamente sin ninguna retribución dineraria en específico, beneficiándose del anonimato relativo que proporciona el internet. Entre estos se encuentran: *Cyberbullying*, *grooming*, pornografía infantil, usurpación de identidad, entre otros que ataquen directamente a la persona y su dignidad, con la finalidad de causar daño emocional y manipular a las personas. Estos pueden denominarse delitos informáticos contra las personas.

En la iniciativa 5601, la usurpación de identidad, está contemplada en el capítulo II, artículo 14, estableciendo lo siguiente:

> Artículo 14. Apropiación de Identidad ajena. Comete el delito de apropiación de identidad ajena, quien de forma deliberada, sin autoridad o excediendo la que posea, sin permiso o consentimiento legalmente reconocido, y con fin ilícito obtenga, usurpe, falsifique, suplante o adopte la identidad de otra persona, a través de un sistema informático o sistema que haga uso de tecnologías de la información y las comunicaciones, siempre y cuando cause un resultado; y se le impondrá pena de prisión de dos a cuatro años y multa de cuarenta a cien salarios mínimos mensuales vigentes para actividades no agrícolas. Cuando la comisión de este delito, se realice infringiendo medidas de seguridad, se sancionará con pena de prisión de tres a cinco años y multa de cuarenta a doscientos salarios mínimos para actividades no agrícolas.

Con el crecimiento del comercio electrónico y el uso de los servicios de banca por Internet han aumentado en forma alarmante los fraudes electrónicos, especialmente el robo de identidad. Esta nueva modalidad de fraude, comúnmente se refiere a toda aquella información de un individuo como el nombre, fecha de nacimiento, dirección, número Documento Personal de Identificación, de tarjeta de crédito y de cuentas bancarias, nombre de usuario y contraseña de sitios web donde se encuentra inscrita la víctima, que es obtenida y utilizada sin su consentimiento, y con el propósito de cometer actividades fraudulentas, las cuales pueden ser de carácter patrimonial o personal.

Cabe mencionar que, de los delitos informáticos contra las personas, los que son de carácter personal, tienen como víctimas en una gran mayoría a los menores de edad. Esto se debe a que generalmente los menores de edad

carecen de patrimonio personal propio o bien recursos que puedan ser de interés para los criminales. No por esto deja de ser importante, ya que las secuelas de este tipo de delitos, puede tener consecuencias graves como lo es el trauma psicológico a largo plazo, y otras secuelas de carácter emocional que no pueden cuantificarse pero que pueden afectar a lo largo de toda la vida de la víctima.

Los menores de edad, en su carácter de vulnerabilidad, se vuelven objetivo de una demográfica particularmente peligrosa, como lo son los criminales que atentan contra la integridad sexual de los menores, los abusadores en línea (*cyberbullying*), los pederastas (*grooming*), los pedófilos, entre otros. La iniciativa 5601 reconoce este riesgo inminente, por lo que dedica enteramente el capítulo III de su contenido, a los delitos informáticos contra las personas y hace énfasis particular en aquellos delitos relacionados a niños/niñas y adolescentes, quedando de la siguiente forma:

> Ciberdelitos contra las personas y delito contra la integridad sexual de niño, niña o adolescente
>
> **Artículo 18.** Delitos relacionados con abuso infantil. Cuando los delitos sobre explotación sexual en que las víctimas sean niños, niñas y adolescentes, tipificados en el Decreto Número 17-73 del Congreso de la República, Código Penal y en el Decreto Número 09-2009 del Congreso de la República de Guatemala, Ley Contra la Violencia Sexual, Explotación y Trata de Personas y Ley de Protección Integral de la Niñez y Adolescencia; se cometan a través del empleo de sistemas informáticos o cualquier medio de comunicación electrónica, se sancionarán con las penas establecidas en las respectivas leyes para estos ilícitos aumentada en una cuarta parte.

Como se puede observar en el artículo anterior, el hecho de que se haya contemplado un aumento en las penas establecidas para los delitos contenidos en las normativas que comprenden a los niños y adolescentes, implica que el objetivo de la creación de la norma es causar un efecto disuasivo, tipificando la conducta antijurídica configurada en el Delito Informático teniendo como sujetos pasivos a los menores de edad, específicamente en los delitos de carácter sexual y aquellos que atenten contra la integridad personal, como particularmente gravosa.

En los últimos años, conforme las interacciones sociales y comunicaciones cotidianas han migrado de ser ejecutadas tradicionalmente de forma física, a ser llevadas a cabo a través de internet, con ello han migrado también los fenómenos sociales que estas implican, como lo es el acoso, entre muchos otros. En la iniciativa de ley 5601, se desarrolla de forma extensa, ya que a pesar de que no afecta la integridad humana directamente, las secuelas del acoso pueden llegar a ser perceptibles dañando la salud mental de quien lo padece a lo largo de su vida. El acoso está definido en la iniciativa 5601 de la siguiente forma:

> **Artículo 19.** Acoso por medios cibernéticos o ciberacoso. Comete delito de acoso por medios cibernéticos, la persona individual, grupo o grupo de delincuencia organizada, que públicamente, en el ámbito, escolar, laboral u otro ámbito determinado, y en cualquiera de las formas de autoría establecidas en el Código Penal.

Entre las formas que contempla, se encuentran la intimidación a través de cualquier medio electrónico o digital, divulgación de contenido confidencial o sexual a través de cualquier medio electrónico y los casos de acoso cibernético perpetrados por niños y adolescentes en el ámbito escolar, también denominado *bullying.*

Como se ha mencionado anteriormente, los niños y adolescentes son específicamente vulnerables a los ataques de índole sexual, perpetrados por adultos que buscan aprovecharse de su falta de conocimiento y juicio. Esto aunado a que es particularmente difícil de identificar en sus etapas preliminares, ya que el engaño pederasta radica generalmente en la infiltración en el ámbito cibernético infantil, que incluso para las mismas victimas puede considerarse como "seguro". El articulo a continuación lo detalla:

> **Artículo 20.** Engaño pederasta. Comete el delito de engaño pederasta, la persona mayor de edad que contacte a un niño, niña o adolescente por medio de las tecnologías de la información y las comunicaciones y relacionadas; valiéndose o no del anonimato, con el objetivo de ganarse su confianza en forma progresiva, por cualquier método, para proponerle concertar un encuentro en un lugar físico o incluso que no requieran de un contacto corporal entre el sujeto activo y la víctima para cometer cualquier delito que atente contra la sexualidad del niño, niña o adolescente.
>
> En el caso de ser cometido por adolescente, se remitirá al juez competente con el requerimiento de que se dicte la resolución correspondiente de conformidad con la Ley de Protección Integral de la Niñez y Adolescencia, prevaleciendo el interés superior del niño.

Es de suma importancia que se haya hecho énfasis en la población vulnerable en la iniciativa 5601, ya que según una publicación de Save the Children en 2019, un niño agredido sexualmente por un adulto queda marcado de por vida, se tiene que trabajar mucho con él o con ella para poder asumir lo pasado y afrontar el trauma que, aunque en ocasiones ni siquiera lo sepan, ahí está. Se calcula que entre el 10% y el 20% de los adultos sufrieron algún tipo de abuso sexual durante la infancia. Son cifras realmente preocupantes y que, con la amplia disponibilidad de la internet, incrementan las posibilidades y el riesgo para los niños como adolescentes.

Iniciativa de ley 5601: Responsabilidad y Penas Accesorias de las Personas Individuales y Jurídicas

La finalidad de las penas accesorias y los grados de responsabilidad en el contexto de esta ley, es que en los delitos de mayor impacto o bien aquellos que tengan una naturaleza gravosa de acuerdo al daño causado, se añada a la pena principal distada por el tribunal, una medida accesoria que busca resarcir el daño causado a la víctima o bien proteger a esta y a otras potenciales víctimas de su agresor al cumplir este su sentencia. Estas penas accesorias suelen ser penas privativas de derechos o prohibiciones, acompañan a penas privativas de libertad y pueden ser adoptadas por el tribunal de sentencia atendiendo a la naturaleza del delito. Habiendo hecho

esta aclaración, el capítulo IV de la iniciativa 5601 lo define de la siguiente forma:

> **Artículo 22.** Responsabilidad Civil y Penas Accesorias de las Personas Individuales. las sanciones penales estipuladas en la presente ley para las diferentes figuras tipo normadas, se aplicarán sin perjuicio de las responsabilidades civiles correspondientes y los daños y perjuicios que se pudieran generar por la comisión de los actos propios de los respectivos delitos.
>
> Asimismo, aunado a las penas de prisión y multa señaladas, el órgano jurisdiccional competente dependiendo del caso concreto podrá́ disponer el comiso de los objetos instrumentos del delito.
>
> Asimismo, se considerará responsable civilmente a una persona jurídica cuando la falta de vigilancia o de control de su representante legal o empleado haya hecho posible la comisión de un acto ilícito previsto en la presente ley.

Es importante notar que, en términos de responsabilidad civil, cuando el delito informático es perpetrado por un menor de edad, la responsabilidad civil recae sobre su representante legal.

Estado actual de la normativa en Guatemala

Después de tres intentos aún no se ha logrado aprobar una iniciativa de ley que garantice la seguridad cibernética en el país. La ciberdelincuencia es un tema que ha adquirido importancia gubernamental a lo largo de los años; sin embargo, no se ha llegado a un acuerdo para consensuar la creación de una ley. El problema es que sin una legislación sobre la delincuencia cibernética se vuelve complicado el procesamiento de los casos.

Muchos expertos han expresado la necesidad y la importancia de que Guatemala se apegue y se suscriba al Convenio de Budapest contra el cibercrimen, al cual pertenecen más de 60 países. Sin embargo, la seguridad informática, en un país como Guatemala, aun presenta muchos obstáculos. Generalmente se piensa que teniendo un antivirus o instalando licencias es más seguro navegar en Internet, pero los incidentes informáticos han ido evolucionando junto con el resto de la tecnología, por lo tanto, los métodos convencionales ya no logran proteger del todo.

Para poder atacar esta problemática es necesario crear una cultura respecto a la ciberseguridad por medio de la concientización de la gravedad de la ciberdelincuencia y la transformación digital. La mejor manera de afrontar el conflicto es adaptando el sistema a los cambios, reinventando estrategias y capacitando al Estado para el cumplimiento de una ley que es urgente aprobar.

México: Código Penal Federal, título noveno

México en la actualidad tiene un problema grave en materia de ciberseguridad. A pesar de haber sido de los primeros países de la región en modificar su legislación federal a fin de sentar un precedente regional y proteger a sus ciudadanos en el año 1999. Sin embargo, a pesar de esto, es el país más afectado de la región latinoamericana. El estudio

denominado “Reporte sobre defensa contra ciberamenazas 2020” realizado por el Grupo Cyber Edge, posicionó a México como el país donde las organizaciones sufren la mayor cantidad de ataques exitosos del mundo.

De acuerdo con el informe, en México el 93.9% de los ciberataques es exitoso. Esto lo posiciona por encima de potencias como China (83.3%), Estados Unidos (82.6%) y Francia (81.1%). Además, México está segundo entre las naciones con el porcentaje más alto por afectaciones de *ransomware* (un programa que bloquea el acceso al sistema operativo a cambio de un rescate, usualmente económico, a cambio de liberarlo), apenas por debajo de China.

El verdadero reto que presenta el delito informático es la velocidad con la que puede evolucionar y transformarse, la cual no puede compararse con el proceso engorroso y burocrático que conlleva crear y aprobar reformas o proyectos de ley actualizados, y es precisamente eso lo que adolece el Estado de México en el momento. Su legislación no está a la altura de los requerimientos para una tipificación y persecución propia, lo cual la lleva a fallar en su objetivo de prevención de ejecución del delito informático y protección ciudadana. El incorporar el delito informático a su normativa de forma temprana fue una excelente iniciativa, pero que requiere un alto mantenimiento del cual depende su eficacia para su propia aplicación.

Toda la normativa matriz relacionada al delito informático en México, se encuentra en el Código Penal Federal, en el título noveno. Atendiendo cómo funcionan las normativas federales, la contenida en la normativa federal de una materia específica es la que se usa como matriz o base para las normativas estatales.

México: Código Penal Federal: de los delitos informáticos

Curiosamente, el Código Penal Federal carece de una definición propia de lo que constituye un delito informático en si, por lo que se tomará la definición del Código Penal del Estado de Sinaloa en su artículo 217, que establece lo siguiente:

> Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Una definición más simple podría ser: que el Delito Informático es el uso de cualquier sistema informático como medio o fin de un delito. De esta manera se abarcan todas las modalidades delictivas de acuerdo al marco legal de cada país; para esto es conveniente definir qué es un sistema informático.

En general en la legislación federal mexicana, en el título noveno, en su totalidad se omiten los delitos informáticos contra las personas. El Estado mexicano se ha enfocado en tipificar los delitos informáticos de tipo patrimonial y se ha centrado en el acceso ilícito a sistemas y equipos de informática con el afán de sustraer información valiosa de tipo financiero, protegida bajo secretos industriales, gubernamental, etc. El único artículo que contempla el Delito Informático de tipo personal, es el siguiente:

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

En el ordenamiento jurídico mexicano, en el entorno informático, en líneas generales hay dos tipos de delitos de este tipo: aquellos que tienen como finalidad destruir, alterar, modificar o extraer información de manera no autorizada de los sistemas informáticos; y los delitos del orden común que se cometen a través de nuevas tecnologías. La escasa regulación de los delitos de carácter personal, como víctima del Delito Informático al menos de forma específica, es verdaderamente preocupante, considerando que México tiene las cifras más altas de la región en Delitos Informáticos. Cabe mencionar que en México existe el material sustantivo para determinar que estas conductas son punibles. Del año 2000 a la fecha, ha habido reformas legislativas a nivel del Código Penal Federal, como los artículos 210, 211, 211 bis y subsecuentes que incorporaron por primera

vez tipos penales que hablan de sistemas de cómputo. Desde el año 2008 se han incorporado en los códigos penales de diferentes Estados (como Querétaro, Yucatán, Chihuahua y Baja California, entre otros) ilícitos que son considerados delitos informáticos.

Existe una genuina área de oportunidad a nivel de legislación federal, ya que hasta ahora se ha hecho de manera aislada y por entidad federativa, lo cual vuelve la normativa a nivel nacional inconsistente y con muchos vacíos legales los cuales son aprovechados por los cibercriminales.

Se han tomado los primeros pasos en torno a la protección del individuo en materia del ciberespacio, habiendo reconocido como campo del delito informático la violencia digital, que puede comenzar con la difusión sin consentimiento de imágenes, videos o audios personales. El 3 de diciembre del año 2019 se aprobó en el Congreso de la Ciudad de México la llamada “Ley Olimpia”, un conjunto de reformas a códigos penales de las entidades federativas, así como a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia.

Estas reformas reconocen la violencia digital como un tipo de delito que consiste en actos de acoso, hostigamiento, amenazas, vulneración de datos e información privada, así como la difusión de contenido sexual (ya sean

fotos, videos o audios), sin el consentimiento o mediante engaños a una persona.

En marzo del año 2020, la Ley Olimpia ya estaba vigente en 16 estados de la República Mexicana: Puebla, Yucatán, Ciudad de México, Oaxaca, Nuevo León, Querétaro, Baja California Sur, Aguascalientes, Estado de México, Guerrero, Coahuila, Chiapas, Zacatecas, Veracruz, Guanajuato y Tlaxcala. A la fecha, ya se presentó la iniciativa en el Congreso de la Unión para que esta ley tenga aplicación en todo el territorio mexicano.

Costa Rica: Ley 8148: Legislación sobre delitos informáticos

Costa Rica fue el segundo país de la región, después de México, en formalmente adoptar medidas para regular el Delito Informático, modificando su legislación y a su vez abrió la Unidad de Delitos Informáticos del Organismo de Investigación Judicial en el año 1996, a partir de la cual y hasta el año 2001, habían recibido alrededor de 300 casos, un promedio de 60 ilícitos cada año.

La legislación costarricense relativa al Delito Informático es relativamente corta, ya que consta de únicamente 3 artículos que fueron modificados de su forma original para abarcar las nuevas formas de comisión de delitos utilizando las tecnologías de la información (TIC), los cuales se ven a continuación:

Adición de los artículos 196 BIS, 217 BIS Y 229 BIS al Código Penal Ley número 4573, para reprimir y sancionar los delitos informáticos.

Artículo único. -Adiciónese al Código Penal, Ley No 4573, del 4 de mayo de 1970, los artículos 196 bis, 217 bis y 229 bis, cuyos textos dirán:

> **Artículo 196 bis.** -Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.
>
> **Artículo 217 bis. -**Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.
>
> **Artículo 229 bis.** -Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

Al igual que en la legislación mexicana, el ordenamiento jurídico costarricense carece de lineamientos a seguir en materia de delitos informáticos de carácter personal, ya que, en su legislación existente, el énfasis está bastante concentrado en los delitos de carácter patrimonial,

dejando a un gran porcentaje de las víctimas sin resguardo al no poder tipificarse las acciones ilícitas de las cuales sufren en el mundo en línea. De igual forma, al día de hoy, los artículos destinados a la regulación del Delito Informático, fueron sancionados para su aplicación hace ya 19 años, lo cual los pone en riesgo de quedarse rezagados ante el dinamismo del Delito Informático.

Si bien es cierto en Costa Rica desde el año 1997 existe la policía cibernética, la cual tiene como finalidad realizar todas las investigaciones en las cuales la informática es utilizada para cometer actos delictivos, la regulación existente para procesar delitos informáticos es de un carácter tan limitado, que a pesar de que se reciban múltiples denuncias sobre delitos de materia informática, pocas veces pueden tipificarse como tales ya que la regulación existente no resguarda a la mayoría de afectados.

La legislación costarricense ya incluye en varias de sus leyes el concepto de documento electrónico, también ha tipificado el Delito Informático para tres casos exclusivos: violación de comunicación, fraude y sabotaje informático. Sin embargo, existen otros tipos de delitos informáticos que de alguna manera ya se contemplan en la legislación costarricense pero que por la forma en que se dan quedan impunes al no poderse tipificar o no poder recabar medios de prueba necesarios al ser estos en línea como, por ejemplo, acoso y pornografía infantil.

Es de carácter imperativo la ampliación del marco jurídico costarricense para ajustar su normativa relativa a delitos informáticos para incluir aquellos de carácter personal, que a consecuencia de la minoría de edad de la demográfica que los sufre en su mayoría, se encuentran en una posición muy vulnerable al no estar legalmente amparados.

Conclusiones

Se establece que el delito informático se configura al utilizar cualquier sistema informático como medio o fin para llevar a cabo a través de conductas tipificadas como antijurídicas. Sin embargo, derivado de la complejidad de sus elementos e indefinido alcance que le proporciona el internet, se debe legislar atendiendo a los aspectos tanto técnicos como sociales que componen el delito, a fin de crear una legislación funcional que permita actuar a los entes perseguidores de justicia de forma eficaz y evitar la creciente impunidad que acarrean estos hechos.

Se determinó que las épocas festivas y los estímulos económicos son períodos en los que se contabilizó un alza considerable en los reportes de delitos informáticos, pudiendo definirse dichos periodos como épocas vulnerables para los usuarios de internet, sin embargo, la existencia de una normativa específica que regule lo relativo a los delitos informáticos, no es un factor disuasivo para la comisión de los mismos, ya que de acuerdo con los datos recolectados de México y Costa Rica, en comparación con los datos recopilados de Guatemala entre los años 2016 al 2018, las cifras reportadas son proporcionales a la cantidad de usuarios de internet, sin que los países con normativas aprobadas demuestren una baja significativa de delitos informáticos reportados.

En la comparación de legislaciones, se determinó que en América Latina: México y Costa Rica son los únicos países que tienen normativa vigente que regule lo relativo al delito informático. Sin embargo, en sus normativas, ambos se enfocan en los delitos informáticos de carácter patrimonial, sin hacer mención de los delitos informáticos enfocados a las personas, lo cual es preocupante dado el auge de las redes sociales de uso personal en los últimos años. No obstante, en México a la fecha de marzo 2020, se ha implementado la Ley Olimpia en 16 Estados del territorio mexicano, la cual fue promovida e impulsada por un miembro de la sociedad civil, que fue víctima de acoso cibernético.

Se concluyó, que en Guatemala no existe una ley ordinaria que sancione drásticamente el delito informático, solamente se cuenta con una iniciativa de ley 5601 de Guatemala, y a pesar de que aún no se encuentre aprobada, esta apunta a ser una de las legislaciones más completas en comparación con las leyes que se analizaron en los países que fueron objeto de estudio, ya que, esta contempla los delitos informáticos en su carácter patrimonial y personal.

Referencias

Libros

Alvarado, R. (2013). *Cibercrimen*. Guatemala: Ius

Barrio, R. (2007). *Derecho e Informática: Aspectos Fundamentales*. (4ª ed.). Guatemala: Mayte

Barriuso, C. (1996). *Interacción del Derecho y la informática*, Madrid: Dykinson.

Campioli, A. (2004). *Derecho Penal Informático en México*. Mexico: Inacipe.

Correa, M. (1990). *El Derecho Informático en América Latina*. Bogotá: Temis

Hance, O. (1996). *Leyes y Negocios por internet.* México: McGraw Hill.

Leon, M. (2011) *Diccionario de Informática y Telecomunicaciones*. Inglés-Español. España: Ariel

Martínez, E. (2012). *Apuntes de Derecho Informático.* Guatemala: Mayte.

Montaño, A. (2008) *La Problemática Jurídica en la regulación de los Delitos Informáticos*. Universidad Nacional Autónoma de México. México: Facultad de Derecho.

Osorio, M. (2011). *Diccionario de Ciencias Jurídicas, Políticas y Sociales*. 37ª edición
actualizada. Guatemala: Heliasta

Téllez Valdez. (2003). *Derecho Informático*. (3ra ed.). México: McGraw Hill.

Tesis

Bouscayrol Valladares, K. (2014). *Iniciativa de ley 4054, Ley contra el cibercrimen y el problema de regular los delitos informáticos en Guatemala*. (Tesis de licenciatura) Universidad Francisco Marroquín, Guatemala.

Martinez Estrada, A. (1995). *Internet en Guatemala, Pasado, Presente y Futuro*. (Tesis de licenciatura) Universidad Francisco Marroquín, Guatemala.

Sierra López, Y. (2011). *Inclusión de los Delitos Informáticos, que se cometen en Internet, dentro del Código Penal Guatemalteco*. (tesis de licenciatura). Universidad de San Carlos. Guatemala.

Legislación

Nacional

Asamblea Nacional Constituyente. (1985). *Constitución Política de la República de Guatemala*. Publicada el 31 de mayo del año 1985. Guatemala.

Congreso de la República de Guatemala. (1973). *Decreto número 17-73. Código Penal.* Publicado en Diario de Centroamérica, No 4561, del 17 de julio de 1973. Guatemala.

Congreso de la República de Guatemala. (2009). *Iniciativa de ley número 4055: Ley de Delitos Informáticos*. Presentada al pleno del Congreso de la República de Guatemala el 18 de agosto del año 2009. Guatemala.

Congreso de la República de Guatemala. (2017). *Iniciativa de ley número 5254: Ley contra la Ciberdelincuencia*. Presentada al pleno del Congreso de la República de Guatemala el 7 de marzo del año 2017. Guatemala.

Congreso de la República de Guatemala. (2019). *Iniciativa de ley número 5601: Ley de Prevención y Protección contra la ciberdelincuencia*. Presentada al pleno del Congreso de la Republica de Guatemala el 17 de septiembre del año 2019. Guatemala.

Internacional

México

Gobierno Federal. (1931). *Código Penal Federal*. Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, México.

Costa Rica

Asamblea de la República de Costa Rica. (2000) *Ley número 8148: Ley de Delitos Informáticos*. Publicada el 24 de octubre del 2000. Costa Rica.

Artículos de internet

Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (2010 octubre). *Naturaleza jurídica de los delitos informáticos*. Recuperado de https://archivos.juridicas.unam.mx/www/bjv/libros/6/2941/27.pdf

Estadísticas de usuarios de internet y población (2019) *Internet Usage and Population in Central America*. Recuperado de https://www.internetworldstats.com/stats12.htm

Hans Aaron Ortega (2011). *Módulo de delitos informáticos*. Recuperado de http://descargas.idpp.gob.gt/Data_descargas/Modulos/delitosinformaticos.pdf

Ochoa Maricela (2020, 22 de septiembre). *Delitos informáticos en México, Que dice la ley? IT Masters Mag.* Recuperado de https://itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

Organismo de Investigación Judicial de Costa Rica (2021). *Sección especializada contra el cibercrimen.* Recuperado de https://sitiooij.poderjudicial.go.cr/index.php/oficinas/departamento-de-investigaciones-criminales/delitos-informaticos

Panorama de Ciberdelitos en Guatemala (2016) Recuperado de https://ogdi.org/estadisticas