UNIVERSIDAD LATINA DE COSTA RICA
SEDE HEREDIA
CENTRO INTERNACIONAL DE POSGRADOS

MAESTRÍA PROFESIONAL EN DERECHO PENAL

TRABAJO FINAL DE GRADUACIÓN

“LA FALTA DE PREVENCIÓN DE LAS PERSONAS CIBERNAUTAS EN LOS DELITOS INFORMÁTICOS EN COSTA RICA”

ELABORADO POR

ANDREA CHACÓN MARÍN

HEREDIA, COSTA RICA

2018

UNIVERSIDAD LATINA DE COSTA RICA
SEDE HEREDIA
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL TUTOR DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 17 de marzo de 2018

Sres.

Miembros del Comité de Trabajos Finales de Graduación

SD

Estimados señores:

He revisado y corregido el Trabajo Final de Graduación, denominado: "**LA FALTA DE PREVENCIÓN DE LAS PERSONAS CIBERNAUTAS EN LOS DELITOS INFORMÁTICOS EN COSTA RICA",** elaborado por la estudiante: **Andrea Chacón Marín**, como requisito para que la citada estudiante pueda optar por el grado académico **MÁSTER PROFESIONAL EN DERECHO PENAL.**

Considero que dicho trabajo cumple con los requisitos formales y de contenido exigidos por la Universidad, y por tanto lo recomiendo para su entrega ante el Comité de Trabajos finales de Graduación.

Suscribe cordialmente,

Dr. Carlos Góngora Fuentes

UNIVERSIDAD LATINA DE COSTA RICA
SEDE HEREDIA

CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL LECTOR
DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 17 de marzo de 2018
Sres.
Miembros del Comité de Trabajos Finales de Graduación
SD

Estimados señores:

He revisado y corregido el Trabajo Final de Graduación, denominado: "**LA FALTA DE PREVENCIÓN DE LAS PERSONAS CIBERNAUTAS EN LOS DELITOS INFORMÁTICOS EN COSTA RICA",** elaborado por la estudiante: **Andrea Chacón Marín**, como requisito para que la citada estudiante pueda optar por el grado académico **MÁSTER PROFESIONAL EN DERECHO PENAL.**

Considero que dicho trabajo cumple con los requisitos formales y de contenido exigidos por la Universidad, y por tanto lo recomiendo para su entrega ante el Comité de Trabajos finales de Graduación.

Suscribe cordialmente,

MSc. Miguel E. Fernández Calvo

UNIVERSIDAD LATINA DE COSTA RICA
SEDE HEREDIA
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL FILÓLOGO DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 17 de marzo de 2018

Señores
Miembros del Comité de Trabajos Finales de Graduación
SD

Estimados señores:

Leí y corregí el Trabajo Final de Graduación, denominado: **"LA FALTA DE PREVENCIÓN DE LAS PERSONAS CIBERNAUTAS EN LOS DELITOS INFORMÁTICOS EN COSTA RICA",** elaborado por la estudiante: **ANDREA CHACÓN MARÍN,** para optar por el grado académico **MÁSTER PROFESIONAL EN DERECHO PENAL.**

Corregí el trabajo en aspectos, tales como: construcción de párrafos, vicios del lenguaje que se trasladan a lo escrito, ortografía, puntuación y otros relacionados con el campo filológico y desde ese punto de vista considero que está listo para ser presentado como Trabajo Final de Graduación; por cuanto cumple con los requisitos establecidos por la Universidad.

Suscribe de ustedes cordialmente,

Prof. Mario Boza Chacón
Filólogo. Cédula 103580444
Carné Colegio de Licenciados y
Profesores Número 5034

UNIVERSIDAD LATINA DE COSTA RICA
LAUREATE INTERNATIONAL UNIVERSITIES

"Carta Autorización del autor(es) para uso didáctico del Trabajo Final de Graduación"

Vigente a partir del 31 de Mayo de 2016

Instrucción: Complete el formulario en PDF, imprima, firme, escanee y adjunte en la página correspondiente del Trabajo Final de Graduación.

Yo (Nosotros):
Escriba Apellidos, Nombre del Autor(a). Para más de un autor separe con " ; "

Andrea Chacón Marín

De la Carrera / Programa: Maestría Profesional en Derecho Penal
autor (es) del (de la) *(Indique tipo de trabajo):* Trabajo Final de Graduación
titulado:

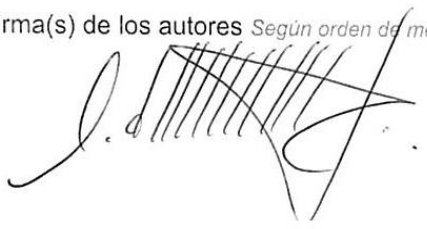
La falta de prevención de las personas cibernautas en los delitos informáticos en Costa Rica

Autorizo (autorizamos) a la Universidad Latina de Costa Rica, para que exponga mi trabajo como medio didáctico en el Centro de Recursos para el Aprendizaje y la Investigación (CRAI o Biblioteca), y con fines académicos permita a los usuarios su consulta y acceso mediante catálogos electrónicos, repositorios académicos nacionales o internacionales, página web institucional, así como medios electrónicos en general, internet, intranet, DVD, u otro formato conocido o por conocer; así como integrados en programas de cooperación bibliotecaria académicos dentro o fuera de la Red Laureate, que permitan mostrar al mundo la producción académica de la Universidad a través de la visibilidad de su contenido.

De acuerdo con lo dispuesto en la Ley No. 6683 sobre derechos de autor y derechos conexos de Costa Rica, permita copiar, reproducir o transferir información del documento, conforme su uso educativo y debiendo citar en todo momento la fuente de información; únicamente podrá ser consultado, esto permitirá ampliar los conocimientos a las personas que hagan uso, siempre y cuando resguarden la completa información que allí se muestra, debiendo citar los datos bibliográficos de la obra en caso de usar información textual o paráfrasis de esta.

La presente autorización se extiende el día *(Día, fecha)* 17 del mes marzo del año 2018 a las 18:00 . Asimismo declaro bajo fe de juramento, conociendo las consecuencias penales que conlleva el delito de perjurio: que soy el autor(a) del presente trabajo final de graduación, que el contenido de dicho trabajo es obra original del (la) suscrito(a) y de la veracidad de los datos incluidos en el documento. Eximo a la Universidad Latina; así como al Tutor y Lector que han revisado el presente, por las manifestaciones y/o apreciaciones personales incluidas en el mismo, de cualquier responsabilidad por su autoría o cualquier situación de perjuicio que se pudiera presentar.

Firma(s) de los autores *Según orden de mención al inicio de ésta carta:*



DEDICATORIA

Primeramente, a Dios por regalarme el don de la vida, por su infinito amor por mí, por haberme permitido conocerlo y cuidarme siempre; por enseñarme que los triunfos se obtienen con esfuerzo y por no soltarme nunca de su mano.

A mi amado esposo Jimmy, quien me ha enseñado que el amor incondicional existe y me lo demuestra día a día; por ser parte de este proyecto de vida que decidimos emprender juntos, por apoyarme en todas las metas propuestas y correr de la mano conmigo hasta alcanzarlas; por ser mi amigo y consejero, por la paciencia que me ha demostrado en todos estos años y por cuidarme y protegerme.

AGRADECIMIENTO

A mis amadísimos compañeros de la Generación 2-2015 de la Maestría Profesional en Derecho Penal: Alejandro, Yulieth, Cristhian, Valeria, Carlos y Pedro, con quienes compartí grandes momentos, con los cuales reí hasta llorar y que compartieron sus conocimientos conmigo, pero principalmente, me enseñaron el significado de la palabra amistad.

A todos los profesores y profesoras que, durante mi vida de aprendizaje, se han dedicado a enseñarme con amor y a motivarme a seguir adelante.

A mis queridos estudiantes de la Universidad Americana, quienes me han enseñado que cuando uno se propone algo lo logra con esfuerzo y dedicación y, por ser mi motivo para superarme más cada día, con el fin de ser una mejor profesional y una mejor persona.

A mi tutor el Dr. Carlos Góngora, que más que un profesor es un gran amigo y tuvo la dedicación de guiarme en este proyecto tan importante.

Al Dr. Franz Vega, por sus enseñanzas y su amistad.

A todas aquellas personas que de una u otra forma me han apoyado y que han influido en la formación de la persona que soy hoy.

Resumen Ejecutivo

La mayoría de las personas tienen la creencia de que no existe suficiente regulación en Costa Rica, que permita una efectiva sanción de los delitos informáticos y es que, este tipo de hechos ilícitos en la vida virtual se han vuelto tan regulares como los delitos en el mundo físico.

La habitualidad, o frecuencia, con que los ciberdelincuentes cometen los actos punibles, deriva principalmente de la facilidad de acceso al mundo virtual, siendo que, hoy en día es muy común que los seres humanos utilicen el Internet como parte de su diario vivir e incluso, este medio sea requerido para la realización de sus trabajos o funciones cotidianas.

Aunado a lo anterior, la tecnología avanza a pasos agigantados y, en esto, los cibercriminales siempre van adelante, son los primeros en innovar sobre métodos para delinquir, con la facilidad de poder cometer sus ciberdelitos desde cualquier parte del mundo. No obstante, pese a ser cierto que los ciberdelincuentes buscan de manera constante aprovechar los avances tecnológicos para cometer los ilícitos, también se puede afirmar que existe una falta de prevención de la mayoría de las personas, al hacer un mayor uso del Internet, pues no han aprendido a protegerse (esto no ocurre en todas las sociedades). Es común y para muchos cibernautas hasta normal, compartir sus usuarios y contraseñas sin el mayor de los cuidados, con familiares, amigos, compañeros de trabajo, pareja sentimental, etc.; sin hacer conciencia del peligro que esto lleva.

Por otra parte, hay personas que son objeto de llamadas telefónicas, donde el cibercriminal se identifica como un funcionario de alguna entidad conocida por su víctima y obtiene información personal, la cual es brindada sin percatarse de que está siendo víctima de la delincuencia.

Contrario a la presunción de la mayoría de personas, en Costa Rica sí existe suficiente regulación en materia de delitos informáticos, máxime que en el año 2017 se adhirió al Convenio de Budapest, el cual tiene como fin contar con mayor

cooperación internacional en la persecución de los ciberdelincuentes, procurando derribar las barreras que obstaculizan la función de los entes judiciales y que permiten la impunidad del cibercriminal e impiden la reparación del daño provocado a los individuos y a la sociedad.

En resumen, no puede afirmarse que la problemática de la ciberdelincuencia derive en una falta de regulación, pues como será analizado en el presente trabajo, existe la normativa suficiente y la misma está en constante cambio, de conformidad con los avances que exija este mundo globalizado; es más certero afirmar, que lo que existe es una falta de prevención de la mayoría de las personas cibernautas, quienes aún no han aprendido a resguardarse en el mundo virtual, por lo que se requiere de manera urgente, la implementación de campañas de prevención que permitan enseñar a las personas, los cuidados necesarios que deben tener en el momento de navegar en la red y así evitar ser víctimas de un ciberdelito.

Tabla de Contenidos

CAPÍTULO I:

1. PROBLEMA Y PROPÓSITO

En la actualidad, es muy común escuchar el término hacking y al oírlo inmediatamente se asocia de manera errónea con un experto en computadoras, quien, de forma ilegal, accede a la información contenida en un ordenador.

El hacking se puede definir como:

> "…la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo. (Recuperado el día 01 de marzo del 2018 a las 3.35 pm de la página http://www.duiops.net/hacking/hacking-cracking.htm)

Sin embargo, no se requiere ser un experto en computadoras para cometer un ciberdelito. Lamentablemente, el ciberespacio no ha quedado exento de la comisión de hechos punibles, pues los ciberdelincuentes han avanzado con más presura que la misma lucha que se hace en contra de los delitos informáticos; es decir, la informática y la regulación legal no se han desarrollado de forma paralela, el derecho siempre se ha quedado rezagado; lo que lleva a que el Estado deba realizar grandes inversiones económicas con el fin de combatir el cibercrimen, el cual no solo puede producir lesiones en el nivel personal sino que podría afectar hasta la seguridad nacional de un país.

En Costa Rica, por medio del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), se está llevando a cabo la "Estrategia Nacional de Ciberseguridad, en su última etapa de construcción", misma que refiere a: "…la necesidad de mejorar la comunicación con actores nacionales, reformar la legislación, y así ofrecer solidez en el nivel de políticas públicas", explicó el Viceministro de Telecomunicaciones, Edwin Estrada Hernández". (Recuperado el día 13 de noviembre del 2017 a las 9:30 pm de: https://micit.go.cr/index.php?option=com_content&view=article&id=9964:estrategia-nacional-de-ciberseguridad-en-su-ultima-etapa-de-construccion-2&catid=40&Itemid=630)

La finalidad es capacitar y empoderar las diversas instituciones estatales, con la cooperación de empresas privadas y Colegios Profesionales, al buscar que los ciudadanos concienticen sobre el tema de la ciberseguridad.

Según refiere el MICITT en la página citada:

> "…Uno de los principales objetivos al implementar la Estrategia de Ciberseguridad, es canalizar acciones para reforzar la consolidación del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), además de continuar el trabajo en el marco legal e impulso de la adhesión al convenio de Budapest, puesto que Costa Rica ha fortalecido su jurisdicción en temas como Delitos Informáticos y Protección de Datos…".

Aunado a lo anterior, en el tema de la ciberseguridad también se encuentra el hecho de que los cibernautas, es decir, todas las personas que de una u otra forma acceden a los medios electrónicos o informáticos, no tienen una cultura de seguridad, nadie se protege en la web, por el contrario, es común observar cómo se comparte información personal con desconocidos y se intercambian fotografías propias o de la familia por medio de las redes sociales, lo que equivale a que alguien se ubique en un lugar público y reparta retratos o imágenes a desconocidos. En la red, una vez que se comparte una imagen, la misma sale del dominio del cibernauta, no pudiendo volverla a recuperar, perdiendo el control sobre la misma y desconociendo el uso que se le vaya a dar, por parte de cualquier otra persona.

El Lic. Mora (2010) indica:

> "…Tanto dependen los países desarrollados de sus redes de computación y la interconectividad, que se estima que el próximo ataque terrorista será un cyber ataque, capaz de paralizar la economía norteamericana. En un tono más local, puedo decirles que en nuestro país el cyber crimen crece cada vez más. Puedo dar fe de ello, porque mi familia se encuentra entre las víctimas del phishing, de tal forma que esta realidad no discrimina y está presente en economías grandes o pequeñas. Para ser víctima, basta estar conectado (p. 24)…".

El término phishing se utiliza para definir uno de los tantos métodos que existen para estafar y obtener información confidencial por Internet. Es muy común entre los ciberdelincuentes que se valen de la tecnología informática, engañando al cibernauta al hacerse pasar por funcionarios de entidades bancarias u otras afines y solicitando dicha información personal, que en una gran parte de las veces es proporcionada por las personas, sin saber que están siendo víctimas de un delito informático.

El Lic. Mora hace evidente una realidad, las redes de computación se han convertido en elementos esenciales del diario vivir hasta el punto, que no se descarta que lleguen a ser utilizadas como armas de ataque, que paralicen a todo un país, por muy desarrollado que sea, causando afectación no solo de manera individual sino colectiva, pues como bien lo dice: “Para ser víctima, basta estar conectado”.

La gran mayoría de las personas en el mundo tienen acceso a una computadora, saben cómo usarla, conocen y disfrutan de Internet. Además, la tecnología avanza a pasos agigantados y la demanda de teléfonos inteligentes es cada vez mayor, los cuales por su valor y portabilidad hacen más fácil dicho acceder a Internet, sin requerir un ordenador. El asunto es que, desde un celular inteligente, es posible navegar en Internet, accesar a redes sociales, intercambiar información, imágenes, audios, etc. y las personas lo hacen sin el menor cuidado, sin protección alguna y lo que es peor, todos los días, son más los menores de edad que utilizan este medio de comunicación con sus amigos y amigas, obviando las precauciones que el mismo requiere.

Este tema ha sido de gran interés desde los años 90, tiempo aproximado en que empezó el auge de las computadoras en Costa Rica y ha sido materia de tesis de tanto estudiantes del Derecho como de la Informática. En el año 2004, Juan Luis Arias, estudiante del grado de Licenciatura de la Universidad Escuela Libre de Derecho, realizó el trabajo titulado: “*La internet y el delito de acceso no autorizado a sistemas informáticos (hacking): nuevos desafíos del Derecho*”. Por su parte, la estudiante de grado Soto (2015), realizó la tesis para obtener la licenciatura en Derecho en la Universidad Americana, con el tema: “*Protección de datos*

personales en medios tecnológicos: desafíos de la actual legislación nacional pro defensa del ciudadano costarricense".

Otro autor quien se ha interesado mucho por el tema debido a las carreras que ha cursado, ha sido el Ingeniero en Sistemas y Licenciado en Derecho, Roberto Lemaître Picado, quien es Especialista en Delitos Informáticos, Protección de Datos, Seguridad de la Información, Derecho y Tecnología y Representante para Costa Rica en la Red Iberoamericana de Derecho Informático, su tesis de grado en Derecho se denominó: "La impunidad de los delitos informáticos en la ciber-sociedad costarricense en el ámbito del Derecho Penal".

También la Universidad de Costa Rica y el Colegio de Abogados y Abogadas de Costa Rica se han llevado a cabo congresos, charlas, ponencias y compendios sobre el tema de la ciberseguridad y los delitos informáticos, donde han participado grandes figuras nacionales como el Lic. Luis Paulino Mora, quien fungió como Presidente de la Corte Suprema de Justicia, el Lic. Alfredo Chirino, Decano de la Facultad de Derecho de la Universidad de Costa Rica, Gabriela Barrantes Sliesarieva, Directora de la Escuela de Ciencias de la Computación e Informática de la Universidad de Costa Rica, Federico Malavassi Calvo, Ex Diputado, Oscar Julio Solís Solís, quien fue uno de los pioneros de la firma digital, entre muchos otros, pues existe un gran interés en que se desarrolle una cultura colectiva, que eduque a las personas en el área de la ciberseguridad y es precisamente lo que el presente trabajo pretende demostrar, que existe suficiente regulación sobre delitos informáticos, pero la alta incidencia se debe no a la falta de normativa que los sancione sino a la falta de prevención de los cibernautas, sea por descuido o por desconocimiento.

2. Planteamiento del problema.

Conocido es que, en la actualidad, existe un mundo virtual en el cual la mayor parte de los seres humanos está inmerso; se depende de los ordenadores o teléfonos inteligentes para hacer transacciones bancarias, compras, pago de servicios, entre muchos otros. La tecnología ha tenido un auge impactante a nivel mundial, desde hace aproximadamente unas tres décadas. Las "*RedesZone"*, que

son portales de comunicaciones y redes, proliferan desmesuradamente y hoy en día una gran cantidad de personas en el nivel mundial tienen acceso a Internet, sea por medio de teléfonos inteligentes, computadoras, tabletas electrónicas, etc., lo que ha producido un impacto hasta en las mismas condiciones humanas, pues ahora es sumamente común observar a niños de muy corta edad, que utilizan estos aparatos con mejores destrezas que muchos adultos. Esta nueva forma de vida tecnológica, es también conocida como ciberespacio y es totalmente real, así como reales también lo son sus riesgos; por lo que, se necesita ciberseguridad.

Es importante que, se analice un tema del cual se ha escuchado mucho de unos años para acá y es el denominado “Internet de las cosas” o “internet of things”, según Frutos (2017) hace referencia a “*la interconexión digital de los objetos cotidianos con Internet, convirtiéndose así en objetos inteligentes*”, es decir, se logra ampliar sus funciones por medio de la conexión a Internet. Por ejemplo, mediante la Internet se puede lograr que una refrigeradora lleve un control de los productos, como tiempo de caducidad o incluso avisar y hasta ordenar algún artículo cuando ya esté por acabarse. (Recuperado el día 13 de noviembre del 2017 a las 10:00 pm de la página http://computerhoy.com/noticias/internet/que-es-internet-cosas-61528)

Internet es una gran red o conjunto de servidores de informaciones multimedia, conectadas y accesibles, que provee a los usuarios un medio de comunicación a distancia, sea por cuentas de correo electrónico, foros de discusión, diversas redes sociales e incluso comunicación visual por tele conferencias. Además, tiene la función de servir como biblioteca virtual, al permitir a través de una amplia cantidad de navegadores, el acceso a todo tipo de información en cuestión de segundos y todo lo anterior, como se indicó anteriormente, desde una computadora, teléfono celular, tabletas electrónicas, etc. Sin embargo, en este ciberespacio, pese a existir amplia regulación, siguen cometiéndose cada día más ciberdelitos, lo que conlleva a creer, que no es por falta de normativa sino por descuido de los cibernautas.

Los beneficios que provee el ciberespacio son incomparables, siendo que es posible aligerar el trabajo, aumentar la eficiencia y llevar a cabo actividades en

mucho menor tiempo, lo cual es de suma importancia en este mundo globalizado de hoy en día. Comprar, vender, pagar los servicios y hasta matricular cursos virtuales son algunas de las ventajas que el avance tecnológico hereda y por ser acciones que se llevan a cabo diariamente, se está expuestos, al igual que en el mundo físico, a ser víctimas en el espacio virtual, con iguales o mayores desventajas, dado que, el ataque puede venir de cualquier parte del planeta.

El presente trabajo pretende demostrar que, gran parte de los delitos informáticos se originan por causa de una sociedad que no ha aprendido a protegerse de la ciberdelincuencia, al navegar de manera insegura en el mundo virtual y es que no existe una cultura de protección ni en el mundo físico ni en el mundo virtual, donde las personas comparten sus datos personales, sin detenerse a analizar lo peligroso que esto puede resultar.

El Estado realiza una clasificación de los delitos, partiendo de una infinidad de conductas humanas, no obstante, con el fin de resguardar una paz social y un respeto a los derechos de cada individuo, se ha realizado una selección de estas conductas, al tipificar aquellas que se consideran afectan los bienes jurídicos tutelados.

Una conducta criminal es entonces, la acción realizada por un ser humano que va contraria a la normativa vigente y que tiende a causar un daño o al menos pone en peligro un bien jurídico tutelado, en la mayoría de las ocasiones con la finalidad de obtener un beneficio propio o de un tercero, aunque puede darse únicamente por simple placer.

En el ámbito virtual, el ciberdelincuente invade de forma ilegal la privacidad de la persona, al atentar contra los datos o los archivos en las bases de datos de los ordenadores e incluso transmiten virus, interceptan mensajes de correo electrónico, descifran claves personales (password), usufructúan el *“software”* (son un conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas, según definición RAE) de un tercero, entre muchas otras cosas, con lo cual provocan afectación.

Pero más que nada, lo que se debe de tomar en cuenta, es que se está frente a un tipo de delincuencia muy nueva y respecto de la cual no son propias las teorías criminológicas a los delitos que se llevan a cabo en el mundo físico, pues ambos ámbitos difieren considerablemente, lo cual provoca que sus métodos de prevención difieran en cada caso.

Por tanto, los condicionantes del delito no pueden ser en el ámbito virtual los mismos que sirvan de parámetros en el espacio físico, siendo necesario una regulación diferente para este tipo de ciberdelitos.

Sin embargo, en Costa Rica existe una amplia regulación respecto del tema de los delitos informáticos, que se actualiza de manera constante según las necesidades y los cambios requeridos, pues al avanzar la tecnología de manera tan acelerada, la normativa debe de irse acoplando. Es casi posible aseverar, que en toda Latinoamérica, es el país más avanzado en cuanto a la implementación de normas que sancionen los delitos informáticos, pero pese a esto, este tipo de actos delictivos se ha multiplicado de manera desproporcional en los últimos años y lamentablemente, refiere Villasuso (2010) "*el sistema jurídico casi siempre va un paso atrás en cuanto a la creación de un marco normativo que permita sancionar a los hackers y a los piratas informáticos*" (p. 13)

Por otra parte, en Costa Rica, no se ha implementado una cultura de ciberseguridad, donde a las personas se les advierta sobre el problema de compartir información personal por los diferentes medios sociales y el riesgo que esto puede representar y una formación que enseñe el respeto de los intereses legítimos de los seres humanos. Partiendo de lo anterior, para la presente memoria de graduación, se plantea la siguiente cuestionante: ¿Ocurren los delitos informáticos, por una falta de prevención de los cibernautas?

3. Justificación.

Las facilidades de acceso y comunicación creadas por la tecnología, han sido aprovechadas también por las organizaciones criminales, quienes utilizan este medio para cometer sus delitos, al trascender las fronteras, pues sus crímenes ya

no se limitan a un determinado lugar, sino que su escala ha llegado a ser de nivel mundial.

El ciberespacio ha permitido la creación de nuevas conductas delictivas, las cuales son viables por medio de las nuevas tecnologías de información y comunicación, las cuales se modernizan día a día. La ciberdelincuencia es todo un reto, no se puede pretender eliminar la delincuencia en el mundo virtual como no ha sido posible hacerlo en el mundo real, por tanto, los países requieren proveerse de nuevos mecanismos que les permitan dar una persecución efectiva contra el cibercrimen, sin obviar que los ciberdelincuentes van años luz adelante, por lo que los Estados deberán centrar sus esfuerzos no solo en procurar que las normas penales en materia de delitos informáticos, cumplan con su propósito, ajustándose a los principios básicos del derecho penal sino también a reconocer la complejidad del mundo informático y ser competitivos.

Tal como se indicó anteriormente, Costa Rica mantiene una normativa actualizada y basta en materia de delitos informáticos, no obstante, lo que no existe es una cultura de protección por parte de los cibernautas, quienes en el final, resultan víctimas de los ciberdelincuentes. Es evidente que existen carencias en el nivel nacional, en cuanto a la implementación de programas educativos, en el tema de ciberdelitos y cómo evitarlos; no se educa a los niños y jóvenes desde las escuelas y colegios en cuanto al uso correcto del Internet y las comunicaciones, el Estado no implementa campañas educativas para la población adulta, que procuren la enseñanza de la ciberseguridad y se pretende demostrar en el presente estudio, que las personas desconocen los peligros del mundo virtual y, por lo tanto, no se protegen.

Y es que la situación de la falta de cultura de protección no se evidencia únicamente cuando se utiliza la red, es común que se manifieste también en el mundo físico, cuando se revelan datos personales a las entradas de los centros comerciales y ferias con tal de participar en rifas y demás, siendo que, por infortunio, la protección no es algo que se tenga presente en la vida diaria, pero se reitera, es una situación de cultura, pues la sociedad costarricense es muy confiada y no piensa en las repercusiones que el brindar dicha información les puede generar, no

obstante, en otros países son más cuidadosos, tales como Alemania, Suecia, Dinamarca, que tiene una amplia cultura informática.

Es evidente que Internet es un medio de comunicación global, que no reconoce fronteras, no tiene límites y más aún, no tiene horario, todo esto permite que la comisión de ciberdelitos sea tan sencilla, principalmente porque el ataque puede venir de cualquier parte del mundo y nadie se escapa de la posibilidad de ser víctima. Es común observar mensajes remitidos a correos electrónicos, donde se utilizan imágenes y logos de diferentes entidades bancarias y se le indica a las personas, que deben de ingresar a una página web determinada (siempre se indica en el mensaje enviado), con el fin de actualizar los datos de su cuenta bancaria, lo anterior, debido a un supuesto “fallo o problema” generado, que se pretende resolver; sin embargo, esto no es más que un engaño, donde el ciberdelincuente les solicita la información personal y en la mayoría de las ocasiones terminan dándola, sin percatarse de que están siendo víctimas de un delito, este tipo de ciberdelito se denomina “Phishing”.

A pesar de que las diferentes entidades financieras y bancarias informan a sus clientes sobre esta modalidad de ciberdelito, los cibernautas siguen incurriendo en estos errores de entregar información de sus cuentas a terceros, nótese que, si la persona no facilita la información, la comisión del delito se torna más difícil, pues ya tendrían que utilizarse mecanismos más complejos, donde el ciberdelincuente debe de ingresar al ordenador o equipo de la víctima, para obtener la información o crear páginas falsas y esperar a que la persona ingrese y facilite sus contraseñas y para esto se requiere un mayor conocimiento en informática, por parte del autor del hecho delictivo.

Las distintas entidades advierten de manera constante a sus clientes sobre los delitos informáticos, por medio de mecanismos de aviso electrónico al teléfono inteligente o a la cuenta de correo y avisan sobre todos los movimientos en las tarjetas de débito y crédito. Además, se han implementado líneas de seguros que la sociedad costarricense no utiliza por falta de conocimiento, propiciándose la “culpa de la víctima” como eximente de responsabilidad.

Pero no todas las intromisiones ilegales a los diversos sistemas informáticos tienen la finalidad explícita de ocasionar un delito, es decir, que el infractor busca beneficiarse a sí mismo o a un tercero en el aspecto patrimonial, sea desviando dineros a otras cuentas u obteniendo información privada que posteriormente puede vender a un interesado, hay quienes acceden a estos sistemas por meros retos o diversión, para demostrar sus destrezas. Lo cierto de todo esto es, que exista o no el ánimo de causar un perjuicio, los delitos informáticos se consideran de peligro abstracto porque violentan la privacidad, intimidad, buena fe, seguridad, entre otros bienes jurídicos, con el solo hecho de ingresar a un lugar sin la debida autorización, independientemente de que se cause un perjuicio directo o un resultado dañoso. (Madrigal, 2015)

Como se indicó anteriormente, Internet ha permitido el acceso directo e inmediato a la información, al transmitir textos, imágenes e incluso a diferentes personas a la vez, al posibilitar el acceso a la sociedad de la información. La finalidad de los avances tecnológicos es precisamente, la simplificación de las labores diarias, trabajos que antes debían de hacerse a mano y demoraban días hoy están al alcance de un simple enter (*click)*.

Las actividades iniciales de la sociedad industrial generaban un tipo de riesgo muy diferente al actual, al existir un contacto más directo entre los trabajadores y la maquinaria que se utilizaba en las labores diarias, los operarios estaban expuestos a lesiones corporales o hasta morir. En el presente, la relación directa entre maquinaria y trabajador se ha vuelto más distante, lo que genera un mínimo efecto nocivo.

Consecuentemente, el desarrollo de la sociedad origina en la actualidad, la aceptación de asumir ciertos riesgos a cambio del beneficio que le genera la tecnología, estos se denominan “riesgos socialmente adecuados” y obviamente requieren regulación para que no se incurra en un abuso o en un incremento injustificado del riesgo, que apareja una sanción en el ámbito administrativo-pecuniario, que devienen en última ratio, en la generación de tipos de conductas penales.

Existen conductas humanas que en un inicio no aparentan ser ilícitas, pero que pueden suscitar un impacto negativo en la sociedad (economía), el simple hecho de que una persona ingrese a una base de datos sin autorización, puede ocasionar grandes estragos, pues, aunque no sea con intención dolosa, la información existente podría ser alterada, lo cual, evidentemente provocaría un perjuicio económico, según de la empresa de la que se trate, es por ello, que estas conductas requieren penalización por medio de leyes y creación de tipos penales.

La tecnología ha venido a simplificar en gran manera los trabajos cotidianos y no cabe duda que sin estos avances tecnológicos el mundo se paralizaría, sin embargo, las nuevas tecnologías informáticas no dejan de ser un problema para la sociedad ante la creciente ola de ciberdelincuencia que se ha desarrollado en los últimos cuarenta años, por lo que los países han tenido que ir adaptando su normativa creando nuevos tipos penales, con el fin de sancionar a quienes practican la ciberdelincuencia.

La ciencia aumenta, la tecnología avanza y en ese constante cambio, donde el ciberespacio provee de amplios beneficios y se ha convertido en una parte fundamental del diario vivir, es necesario hacer conciencia de que como usuario de internet se es responsable del buen uso de esta herramienta, los cibernautas deben de aprender a comportarse de una manera segura y legal y no estaría de más que se implementaran instrumentos legales que los obliguen a hacerlo. Cada persona debe velar por su propia seguridad, al prevenir cualquier tipo de ataque mediante el uso consciente del Internet, para no ser víctimas ni autores de hechos delictivos en línea (*online)*.

4. Objetivo general y objetivos específicos.

OBJETIVO GENERAL

Demostrar que la incidencia de delitos informáticos en Costa Rica, no se debe a una regulación insuficiente, sino a la falta de prevención de los cibernautas.

OBJETIVOS ESPECÍFICOS

1. Definir qué es ciberdelito y cuáles son sus tipos más frecuentes.
2. Conocer la normativa vigente en Costa Rica que regula los delitos informáticos.
3. Distinguir cuáles son los delitos informáticos más comunes en Costa Rica.
4. Determinar que la mayoría de las personas en Costa Rica, son víctimas de los ciberdelincuentes, debido a la falta de prevención en el momento de navegar en el ciberespacio.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Historia de la computación.

Desde eras remotas, el ser humano ha buscado como simplificar la forma de realizar el trabajo, al inventar maquinaria para la ejecución de sus labores diarias.

Este avance también ha alcanzado al mundo virtual, donde cada día se crean mejores herramientas que ayudan a la realización de las tareas cotidianas. El Internet ha permitido el acceso directo e inmediato a la información, transmitiendo textos e imágenes a diferentes personas a la vez, al posibilitar el acceso a la sociedad de la información.

La finalidad de los avances tecnológicos es precisamente esa simplificación de las labores diarias, trabajos que antes debían de hacerse a mano y demoraban días hoy están al alcance de un simple enter (click), por lo cual, se puede decir, que dentro de las ventajas de este desarrollo están la modificación de la distribución de la fuerza de trabajo (distribución de cargas) y la disminución de jornadas laborales, dado que, los programas pueden ser reutilizados las veces que se requiera, al permitir que los procesos se realicen en menor tiempo (por ejemplo, los cálculos de planillas).

Los beneficios que provee el ciberespacio son incomparables, siendo que es posible aligerar el trabajo, aumentar la eficiencia y llevar a cabo actividades en mucho menor tiempo, lo cual es de suma importancia en este mundo globalizado de hoy en día. Comprar, vender, pagar los servicios y hasta matricular cursos virtuales son algunas de las ventajas que el avance tecnológico hereda y por ser acciones que se llevan a cabo diariamente, las personas están expuestas, de la misma manera que en el mundo físico a ser víctimas de los delincuentes en el espacio virtual, con iguales o mayores desventajas, dado que, el ataque puede venir de cualquier parte del planeta.

Fue en el Siglo XIX cuando el inventor Charles Babbage creó la primera computadora (diseño original), el cual sería comercializado muchos años después. Posteriormente, otros inventores generaron sistemas de programación que les

ahorraba tiempo en tabulaciones de datos, tal fue el caso de Herman Hollerith quien en 1879 "*inventó un sistema para mecanizar el censo de 1880 de su país, utilizando un sistema de programación con tarjetas perforadas que le hizo ahorrar mucho tiempo en la tabulación de datos*". Hollerith fue el precursor de la Computer Tabulating Recording Company, la cual en 1924 se constituyó en International Business Machine (IBM). (Recuperado el día 20 de noviembre del 2017 a las 8:30 pm de la página https://vinv.ucr.ac.cr/es/noticias/conozca-matilde-la-primera-computadora-del-país)

La historia de la computación data desde los años 1870 y a partir de ahí, muchas personas han sido las encargadas de ir mejorando los modelos y diseños hasta llegar a la diversidad de versiones que hoy en día se conocen. Incluso, se han clasificado los prototipos denominándolos como "Primera Generación", la cual usaba tarjetas perforadas, tenía tubos al vacío, con lenguaje muy simple y cuyo uso fue industrial.

En 1956, Waltter Brattain, William Schockley y John Bardeen ganan el Premio Nobel de Física al inventar el transistor, con lo que dieron inicio a la "Segunda Generación", con computadoras más pequeñas, más veloces, con memoria interna y poco consumo eléctrico. Un ejemplo de computadora de esta generación fue la IBM 1620 denominada "Matilde", instalada en 1967 en la Universidad de Costa Rica, de la cual se hará referencia más adelante.

Entre los años 1964 a 1979 se crearon computadoras más pequeñas, con circuitos integrados, mayor confiabilidad y multiprogramación, caracterizadas como la "Tercera Generación".

Se dice que, la "Cuarta generación" inicia a partir del año 1971, cuando se logra desarrollar el microprocesador por lntel Corp, que en un cm2 implanta el equivalente a un millón de tubos al vacío. Esta generación cuenta con transferencia electrónica de datos y memorias electrónicas. En teoría, aún no se ha migrado a la "Quinta Generación", sin embargo, existe polémica entre los sectores informáticos, quienes argumentan que ya se están utilizando "programas de inteligencia artificial" para equipos de robótica, los cuales se ubican en esa generación, aunque se implementen en equipos de cuarta generación.

2.2. Sociedad, información y generación de riesgos.

Las actividades iniciales de la sociedad industrial generaban un tipo de riesgo muy diferente al actual, al existir un contacto más directo entre los trabajadores y la maquinaria que se utilizaba en las labores diarias, los operarios estaban expuestos a lesiones corporales o hasta morir. En el presente, la relación directa entre maquinaria y trabajador se ha vuelto más distante, lo que genera un mínimo efecto nocivo.

La nueva actividad de la información o "Era de la información", abarca el tratamiento de datos, nombres o símbolos, al utilizar la computadora como instrumento que consigue "automatizar" los procesos, convirtiéndola en una de "las herramientas más poderosas de la sociedad actual".

Pero, el desarrollo de la sociedad origina en la actualidad, la aceptación de asumir ciertos riesgos a cambio del beneficio que le genera la tecnología, estos se denominan "riesgos socialmente adecuados" y obviamente requieren regulación para que no se incurra en un abuso o en un incremento injustificado del riesgo, que apareja una sanción en el ámbito administrativo-pecuniario, que devienen en última ratio, en la generación de tipos de conductas penales.

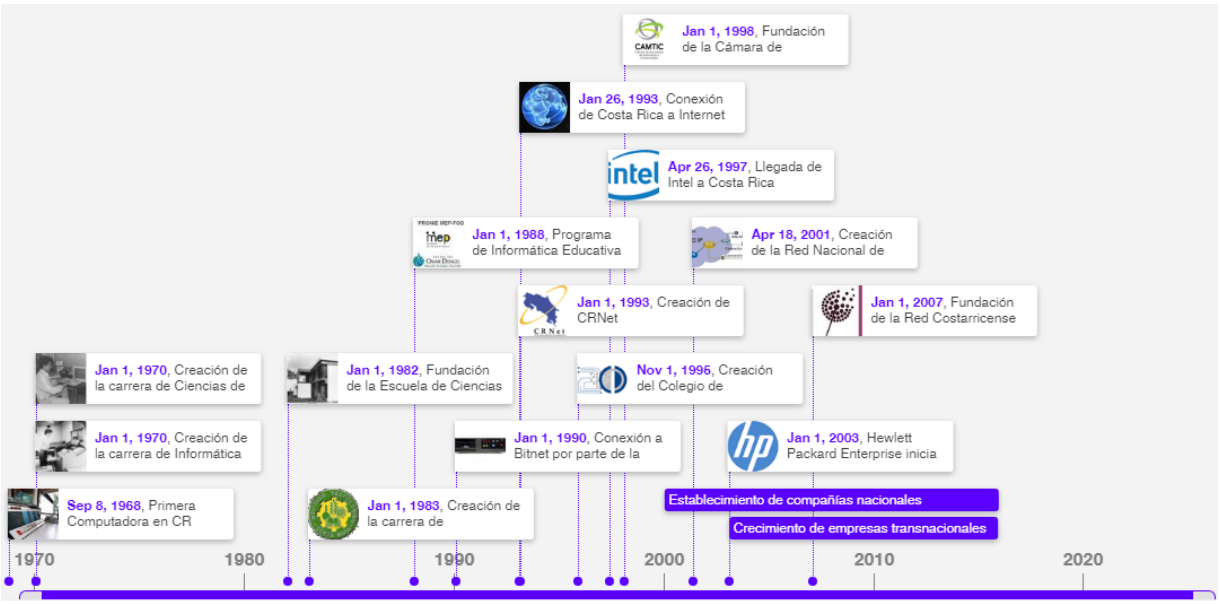
Existen conductas humanas que en un inicio no aparentan ser ilícitas, pero que pueden suscitar un impacto negativo en la sociedad (economía), el simple hecho de que una persona ingrese a una base de datos sin autorización, puede ocasionar grandes estragos, pues, aunque no sea con intención dolosa de causar daño, la información existente podría ser alterada, lo cual, evidentemente provocaría un perjuicio económico, según de la empresa de la que se trate, es por ello, que estas conductas requieren penalización por medio de leyes y creación de tipos penales.

2.3. El ingreso de la era tecnológica a Costa Rica

En el año 1968 la Universidad de Costa Rica adquiere a "Matilde", la primera computadora para aplicaciones científicas que llegó al país, se trataba de una IBM, la cual no contaba con sistema operativo y el peso de sus componentes rondaba las tres toneladas. Fue utilizada por los estudiantes de ingeniería del segundo

semestre del año 1969, era considerada muy potente para su época, con una unidad lectora y una perforadora. Posteriormente, en 1974 llegó “Clotilde”, más veloz y moderna que su antecesora. (Recuperado el día 20 de noviembre del 2017 a las 8:30 pm de la página https://vinv.ucr.ac.cr/es/noticias/conozca-matilde-la-primera-computadora-del-pais)

Breve historia de la computación en Costa Rica



2.4. Concepto y características

Según Chinchilla (2002), se puede definir el delito informático como: “…*La acción delictiva que realiza una persona con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático (se trata de las máquinas –hardware- o programas –software-)*…”. (p. 26)

Anteriormente se indicó, que la tecnología ha venido a simplificar en gran manera los trabajos cotidianos y no cabe duda que sin estos avances tecnológicos el mundo se paralizaría, sin embargo, las nuevas tecnologías informáticas no dejan de ser un problema para la sociedad ante la creciente ola de ciberdelincuencia que se ha desarrollado en los últimos cuarenta años, por lo que los países han tenido que ir adaptando su normativa creando nuevos tipos penales, con el fin de sancionar a quienes practican la ciberdelincuencia.

En razón de lo anterior, existen países que han implementado en su Código Penal estas acciones como delito, por ejemplo, España en el año 2010 modifica el artículo 197 inciso 3 de ese cuerpo normativo, con la finalidad de acoplarlo al "*Convenio sobre la ciberdelincuencia de Budapest*" ratificado por ese Estado en mayo del mismo año, por lo cual, dicho numeral en la actualidad cita:

> "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

Sobre el tema refiere Leiva (1992) que los delitos informáticos son: *"... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma…*". (p.225).

Definiciones de delitos informáticos podemos encontrar muchas, emitidas por los más prominentes juristas que se han esmerado por definir esta nueva rama, además, no es posible dar una especificación única a una materia que varía constantemente por estar en relación con la tecnología, aunado a que conlleva la mezcla del derecho y la informática, lo que vuelve más compleja su descripción.

Los ciberdelitos o delitos informáticos son pues, la figura más novedosa de delincuencia, Sieber Ulrich (1992) refiere que hay cuatro tipos de modalidades de delitos informáticos:

1. **Alimentación de datos.** Se accede a una computadora o red y se ingresan datos ajenos al propietario del sistema.
2. **Manipulación de programas.** Se altera el software implementando órdenes al sistema para que ejecute determinada función.
3. **Manipulación de consolas.** Alteran el hardware, es decir, se ataca directamente a los componentes físicos.

4. **Manipulación de resultados.** Por ejemplo, un uso indebido de bases de datos.

La comisión de hechos delictivos donde se utilizan medios informáticos o telemáticos es sumamente mutable, lo que hace difícil que se puedan encasillar en un solo delito, pues las acciones varían en cuanto a su forma o método de ejecución al igual que los resultados, al limitar su alcance y la posibilidad de establecer una sanción al infractor.

Por su parte, la jurista mexicana Lima (1984) define el delito electrónico de la siguiente manera:

> "... en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin…". (p. 100)

El delito electrónico y el delito informático difieren en cuanto a que el primero es más amplio, abarca la tecnología electrónica cualquiera que fuere su tipo (celulares, tabletas electrónicas, líneas telefónicas, cajeros automáticos, señales electromagnéticas, etc.) y el delito informático requiere que el infractor utilice como medio para la comisión del hecho una computadora: INFORMÁTICA + TELECOMUNICACIONES = TELEMÁTICA

Los delitos informáticos se clasifican según su finalidad como:

Instrumento o medio. Esto es utilizando una computadora para la realización del hecho punible, por ejemplo: alterar una base de datos y como.

Fin u objetivo. Cuando lesionan propiamente el equipo de cómputo o las redes, por ejemplo: formatear un disco duro para eliminar la información.

Obvio es, que no se pueden generalizar los delitos informáticos ni mucho menos tratar de adecuarlos en ese mundo virtual a las conductas de un infractor en el mundo físico, verbigracia el robo, la extorsión, el hurto, principalmente por el medio que utilizan estos delincuentes en el momento de la comisión del ilícito, así como los resultados posibles o generados, lo que lleva, como se citó anteriormente a la creación de nuevos tipos penales.

Los ciberdelitos son delitos dolosos, por lo cual, necesariamente deben de estar presentes los elementos subjetivos que caracterizan al dolo: elemento cognocitivo (conocimiento) y el elemento volitivo (voluntad), además, requieren que al autor se le pueda hacer el reproche del injusto penal, sin que medie ninguna causa de inimputabilidad, es decir, que le sea atribuible la ejecución del hecho.

En cuanto al sujeto activo, se puede decir que por lo general tiene amplios conocimientos en informática, pero no siempre es así, porque existe lo que se conoce como delitos ocupacionales, donde el autor de la conducta ilícita se ubica dentro de la misma empresa (trabajador); por lo que se concluye, que el sujeto activo puede ser una diversidad de personas.

La problemática de los delitos informáticos data de su dificultad para descubrir al autor de la acción punible y, por ende, casi nunca se logra una sanción. Lo anterior se debe a dos factores, el primero por el gran poder económico que hay detrás de estos delitos, lo que facilita su encubrimiento y lo segundo, porque la mayor parte de las veces, las compañías afectadas no denuncian, pues temen la pérdida de confianza de sus clientes, lo que a la postre sería más perjudicial, que el mismo agravio producido por el ciberdelincuente.

Además, el ciberdelito tiene de su lado el factor rapidez (tiempo), pues el ciberdelincuente está a solo un enter de su ilícito; los diversos medios informáticos facultan al sujeto activo a llevar a cabo el delito de forma rápida. Otro factor por destacar es el asunto del acercamiento (espacio), debido a que el autor del hecho punible se puede ubicar en cualquier parte, no importa la distancia, pues la red informática hace posible sobrepasar las fronteras y cometer la acción desde lugares remotos.

Todo lo anterior hace posible que el hecho pueda encubrirse con facilidad, permitiendo, dentro de otras cosas: Dejar el programa como estaba al inicio, modificar los programas a conveniencia, procedimientos de control muy costosos y seguridad en manos de terceros.

Existe mucha facilidad para borrar la prueba, la mayoría de las veces por la pertenencia del ciberdelincuente a la planilla profesional o por la capacidad de poder dejar el programa en el estado inicial.

Al reiterar, uno de los grandes problemas que presenta este tema, es que al tratarse de delitos cometidos por medio de la tecnología informática, el sujeto activo puede estar en cualquier parte del mundo, lo cual dificulta su persecución, posible detención y por ende la aplicación de la debida sanción, al ocasionar que la mayoría de las veces, estos hechos queden impunes, no en vano se les denomina delitos silenciosos, más que nada por la facilidad en que pueden ser borradas las huellas del ciberdelincuente.

Además, al existir un incremento de la tecnología disponible, así como, el escaso conocimiento de los cibernautas para protegerse de un posible delito informático, provoca que este sea un campo fácil de atacar por parte de los ciberdelincuentes. Según Ignacio en su ensayo "*Delitos Informáticos en Latinoamérica. Un estudio de derecho comparado. 1 era Parte*", cada segundo, 18 adultos son víctimas de un ciberdelito, lo que implica que diariamente hay más de millón y medio de personas afectadas por este tipo de trasgresores, quienes conocedores de que en muchos países hay poca legislación sobre el tema, aprovechan y realizan sus acciones dolosas desde esos lugares, procurándose una impunidad: "paraísos legales informáticos".

2.4.1. Algunos de los tipos penales más frecuente en el nivel mundial

a. Suplantación de identidad

Es muy común observar, como en diferentes redes sociales las personas se identifican con seudónimos u apodos para no utilizar su identidad real, esta acción por sí sola no constituye delito; la actuación delictiva se configura en el momento en que una persona utiliza el nombre, los datos y hasta las fotografías de un tercero

sin su consentimiento, es decir, una apropiación sin autorización del nombre, la imagen, las contraseñas y hasta el patrimonio. Este delito está regulado en el artículo 230 del Código Penal y establece una pena de 1 a 3 años.

Entonces, en síntesis, que este delito consiste en la usurpación de la identidad de una persona, mediante la utilización de una identidad falsa, con la existencia de un perjuicio a un tercero que no requiere ser económico porque puede ser moral.

La finalidad del ciberdelincuente en este delito es la comisión de fraudes, realizar ciberacoso o mejor conocido como ciberbullying (acoso psicológico por medio de medios informáticos o telemáticos) e incluso lesiones al honor, entre otros.

Para evitar ser víctimas de esta modalidad, se requieren de mecanismos que protejan nuestra identidad, al sancionar conductas constitutivas de delitos informáticos, como lo son la intromisión indebida o no autorizada a sistemas informáticos o telemáticos, regulación que se contempla en la normativa costarricense actual.

b. El fraude informático

Al hablar de fraude informático se debe de tener clara la diferenciación que existe entre esta figura y el fraude penal común, esto por cuanto este delito comprende: estafas informáticas, sabotajes informáticos, sustracciones de identidad, sustracción de claves de acceso, hurtos y robos informáticos, daños informáticos, etc., mientras que el fraude tradicional se dirige más hacia el ámbito de la estafa.

No es lo mismo el fraude informático que la estafa informática, el primero es el género y la segunda es la especie, por lo que se puede decir, que no todo fraude informático es una estafa informática, pero toda estafa informática es un fraude informático.

Existen tres momentos en los que en los sistemas se verifica el fraude informático, que se dirigen al procesamiento de la información, lo cuales se detallan a continuación:

- **Manipulación en el ingreso de los datos (INSIDERS)**

  Aquí se comete un verdadero fraude informático, es el delito informático más común y el de más fácil comisión, pero difícil de descubrir.

  No requiere que el sujeto activo posea amplios conocimientos en informática, sino que ocupe un puesto estratégico en la empresa y cuente con una clave de acceso de uso restringido. Es el paso inicial, una vez ingresados los datos la misma computadora se encarga, por medio de sus programas de ordenarla y ejecutarla.

- **Manipulación de los datos ingresados (TÉCNICA DEL CABALLO DE TROYA)**

  Para la comisión de este delito sí se requiere que el autor del hecho tenga amplios conocimientos en sistemas informáticos, pues lo que se busca es alterar programas, sea manipulándolos directamente desde una plataforma externa o insertando programas, rutinas o instrucciones para realizar una función no autorizada como una función normal, lo cual hace muy difícil su descubrimiento.

  El método más utilizado es la técnica del caballo de troya, que consiste en introducir un programa legítimo con un código oculto, mediante un correo electrónico o una página web y a simple vista no pareciera que perjudica el sistema, sin embargo, al procesarse, provoca serios trastornos.

- **Manipulación de los datos de salida (OUTSIDERS)**

  Este es el último paso, una vez llevadas a cabo las dos acciones anteriores, lo que queda es la transmisión de los datos por medio de impresión o actualización, esta es una de las formas de ejecución más complejas de detectar.

c. Suplantación de páginas electrónicas

Regulado en el artículo 233 del Código Penal Costarricense, esta modalidad de delito es utilizada para la captura de identidades, de información personal, de claves de acceso o para vulnerar la seguridad de los sistemas, el ciberdelincuente clona una página y espera a que esta sea accesada por el usuario, con la creencia de que está accediendo a un sitio seguro, cuando no lo es.

Esta suplantación se lleva a cabo mediante las técnicas del “Phising” o el “Pharming”

d. El phising (pescando)

Por este medio no se vulnera la computadora, sino que se induce a la víctima a un engaño o confusión, mediante la clonación de una página de uso común, es una verdadera ingeniería social, donde no existe ataque de malware (programas maliciosos o malignos conocidos como troyanos), sino que, por desconocimiento o confusión, la persona ingresa a un sitio no deseado sin percatarse, es ahí en donde la víctima digita información personal y confidencial en esta página falsa, datos que luego son obtenidos por el ciberdelincuente y utilizados para sus fines delictivos.

e. El pharming

Se modifica el DNS (Domain name server o sistema de nombres de dominio de todos los usuarios) del equipo de la víctima, por medio de la implantación de un programa malicioso. Es una de las modalidades más peligrosas, pues no depende totalmente de la ingenuidad del usuario, sino que, el ciberdelincuente altera el sistema operativo, por medio del DNS que es donde se almacena toda la información asociada al propietario de la computadora (claves, bases de datos, información personal, etc.). Es una de las técnicas más sofisticadas y lo que realiza es una modificación del fichero hosts (elemento determinado del DNS), ahí el autor del ilícito nada más espera el momento en que el usuario acceda al sistema, para que se ejecute la acción programada, con lo cual finiquita el delito.

2.5. Tipos penales sobre delitos informáticos en Costa Rica

En Costa Rica nuestro Código Penal fue reformado en el año 2001 mediante la Ley 8148 que incluye los artículos 196 bis, 217 bis y 229 bis para reprimir y sancionar los delitos informáticos. Posteriormente, en el año 2012 se reforma nuevamente el Código Penal mediante la Ley sobre delitos informáticos y conexos (9048), que adicionó a esta norma la sección VIII del Título VII y modificó algunos de los artículos ya existentes, al considerar como delitos el sabotaje informático, la estafa informática, la suplantación de identidad, el espionaje informático, la suplantación de páginas electrónicas, entre otros.

Otras de las conductas que pueden considerarse como delito informático son: lectura, sustracción o reproducción de información confidencial, destrucción o uso no autorizado de programas de cómputo, alteración de los sistemas por la implementación de “virus” (caballo de troya o troyanos), modificación de datos, robo o fraude por medio de transferencias electrónicas, phishing (intentar adquirir información personal de manera fraudulenta: claves, datos confidenciales, etc.), así como difundir propaganda terrorista, entre otros, todos estos ejecutados por sujetos activos que van desde los denominados hackers (los más expertos) hasta los lamers (carentes de conocimiento pero intentan ser hackers) y donde el sujeto pasivo (quien recibe el agravio) puede ser cualquier persona o la sociedad en general.

Con la promulgación de la Ley N° 9048 (2012), se ubica a Costa Rica dentro de los niveles más importantes de regulación y combate de conductas delictivas del ciberespacio, en el ámbito Iberoamericano, al contar con una amplia legislación que permita la persecución y posible sanción de los ciberdelincuentes, máxime que a esto se le suma la reciente adhesión al Convenio de Budapest, tema que será ampliado más adelante.

2.5.1 Legislación derogada y vigente

El Código Penal Costarricense establece la mayor parte de la normativa sobre delitos informáticos, incluyendo las más recientes y significativas reformas realizadas en los años 2012 y 2013.

En las modificaciones realizadas en el año 2012 se incluyó el artículo 162 bis que refiere al turismo sexual, en este delito se sanciona con pena de cuatro a ocho años de prisión a la persona que proyecte al país, sea en el ámbito nacional o internacional, como un destino turístico accesible para la explotación sexual comercial o la prostitución y la razón de que se incluya dentro de los delitos informáticos, es que la norma señala la utilización de "*cualquier medio*", pudiendo tratarse de páginas web, redes sociales u otros afines. Esta reforma se realizó con la finalidad de penalizar la trata de personas y el tráfico ilícito de migrantes.

También fue reformado el artículo 167 que refiere a la corrupción de personas menores de edad o incapaces, al agravar la pena (cuatro a diez años de prisión) si el actor utiliza las redes sociales o cualquier otro medio informático o telemático (aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computarizada, definición según el Diccionario de la Real Academia Española), incluso si la víctima da su consentimiento.

En el año 2013, mediante la ley N° 9135, se adiciona el artículo 167 bis que se titula "*Seducción o encuentros con menores por medios electrónicos*", al reprimir con pena de prisión de uno a tres años a quien establezca comunicaciones de contenido sexual con personas menores de quince años o a quien al suplantar una identidad o utilizar una falsa, procure establecer una comunicación de este tipo, por cualquier medio, con una persona menor de edad (menor de 18 años) o incapaz. Es precisamente la implementación de la frase "por cualquier medio", la que permite tipificarse como un delito informático, máxime que la norma refiere a la posible inclusión de imágenes, videos o audios, difundibles por medios electrónicos o informáticos.

Por medio del artículo 173 el cual también fue reformado en el año 2013, se sanciona la fabricación, producción o reproducción por cualquier medio, de materia pornográfico infantil y el numeral 174 modificado ese mismo año, se establece una pena privativa de libertad que oscila entre los tres y siete años o su agravante de cuatro a ochos años, para la persona que difunda, distribuya, exhiba pornografía a menores de edad o incapaces o a quien comercialice de alguna manera material pornográfico, al utilizar cualquier medio (puede ser electrónico o informático) y el ordinal 174 bis que sanciona con pena de prisión de seis meses a dos años a la

persona que posea, produzca, venda, distribuya, exhiba o facilite dicho material, donde personas adultas simulen ser menores de edad y realicen actividades sexuales o su representación se realice por medio de caricaturas, imágenes o dibujos.

Los artículos 196 Violación de correspondencia o comunicaciones en su inciso b); 196 bis Violación de datos personales; 214 Extorsión; 217 Estafa informática; 229 Daño agravado en el inciso 6); 229 bis Daño informático y 295 Espionaje, fueron modificados mediante la Ley 9048, adecuándolos de manera tal, que puedan ser aplicados en la normativa de delitos informáticos. En cuanto a los artículos 229 ter Sabotaje informático; 230 Suplantación de identidad; 231 Espionaje informático; 232 Instalación o propagación de programas informáticos maliciosos; 233 Suplantación de páginas electrónicas; 234 Facilitación del delito informático; 235 Narcotráfico y crimen organizado y 236 Difusión de información falsa, son los nuevos delitos agregados al Código Penal, por la ley referida.

Esta reforma realizada en el año 2012, deroga el artículo 217 bis “fraude informático”, por referir a la estafa informática como tal y además, porque solo aludía al procesamiento de los datos y la salida de estos, pero no contemplaba su ingreso, uno de los momentos más importantes en el momento de la configuración del ciberdelito. El numeral supra citado se modifica, pasando a regular en la actualidad la “estafa informática”. Este tipo penal incorpora muy asertivamente los verbos “influir” y “modificar” que su antecesor no contemplaba, al ampliar la cobertura de las acciones del autor.

Por su parte, la Ley General de Aduanas en su título X, capítulo II hace referencia a los delitos informáticos por medio de sus numerales 221 y 222, al sancionar con una pena privativa de libertad entre uno y tres años o tres y cinco años (agravante) a quien acceda sin autorización a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas; se apodere copie, destruya, altere, facilite, transfiera, sin autorización, cualquier base de datos (que sea de uso restringido); dañe los componentes físicos o materiales, máquinas o accesorios, con el fin de entorpecerlas u obtener beneficio para sí o para otras personas o si facilita el uso de código o clave de acceso asignado para ingresar a dichos sistemas informáticos, sea dolosa o culposamente.

El Código de Normas y Procedimientos Tributarios sanciona en el artículo 94 el acceso desautorizado a la información o bases de datos, sea de forma directa o por autoría mediata, al imponer pena de prisión desde tres hasta seis años (la máxima). Además, el ordinal 95 establece penas de prisión que van desde los cinco hasta los diez años, a la persona o personas que realicen un manejo indebido de la información (sin autorización), sea apoderándose, copiándola, destruyéndola, inutilizándola, alterándola, conservándola o transfiriéndola, si la misma no es de uso público, es decir, que se haya declarado su restricción mediante una resolución administrativa.

De igual manera, la norma supra citada sanciona por medio de los artículos 96 y 97 al funcionario o funcionarios públicos (delito especial) que faciliten su código o clave de acceso, pudiendo hacerlo con dolo o culpa, al establecer una pena de prisión entre los tres a cinco años si el delito es doloso y de seis meses a un año si es culposo.

Finalmente, la Ley de la Administración Financiera de la República y Presupuestos Públicos, regula en su ordinal 111 el delito informático, al sancionar con uno a tres años de prisión a los funcionarios públicos o particulares que realicen acciones ilícitas contras los sistemas informáticos de la administración financiera y de proveeduría, sea apoderándose, copiando, destruyendo, alterando, transfiriendo o manteniendo en su poder, sin la autorización correspondiente, la información de programas o bases de datos, cuyo uso haya sido establecido como restringido. De igual manera, se sanciona la conducta que busque causar un daño doloso a los componentes físicos, máquinas o accesorios de los sistemas informáticos o que se facilite a terceras personas la clave de acceso o el código personal que permita el acceso a estos sistemas, para beneficio propio o de terceros

2.5.2. Reformas o implementaciones actuales

Para complementar la normativa existente, Costa Rica mediante el Proyecto N° 18484, presentado en el año 2012 ante la Asamblea Legislativa, se adhiere el 19 de mayo del 2017 al Convenio de Budapest (convenio sobre ciberdelincuencia), constituido en noviembre del 2001 por el Consejo de Europa en Estrasburgo y que comprende a más de 30 países desarrollados como Dinamarca, Francia o Estados

Unidos y les permite cooperar para buscar pruebas o investigar delitos. Este convenio busca hacer frente a los delitos informáticos, mediante una idea de armonizar las leyes internacionales. Es el primer tratado internacional sobre este tema, que procura la aplicación común de las normas penales, donde cada Estado firmante se compromete a transponer la lista de delitos que lo conforman a su propia legislación, al proteger a la sociedad del cibercrimen, su objetivo, la aplicación de una ley de delitos informáticos sin fronteras.

"…*Es un instrumento fundamental en la lucha contra el cibercrimen, al agilizar la asistencia mutua entre diversos países para el enfrentamiento de delitos informáticos, dado que su naturaleza y complejidad tecnológica, es en muchos casos un crimen transfronterizo*…", dice Edwin Estrada, Viceministro de Telecomunicaciones. (Recuperado el día 9 de marzo del 2018, al ser las 7;37 pm, de la página hhttps://www.elfinancierocr.com/economia-y-politica/costa-rica-enfrenta-el-cibercrimen-con-armasoxidadas/RIDQNOWPORGAJEES3DRE7KKEPE/story/)

Lo anterior constituye un paso muy importante y un gran avance para el país en el tema de persecución de los delitos informáticos, sin embargo, la normativa costarricense no contempla un apartado para efectuar este tipo de intercambios de pruebas o cooperaciones entre países, por lo cual, esto podría significar un obstáculo en el momento de querer hacer efectivo el convenio.

Como se puede observar, la regulación en Costa Rica, respecto de los delitos informáticos es sumamente amplia y está en constante actualización, al implementar nuevo personal encargado de investigar este tipo de ilícitos, equipo forense modernizado y normativa que permita la persecución de los ciberdelincuentes, aún fuera de las fronteras nacionales.

2.5.3. Creación de la Sección de Delitos Informáticos del OIJ

Actualmente se cuenta con una Sección de Delitos Informáticos del Organismo de Investigación Judicial, la cual da inicio en el año 1996, debido a que, los funcionarios de la Sección de Soporte Técnico del Poder Judicial, eran solicitados constantemente por otras secciones del OIJ, con el fin de ayudarlos en

allanamientos para decomisar equipo de cómputo o sacar copias de respaldo de la información o analizar la contenida en los equipos decomisados.

A raíz de lo anterior, el 16 de diciembre de 1996 en sesión de la Corte Plena, se aprobó la creación de dos plazas de "Investigador de Delitos Informáticos" a partir del 1° de enero de 1997, las cuales serían otorgadas al Departamento de Investigaciones Criminales del OIJ. (Recuperado el día 9 de marzo del 2018 al ser las 8:04 pm de la página https://www.poder-judicial.go.cr/oij/index.php/comunicacion/noticias/avisos-y-noticias-policiales/item/3864-seccion-de-delitos-informaticos)

Posteriormente, en abril de 1997, se crea la Unidad de Investigación Informática y en enero del 2002 esta unidad cambia su nombre a Sección de Delitos Informáticos, la cual funge actualmente, siendo una de las más antiguas de América Latina. Cabe destacar, que en un inicio las herramientas utilizadas eran poco eficaces para la recuperación de datos.

En la actualidad, esta sección “mantiene técnicas de computación forense alineadas con estándares internacionales, para la recolección, preservación y análisis de indicios, al garantizar la cadena de custodia de los mismos, sean computadoras, teléfonos celulares, u otras unidades de procesamiento y almacenamiento de datos”. (Recuperado el día 9 de marzo del 2018 al ser las 8:04 pm de la página https://www.poder-judicial.go.cr/oij/index.php/comunicacion/noticias/avisos-y-noticias-policiales/item/3864-seccion-de-delitos-informaticos)

El personal que labora en esta Sección está conformado por una Jefatura (el MSc. Erick Lewis), 2 supervisores, 19 profesionales en Informática y 2 asistentes administrativos.

Dentro de los casos más destacados investigados por la Sección de Delitos Informáticos se encuentra el cierre del Banco Anglo, así como, casos de fraudes registrales en el Registro Nacional, fraudes en licencias y pasaportes e infracciones a la ley de derechos de autor.

Según información que se encuentra en la página oficial del OIJ, indica que, en la Sección de Delitos Informáticos se tramitan causas como:

- Estafas Informáticas
- Sabotaje Informático
- Tenencia, Difusión y Producción de Pornografía Infantil
- Suplantación de Identidad en Internet
- Violación a las Comunicaciones Electrónicas
- Violación de Datos Personales
- Amenazas por Medios Electrónicos
- Extorsiones a través de Internet
- Secuestros de Personas donde han mediado comunicaciones digitales
- Solicitudes de rescates pagando con moneda digital
- Cualquier otro delito que utilice la tecnología para su comisión.

2.6. Delitos informáticos más comunes en Costa Rica

Los delitos informáticos más denunciados en Costa Rica, según información suministrada en el diario digital El Financiero, en abril del 2017 son:

2.6.1. La suplantación de identidad en redes sociales

Tercer delito más denunciado en Costa Rica, se regula en el ordinal 230 del Código Penal, adicionado mediante la Ley N° 9048 aprobada en el año 2012 y reformado en el año 2013, donde su protección se amplió a las personas jurídicas y las marcas comerciales.

Los medios digitales permiten la creación de diferentes identidades, es decir, una persona jurídica o comercial podría tener varios perfiles en una red social, siendo siempre la misma persona, pero con diferentes fines u objetivos, diferenciando áreas o departamentos que la conforman.

Esta nueva forma de publicidad utilizada por las empresas o comercios es un medio idóneo para los ciberdelincuentes, quienes con imágenes y logotipos falsos (o tomados de las páginas originales), logran crear nuevos perfiles falsos,

haciendo creer a las víctimas que están ingresando a una página oficial, todo con la finalidad de procurar estafas, obtención de datos personales o información confidencial e inclusive, la proliferación de programas maliciosos.

Es decir, mediante esta práctica, el cibercriminal crea una página falsa utilizando logos o imágenes obtenidas de las páginas oficiales de personas físicas o jurídicas o empresas comerciales, para engañar a las víctimas, quienes ingresan a estos perfiles sin conocer del engaño y proceden a compartir información personal o confidencial o en su defecto, podrían descargar programas maliciosos que ocasionen daños en sus equipos de cómputo.

Es muy común observar como aparecen en las redes sociales, principalmente en Facebook, concursos de reconocidas marcas comerciales, como automóviles, viajes u otros, donde se solicita compartir la publicación para así, poder participar en la rifa; este tipo de concursos en su mayoría son falsos y lo que buscan es la recopilación de datos confidenciales, sin embargo, las personas no son cuidadosas y en su mayoría, caen en este tipo de engaños, lo cual queda demostrado en la cantidad de veces que se comparte el anuncio, sin que se haya verificado la veracidad del mismo. La mayor problemática en el caso de los ilícitos en Facebook, es que las oficinas se encuentran en Estados Unidos, y se hace más difícil la investigación del delito.

También son frecuentes las suplantaciones de identidad de figuras públicas como, artista, jugadores de futbol, políticos, entre otros, a los cuales se les atribuyen actos falsos con la finalidad de lesionar su honor o aprovecharse de su reputación.

Ante esta situación y por lo difícil que resulta distinguir una página oficial de una suplantada, lo recomendable es no compartir ningún tipo de datos que puedan dar pie a la ciberdelincuencia para la consecución de sus delitos, estando siempre prevenidos, pues el cibercriminal en muchas ocasiones logra incluso la alteración de páginas o perfiles oficiales, para la comisión de sus estafas u otros ilícitos.

2.6.2. La violación de las comunicaciones electrónicas o accesos no autorizados al correo electrónico u otras cuentas

Regulado en el numeral 196 del Código Penal, penaliza la conducta de acceder a las comunicaciones privadas, en este caso, por medios electrónicos, con lo cual, podría ocasionar daños a la víctima, al conculcar su intimidad y privacidad.

Como acceso no autorizado se puede entender el uso de cualquier recurso informático o acceso a la red, sin autorización del titular.

Por lo general, el ciberdelincuente utiliza esta modalidad de delito, con el fin de interceptar correos electrónicos y apropiarse de información confidencial e importante, pudiendo incluso obtener datos de personas físicas o jurídicas o empresas comerciales, los cuales en poder de la competencia pueden ser utilizados para ocasionar serios agravios financieros o de cualquier índole.

Pero este delito no siempre es perpetrado por cibercriminales, sino que, es muy común que la violación de comunicaciones se presente en el nivel de pareja, en donde alguno o ambos intenten acceder a conversaciones (WhatsApp) o correos electrónicos, máxime si se sospecha de una infidelidad; lo cual, también configura delito.

Son consideradas delitos las siguientes acciones. Pagar u ofrecer pago a un tercero para que conculque las comunicaciones de una persona, hacer respaldos o ingresar a comunicaciones privadas sin autorización del titular e incluso, compartir “pantallazos” de conversaciones sostenidas en WhatsApp sin autorización de su emisor, si con esto peligra o se daña su intimidad y la comunicación difundida carezca de un interés público.

2.6.3. El robo de datos personales

El robo de la identidad virtual se ha vuelto tan común como en el mundo real y esto se genera en su mayoría, porque las personas aún no aprenden a proteger sus datos personales.

La sociedad costarricense tiende a ser sumamente confiada, comparte con mucha facilidad información confidencial, pese a que, de manera constante, las entidades bancarias y otros afines, previenen por diferentes medios, de los peligros que se generan en la red como consecuencia de la ciberdelincuencia.

Este tipo de delito se comete principalmente con el fin de utilizar los datos personales de la víctima, para obtener créditos, contratar servicios, comprar artículos o simplemente para manchar el honor de una personas física o jurídica.

Algunos de los métodos utilizados por los cibercriminales para el robo de datos personales son: anuncios de participación en rifas virtuales (por lo general solicitan datos personales); promesas de becas u otras comodidades de estudio; avisos de empleos, ofrecimiento de premios gratis, contribuciones de caridad falsas.

También es frecuente recibir llamadas telefónicas de personas que afirman ser funcionarios de una entidad bancaria (por lo general en donde la víctima es cliente) e indican que, surgió un problema con su cuenta y que necesitan actualizar algunos datos personales para poder regularizar la gestión y es aquí, en donde la víctima en la mayoría de las ocasiones cae en la trampa y facilita los datos confidenciales e incluso hasta las claves de las cuentas o tarjetas de débito o crédito, se reitera, pese a que, son múltiples los anuncios y las advertencias de no facilitar información personal por teléfono, correo electrónico o cualquier otro medio.

2.6.4. Compras indebidas por Internet

Lo más común son los fraudes con tarjetas de débito o de crédito; esto se logra por medio de páginas falsas, en donde la víctima cree estar ingresando a la página oficial y decide realizar alguna compra por Internet, para lo cual digita la información de la tarjeta, sin darse cuenta que con esto está facilitando la información al ciberdelincuente, quien a su vez, la aprovecha para realizar compras indebidas.

"…Datos de Nilson Report indican que las pérdidas mundiales por fraude con tarjetas se elevaron a más de US$21.000 millones en 2015, frente a los 8.000 millones de dólares registrados en 2010. Para 2020, se espera que la cifra llegue a los US$31.000 millones…". (Recuperado el día 10 de marzo del 2018 al ser las 11:05 am de la página http://www.bbc.com/mundo/vert-cap-40638275)

Las compañías de tarjetas de crédito o débito se ven afectadas, pues en la mayor cantidad de veces, deben de realizar reembolsos a los clientes que han sido víctimas del atraco.

Estos fraudes pueden realizarse teniendo el delincuente la tarjeta en su poder o no, sea, por el robo físico de la misma o por el almacenamiento de su información. El problema que genera este tipo de delito, es que una vez autorizada la compra, el dinero se desembolsa casi de forma inmediata de la cuenta, solo siendo posible que se deniegue la transacción en caso de insuficiencia de fondos o por sospechas del emisor de que se esté perpetrando un delito.

Las compras por Internet han venido a facilitar enormemente la vida de las personas, cada vez es más sencillo poder adquirir productos en otros países, los cuales son pagados en línea y remitidos a un casillero físico en su propio país. Sin embargo, no todas las compras son seguras, por lo cual, se debe de tener mucho cuidado antes de dar el enter definitivo, verificando si la página web mediante la cual se está realizando la compra es oficial (siempre deben de comenzar con "https://" que constituye un protocolo de comunicación para la transferencia segura de datos).

Las cinco formas más comunes de fraude de tarjetas de crédito y de débito son clonación, robo de identidad, phishing (“pescando”, puede aparecer como spam, con el fin de averiguar los datos y se hace frecuentemente por medio de las cuentas de correos electrónicos), hacking (realizado a través de programas malignos o virus troyanos, que se autoinstalan en la computadora con el fin de copiar datos de cuentas y reenviarla al ciberdelincuente) y smishing (similar el phishing pero utilizando mensajes de texto SMS).

Otros tipos de delitos comunes refieren a la divulgación de material ilegal, modificación de los programas existentes o inserción de nuevos programas o rutinas (virus y gusanos), fraude bancario, espionaje informático e incluso ataques de naturaleza militar a las plataformas informáticas de cualquier país (ciberguerra), etc. (Recuperado el día 10 de marzo del 2018 al ser las 11:05 am de la página http://www.bbc.com/mundo/vert-cap-40638275)

Casos atendidos por la Sección de Delitos Informáticos en Costa Rica
Los tipos penales marcados en gris corresponden a los delitos Informáticos y no corresponden al original.

Delitos Atendidos

Delito	2011	2012	2013	2014	2015 Mayo, 20
Delitos Sexuales contra Menores	31	32	50	36	26
Alteración de Datos y sabotaje Informático	2	2	1	0	1
Amenazas	17	22	9	12	3
Estafas	27	56	71	37	10
Extorsión	11	11	3	8	1
Fraude Informático	190	84	217	64	31
Homicidio	15	12	1	1	4
Legitimación de Capitales	8	2	7	7	0
Violación de las comunicaciones Electrónicas	43	43	56	51	44
Falsedad Ideológica	5	10	20	13	4
Suplantación de Identidad			25	15	9

Fuente: OIJ, Sección de delitos Informáticos.

2.7. Delitos informáticos como delitos de peligro abstracto

No se puede abordar el tema de los ciberdelitos, sin indicar, primeramente, que estos delitos están dentro de los que se catalogan como “Delitos de peligro abstracto”, pues no es necesario que se dé un resultado lesivo, sino que se conforman con solo el hecho de poner en peligro un bien jurídico tutelado. Según el alemán Claus Roxin, los delitos de peligro abstracto se definen como: *“... aquellos en los que se castiga una conducta típicamente peligrosa como tal, sin que en el caso en concreto tenga que haberse producido un resultado de puesta en peligro*”.

Desde una conceptualización u óptica más amplia, se puede decir que los delitos de peligro abstracto son “delitos de obediencia”, es decir, existe un tipo penal

que prohíbe una conducta, por lo tanto, las personas deben de motivarse en la norma y abstenerse de llevar a cabo dicha acción, sino lo hacen, aunque no pongan en peligro el bien jurídico tutelado, ya se configura el delito y por ende es aplicable la respectiva sanción, se da una mayor valoración del desvalor de la conducta en función del desvalor del resultado.

Pero, la presencia de un delito de peligro abstracto se denota precisamente, cuando la conducta es inherente a la puesta en peligro de los bienes jurídicos tutelados, refiérase al ámbito de los intereses difusos (intereses supraindividuales, generales, colectivos y comunitarios).

Los delitos de peligro abstracto se caracterizan porque sobrepasan un riesgo permitido, lo cual puede provocar daños cuantiosos a la sociedad, al no poderse determinar el número potencial de personas a las que pueden afectar. Madrigal (2015) en su ensayo "Delitos de peligro abstracto" publicado en la Revista Judicial, Costa Rica, N° 115 indica: "*Los delitos de peligro abstracto son siempre delitos de mera actividad cuya punición descansa en la peligrosidad general de la acción típica para un determinado bien jurídico, según la valoración del legislador*".

Entonces, se puede decir que, en los delitos de peligro abstracto el resultado es la propia acción del autor, quien realiza el tipo penal, siendo suficiente que se compruebe que el autor llevó a cabo la acción típica sin que sea necesario verificar la lesión o el peligro generado al bien jurídico tutelado, sino simplemente la producción de un peligro.

Por otro lado, Bacigalupo (1984) nos dice que: "…La teoría ha distinguido tradicionalmente entre los delitos de peligro concreto, en los que el bien jurídico debe haber sufrido un riesgo real de lesión, y los delitos de peligro abstracto, en los que ese riesgo real no es necesario…". (pp. 101-102)

De lo anterior se puede concluir, que los delitos de peligro abstracto son aquellos que se configuran en el momento mismo en que el bien jurídico tutelado corrió el riesgo de ser lesionado, sin que sea necesario que se demuestre dicho peligro (tutela anticipada del bien jurídico), no obstante, admiten la prueba en contrario, donde se puede demostrar que nunca existió tal peligro.

Son muchos los que sostienen que este tipo de delitos violenta el principio de lesividad, mismo que exige que se produzca el daño para que la conducta sea punible y hasta que se invierte la carga de la prueba, debiendo el infractor demostrar que no puso en peligro el bien jurídico tutelado, conculcando así el principio de inocencia.

Se recalca que, lo que la legislación trata de proteger en el caso de este tipo de delitos es el peligro al que se pueden exponer estos bienes jurídicos tutelados y la repercusión patrimonial que puedan generar estos agravios, por esto mismo es que también se analizan desde el punto de vista del Derecho Penal Económico.

Diferentes periódicos nacionales han publicado notas sobre casos de ciberdelincuencia en nuestro país, por ejemplo, en setiembre del 2013 se dio a conocer la noticia de un hacker que ingresó a la plataforma en línea del Banco Davivienda y modificó el tipo de cambio del dólar, con lo cual logró comprar y vender esta moneda, sustrayendo 200 millones de colones en un lapso de cuatro meses. El principal sospechoso es un hombre de 26 años y junto con él fueron detenidos siete personas más y todos enfrentan cargos por fraude informático.

Uno de los casos más publicitados es la detención de un estudiante de la Universidad Nacional, en el año 2015 a solicitud del FBI, por estar vinculado a una red mundial de ciberdelincuentes.

No todas las intromisiones ilegales a los diversos sistemas informáticos tienen la finalidad explícita de ocasionar un delito, es decir, que el infractor busca beneficiarse a sí mismo o a un tercero en el aspecto patrimonial, sea desviando dineros a otras cuentas u obteniendo información privada que posteriormente puede vender a un interesado, hay quienes accesan a estos sistemas por meros retos o diversión, para demostrar sus destrezas. Lo cierto de todo esto es, que exista o no el ánimo de causar un perjuicio, los delitos informáticos se consideran de peligro abstracto porque violentan la privacidad, intimidad, buena fe, seguridad, entre otros bienes jurídicos, con el solo hecho de ingresar a un lugar sin la debida autorización, independientemente de que se cause un perjuicio directo o un resultado dañoso.

La lista de casos conocidos no solo en el nivel nacional sino también en el nivel mundial es interminable, la delincuencia alcanzó el ciberespacio y así como es de difícil mitigarla en el mundo físico lo es en el mundo virtual, donde suele haber desproporción entre las conductas del ciberdelincuente y la legislación que las sanciona, pues la mayor parte de las veces esta última se encuentra rezagada años luz, porque quienes se dedican a este tipo de ilícitos tienen en la mayoría de las ocasiones, grandes conocimientos informáticos y ya solo con eso llevan una considerable ventaja.

2.8. Falta de prevención de los cibernautas

Existe un gran desconocimiento de las personas en cuanto al tema de delitos informáticos, lo que facilita a los ciberdelincuentes la comisión de los hechos ilícitos. Los usuarios fácilmente comparten información y datos personales en tiempo real, dado que, no son conscientes del peligro que esto significa debido a la gran variedad de delitos que existen en la red.

En el nivel mundial, se utilizan modalidades de ciberdelitos como los secuestros de datos o información confidencial de personas físicas y jurídicas, donde los más comunes son: ransonware que se aplica por medio de la implementación de un programa malicioso y el compromiso del correo electrónico comercial o fraude sofisticado, donde los ciberdelincuentes pueden accesar a información sensible, como el pago o transferencia de fondos, consistiendo en una nueva forma de phishing donde se imitan páginas de empresas reconocidas.

Otra situación que lleva a que los cibernautas sean víctimas de la ciberdelincuencia es su confianza de que nunca sufrirán un ataque de este tipo y esto se demuestra con la cantidad de información personal que comparten en las redes sociales; fotografías de automóviles, sus casas, sus vacaciones (donde además, se indica que anda toda la familia, dando a conocer que su casa quedó sola); todo esto ayuda a actualizar las bases de datos de los ciberdelincuentes, pues se puede determinar situación social, estatus económico, lugar de trabajo, entre otros detalles personales. Todo lo que se comparte en las redes sociales se convierte en información pública, el cibernauta pierde control sobre ella y no tiene límites de fronteras, equivale a ubicarse en una plaza pública a entregarle a desconocidos cualquier tipo de datos personales o fotografías.

Los cibercriminales utilizan muchos métodos para delinquir, que van desde la creación de páginas falsas en donde se solicita información personal como claves dinámicas o contraseñas hasta la identificación de estas contraseñas, debido a que, las mismas no son suficientemente seguras o el ingreso de los cibernautas en redes públicas, las cuales son fácilmente hackeadas.

Según información suministrada por el diario digital El Financiero, en el año 2016 hubo un incremento en las denuncias de los delitos informáticos del 33% con relación con el año 2015. (Recuperado el día 9 de marzo del 2018, a las 10:18 pm de la página https://www.elfinancierocr.com/tecnologia/ciberdelincuentes-se-alimentan-de-las-redes-sociales/FUGB3DB6UZHDLNZDFJLKJSIPSY/story/)

En cuanto a las empresas, en el 2016 se indica que un 45% sufrió de ataques informáticos, lo que equivale a casi la mitad de las existentes. Esto puede provocar mal funcionamiento en servicios básicos e incluso, se conoció la noticia de un hotel en el extranjero, en donde los ciberdelincuentes bloquearon todas las llaves de las habitaciones, lo que provocó que los huéspedes no pudieran ingresar, causando un caos durante varias horas. (Recuperado el día 9 de marzo del 2018, a las 10:46 pm de la página https://www.elfinancierocr.com/economia-y-politica/costa-rica-enfrenta-el-cibercrimen-con-armas-oxidadas/RIDQNOWPORGAJEES3DRE7KKEPE/story/).

El Banco Interamericano de Desarrollo (BID) categoriza tres tipos principales de delitos informáticos:

Delitos tradicionales. Aquellos relacionados con los delitos que se realizan fuera de la nube. Se incluye el fraude o la falsificación, cuando son cometidos por medio de formas electrónicas.

Publicación de contenidos. Incluye la divulgación de materiales ilegales a través de medios electrónicos, como la pornografía infantil, el ciberbullying (acoso en Internet) y divulgación de datos privados, entre otros.

De naturaleza electrónica específica. Ataques contra sistemas de información, denegación de servicio (ataques a sistemas o páginas web para impedir que sean accesibles a usuarios) y piratería informática. (Recuperado el día 9 de marzo del 2018, a las 10:46 pm de la página

https://www.elfinancierocr.com/economia-y-politica/costa-rica-enfrenta-el-cibercrimen-con-armas-oxidadas/RIDQNOWPORGAJEES3DRE7KKEPE/story/).

Por su parte, el ciberdelincuente tiene la ventaja de que no requiere ser un experto en informática para cometer un delito informático y generalmente suelen ser amables e inspiran confianza, aunado al hecho de que, se pueden ubicar en cualquier lugar, lo cual, dificulta su captura y si a esto le sumamos que las páginas de gobierno permiten el acceso a datos personales de sus administrados (Registro Civil, Registro Nacional, entre otros), el ambiente para delinquir se vuelve sumamente amigable.

En la mesa redonda “Los delitos informáticos en Costa Rica” llevada a cabo en el año 2011, el Dr. Carlos Chinchilla explicó que: *“…en los sistemas informáticos hay tres fases importantes: el ingreso, procesamiento y salida de información. Está comprobado estadísticamente, que el 85% de los ataques cibernéticos ocurren en la primera etapa…*”. Para ese entonces, nuestra legislación solo contaba con regulación en las etapas de procesamiento y la salida de datos, no obstante, con la reforma a la ley en el año 2012, se logró implementar la sanción, al configurar como delito también la primera etapa “el ingreso de los datos”.

Expuesto lo anterior, se puede concluir que en Costa Rica existe regulación suficiente en materia de delitos informáticos, además, hay una Sección del OIJ dedicada a la investigación de este tipo de hechos delictivos, no obstante, hasta que los cibernautas no aprendan a protegerse ni utilicen de forma segura la red, seguirán siendo víctimas de la ciberdelincuencia.

CAPÍTULO III: METODOLOGÍA

3.1. El paradigma, el enfoque metodológico y el método seleccionado

Con la finalidad de establecer un mejor parámetro de interpretación, se ha realizado el presente trabajo mediante el método de investigación “descriptivo”, al analizar cuáles han sido las principales causas que llevaron a las personas a ser víctimas de un delito informático.

Dicho análisis tendrá como base la información recopilada y las estadísticas que refieren a este tipo de delitos, buscando identificar los motivos más comunes que conllevan a la perpetración del hecho ilícito, es decir, las causales más frecuentes, utilizadas por los ciberdelincuentes.

(Ary, 1990, pág. 55) refiere sobre el tema:

> “…La investigación descriptiva es una etapa preparatoria del trabajo científico que permite ordenar el resultado de las observaciones de las conductas, las características, los factores, los procedimientos y otras variables de fenómenos y hechos. El tipo de investigación no tiene hipótesis explícita...”.

De lo anterior se colige que, la investigación descriptiva lo que pretende es realizar una efectiva interpretación de las causas por las cuales las personas son víctimas de delitos informáticos, al indagar cuáles son los métodos más utilizados por los autores de este tipo de hechos ilícitos, con el fin de concluir, si en realidad existe una falta de seguridad o de prevención de los cibernautas.

El enfoque metodológico por aplicar será el cualitativo, por tratarse de una Ciencia Social, lo cual permite determinar o definir la naturaleza del conocimiento y de la realidad de estos tipos penales. Su objetivo es describir las cualidades de un hecho, considerándolo como un todo, aproximándose a las fuentes de su investigación, pero no con el fin de probar alguna teoría o hipótesis sino más bien para generarlas.

Su elemento principal es la interacción con las personas objeto de la investigación, que en el presente caso refiere a las víctimas de delitos informáticos.

(Rodríguez, 1996, pág 32) conceptualiza la investigación cualitativa como:

> "…Estudia la realidad en su contexto natural, tal y como sucede, intentando sacar sentido de, o interpretar los fenómenos de acuerdo con los significados que tienen para las personas implicadas. La investigación cualitativa implica la utilización y recogida de una gran variedad de materiales—entrevista, experiencia personal, historias de vida, observaciones, textos históricos, imágenes, sonidos – que describen la rutina y las situaciones problemáticas y los significados en la vida de las personas…".

Es importante indicar que, las investigaciones son procesos sistematizados que buscan resolver situaciones o problemas, mediante soluciones acordes con la realidad y el contexto de lo investigado.

3.2. Descripción del contexto o del sitio, en dónde se lleva a cabo el estudio.

El motivo de análisis es la problemática existente en materia de delitos informáticos, siendo que, en su mayor parte, los hechos ilícitos se configuran porque las víctimas se exponen en la red, pues navegan en Internet sin tener las debidas precauciones, compartiendo fotografías, datos personales e información que puede resultar peligrosa en manos de un delincuente. Además, existen complicaciones en cuanto al espacio utilizado por los ciberdelincuentes al momento de la comisión del hecho, por la circunstancia de que este tipo de delitos pueden ser realizados desde cualquier parte del mundo, lo que dificulta la persecución penal y, por ende, la sanción al autor del ilícito.

Pese a existir suficiente normativa sobre el tema, la cual se amplió con la promulgación en el año 2012 de la Ley de Delitos Informáticos y que fue modificada en el año 2013, lo que permitió la creación y adecuación de tipos penales en materia de delitos informáticos, la investigación de estos hechos ilícitos se vuelve un

desafío, máxime que de manera constante las tecnologías de información se modernizan, permitiendo la generación de nuevas actividades delictivas, lo cual obliga a los países a recurrir a otros métodos o instrumentos legales no solo en el nivel nacional sino multinacional, que permitan combatir la ciberdelincuencia, por medio de un convenio entre los Estados, donde se brinden un auxilio mutuo.

Por esta razón, el 23 de noviembre del 2003 se firma en Budapest el "Convenio Europeo sobre ciberdelincuencia", el cual entra en vigencia el 1 de julio del 2004, es el primer instrumento internacional, creado con la finalidad de combatir la tipicidad penal en materia de delitos informáticos.

Lo anterior permite que, los países que sean miembros del Consejo de Europa, cooperen ante las investigaciones de un ciberdelito, se reitera, por el hecho de que los mismos pueden ser cometidos desde cualquier parte del mundo y lo que se busca es dar una respuesta conjunta.

Además, no todos los Estados cuentan con regulaciones en este ámbito legal o los tipos penales creados en esta materia son escuetos o insuficientes, por lo cual, el Convenio supra citado permite uniformar criterios en cuanto al tema de los delitos informáticos.

Este convenio se divide en cuatro capítulos que son: 1. Definiciones; 2. Medidas que se sugieren en el nivel nacional; 3. Cooperación Jurídica Internacional y 4. Cláusulas finales y regula tipos penales como: delitos relacionados con pornografía infantil, tentativa y complicidad, fraude informático, interferencia de datos (este regulado parcialmente), entre otros.

Cuando un Estado que es invitado a adherirse al Convenio de Budapest no lo ratifica, se presume su falta de interés en perseguir la ciberdelincuencia, esto por cuanto, la esencia del delito informático es principalmente el crimen organizado.

Los países que se adhieren cooperan internacionalmente con el combate de la ciberdelincuencia y los que no lo hacen, pueden sufrir serios problemas en la persecución penal de los ciberdelincuentes.

Al respecto, en el año 2012 se presentó ante la Asamblea Legislativa el proyecto N° 18484, el cual fue aprobado el 19 de mayo del 2017, es decir, 5 años después de su presentación Costa Rica decide adherirse al "Convenio de Budapest", es el primer instrumento internacional en materia de delitos informáticos, que viene a complementar la normativa vigente y mejorar de este modo la lucha contra la ciberdelincuencia, pudiendo solicitarse colaboración a todas las jurisdicciones de los países adheridos, para la obtención de pruebas o investigación de ciberdelitos.

Según la Fiscalía de Delitos Informáticos de San José, en el años 2013 se recibieron 138 denuncias, en el 2014 la cantidad fue de 295 y en el 2015 bajó a 115, todas relacionadas con Violación de comunicaciones, Violación de Datos Personales, Sabotaje Informático, Suplantación de Identidad, Daño Informático entre otros, es difícil para el Organismo de Investigación Judicial o el Ministerio Público, la consecución de estas transgresiones a la norma penal, por lo cual, adherirse al Convenio de Budapest ha sido de gran importancia.

Eset Security Report quien realiza investigaciones y emite estadísticas sobre delitos informáticos en el nivel internacional, sitúa a Costa Rica en la sétima posición en cuanto a mayor cantidad de ataques cibernéticos a empresas e instituciones en el nivel latinoamericano, es sumamente vulnerable.

> Luis Paulino Mora Lizano, Viceministro de la Presidencia expresó:
> "…Con este proyecto se busca hacer frente en general a los delitos informáticos, de Internet, e incluso de propagación de mensajes racistas o xenófobos, mediante la armonización de las leyes de los Estados parte. Esperamos que este impulso en pro de la seguridad ciudadana continúe, y podamos tener pronto dentro de nuestra legislación otras herramientas, como la Extinción de Dominio, que se constituirían en verdaderos hitos en la lucha contra el narcotráfico, el terrorismo, el crimen organizado y el blanqueo de capitales…" (Recuperado el día 15 de febrero del 2018 a las 12:19 am de la página https://www.camtic.org/actualidad-tic/costa-rica-se-adhiere-a-convenio-contra-ciberdelincuencia/)

Este convenio también faculta la sanción penal a personas jurídicas, al superar el conocido principio de “societas delinquere non potest”, mismo que refería a la imposibilidad de atribuirles una responsabilidad penal subjetiva.

Por otra parte, establece procedimientos para la extradición (quedando a la facultad del país requerido); la anteriormente citada asistencia mutua y una serie de medidas que, de manera provisional, buscan la conservación de datos informáticos que se encuentren almacenados en diferentes equipos (soportes digitales) y permite a las autoridades judiciales, el acceso a pruebas y la colaboración en el proceso investigativo.

3.3. Las características de los participantes y las fuentes de información.

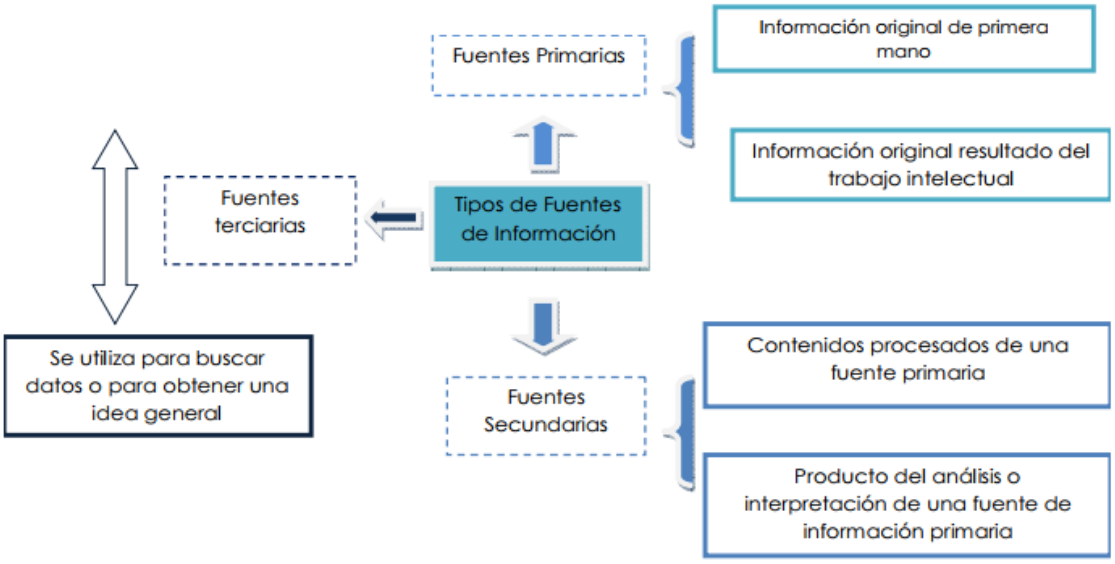
Las víctimas de delitos informáticos no cuentan con características particulares, es que, puede tratarse de cualquier persona física o jurídica. Por ende, se ha procurado entrevistar a una población variada en cuanto a edad, profesión u oficio, sexo, entre otros, con el objetivo de obtener información sobre el conocimiento de este tipo de hechos delictivos y de qué manera se protegen al momento de navegar en Internet.

Dado que, las entrevistas se realizan de manera directa a cada persona, se consideran fuentes de información primaria, pues los datos obtenidos corresponden al conocimiento o vivencias individuales, al derivar en un resultado, se reitera, primario y directo.

En cuanto a las demás fuentes de información consultadas, las mismas corresponden a monografías, ensayos, tesis, libros físicos y electrónicos, conferencias, revistas, diccionarios, estadísticas y todo aquel material necesario para recopilar los antecedentes y referencias necesarios para la elaboración del proyecto. Maranto (2015) define: “…Una fuente de información es todo aquello que nos proporciona datos para reconstruir hechos y las bases del conocimiento Las fuentes de información son un instrumento para el conocimiento, la búsqueda y el acceso de a la información. Encontraremos diferentes fuentes de información, dependiendo del nivel de búsqueda que hagamos...”. (Recuperado el día 15 de

febrero del 2018 a las 1:23 pm de la página http://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/16700/LECT132.pdf?sequence=1)

De la página web supra citada se obtiene el siguiente esquema que comprende los diferentes tipos de fuentes de información:



Concluye Maranto indicando que, la elección de fuentes de información para realizar una investigación, debe de comprender aspectos como: lectura, comparación y evaluación de la información recopilada, con el fin de obtener el material suficiente y poder realizar las comparaciones necesarias que permita emitir conclusiones o respuestas, según el tema a analizar.

3.4. Las técnicas e instrumentos para la recolección de los datos.

Para la recopilación de los datos expuestos en el presente trabajo, se requirió de una amplia investigación, al consultar textos legales, legislación aplicable, libros sobre delitos informáticos, audios de conferencias realizadas, material aportado en clases por los docentes y cualquier otro documento que comprendiera el tema por abarcar.

Además, se entrevistó a 15 personas de manera aleatoria, con el fin de determinar su conocimiento en materia de delitos informáticos y el grado de seguridad que aplican en el momento de navegar en la red. "*La entrevista no se considera una conversación normal, sino una conversación formal, con una intencionalidad, que lleva implícitos unos objetivos englobados en una Investigación."* (González, Peláez, Pérez, Rodríguez y Vásquez.p.2)

CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Una vez realizadas las entrevistas a las 15 personas, es necesario realizar un análisis de la información recopilada, la cual busca dar una respuesta al objetivo general planteado en el presente trabajo, sea, la falta de prevención de los cibernautas en los delitos informáticos.

Para una mejor comprensión de los resultados obtenidos en las citadas entrevistas, se realizan cuadros y gráficos, que muestran de manera concreta las respuestas facilitadas por las personas entrevistadas.

Aunado a lo anterior, se clasificó la información por temas que van enfocados en el conocimiento sobre qué es un delito informático, experiencia sobre compras por Internet, participación en redes sociales y apreciaciones personales sobre la falta de prevención al navegar en internet.

En lo que respecta al nivel de conocimiento sobre delitos informáticos, se consultó a las 15 personas si sabe qué es un delito informático (ítem 1) y el 100% respondió que sí.

Al preguntárseles si pueden nombrar 5 ejemplos de delitos informáticos el 27% respondió que sí, el 67% que no y un 6% señaló la casilla N/R (ítem 2).

En el ítem 3 se pregunta a las personas entrevistadas si conocen que existe una Ley de delitos informáticos en Costa Rica y el 80% responde que sí, el 13% que no y solamente un 7% marca la casilla N/R.

El 93% de las personas entrevistadas acepta haber realizado compras por Internet, pero solo un 60% las consideran seguras (ítemes 4 y 5).

Sobre las redes sociales (Facebook, twitter, whatsaap) el 93% participa en la actualidad en algún grupo de este tipo (ítem 6) y solo un 26 % admite que

acostumbra compartir fotografías (ítem 7) y un 6% ha brindado datos personales a un tercero (ítem 8).

Según el ítem 9, el 80% considera que la falta de prevención de los cibernautas, es una de las principales razones para ser víctima de un delito informático, pero solamente un 6% ha sido víctima en alguna ocasión de algún ilícito de este tipo (ítem (10).

Finalmente, se concluye la entrevista con las preguntas sobre el conocimiento en cuanto a la manera de actuar en caso de ser víctima de un delito informático (ítem 11), donde un 60% responde que sí versus un 40% que admite no saber qué hacer en este caso. Por su parte, un 34% indica que sí consideran que los instrumentos legales existentes en Costa Rica en la actualidad, son suficientes para llevar a cabo una efectiva investigación, en el caso de denunciar un delito informático (ítem 12), un 46% que no y un 20% marcó N/R.

Cuadro N° 1:
Cuestionario aplicado

	SI	NO	N/R
1. ¿Sabe qué es un delito informático?	15	0	0
2. ¿Puede mencionar 5 delitos informáticos	4	10	1
3. ¿Conoce que existe una Ley de delitos informáticos en Costa Rica?	12	2	1
4. ¿Ha realizado compras por Internet?	14	1	0
5. ¿Considera las compras de Internet seguras?	9	6	0
6. ¿Es parte de alguna red social como Facebook, twitter, whatsapp, etc.?	14	1	0
7. ¿Acostumbra subir fotos personales o de su familia a las redes sociales?	11	4	0
8. ¿Ha brindado información personal a terceros, como claves, números de tarjetas de crédito u otros?	1	14	0
9. ¿Considera usted que la principal razón de que una persona sea víctima de un delito informático es la falta de prevención cuando navega en la red?	12	3	0
10. ¿Ha sido víctima de algún delito informático?	14	1	0
11. ¿Sabe usted qué medidas debe de tomar si es víctima de un delito informático?	9	6	0
12. ¿Considera usted que existen los instrumentos legales suficientes para una efectiva investigación, en caso de denuncia de un delito informático?	5	7	3

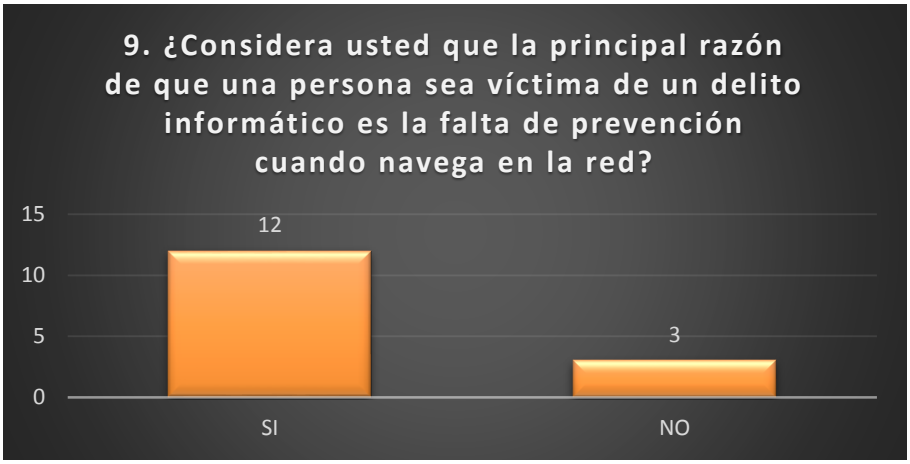
Gráfico N° 1

Análisis. Como puede observarse en este primer gráfico, un 67% de las personas entrevistadas no conoce al menos 5 tipos de delitos informáticos, pese a que el 100% de los entrevistados manifestó que sabe en qué consiste un delito de este tipo. Lo anterior, denota que, a pesar de existir una ley que sanciona dichos ilícitos, la misma no es consultada por los ciudadanos.

Gráfico N° 2

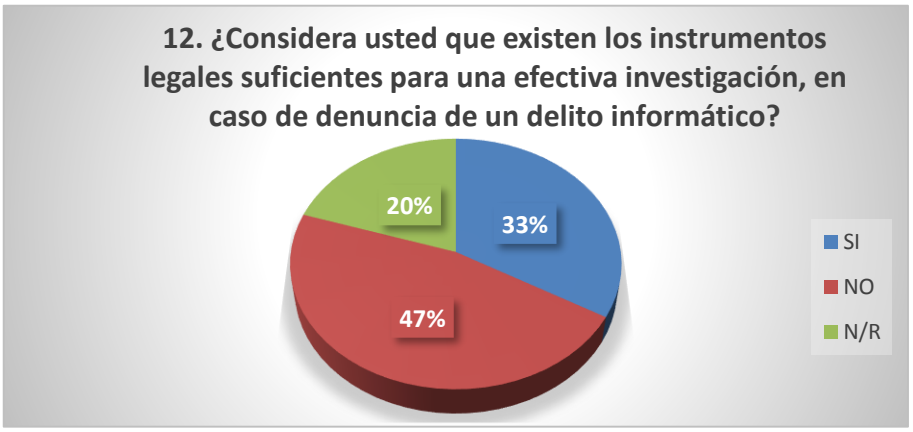
Análisis. De las 15 personas entrevistadas, 12 indicaron conocer que existe una Ley de delitos informáticos, sin embargo, retomando el gráfico anterior, se observa que, pese a conocer de la normativa, no es posible que logren identificar algunos de los delitos que dicha ley contempla.

Gráfico N° 3



Análisis. Según la entrevista realizada de manera aleatoria a 15 personas, la gran mayoría (12) coinciden en que la falta de prevención, es una de las principales razones por las que se puede ser víctima de un delito informático, lo cual, demuestra que, existe entre los cibernautas la noción de que deben tomar en el mundo virtual las mismas o mayores prevenciones que se toman en el mundo físico, para evitar ataques de los ciberdelincuentes.

Gráfico N° 4



Análisis. De este último gráfico se desprende que, el 47% de las personas entrevistadas consideran que, no existen en Costa Rica los instrumentos legales suficientes para combatir la ciberdelincuencia, sin embargo, es claro, según el ítem 2, que la mayoría que participó en la entrevista, desconoce la normativa vigente en materia de delitos informáticos.

Cuadro N° 2

Resultados obtenidos del análisis del contenido de la Reforma de la Sección VIII, Delitos Informáticos y Conexos (N° 9048) del Código Penal Costarricense

ARTÍCULO	OBSERVACIONES
162 bis: Turismo sexual	Adicionado mediante la Ley N° 9095
167: Corrupción	Modificado por la Ley N° 9048
167 bis: Seducción o encuentros con menores por medios electrónicos	Adicionado mediante la Ley N° 9135
173: Fabricación, producción o reproducción de pornografía	Modificado por la Ley N° 9177
174: Difusión de pornografía	Modificado por la Ley N° 9177
174 bis: Pornografía virtual y pseudo pornografía	Modificado por la Ley N° 9177
196 inciso b): Violación de correspondencia o comunicaciones	Modificado por la Ley N° 9048
196 bis: Violación de datos personales.	Modificado por la Ley N° 9048
214: Extorsión	Modificado por la Ley N° 9048
217 bis: Estafa informática	Modificado por la Ley N° 9048
229 inciso 6): Daño agravado	Modificado por la Ley N° 9048
229 bis: Daño informático	Modificado por la Ley N° 9048
229 ter: Sabotaje informático	Agregado mediante la Ley N° 9048
230: Suplantación de identidad	Agregado mediante la Ley N° 9048
231: Espionaje informático	Agregado mediante la Ley N° 9048
232: Instalación o propagación de programas informáticos maliciosos	Agregado mediante la Ley N° 9048
233: Suplantación de páginas electrónicas	Agregado mediante la Ley N° 9048
234. Facilitación del delito informático	Agregado mediante la Ley N° 9048
235. Narcotráfico y crimen organizado	Agregado mediante la Ley N° 9048
236: Difusión de información falsa	Agregado mediante la Ley N° 9048
295. Espionaje	Modificado por la Ley N° 9048

Fuente: Chacón, 2018.

Análisis. La reforma del 10 de julio del 2012, mediante la cual se incorporó al Título VII del Código Penal la Sección VIII “Delitos Informáticos y conexos” con 8 nuevos artículos, así como la modificación de otras 8 normas del mismo cuerpo normativo, viene a proteger de manera considerable a las personas en materia de delitos informáticos, contemplándose en total 16 numerales que regulan este tipo de hechos ilícitos.

Cuadro N° 3
Tipos penales regulados en el Convenio de Budapest

BUDAPEST	CÓDIGO PENAL	ESTADO
Interferencia en el Sistema (Art. 5)	229 bis y 229 te	Regulado
Fraude Informático (Art. 8)	217 bis	Regulado
Delitos relacionados con pornografía infantil (Art. 9)	167, 167 bis, 173, 173 bis, 174 y 174 bis	Regulado
Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Art. 10	Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual	Regulado
Tentativa y complicidad (Art. 11	24, 73 y 74	Regulado

Fuente: Serrano, 2016

Cuadro N° 4
Denuncias ingresadas a la Fiscalía de San José por Delitos Informáticos (Violación de comunicaciones, Violación de Datos Personales, Sabotaje Informático, Suplantación de Identidad, Daño Informático entre otros)

Año 2013	Año 2014	Año 2015
138	295	115

Fuente: Serrano, 2016

Cuadro N° 5
Países miembros del Consejo de Europa: Ratificaciones

Firmado	Ratificados	Países ratificados	
43 de 47 países	**29**	Albania Armenia Azerbaijan Bosnia y Herzegovina Bulgaria Croacia Chipre Dinamarca Estonia Finlandia Francia Alemania Hungría Islandia Italia	Letvia Lituania Moldavia Montenegro Países Bajos Noruega Portugal Romania Serbia Eslovaquia Eslovenia Yugoslava de Macedonia Ucrania Costa Rica

Fuente: Serrano, 2016.
Actualizado: Chacón, 2018

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

En este mundo globalizado, donde se depende de la tecnología hasta para realizar compras en un supermercado, es necesario aprender a protegerse de la delincuencia. Se reitera, ha sido imposible eliminar la delincuencia en el mundo real, con mucha más razón esa imposibilidad se traslada al mundo virtual, en donde día a día, los ciberdelincuentes están encontrando nuevas formas de delinquir, lo cual se facilita con la falta de cuidado de las personas al navegar en la red de Internet.

Los delincuentes han ideado muchas formas de obtener las claves de cuentas bancarias de sus víctimas, quien aún después de ser advertidos por las propias entidades financieras, siguen suministrando su información personal o password, por medio de correos electrónicos que les ofrecen premios o los previenen de que su cuenta fue accesada de manera riesgosa, siendo falso, pues lo que buscan es que el propio cibernauta proporcione los detalles de dichas cuentas.

El ciberdelincuente se puede ubicar en cualquier lugar del mundo, lo que deviene en uno de los mayores problemas para investigar los delitos informáticos, al generar que, en su mayor parte queden impunes. Dado lo anterior, es que los Estados han procurado unirse por medio de convenios internacionales de ayuda mutua, donde lo que se busca es facilitar la aplicación de una ley penal común, cuyo fin es la protección de las personas ante la ciberdelincuencia, por medio de "una cooperación internacional reforzada, rápida y eficaz".

Por esto, uno de los mayores avances de Costa Rica en el tema de la prevención y persecución de la ciberdelincuencia, es la reciente adhesión (mayo 2017) al convenio de Budapest, suscrito por varios Estados principalmente Europeos y que hoy es complemento de la actual Ley 9048 de Delitos Informáticos, que permitirá la protección de "*actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como datos personales, la identidad y los derechos de los niños y niñas*" (recuperado el día 01 de marzo del 2018 a las 10:02 am de la página

http://presidencia.go.cr/comunicados/2017/05/costa-rica-se-adhiere-a-convenio-contra-ciberdelincuencia/).

Este convenio procura, además, facilidad en la obtención de pruebas electrónicas de ciberdelitos, que deban de ser recopiladas fuera de las fronteras costarricenses y una colaboración constante con las fuerzas policiales en el nivel mundial.

Internet y los avances tecnológicos nos abren las puertas a la comodidad y simplifican en gran manera la realización de acciones que antes nos quitaban mucho tiempo; ya no es necesario ir a un banco a efectuar un depósito o un pago, los servicios públicos pueden ser cancelados desde plataformas virtuales y ni que decir la gran cantidad de compras por medio de la red. Sin embargo, la tecnología también trae riegos y peligros, como lo pueden ser los robos, fraudes, suplantación de identidades, entre los muchos delitos que pueden ser perpetrados por medios electrónicos.

Cada día son más los cibernautas, debido a los nuevos puntos de acceso a Internet, las redes sociales y la posibilidad de buscar información de toda índole, la cual prolifera de manera impresionante. No hay duda que la Internet ha venido a promover un cambio total en la forma de vida de las personas, debido a los beneficios que proporciona, no obstante, se debe de tener mucha precaución y procurar una navegación segura, al evitar realizar acciones que faciliten ser víctimas de la ciberdelincuencia, pues como dijo el apreciado y recordado Lic. Luis Paulino Mora: “Para ser víctima, basta estar conectado”.

RECOMENDACIONES

1. La ciberdelincuencia aumenta cada día, pues conforme avanza la tecnología las formas de delinquir se incrementan en este ámbito, donde los cibercriminales de manera constante se actualizan y buscan nuevos medios para llevar a cabo sus ilícitos, aunado al hecho de que, la mayoría de las personas no saben protegerse en Internet, se considera necesaria la creación de campañas educativas (iniciando en las escuelas, ya que, desde muy corta edad los niños y niñas tienen acceso a la tecnología), que permitan un asesoramiento en este tema, pues la prevención es la mejor forma de combatir la ciberdelincuencia.
2. Los cibernautas deben de procurar mantener actualizados los programas en sus equipos de cómputo, para que los ciberdelincuentes no se aprovechen de las debilidades que puedan tener, pues en programas desactualizados es más sencillo el ingreso, por lo cual, la constante mejora es de suma importancia.
3. Otra buena práctica es mantener diferentes respaldos de la información, los cuales deben de ser actualizados diariamente de ser posible, para evitar la pérdida de datos importantes.
4. El Estado es garante de la protección de los ciudadanos en todos los ámbitos de su vida. Los delitos informáticos son conductas típicas de un mundo real adaptadas a un mundo virtual, siendo la tecnología el canal efectivo para la realización de las acciones ilícitas, por ende, es su deber mantenerse constantemente actualizado en cuanto a la normativa vigente, al procurar uniones y convenios internacionales que permitan la persecución de los ciberdelincuentes, así como, la búsqueda de formas efectivas de prevención de los ciberdelitos, para lo cual, debe de procurar ir adelante de los cibercriminales en cuanto a tecnología y conocimientos.
5. En caso de ser víctima de un ciberdelito, se debe acudir de inmediato a la Sección de Delitos Informáticos del OIJ para entablar la denuncia correspondiente y no se deben de borrar los correos electrónicos recibidos ni bloquear la información remitida por el ciberdelincuente, siendo que, todo puede ayudar en la investigación e identificar el origen del cibercriminal. Tampoco se deben realizar amenazas como prevenirlo de que se acudirá a la policía o pagar algún tipo de extorsión.

BIBLIOGRAFÍA

- Luis Paulino Mora, basta estar conectado, recuperado de la página web http://kerwa.ucr.ac.cr/bitstream/handle/10669/500/libro%20completo%20Ciber.pdf?sequence=1 el día 07/11/2017 a las 6:45 pm)
- https://micit.go.cr/index.php?option=com_content&view=article&id=9964:estrategia-nacional-de-ciberseguridad-en-su-ultima-etapa-de-construccion-2&catid=40&Itemid=630
- Revista Judicial Costa Rica, N° 115, marzo, 2015. DELITOS DE PELIGRO ABSTRACTO. FUNDAMENTO, CRÍTICA Y CONFIGURACIÓN NORMATIVA. Lic. Javier Madrigal Navarro
- http://dle.rae.es/?id=YErlG2H
- http://www.duiops.net/hacking/hacking-cracking.htm
- https://vinv.ucr.ac.cr/es/noticias/conozca-matilde-la-primera-computadora-del-pais
- EL DESARROLLO DE LA COMPUTACIÓN Y SU INFLUENCIA EN LA MEDICINA Enrique Freer Bustamante.* Johnny Chavarría Cerdas.** http://www.binasss.sa.cr/revistas/rccm/v13n1-2/art10.pdf
- Chinchilla Sandí Carlos, Delitos Informáticos, San José, Editorial Investigaciones Jurídicas S.A, 2002, p.26
- LEIVA JIJENA, Renato, “CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO”, Editorial Andrés Bello, 1992, pp. 225
- Lima De La Luz, María. Delitos Electrónicos en Criminalia. México. Academia Mexicana de Ciencias Penales. Porrúa. . No. 1-6. Año L. Enero-Junio 1984. Pp.100.
- SIEBER, Ulrich, “Criminalidad Informática Peligro y prevención”, PPU, Barcelona, 1992. Pp. 75
- Marcelo http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf
- https://www.elfinancierocr.com/economia-y-politica/costa-rica-enfrenta-el-cibercrimen-con-armas-oxidadas/RIDQNOWPORGAJEES3DRE7KKEPE/story/
- https://www.poder-judicial.go.cr/oij/index.php/comunicacion/noticias/avisos-y-noticias-policiales/item/3864-seccion-de-delitos-informaticos
- https://www.elfinancierocr.com/tecnologia/ciberdelincuentes-se-alimentan-de-las-redes-sociales/FUGB3DB6UZHDLNZDFJLKJSIPSY/story/
- https://adalidmedrano.com/tag/suplantacion-de-identidad/
- https://adalidmedrano.com/tag/violacion-de-comunicaciones-electronicas/
- http://www.ticovision.com/cgi-bin/index.cgi?action=printtopic&id=10841

- http://www.bbc.com/mundo/vert-cap-40638275
- https://www.lanacion.com.ar/1862899-tarjetas-de-credito-las-5-formas-de-estafas-que-mas-preocupan-a-todos
- MIRÓ, Fernando y LLINARES, Roxin. LA OPORTUNIDAD CRIMINAL EN EL CIBERESPACIO
- Revista Judicial, Costa Rica, N° 115 (marzo 2015) DELITOS DE PELIGRO ABSTRACTO.
- BACIGALUPO, Enrique, Manual de Derecho Penal, (Parte General), Exposición referida a los derechos vigentes en Argentina, Colombia, España, México y Venezuela, 2ª Edición, Temis-ILANUD, 1984, p.p. 101-102
- Ary Donald, Jacobs Lucy, Razabieh Asghar. Introducción a la investigación pedagógica. México. Editorial McGraw-Hill. Segunda Edición. 1990.
- Rodríguez Gregorio, Gil Javier, García Eduardo. Metodología de la Investigación Cualitativa. España. Ediciones Aljibe. 1996
- https://www.camtic.org/actualidad-tic/costa-rica-se-adhiere-a-convenio-contra-ciberdelincuencia/
- http://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/16700/LECT132.pdf?sequence=1
- González. A, Peláez. A, Pérez .C, Rodríguez. A y Vásquez. H. (s.f.). La entrevista. Obtenido desde https://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Curso_10/Entrevista_trabajo.pdf.