Facultad de Ciencias Jurídicas y Justicia

Licenciatura en Ciencias Jurídicas y de la Justicia

La suplantación de identidad (phishing) en Guatemala y en el derecho comparado

(Tesis de Licenciatura)

Miguel Angel Tzoc Borrayo

Guatemala, febrero 2024

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

La suplantación de identidad (phishing) en Guatemala y en el derecho comparado

(Tesis de Licenciatura)

Miguel Angel Tzoc Borrayo

Guatemala, febrero 2024

Para los efectos legales y en cumplimiento a lo dispuesto en el artículo 1°, literal h) del Reglamento de Colegiación del Colegio de Abogados y Notarios de Guatemala, **Miguel Angel Tzoc Borrayo**, elaboro la presente tesis, titulada **La suplantación de identidad (phishing) en Guatemala y en el derecho comparado.**

AUTORIDADES DE UNIVERSIDAD PANAMERICANA

M. Th. Mynor Augusto Herrera Lemus
Rector

Dra. Alba Aracely Rodríguez de González
Vicerrectora Académica

M. A. César Augusto Custodio Cóbar
Vicerrector Administrativo

EMBA. Adolfo Noguera Bosque
Secretario General

FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA

Dr. Enrique Fernando Sánchez Usera

Decano de la Facultad de Ciencias Jurídicas y Justicia

Guatemala, 3 de mayo de 2023

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

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como asesor del estudiante Miguel Angel Tzoc Borrayo, ID 000128912. Al respecto se manifiesta que:

a) Brinde acompañamiento al estudiante en referencia durante el proceso de elaboración de la tesis denominada La suplantación de identidad (phishing) en Guatemala y en el derecho comparado.
b) Durante ese proceso le fueron sugeridas correcciones que realizó conforme los lineamientos proporcionados.
c) Habiendo leído la versión final del documento, se establece que el mismo constituye un estudio serio en torno al tema investigado, cumpliendo con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

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

Se hace la aclaración que el estudiante es el único responsable del contenido de la tesis ya indicada.

Atentamente,

Lcda. Mónica María Morales Muñoz

Mónica María Morales Muñoz
ABOGADA Y NOTARIA

Guatemala, 11 de julio de 2023

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

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como revisor metodológico de la tesis del estudiante Miguel Ángel Tzoc Borrayo, ID 000128912, titulada "La suplantación de identidad (phishing) en Guatemala y en el derecho comparado". Al respecto me permito manifestarles que, la versión final de la investigación fue objeto de revisión de forma y fondo, estableciendo que la misma constituye un estudio serio que cumple con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

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

Se hace la aclaración que el estudiante es el único responsable del contenido de la tesis ya indicada.

Atentamente,

Licenciado Julio Raúl Mazariegos Pérez

LICENCIADO
Julio Raúl Mazariegos Pérez
ABOGADO Y NOTARIO

UNIVERSIDAD PANAMERICANA
"Sabiduría ante todo; adquiere sabiduría"

Ref. O.I. 6-2024
ID: 000128912

ORDEN DE IMPRESIÓN DE TESIS DE LICENCIATURA

Nombre del Estudiante: **MIGUEL ANGEL TZOC BORRAYO**
Título de la tesis: **LA SUPLANTACIÓN DE IDENTIDAD (PHISHING) EN GUATEMALA Y EN EL DERECHO COMPARADO**

El Decano de la Facultad de Ciencias Jurídicas y Justicia,

Considerando:

Primero: Que previo a otorgársele el grado académico de Licenciado en Ciencias Jurídicas y de la Justicia, así como los títulos de Abogado y Notario, el estudiante ya mencionado, ha desarrollado el proceso de investigación y redacción de su tesis de licenciatura.
Segundo: Que tengo a la vista el dictamen favorable emitido por la tutora, Licenciada Mónica María Morales Muñoz, de fecha 3 de mayo del 2023.
Tercero: Que tengo a la vista el dictamen favorable emitido por el revisor, Licenciado Julio Raúl Mazariegos Pérez, de fecha 11 de julio del 2023.

Por tanto,

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

Guatemala, 31 de enero del 2024

"Sabiduría ante todo, adquiere sabiduría"

UNIVERSIDAD PANAMERICANA · FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA · Dr. Enrique Fernando Sánchez Usera · DECANO

Dr. Enrique Fernando Sánchez Usera
Decano de la Facultad de Ciencias Jurídicas y Justicia

Dedicatoria

A Dios,	Por el don de la vida, por su amor incondicional, por la bendición de la salud, sabiduría, y por las fuerzas brindadas para luchar por mis metas.
A mi madre,	Jobita Borrayo por su apoyo sin condición tanto económico como anímico, por sus palabras de ánimo para seguir luchando y ser mejor persona y un buen profesional, por su amor y comprensión.
A mis hermanos,	Por su cariño y apoyo económico y emocional, por sus oraciones, les dedico esta meta alcanzada.
A la Universidad Panamericana,	Por la formación profesional en mi vida.

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

Índice

Resumen i

Palabras clave ii

Introducción iii

La suplantación de identidad como delito informático 1

La suplantación de identidad (phishing) en Guatemala 18

Derecho comparado 35

Conclusiones 68

Referencias 70

Resumen

En este estudio de derecho comparado, se abordó la suplantación de identidad o phishing en Guatemala y en el derecho comparado. El objetivo general fue comparar la regulación extranjera contra el delito de la suplantación de identidad para determinar los aspectos que pueden ser utilizados en la legislación guatemalteca. El primer objetivo específico consistió en describir la suplantación de identidad y los demás delitos informáticos. Asimismo, el segundo objetivo se refirió, a examinar la vulnerabilidad que existe en Guatemala ante los ataques de la suplantación de identidad. Luego de analizar las legislaciones de Costa Rica, Colombia, República Dominicana que son aplicables en el presente estudio.

Se concluyó que, en la actualidad no se encuentra tipificado dentro del ordenamiento jurídico guatemalteco el delito de suplantación de identidad o el llamado *phishing*. Por lo cual en Guatemala se tiene un nivel de vulnerabilidad muy alto ante este ilícito, el cual se realiza de forma impune utilizando los medios informáticos, ya que no se puede realizar una investigación correcta para imponer una sanción y lograr resarcir el daño causado a las víctimas. En consecuencia, con el estudio de las legislaciones extranjeras se llegó a la conclusión, que se debe realizar una reforma al código penal guatemalteco de forma urgente, para la prevención de dicho delito, esto con la finalidad de normar dicho ilícito

mientras que posteriormente se legisle una ley especial que norme en su totalidad los delitos informáticos.

Palabras clave

Delitos informáticos. Suplantación. Phishing. Reforma.

Introducción

En esta investigación se abordará el tema de la suplantación de identidad (*phishing*) en Guatemala y en el derecho comparado, debido a la vulnerabilidad que existe en la actualidad por no poseer una norma que tipifique este delito, por lo cual los autores de este delito no reciben un castigo adecuado. En el objetivo general de la investigación será comparar la regulación extranjera con el delito de la suplantación de identidad, para determinar los aspectos que pueden ser utilizados en la legislación guatemalteca. En consecuencia, el primer objetivo específico es describir la suplantación de identidad y los demás delitos informáticos los cuales afectan en un gran porcentaje a la población. Por lo cual el segundo es examinar la vulnerabilidad que existe en Guatemala ante los ataques de la suplantación de identidad, al no tener una legislación que regule este ilícito.

Las razones que justifican el estudio consisten en que Guatemala actualmente su legislación ha quedado desactualizada y no contempla los delitos informáticos que han surgido con el pasar del tiempo, entre estos ilícitos esta la suplantación de identidad, el cual es uno de los delitos que más afectan a los guatemaltecos. Además, el interés del investigador en el tema radica en que se debe reformar el Código Penal adicionando el delito de suplantación de identidad para que se sancione a los infractores del mismo. Para el desarrollo del trabajo, la modalidad de la investigación es

la comparación de legislaciones extranjeras, siendo estas de Costa Rica, Colombia, República Dominicana, que cuentan con leyes especiales o reformas que regulan este delito.

En cuanto al contenido, el primer subtitulo se estudiará la suplantación de identidad como delito informático, donde se desarrolla los tipos de delitos informáticos, su clasificación y la definición de la suplantación de identidad. Dentro del segundo subtitulo se desarrollará la suplantación de identidad en Guatemala, la evolución que ha sufrido este delito, de igual forma se establecerá el porcentaje de ataques que sufren los ciudadanos guatemaltecos. También se establecerá los bienes jurídicos que son afectados y que el estado debe garantizar su debida protección. Por lo tanto, el tercer subtitulo contendrá el derecho comparado, estableciendo las normas jurídicas que aplica Costa Rica, Colombia y República Dominicana, así como forma la propuesta para la reforma del Código Penal de Guatemala.

La suplantación de identidad como delito informático

La suplantación de identidad se puede establecer que es un acto utilizado para cometer actividades malintencionadas en contra de personas, las cuales son seleccionadas de forma aleatoria. El método más utilizado por los delincuentes para cometer este delito, es por medio de correo electrónico que estos sujetos adquieren grandes cantidades de nombres de usuarios a quienes les envían mensajes con remitentes que se hacen pasar por empresas legitimas. En consecuencia, dentro del mensaje enviado adjuntan un enlace que al abrirlo las víctimas son redireccionadas a páginas externas las cuales son falsas. De este modo, al momento que se ingresan datos en esta página quedan grabados en una base de datos, que son utilizados posteriormente para robar información personal, contraseñas, cuentas, números de tarjetas de crédito y débito, documentos personales de identificación y dinero que posean los afectados dentro de sus cuentas bancarias.

La suplantación de identidad es conocido comúnmente como *phishing*, esta actividad se ha incrementado a través de campañas de ataques a los usuarios de los medios informáticos. Ciertamente los delincuentes adquieren bases de datos que contienen correos electrónicos, estos son utilizados para realizar los ataques, los delincuentes obtienen esta información por medio del mercado negro o también llamado *deep web*. Cabe mencionar que este tipo de engaños, puede ser realizada por medio

de mensajes de whatsapp o telegram, o por mensajes privados dentro de alguna red social, los usuarios al momento de abrir el enlace que contiene el mensaje, suelen estar en peligro de perder su información personal. Esta forma de sustraer y suplantar la identidad de los usuarios ha sido muy lucrativa, según el informe de Garther de 2007, indica que 3.6 millones de adultos perdieron 3,200 millones de dólares entre agosto de 2006 y agosto de 2007.

Definición de delito informático

Es conveniente definir en sí que es el delito, y se puede indicar que es una conducta humana la cual debe ser típica y antijuridica, esta debe poseer elementos de culpabilidad del sujeto quien deberá ser sometido a las condiciones objetivas que establecen la imputabilidad para ser sometido a una sanción penal. En consecuencia, los delitos informáticos son todos aquellos actos realizados de forma voluntaria y consciente, que poseen el ánimo de crear, modificar y falsificar, medios de comunicación legítimos para vulnerar la seguridad que se posee y de esa forma conseguir información privada de los usuarios induciéndolos al error y de esa forma conseguir beneficios económicos con los datos obtenidos.

Cabe citar al licenciado Davara Rodríguez (1990), quien en su trabajo llamado delitos informáticos proporciona una definición bastante interesante que es de gran importancia para el presente trabajo. y establece que:

> La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (p.10)

Cuando se menciona con el ánimo de crear, modificar y falsificar medios de comunicación, debe entenderse que los ciberdelincuentes poseen habilidades y conocimientos avanzados en informática, con lo cual tienen la capacidad de crear *malware*, los cuales son programas maliciosos, que contienen códigos creados para dañar equipos de cómputo y robar silenciosamente información privada del propietario de dichos dispositivos. Los ciberdelincuentes suelen modificar programas originales que requieren de una licencia para su uso, modifican los códigos fuente e introducen *malwares* que actúan sin ser detectados, lo distribuyen dentro de la red y son utilizados comúnmente por personas que buscar utilizarlos de forma gratuita.

En la actualidad la tecnología ha evolucionado rápidamente, por lo cual se puede mencionar que gran parte de los delitos tradicionalmente conocidos y tipificados, dentro de los ordenamientos jurídicos ya están siendo realizados a través de los medios informáticos. Por lo cual está ocasionando que sea realmente complicado en Guatemala, la regulación y control de la suplantación de identidad. De este modo con el surgimiento de nuevos métodos de seguridad informática, el hombre siendo fiel a su capacidad de adaptación, busca medios para evadir las protecciones y encontrar vulneraciones dentro de los sistemas informáticos y de esa forma seguir cometiendo este delito.

Para entender más sobre este tema, se debe realizar una diferencia entre quien es un ciberdelincuente y quien no lo es, se ha dicho por mucho tiempo que los *hackers* son aquellas personas que realizan hechos delictivos a través de medios informáticos vulnerando la privacidad de los usuarios, esto no es del todo cierto. Los *hackers* son aquellos expertos en informática capaces de modificar programas de cómputo, con el objetivo de encontrar y solucionar errores de seguridad que puedan poner en riesgo a los usuarios, la actividad de los *hackers*, es buscar la protección de la información de los usuarios. Los ciberdelincuentes o bien llamados *cracker* son aquellos expertos en informática capaces de modificar programas aprovechándose de errores de seguridad para dañar a los usuarios, suelen programar *malwares* para robar información de sus víctimas, su fin principal es lucrar con la información privada.

Hay que mencionar que los *crackers* surgieron junto al avance tecnológico, con la creación de nuevos medios de comunicación vía electrónica, donde los usuarios ven en las nuevas modalidades informáticas un medio de ahorrar tiempo, ya que evitan acudir a los distintos bancos para realizar pagos, depósitos y otras transacciones. En la actualidad existen gran cantidad de tramites que se pueden realizar por medio de la red, utilizando dispositivos electrónicos como teléfonos inteligentes. Es por tal motivo que los *crackers* ven en estos sistemas una oportunidad para realizar el robo de contraseñas, usuarios de cuentas

bancarias, copiar números de tarjetas de crédito y débito, apropiarse de contenidos privados que son usados para extorsionar a sus víctimas.

Tipos de delitos informáticos

Debido al desarrollo tecnológico y a la capacidad que poseen los delincuentes para utilizar los medios informáticos a su favor para cometer delitos aprovechando el gran potencial que tiene el internet. Los ciberdelincuentes obtienen de forma ilegal acceso a los usuarios de terceras personas, donde realizan daños al patrimonio de sus víctimas. Por lo cual se pueden mencionar diversos actos delictivos, el más utilizado es la estafa, que esta se comete por lo general por medio del *phishing* o suplantación de identidad, que como ya se mencionó anteriormente se utilizan páginas falsas y programas modificados para robar información, infectando con *malwares* que roban datos sin ser detectados por los usuarios de los dispositivos inteligentes.

Dentro de los delitos informáticos se encuentran, *sexting* y *stalking* y de igual forma que la pornografía infantil. El *sexting* consiste en el envío de fotografías, videos, audios y mensajes de texto con contenido sexual, por medio de redes sociales o aplicaciones de mensajería instantánea como whatsapp, telegram, facebook, instagram y twitter. Por supuesto, este acto por sí solo no es ilegal si se realiza entre adultos, mientras exista consentimiento entre las dos partes, no es considerada como una actividad

ilícita ya que no se encuentra tipificada dentro de la norma jurídica. Por el contrario, este acto cambia completamente su panorama y adquiere carácter de delito cuando las fotografías, videos, notas de audio y mensajes de texto con contenido sexual son enviados sin consentimiento de las partes o son enviadas por un adulto hacia un menor de edad, el cual constituye violencia psicológica, por el estado de vulnerabilidad que poseen.

El *stalking* consiste en el acecho u hostigamiento que provoca un sujeto hacia una persona determinada, este acoso que se produce puede realizarse mediante mensajes de texto, mensajes privados por medio de redes sociales, llamadas telefónicas y correos electrónicos. En consecuencia, de estos actos, la persona que está siendo víctima de este delito pierde su libertad de actuar por las amenazas sufridas, ya que la persona que sufre de este delito debe cambiar de una forma no voluntaria su forma de desarrollar sus actividades cotidianas ya que sufre la constante vigilancia y acoso de su victimario. Se puede mencionar que unos de los factores que desatan este acto ilícito, es la ruptura de una relación amorosa, donde una de las partes inicia con el acoso.

Dentro de una gran cantidad de definiciones sobre lo que es el *stalking*, se puede observar lo que establece la licenciada Constantinescu M.R. (2020), quien desarrollo esta definición en su trabajo de fin de master en abogacía, la cual es de gran aporte informático, para la comprensión de este ilícito penal y establece que:

> Se entiende por stalking la persecución continuada e intensiva de un sujeto, denominado stalker, contra una persona determinada, sin su consentimiento, con la finalidad de iniciar o restablecer un contacto personal con la misma, produciendo miedo o preocupación en la víctima, de manera que ésta se vea obligada a modificar sus hábitos de vida cotidianos. (p.5)

Como se observa en dicha definición se establece que la victima de este delito recibe una persecución en sus actividades cotidianas. Ciertamente este acecho que recibe es sin su consentimiento, este hostigamiento puede ser muy intenso por parte de su victimario, quien recibe el nombre de *stalker*. Por este motivo la víctima, puede llegar al punto de sentir miedo por su vida por los actos que realiza la persona que se encuentra realizando este ilícito. En *stalker*, realiza el uso de sistemas informáticos para realizar una persecución dentro de redes sociales, creando perfiles falsos para observar los actos realizados por la persona a quien persigue, este puede hacer uso de sistemas de *GPS*, para monitorear la ubicación exacta y de esa forma realizar contacto físico con la persona afectada.

En cuanto a la pornografía infantil, se puede establecer que se ha vuelto un delito muy frecuente, ya que se ha vuelto un negocio muy lucrativo por el aumento de sujetos que consumen este tipo de material sin importar que se denigre y vulneren los derechos de los menores de edad. Ciertamente este acto ilícito, obtuvo un incremento por la fácil obtención de dispositivos de grabación de audio y video, así como cámaras fotográficas que son utilizadas para la creación este contenido. En consecuencia, los delincuentes y acosadores suelen utilizar plataformas como redes sociales, aplicaciones de juegos y muchas aplicaciones utilizadas por menores de

edad donde por medio de engaños o amenazas obtienen imágenes y videos de contenido sexual, que son posteriormente comercializados dentro del internet.

Ya se han mencionado delitos contra la información privada de las personas, también delitos contra la integridad física y mental de mayores y menores de edad, pero existen delitos de revelación de información y descubrimiento de secretos. Estos delitos perjudican específicamente la intimidad de documentos, conversaciones privadas, secretos empresariales o de estado y violaciones al derecho de autor. Por supuesto estos ilícitos son cometidos por *cracker,* que por medio de un *malware* o *spyware* que son programas maliciosos que actúan de forma silenciosa dentro de un equipo de cómputo, estos recopilan información de chats, correos, llamadas, video llamadas etc. Comúnmente trabajan sin dejar rastro dentro de la computadora o dispositivo móvil, en ocasiones estos programas pueden controlar las cámaras y micrófonos de los dispositivos para interceptar información para posteriormente lucrar con la misma.

En la actualidad que vive Guatemala con el avance tecnológico se ha observado que a pesar que no todos los ciudadanos tienen acceso al servicio de internet, si ha existido un incremento en la contratación de este servicio en los hogares de los habitantes. Por lo tanto, al poseer acceso a internet los menores de edad, hacen uso del mismo y en gran porcentaje no tienen supervisión de un adulto y acceden a redes sociales y

aplicaciones o programas de mensajería instantánea por medio de dispositivos inteligentes. En consecuencia, del uso de estos medios informáticos por niños, se encuentran en una situación de vulnerabilidad, donde pueden ser acosados y hostigados, pueden recibir burlas, mensajes de discriminación por compañeros de escuela o vecinos, estos actos realizados por los medios informáticos se le conoce como ciberbullying.

Con lo expuesto en al párrafo anterior es necesario establecer lo relativo al ciberbullying, y la licenciada Fernández Tomé A. (2015), en su tesis doctoral en psicología, entrega una definición que enriquece el conocimiento del presente trabajo y establece que:

> En la última década estamos observando un rápido desarrollo y utilización de nuevas modalidades de bullying, una de éstas es el cyberbullying (CB) (también denominado ciberacoso, acoso cibernético, electrónico, digital… entre iguales). EL CB es una forma de bullying, una forma de violencia entre iguales, que utiliza las nuevas tecnologías de la información y la comunicación (TIC) (principalmente Internet y el teléfono móvil) para acosar y hostigar a otros compañeros (p.28).

Cabe mencionar que con el avance tecnológico se obtenido una gran variedad de beneficios, pero a su vez se han adquirido situaciones desfavorables. Una de ellas se da por la falta de supervisión de los padres que dan acceso a los menores de edad a las diferentes plataformas electrónicas y redes sociales. Por lo cual dentro de estas aplicaciones son susceptibles de ser víctimas del ciberacoso que se realiza por compañeros del centro educativo al que asisten, así como puede ser de vecinos o incluso familiares. En consecuencia, este acoso cibernético que tiene

todas las características de lo que es el bullying, que se realiza por medio de los dispositivos electrónicos se le conoce como ciberbullying. Con estas acciones que son hechas por menores de edad burlándose, humillando o amenazando a otro menor de edad, perjudican psicológicamente a la víctima y su autoestima y rendimiento académico se ve disminuido considerablemente.

La suplantación de identidad o phishing

La suplantación de identidad o *phishing* es el robo de información confidencial, de usuarios a través de medios tecnológicos, usando páginas maliciosas que se hacen pasar por web legitimas. Los *phisher,* que son aquellas personas que realizan actividades ilícitas con el objeto de robar información de los usuarios de diversos sistemas informáticos, tales como pueden ser datos de tarjetas de crédito y débito, usuarios de redes sociales y de entidades bancarias, informaciones corporativas o estatales. Los ciberdelincuentes obtienen estos datos por medio de engaños para inducir en error a los usuarios, utilizando páginas web maliciosas y programas que tienen como fin especifico espiar a su víctima para obtener información confidencial.

Es de gran importancia citar al licenciado Sánchez Bernal (2009) que entrega una definición con respecto al *phishing,* la cual proviene de su trabajo titulado el bien jurídico protegido en el delito de estafa informática y establece que:

> Se trata de una práctica encuadrada en el campo de la estafa, que consiste en la adquisición de información confidencial (de carácter económico, personal o de cualquier otra índole) de forma ilícita, sin consentimiento de su titular, mediante el uso de ingeniería social. El infractor, conocido como phisher, puede simular ser una persona o empresa de confianza, cometiendo el hecho ilícito mediante una comunicación electrónica aparentemente normal (correo electrónico, mensajería instantánea) o incluso, mediante una llamada telefónica. La persona que lleva a cabo esta actividad delictiva suele camuflarse bajo el nombre de la entidad bancaria habitual u otros. (p. 106, 107).

Como lo establece el licenciado Bernal, la suplantación de identidad contiene elementos del delito de estafa que contempla la legislación guatemalteca en su artículo 263 del Código Penal que establece "comete estafa quien, induciendo a error a otro mediante ardid o engaño, lo defraudare en su patrimonio en perjuicio propio o ajeno". Por lo cual los *phisher* crean web, *malwares* y programas maliciosos para inducir a error a los usuarios haciéndoles creer que son páginas legitimas, engañando totalmente al sujeto. Comúnmente se hacen pasar por entidades bancarias donde se solicita el ingreso de datos como usuarios y contraseñas para la verificación y protección de sus cuentas, estos datos son almacenados ilícitamente para posteriormente realizar transacciones en los usuarios legítimos, causando daños irreparables en el patrimonio de sus víctimas.

Dentro de este delito informático se observan los elementos de inducir a error, el engaño y el daño al patrimonio ajeno, solo con estos elementos podemos establecer que es el delito de estafa, pero para poder encuadrarlo en el delito de suplantación de identidad o *phishing*, estos deben estar realizados por medio de algún sistema informático. Es decir, debe mediar

la tecnología en la realización de estos elementos donde se viola la privacidad de los usuarios, robando datos personales. Por lo tanto, con el uso de páginas web maliciosas o programas que recopilan información sin ser detectados, buscan causar daños al patrimonio e integridad, como lo son el robo de dinero en cuentas bancarias y la amenaza de la no publicación de contenido intimo a cambio de una cantidad de dinero.

En la actualidad, existen diversas señales que pueden ser observadas para determinar si los mensajes recibidos se tratan de campañas de *phishing* para suplantar su identidad. Como se ha mencionado con anterioridad el método más utilizado por los *phisher* es él envió de enlaces por medio de correos electrónicos, donde se hacen pasar por los diferentes bancos del sistema. Por lo tanto, los remitentes de los mensajes no pueden ser considerados como legítimos, ya que estos cuentan con nombres de personas individuales o suelen tener una alteración de letras o palabras en los correos que aparentan ser corporativos de entidades bancarias. De esta forma en estos correos se adjuntan enlaces de páginas donde las víctimas son redireccionadas a otros sitios, para que ingresen datos y así obtener la información personal.

Existen varios métodos de protección para evitar ser víctima de la suplantación de identidad o *phishing,* dentro de los cuales se pueden utilizar programas de seguridad como antivirus, que posean la capacidad de detectar y eliminar *malware,* además que protejan de páginas web

maliciosas. Vale recordar que, un método que es muy efectivo es mantener las actualizaciones que recomiendan los fabricantes de computadoras y sistemas operativos, ya que mejoran constantemente sus sistemas de seguridad para el usuario. De igual forma se puede establecer que el método más efectivo para evitar ser víctimas de este delito es la prudencia al momento hacer uso de los medios informáticos, por lo cual es importante verificar el remitente de los mensajes que se recibe, así como ingresar manualmente la dirección de la página web dentro del navegador, y no ingresar datos personales en sitios donde la privacidad sea nula.

Clasificación de la suplantación de identidad o phishing

Como se ha mencionado con anterioridad la suplantación de identidad o *phishing* ha evolucionado constantemente con las nuevas tecnologías que surgen, los delincuentes se adaptan y buscan nuevos métodos para lograr su objetivo. En consecuencia, en la actualidad se ha dividido este delito en diversas categorías según el fin que persiguen, el objeto de esta división es poder identificar de una mejor manera la vulnerabilidad existente en los medios informáticos en distintas áreas de la vida cotidiana de los usuarios. Por lo cual, el uso del correo electrónico, acceder a redes sociales, enviar y recibir mensajes por aplicaciones de mensajería instantánea, descargar información del internet, consumir contenido audio visual en plataformas digitales, la verificación de saldos de cuentas, todas

estas actividades poseen el riesgo de ser vulneradas para el robo de información.

Dentro de esta clasificación se encuentra el *spear phishing*, este tipo de delito se caracteriza por ser selectivo al momento de realizar los ataques, ya que se envían correos electrónicos a personas especificas con el objetivo de engañar y obtener información confidencial. Los *phishers*, realizan una serie de investigaciones detalladas sobre el sujeto a quien se dirigirá el ataque, para lograr parecer una fuente confiable e incentivar a que ingrese al enlace adjunto en el correo. En consecuencia, la persona que sufre del ataque sin tener conocimiento da acceso con sus credenciales al sistema informático que poseen las organizaciones o corporaciones internacionales y entidades estatales. El objetivo de dicha actividad, es robar información privada y secreta para posteriormente revelarla o venderla para obtener un beneficio económico.

Dentro del trabajo titulado análisis sistemático de ataques de *spear phishing* utilizando inspección profunda de paquetes realizado por el licenciado Cáceres Díaz I.F. (2021), proporciona una definición del *spear phishing* y establece que:

> En Spear Phishing, los ataques son selectivos e implican engañar a individuos particulares dentro de una organización específica para obtener información o infectar equipos. Estos ataques son exitosos ya que envían correos electrónicos personalizados y creíbles que parecen provenir de una fuente confiable. De hecho, las estadísticas de la industria muestran que los ataques de Spear Phishing tienen una tasa de éxito del 19%, en comparación con solo el 5% para los ataques de Phishing estándar y menos del 1% para el spam (p.8).

Se puede mencionar que en este tipo de suplantación de identidad o *phishing* normalmente es utilizado por los *phisher* o ciberdelincuentes que buscan aprovecharse de los usuarios para adquirir información privada de empresas, como cuentas bancarias de empleados, secretos corporativos o de estado. Estos datos son utilizados para dañar la reputación de empresas, así como de los organismos estatales. Este delito ha avanzado en la actualidad se ha utilizado por activistas que son patrocinados por gobiernos, para luchar por sus intereses, existen *cracker* que trabajan para gobiernos que aprovechan el alcance de esta actividad y lo utilizan como método de espionaje y poder ingresar a los sistemas informáticos de estados enemigos y obtener secretos de estado que son utilizados a su favor.

El *whaling* se puede indicar que es el tipo de suplantación de identidad que se caracteriza especialmente, en hacer un estudio jerárquico de los trabajadores de una corporación, para suplantar la identidad de un alto ejecutivo. Como es evidente al obtener los datos proceden a crear un correo electrónico falso, que contiene todas las características de un usuario real, con el cual solicitan datos privados a los empleados que son inferiores jerárquicamente. Ciertamente la información solicitada por estos delincuentes, puede llegar a ser planillas completas donde contengan nombres y usuarios de bancos, direcciones de correos electrónicos, estados financieros, números de teléfonos. Este tipo de *phishing* suele

tener éxito debido a que suplantan la identidad de una persona superior laboralmente quien ordena el envío de dichos datos.

El *shellphish* se puede establecer que es un programa creado específicamente para imitar páginas legitimas, copiando la imagen completa de una red social, con el objetivo de engañar y hacer caer en error a los usuarios a quien se envía el enlace malicioso. El método de operar es parecido al *phishing* común, se utiliza un correo electrónico de apariencia legítima, donde se solicita la verificación de los usuarios de redes sociales. De esta manera se adjunta un enlace donde se redirecciona a páginas ilegitimas, donde se requiere el ingreso de usuario y contraseñas. Desde luego que al ingresar al vinculo, se activa un *malware*, el cual graba y almacena los datos interceptados por los ciberdelincuentes.

Como es sabido en la actualidad que se vive, han surgido gran cantidad de redes sociales que el objetivo principal es mantener a la humanidad comunicada entre sí. Desde luego facilitan la comunicación entre personas de un país a otro sin retraso, algo que si se analiza décadas atrás era casi imposible. Indudablemente la comunicación a larga distancia era inaccesible para la mayoría de los ciudadanos por lo cual con el auge tecnológico los medios de comunicación también evolucionaron de tal manera que se puede observar sucesos internacionales en tiempo real. Sin embargo, esto también facilito a los delincuentes realizar delitos a través de la red, lo cual ha sido sin duda alguna muy lucrativo al vender

información privada de terceros o utilizando los mismos para beneficios propios.

El *phishing* telefónico, es otro método utilizado por los delincuentes, este es realizado por medio de llamadas telefónicas donde se hacen pasar por empresas que prestan servicios públicos y entidades bancarias. Al comunicarse con las potenciales víctimas, los *phisher* les proporcionan información falsa con la cual intimidan a las personas, indicándoles que tienen problemas por deudas adquiridas y que pueden tener serias consecuencias jurídicas al no cumplir con sus obligaciones. Finalmente, al tener a su víctima con la falsa creencia que están en problemas les solicitan realizar pagos de grandes cantidades de dinero, con la falsa promesa de eliminar cualquier proceso legal en su contra, dichos actos legales son falsos al no existir.

Este tipo de *phishing* suele confundirse con el delito de extorción, en el cual por medio de intimidaciones obligan a las víctimas a pagar una suma de dinero, con la promesa de no ocasionar daño a los familiares de la víctima. Sin embargo, el *phishing* a través del teléfono funciona de tal forma que las personas al momento de vincular sus datos personales a sus redes sociales suelen crear riesgos de seguridad. En consecuencia, los *phisher* roban estos datos para comunicarse con los usuarios y fingir ser empleados de empresas legitimas. Para lo cual solicitan el pago de una suma de dinero con la promesa de no generar consecuencias jurídicas,

solicitan el pago de una deuda bancaria, el pago de multas, pago de servicios por medio de tarjetas de crédito o transferencias electrónicas.

De lo anteriormente establecido se puede deducir que todos los usuarios de algún medio o dispositivo electrónico pueden ser víctimas de la suplantación de identidad. Indudablemente el uso de redes sociales, correos electrónicos y demás medios informáticos, pueden llegar a sufrir violaciones de seguridad y de esa forma robar información privada. Ciertamente el *phishing* sufrió un aumento de víctimas debido a que, en los últimos tres años, el uso de la tecnología se vio incrementada por la utilización del teletrabajo. Por lo cual, al hacer uso por más tiempo de los dispositivos electrónicos, hace más vulnerables a los usuarios, ya que los sistemas informáticos son utilizados para realizar una variedad de transacciones, sin tener que salir de casa.

La suplantación de identidad (phishing) en Guatemala

La suplantación de identidad como ya se ha establecido, es aquella actividad por medio de la cual delincuentes obtienen de forma ilegal información de terceras personas para utilizarlas buscando un beneficio económico dañando el patrimonio de la víctima. Por lo cual el medio más común donde se realizan los ataques de *phishing*, es vía correo electrónico, donde los delincuentes adjuntan un enlace que dirige al usuario a una página web falsa, creada específicamente para robar datos

personales. Desde luego las personas al ingresar a estos sitios ilegítimos, son engañados para que introduzcan nombres de usuarios y contraseñas, tanto de redes sociales como de cuentas bancarias, números de tarjetas de crédito y débito.

Desde luego la información obtenida dentro de estas páginas falsas, son almacenadas dentro de la base de datos que poseen los delincuentes. Seguidamente de obtener la información de forma ilegal los *phisher* pueden hacer uso de los usuarios y contraseñas para ingresar al sistema de los bancos para realizar transacciones sin el consentimiento del titular de la cuenta. Además, pueden lucrar con la información obtenida, como los números de tarjetas de crédito, donde son vendidas por medio del internet en páginas de piratería. Las personas que compran estos datos suelen realizar compras en línea utilizando los números de las tarjetas obtenidas de forma ilícita, donde adquieren productos dentro y fuera del país, sobregirando el crédito disponible.

En Guatemala está siendo habitual recibir correos electrónicos que contienen enlaces evidentemente maliciosos, que solicitan ingresar al enlace adjunto con el fin de realizar una estafa. Los ataques de *phishing* han tenido un incremento considerable en el territorio guatemalteco, debido al desconocimiento que existe de este delito, por los usuarios de redes sociales y de todo tipo de dispositivo electrónico que cuente con acceso a internet. Eventualmente las entidades bancarias realizan

campañas de información, donde se da a conocer todo lo relativo al delito de la suplantación de identidad o *phishing*, a pesar de los esfuerzos para prevenir, los usuarios siguen siendo víctimas de los ciberdelincuentes.

Gran parte de los guatemaltecos, tienen la costumbre de adquirir productos conocidos como piratas y los programas de cómputo no son la excepción. Los ciberdelincuentes utilizan todo tipo de sistema informático para realizar ataques de *phishing*, ya que estos modifican el código fuente, donde insertan *malwares* que no pueden ser detectados una vez ingresan a la computadora. Estos programas no originales, al momento se ser instalados requieren que se desactive el antivirus que se encuentre protegiendo al usuario, de este modo logran ingresar al sistema operativo silenciosamente. Vale decir que existen aplicaciones conocidas como *crack* informático, estos son creados y utilizados sin autorización del desarrollador, que modifican el comportamiento del programa, estos pueden desarrollar una licencia falsa para activar la aplicación, estos en gran parte de las veces contienen virus y *malwares* capaces de interceptar información privada del usuario.

Evolución histórica del delito de suplantación de identidad o phishing

Para entender el surgimiento de la suplantación de identidad, debemos remontarnos a mediados del año 1996, donde fue nombrado este delito como *phishing*. Esto sucede al momento de dar a conocer este delito

informático, el autor de dicho nombre cambio la ortografía de *fishing*, que traducido al español se refiere a la pesca, y lo modifico a *phishing*. De esta manera hace referencia a la pesca cibernética que se realiza por los delincuentes, ya que se lanza un anzuelo y buscan que los usuarios caigan en ellas para poder robar su información. La suplantación que se llevó a cabo se realizó contra los usuarios de cuentas AOL (América Online) donde les fueron robados datos de tarjetas de crédito de miles de personas, que eran usuarios de dichas cuentas, perdiendo así grandes cantidades de dinero.

En los inicios del *phishing*, los estafadores operaban por medio de foros, chat y empezaban por medio de correos electrónicos, los ciberdelincuentes realizaban el engaño por medio de los anuncios de ofertas de empleos en los cuales se ofrecían salarios competitivos y llamativos. Desde luego el objetivo era engañar a las personas para aplicar a dichos trabajos donde tenían que otorgar sus datos completos, números de cuentas bancarias, números de seguro social etc. Los delincuentes al tener la información retiraban el dinero y las trasladaban a otras cuentas obteniendo así un beneficio económico sencillo y repartiéndose lo robado entre los cómplices del delito. Las víctimas sin tener conocimiento de lo que había sucedido perdían su patrimonio en manos de los ciberdelincuentes.

Como se ha mencionado los ciberdelincuentes en sus inicios realizaban ataques a personas que contaban con tarjetas de crédito y débito, o a quienes se dejaban seducir por ofertas de trabajo bien remuneradas. Así mismo con el paso del tiempo los ciberdelincuentes utilizaron los mensajes por correo electrónico, donde enviaban enlaces en su interior solicitando información confidencial, haciéndose pasar por entidades bancarias de confianza. Se puede mencionar que en el inicio de este método los usuarios desconocían en su totalidad modalidad de estafa, se iniciaron campañas dando a conocer información sobre este ilícito para la protección de los datos privados. No obstante, estas no dieron resultados ya que los delincuentes envían miles de correos diarios con *malwares*, esperando a usuarios inexpertos que caían en la trampa y de esa forma robar sus datos.

En consecuencia, los delincuentes informáticos en sus inicios obtenían ingresos ilícitos a través de engaños hacia sus víctimas. Estos *phisher* solían trabajar de forma individual obteniendo por sí solos, los usuarios de los correos electrónicos donde se enviarían los mensajes de *phishing*. Con el avance tecnológico, los ciberdelincuentes también han sufrido una evolución donde actualmente tienen una estructura para realizar estos actos ilícitos. Ciertamente estos delincuentes modernizaron su forma de atacar a los usuarios, ya que poseen expertos informáticos que se encargan de la programación y creación de *malwares* y páginas web maliciosas, así

como de personas que realicen los ataque y otros encargados de realizar las transacciones.

Estadísticas de ataques informáticos en Guatemala

Guatemala al igual que muchos países de Latinoamérica, han sido objeto fácil de los ataques informáticos. Desde luego el *phishing* siendo ya un delito informático bastante conocido, aún tiene un gran porcentaje de efectividad donde robar información de los usuarios que caen en el engaño. Por lo tanto, al ser un ilícito ya conocido es posible identificar los mensajes de *phishing* que contienen *malwares*. Es necesario considerar que los ciberdelincuentes poseen basto conocimiento en informática y haciendo uso de la ingeniería social, realizan efectivos ataques donde buscan encontrar un punto vulnerable del usuario para hacerlo caer en error y de esa forma robar su información. Por otra parte, este acto ilícito aún tiene un porcentaje alto de efectividad, donde los *phisher* obtienen ganancias, lo que hace una actividad lucrativa y muy perjudicial para sus víctimas.

Al hacer referencia a la ingeniería social se utilizará la definición del ingeniero Gonzales Juárez D.D. (2012). De su tesis profesional, dicho concepto es de gran importancia ya que da una definición de una forma sencilla y muy completa y establece que.

> El conjunto de técnicas destinadas a explotar las vulnerabilidades de seguridad de un sistema recibe el nombre de Ingeniería Social, el Ingeniero Social intenta persuadir y manipular a una persona para obtener información personal sensible o información sobre las empresas donde trabajan (p.4).

Los ataques informáticos han incrementado desde su origen por el avance tecnológico que se vive, cada año se crean nuevos medios de comunicación, programas, aplicaciones y plataformas de contenido en línea. Por lo cual, se crean vulneraciones de seguridad para los usuarios, según el reporte de ciberseguridad del año 2020 realizado por la Organización de los Estados Americanos (OEA), se estableció que en Guatemala existen 19,986,482 abonos a teléfonos celulares. Esto se refiere a los abonos a un servicio de telefonía móvil que dan acceso a una red, esta puede ser de tercera o cuarta generación. En consecuencia, se puede indicar que los guatemaltecos hacen un uso continuo de la red de internet, por lo cual se encuentran susceptibles de caer en engaños que dañen su patrimonio.

En Guatemala en el año 2020, según la Superintendencia de Telecomunicaciones, existían 20 millones de usuarios de teléfonos celulares, lo cual nos indica que existen ciudadanos con más de un teléfono inteligente a su disposición. Así mismo, en el año 2018 la cantidad de estos dispositivos era de 8 millones, lo que demuestra el crecimiento considerable en la adquisición de estos aparatos tecnológicos. Por lo cual teniendo en cuenta la cantidad de usuarios de estos medios de comunicación, con posible acceso a internet, existe una gran variedad de

delitos que pueden ser cometidos a través de los sistemas informáticos esto derivado a que la legislación guatemalteca no cuenta con una norma que tipifiquen estos actos ilícitos.

Las estadísticas muestran un panorama de los ataques de delitos informáticos realizados a los usuarios en Guatemala. Por lo cual, a través de la unidad de combate contra los delitos informáticos de la Policía Nacional Civil en el año 2016, se estableció que los usuarios de los medios informáticos poseen una fragilidad al hacer uso de estos sistemas. En consecuencia, entre los delitos más frecuentes tenemos la suplantación de identidad que ocupa el primer lugar con un 49%, del total de denuncias de delitos informáticos, así mismo con un porcentaje alto se encuentra la pornografía infantil 31% y el ciberacoso 27%. También la Superintendencia de Bancos, en el año 2016 detecto más de 300 casos de suplantación de identidad donde se solicitaba la apertura de operaciones bancarias, donde 173 de estos procedieron y lograron su objetivo mientras que 142 gestiones fueron denegadas por el origen de las mismas.

La Superintendencia de Bancos de Guatemala, en el año 2020 recibió 193 casos de suplantación de identidad donde se realizaron aperturas de operaciones. Por lo tanto, se ve un incremento en los ataques que logran su objetivo, donde obteniendo datos de forma ilegitima que son utilizados para realizar operaciones que dañan a una tercera persona. Del mismo modo, en el año 2020, la SIB observo 206 casos donde se clonaron tarjetas

de crédito y debido, estos datos fueron recopilados por medio de programas maliciosos que al momento de ingresar a un enlace y proporcionar información sensible creyendo que se encuentran en una página legitima. Esto muestra que este ilícito obtuvo un incremento del 42.1% con relación al año 2019.

Según el reporte de la Policía Nacional Civil y la Subdirección General de Investigación Criminal, se estableció que, en el año 2021, fueron denunciados 893 casos de delitos informáticos. Es necesario indicar, que se cometieron 99 estafas, 64 robos de identidad, 26 robos, 19 casos de acoso sexual y 10 casos de pornográfica infantil, entre otros. Desde luego estas cantidades de delitos informáticos son únicamente los denunciados, ya que existen muchos ciudadanos que no realizan la respectiva denuncia. Como es evidente estos casos lamentablemente no pueden ser contabilizados, pero se sabe que son múltiples los ataques que se realizan en contra de los usuarios, robando la información y lucrando con los datos obtenidos de forma ilegal.

Tal y como se mencionó sobre los ataques de *phishing*, se debe abordar sobre los ataques por *malwares*, ya que muchos de estos son utilizados para realizar *phishing.* Desde luego estos programas son creados con el objetivo de tomar el control de equipos de cómputo de usuarios individuales y grandes corporaciones. Estos archivos maliciosos son enviados por medio de correos electrónicos para captar información

sensible del usuario para ser utilizada con fines lucrativos que perjudican a las víctimas. Como es evidente existen una gran diversidad de estos *malwares*, que se encuentran dentro de la red y suelen ser muy difíciles de detectar y contrarrestar, los ataques han tenido un incremento considerable, que pone en riesgo a los usuarios tanto a personas con experiencia en informática, así como a sujetos inexpertos.

Con el incremento exponencial del uso de las plataformas virtuales, de igual forma incrementaron los ataques informáticos, aprovechándose los ciberdelincuentes, del mayor tiempo de los usuarios que permanecían haciendo uso de dichos medios y con la automatización de muchas funciones por medio de las vías electrónicas. Es necesario considerar que Guatemala sufrió un aumento en cuanto a los ataques de *phishing,* de igual forma el resto de Latinoamérica. Esto se ha debido en su mayor parte a que muchos países no cuentan con leyes que tipifiquen este delito. Sin embargo, cabe mencionar que en Europa y Norteamérica este delito sufrió una disminución de ataques efectuados, por las legislaciones que protegen a los usuarios y castigan a los infractores.

Como se observa con lo anteriormente expuesto se puede establecer que Latinoamérica sufrió un incremento significativo con respecto a los ataques de *phishing*. Guatemala con un porcentaje alto de ataques se encuentra entre los países que más han sido vulnerables a los ataques de este delito el cual roba información privada de los usuarios. Desde luego

los ataques recibidos no siempre son de delincuentes guatemaltecos, estos suelen ser realizados por personas que se encuentran fuera del territorio nacional. De esta manera logran obtener beneficios económicos con la información obtenida de forma ilegal, la cual pueden vender para que otros realicen las transacciones o pueden ser utilizadas por sí mismos.

El incremento de los ataques como se mencionó en párrafos anteriores, el *phishing* sigue siendo el delito informático con un porcentaje alto. Por lo tanto, los *phisher* han utilizado como anzuelo páginas web modificadas que contienen información falsa con respecto a diversos sucesos del acontecer diario. En síntesis, se puede establecer que los ataques de este delito van en incremento, esto sucede por la falta de legislación que tipifique este ilícito penal. Esta situación de no poseer una norma jurídica que lo regule, hace que su investigación se dificulte aún más, por el motivo que no existen estrategias de investigación, de igual forma se tiene la falta de personal capacitado que pueda realizar la recolección de los indicios y pruebas para dar con el verdadero delincuente.

Bien jurídico tutelado violado por la suplantación de identidad o phishing

Los bienes jurídicos tutelados se pueden definir, como aquellos derechos inherentes a la persona humana, los cuales son necesarios para poseer una vida digna dentro de la sociedad. Por lo tanto, estos están protegidos dentro de cada legislación, donde el estado es el obligado de garantizar

que sean respetados y que en caso de sufrir una violación sean reparados al estado que se encontraban. En otras palabras, los bienes jurídicos son aquellos que el hombre utiliza en su diario vivir dentro de la sociedad y son necesarios para satisfacer sus necesidades, tales como el derecho de la libertad, la vida, la dignidad humana, el trabajo, la propiedad privada entre muchos más. Por lo tanto, se encuentran resguardados dentro de la norma constitucional guatemalteca, donde se protegen desde la norma suprema.

El estado siendo el único que posee el *ius puniendi*, el cual se debe entender como la facultad que tiene con exclusividad para impartir justicia y castigar. Por lo cual el sistema de gobierno se encuentra organizado para velar por la protección de los valores que son necesarios para que el ser humano tenga una correcta convivencia social respetando los derechos y valores de los demás habitantes. Desde luego los bienes pueden ser tanto humanos, morales y materiales, los cuales por su grado de importancia el estado los convierte en intereses que deber ser protegidos jurídicamente. Finalmente deben ser tutelados por el estado el cual debe crear normas penales por medio de su órgano legislativo, que protejan dichos bienes y castigando a los infractores de las violaciones cometidas.

Como se observa con lo expuesto anteriormente, poseer bienes jurídicos tutelados es de suma importancia, ya que solo de esa forma se pueden realizar normas eficientes que castiguen a los infractores. Por lo tanto, se

debe entender que todos los delitos cometidos son violaciones a diferentes bienes jurídicos tutelados. En consecuencia, con la tipificación como ilícitos de estos actos que se cometen contra de los derechos de los habitantes, los legisladores han impuesto diferentes penas y sanciones que buscan dar justicia a las víctimas. Así mismo se debe recordar que unos de los fines del derecho penal es la prevención del delito y la efectiva rehabilitación del delincuente para que luego de cumplir la pena impuesta sea integrado a la sociedad y sea útil para la misma.

En el ordenamiento jurídico guatemalteco se observa que las figuras delictivas tipificadas en el Código Penal se encuentran agrupadas, según el bien jurídico tutelado que protegen. Tal es el caso de los delitos contra la vida y la integridad de la persona, delitos contra el honor, delitos contra la libertad y la seguridad sexuales y contra el pudor. También delitos contra la libertad y seguridad de la persona, delios contra el orden jurídico familiar y contra el estado civil, delitos contra el patrimonio, delitos contra la seguridad colectiva, delitos contra la fe pública y el patrimonio nacional, la falsedad personal, delitos contra la economía nacional el comercio la industria y el régimen tributario, delitos contra la seguridad del estado, entre otros.

Con respecto a los bienes jurídicos tutelados el reconocido licenciado De Mata Vela (2011), proporciona una definición breve y concisa, con gran contenido que enriquece la presente investigación y establece que:

> Los intereses o bienes jurídicos tutelados que corresponden generalmente a una persona individual son: la vida, su integridad personal, su honor, su seguridad y libertad sexual, su libertad y seguridad personal, su patrimonio, su orden jurídico familiar, su estado civil, etc.; en tanto que las personas jurídicas o colectivas pueden verse lesionadas o puestas en peligro en su patrimonio o en su honor. El estado particularmente puede verse amenazado, tano en su seguridad interna como externa, y la sociedad se protege de los delitos que atentan contra la seguridad colectiva (p.231).

Una vez entendido lo que son los bienes jurídicos tutelados se deben de establecer cuáles de estos son vulnerados por el delito se suplantación de identidad o *phishing*. Por lo cual se puede indicar que este delito se encuentra dentro de legislaciones extranjeras y convenios internacionales como un delito informático. Este al momento de realizarse, vulnera varios bienes jurídicos que son afectados en conjunto, los mismos son violados por estos actos ilícitos que son realizados por medio de cualquier dispositivo electrónico a través del internet. En consecuencia, los bienes jurídicos violados por estos actos ilegales son, honor, la seguridad de la persona, el patrimonio, la seguridad del estado, la economía nacional. Como se observa los delitos informáticos vulneran derechos que el estado está obligado a proteger.

Cabe mencionar que el bien jurídico tutelado del patrimonio es el área donde el delito de *phishing* causa más daños. El patrimonio puede ser definido como el conjunto de obligaciones y derechos que posee una persona y pueden ser representados por un valor económico. Estos constituyen una agrupación donde se incorporan todos los bienes que tiene en su poder un sujeto, siendo estos materiales e inmateriales,

existentes o que en su caso aun no existan, divisibles o indivisibles, fungibles o no fungibles. Desde luego el estado guatemalteco es el obligado de proporcionar la seguridad adecuada para la protección del patrimonio de todos los ciudadanos, y crear recursos que restituyan los daños causados en su momento por los delincuentes.

En el trabajo titulado el bien jurídico protegido en el delito de estafa informática el licenciado Sánchez Bernal (s.f.), de la universidad de salamanca proporciona una definición que enriquece el contenido del presente trabajo y establece que:

> Debe señalarse la existencia de tres concepciones diferentes de *patrimonio*: la jurídica, la económica y la económico-jurídica. En lo que se refiere a la concepción jurídica, el patrimonio está integrado por "…el conjunto de derechos patrimoniales de una persona, esto es, aquellos valores económicos que son reconocidos como derechos subjetivos patrimoniales por el derecho objetivo". Este concepto ha sido severamente criticado por cierto sector de la doctrina, por su imprecisión al referirse a "derechos subjetivos patrimoniales", tanto como su vaguedad por cuanto excluye valores no integrados en el derecho objetivo, como las expectativas, que tienen su importancia en el tráfico y, desde el punto de vista económico, son incluso cuantificables en dinero (p.116).

En consecuencia, se establece que el patrimonio individual es el conjunto de bienes materiales e inmateriales en los cuales se engloba todos los derechos y obligaciones que este sujeto a una persona. Por lo cual con lo expuesto y analizando el método de operar el *phishing* se observa que este vulnera directamente el patrimonio de su víctima violando así un bien jurídico tutelado el cual es protegido por el Estado guatemalteco. Desde luego el usuario es susceptible de caer en las trampas enviadas por los

phisher. Obviamente la víctima será sujeto del robo de información privada como los datos de identidad, usuarios de redes sociales, números de tarjetas de crédito y débito, datos de cuentas bancarias para retirar dinero y robarlo sin que las víctimas puedan hacer algo al momento que se esté realizando el ilícito.

Según el artículo 3 “El Estado de Guatemala se organiza para proteger a la persona y a la familia; su fin supremo es la realización del bien común” (Constitución Política de la República de Guatemala, 1985). Por lo cual, analizando lo establecido en la norma constitucional, si el estado protege a la persona que es todo ente capaz de adquirir derechos y contraer obligaciones, esa protección se extiende más allá y adquiere un fin adicional que es velar que se respeten todos los atributos que poseen los ciudadanos, es decir, todos aquellos que son inherentes a la persona humana y que la propia legislación respeta y está obligada a proteger. Por supuesto estos pueden, ser el nombre, la capacidad, el patrimonio, el estado civil, el domicilio, la nacionalidad entre otros, como se observa son derechos que van inmersos en la persona por lo cual el estado está obligado a protegerlos.

El patrimonio siendo un atributo esencial de la persona, el estado le dio la calidad de bien jurídico tutelado. Por lo cual, al momento de darle dicha categoría se obligó a velar por su protección en cumplimiento de la norma constitucional. En consecuencia, el estado debe de desarrollar una ley que

regule la suplantación de identidad o *phishing* como delito, el cual debe poseer una pena para reprimir a sus infractores y los medios a seguir para el resarcimiento de los daños causados. Así mismo, el *phishing* o suplantación de identidad al momento de ser realizado este afecta directamente el patrimonio, al robarle dinero de cuentas bancarias y tarjetas de crédito y débito, ya que al inducir a error estos ciberdelincuentes tienen el control y manejo de las cuentas robadas y con ello acceso a información personal privada que puede ser vendida a través de la red para percibir un beneficio económico.

Métodos de defensa contra delitos informáticos

Como se ha establecido con anterioridad los delitos informáticos son todos aquellos actos delictivos que se realizan a través de los medios informáticos a través de dispositivos electrónicos. Por lo cual en la actualidad que se vive, la informática ha tomado mayor relevancia en la vida cotidiana de los ciudadanos, ya que por medio de las aplicaciones digitales o plataformas en línea se realizan gran cantidad de tramites, transacciones, compras y ventas de productos o bienes. De este modo se interactúa con personas de diferentes países a través de la red y se realizan actividades laborales inclusive estatales. De esta manera, los usuarios de las aplicaciones anteriormente identificadas poseen una vulnerabilidad en seguridad, por lo cual pueden llegar a ser víctimas de ciberdelincuentes. Estos cometen delitos utilizando los medios informáticos, y atentan contra

la integridad psicológica o física, daños irreparables dentro del patrimonio y daños contra el honor.

Los usuarios actualmente cuentan con gran variedad de métodos para protegerse y no ser víctima de los ciberdelincuentes. Ciertamente podemos mencionar programas que fueron desarrollados para la protección e identificación de *malwares,* así como de páginas maliciosas. Desde luego la efectividad de estos medios de seguridad informática tiene un porcentaje alto, a pesar de esto no se tiene la garantía de una protección total, que mantenga a salvo el equipo y la información del usuario. Sin embargo, a pesar de tener estas aplicaciones de seguridad, el método más efectivo es la prudencia que se debe poseer, al ingresar en sitios web, así como analizar la información que se recibe en mensajes por correos electrónicos que pueden solicitar llenar formularios o encuestas con información confidencial.

Derecho comparado

Se puede establecer que el derecho comparado, es el estudio de las normas jurídicas vigentes dentro de países con similares legislaciones. El objetivo de realizar esta comparación es encontrar una solución a problemáticas que en el pasado afectaron a un país en específico y que actualmente afecta a otro. Para realizar estos estudios es necesario conocer la historia del motivo la creación de un cuerpo legal y los principios en que se basa.

En consecuencia, al tener estos elementos básicos del estudio, se debe determinar los beneficios que fueron obtenidos desde el momento de la incorporación a la legislación de un estado, así como su funcionamiento, niveles de efectividad y sobre todo si el problema que motivo la creación de la norma se vio resuelto. Por lo cual, observando estos resultados, se realiza el análisis de la forma más efectiva para la incorporación de esta solución a un país que afronta casos similares al país comparado.

La licenciada Morineau M. cita al licenciado Rene David (2002), quien presenta una definición en cuanto al derecho comparado el cual es de suma importancia por su contenido doctrinario, y establece que:

> El papel del derecho comparado es parecido al de la historia; dándole al estudioso del derecho nacional la perspectiva necesaria para tener una visión adecuada de los puntos fundamentales y la evolución de su derecho, y permitiéndole, por otro lado, un planteamiento más exacto de los posibles problemas que se presenten, para lograr una mejor solución a las cuestiones jurídicas que se deban resolver" (p.22)

Los estudios de legislaciones extranjeras cuentan con una larga tradición dentro del mundo jurídico, ya que desde hace muchos años se han realizado estos análisis de los modelos de las regulaciones existentes en diferentes ciudades. El objetivo siempre ha estado enfocado en la búsqueda del mejor método para su adaptación y aplicación de dichas normas dentro de otro territorio. La comparación de legislaciones ha sido de suma importancia dentro de la historia ya que con ella se ha realizado un mejoramiento a las leyes cuya existencia era anterior, siendo estas de menor alcance y de inferior fuerza punitiva. Por lo cual estos cuerpos

legales fueron mejorados en su esencia por medio de la ampliación o por la creación de normas específicas donde se regulaban aspectos que no contaban con una tipificación.

En 1900 se celebró el primer congreso internacional de derecho comparado que fue realizado en Paris, Francia. Ciertamente gracias a este congreso se comenzó a utilizar el término “derecho comparado” con más frecuencia, desde este primer evento ha tenido una evolución en cuanto a su concepto, fines y métodos que se utilizan, estos han surgido en distintos congresos que se realizan cada cuatro años en distintos países. Indudablemente la visión de sus inicios era la creación de un derecho común para toda la humanidad, con el transcurso del tiempo tuvo una orientación más realista a la actualidad donde el derecho comparado tiene un papel muy importante en el derecho internacional que se ha considerado como necesario y de gran utilidad para el mismo.

Se debe mencionar que el estudio del derecho comparado en sus inicios no fue nada sencillo por diferentes factores que influyeron en su complicación. Desde luego los obstáculos no fueron siempre de carácter jurídico, es decir existían factores que impedían concretamente su análisis, siendo estas el idioma, la lingüística, la escritura y la cultura. Definitivamente al establecer lo anterior se debe entender que aun conociendo el idioma y teniendo una cultura semejante, existía la falta de comprensión en los términos utilizados por los legisladores, ya que

existían términos semejantes, pero con significados diferentes. Por tal motivo ese problema se observaba en sus conceptos, términos, instituciones jurídicas y principios, lo cual complico considerablemente en el inicio al estudio del derecho comparado.

Dentro de la comparación jurídica de legislaciones extrajeras se debe tener conciencia que existe una gran diversidad de puntos de vistas que ayudarán a tener una mejor perspectiva dentro del estudio de las mismas. Por lo cual se puede buscar similitudes dentro de las dos legislaciones, así como las diferencias entre las mismas, de igual forma analizar las razones de la creación de las normas. De este modo el estudio de las bases permitirá evaluar el fondo y el ámbito de aplicación de cada cuerpo legal, esto ayudará dentro de la comparación a encontrar una solución al problema. En general se toman vías semejantes, pero con variaciones para adaptar dichas normas jurídicas a la legislación del país que posee el problema y de esa forma contrarrestar con la realización de los delitos que carecían de tipificación.

El profesor Gutteridge H.C, nos entrega una explicación bastante interesante, donde señala dos formas de observar el derecho comparado. Por lo cual, lo que establece el profesor Gutteridge, ayudara a la comprensión en la forma en que se debe realizar una comparación para conocer lo que origina la necesidad de la creación de la norma y la aplicación de la misma. En consecuencia, establece que el:

> Derecho comparado descriptivo. Rama que se refiere al análisis de las variantes que se puedan encontrar entre los sistemas jurídicos de dos o más países. Derecho comparado aplicado: Esta rama va más allá de la mera obtención de información del derecho extranjero y su utilidad puede ser tanto teórica, como práctica. En el primer caso puede referirse a un estudio comparativo que ayude a un filósofo del derecho a elaborar teorías abstractas que, a su vez, apoyen al historiador en el conocimiento de los orígenes y desenvolvimiento de instituciones y conceptos jurídicos. Desde el punto de vista de la práctica, el derecho comparado aplicado puede referirse a reformas jurídicas, tanto como a la unificación de derechos distintos (p.20).

De lo anterior expuesto se observa que se puede orientar la investigación desde los puntos de vista descriptivo y aplicado, este a su vez se divide en la teoría y la práctica. En todo caso estas formas de tomar una comparación jurídica, son de suma importancia ya que una va respaldada de la otra. De este modo no podemos separarlas entre sí, ya que se necesita que se realice una descripción exacta de las posibilidades que se generan al contemplar la adopción de una norma para ser implementada dentro de otro estado. Es decir, se deben tomar en cuenta todos los resultados que puedan ayudar, así como perjudicar al momento de la aplicación de esta norma, ya que cada país es completamente diferente al otro y los resultados de las leyes suelen ser diferentes si no se realizan los estudios adecuados.

Dentro del estudio del derecho comparado en el ámbito penal, se deben tomar en consideración la aplicación de estas nuevas normas dentro de un país determinado que necesite una solución a conflictos legales surgidos por actos de carácter ilícitos. Por lo cual se debe realizar desde el punto de vista aplicado y a la teoría, que ayuda al análisis histórico para observar

los motivos que generaron la necesidad de la creación de una norma jurídica, y estudiar el fondo de los conceptos jurídicos, así como la estructura y funcionamiento de las instituciones creadas. En consecuencia, se debe observar la forma de aplicación de estas normas jurídicas, así como la forma idónea para la incorporación de estas leyes, ya sea por medio de la creación de un cuerpo legal nuevo o la reforma de uno ya existente para la tipificación de uno o varios delitos.

Regulación de delitos informáticos en Guatemala

Guatemala cuenta actualmente con el Código Penal, Decreto número 17-73 que fue emitido por el Congreso de la República y entró en vigor en el año 1974. Ciertamente dicho cuerpo legal esta desarrollado de una forma ordenada de fácil uso y estudio, dentro del mismo se detallaron definiciones como lo es la legalidad, el delito y la pena, entre otros. Dentro de los considerandos del Código Penal se encuentra una frase que es interesante y establece que la creación se hace necesaria y urgente acorde con la realidad guatemalteca y los avances de la ciencia penal. Con lo antes mencionado deja ver que fue creado según las necesidades que existían en 1974, las cuales no son las mismas que se tienen en la actualidad dentro del territorio guatemalteco. Ciertamente con el avance tecnológico han surgido nuevas figuras delictivas que no han sido incorporadas dentro del ordenamiento jurídico penal guatemalteco.

El Código Penal guatemalteco ha sufrido varias reformas donde ha incorporado una serie de nuevos delitos, los cuales han sido tipificados de una forma certera según la época y a las necesidades que se tenían al momento de efectuarse las mismas. Ahora bien, la reforma que compete al presente trabajo es el Decreto número 33-96, reformas al decreto 17-73, emitido por el Congreso de la República y publicado en el diario de Centro América el 25 de junio de 1996 que contiene 39 artículos. De hecho, se puede resaltar que se incorporan delitos contra el derecho de autor, la propiedad industrial y delitos informáticos. También se observa nuevamente en el tercer considerando de la reforma que establece que los avances tecnológicos obligan al estado a legislar para la protección de los derechos de autor en materia informática.

Con respecto a lo establecido anteriormente, Guatemala cuenta con una legislación penal, la cual fue desarrollada según las necesidades que surgían al momento de su creación. Por consiguiente, el Decreto número 33-96 que reformo el Código Penal, fue de importancia ya que agrego los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos. Por lo cual se debe hacer mayor énfasis en el apartado de delitos informáticos, ya que fue una incorporación novedosa y que cubría las necesidades existentes. Cabe mencionar que desde 1996, en Guatemala no se generado nuevamente una modernización en cuanto a legislación, que regulen los nuevos delitos informáticos y al no contar con

una norma jurídica que las regule las mismas no pueden ser perseguidas penalmente.

Guatemala con el Decreto número 33-96, fue la última vez donde adapto su legislación a los avances tecnológicos que existen, por lo cual el Código Penal quedo rezagado por casi 27 años, ante la evolución de los delitos que se realizan mediante los medios informáticos. En consecuencia, estos actos ilícitos han tenido un crecimiento exponencial cada año, quedando muchos sin una tipificación dentro de un cuerpo legal vigente. Es decir, se hace necesario de forma urgente la creación de nuevas reformas que modifiquen el Código Penal guatemalteco, agregando nuevos delitos informáticos, como lo es la suplantación de identidad o *phishing*, o la creación de una norma especial que contenga todos estos delitos informáticos, junto a sus multas, sanciones, instituciones, medios de investigación y formas de resarcimiento a las víctimas.

Como se estableció en párrafos anteriores la legislación penal guatemalteca ha quedado rezagada con respecto a los delitos informáticos, los cuales han evolucionado rápidamente afectando así a cientos de personas en el territorio guatemalteco. Aunque el Estado, se encuentra organizado para proteger a la persona, así como garantizar su libertad, la justicia y la seguridad, debe generar los medios suficientes tanto legales como de forma institucional que funcionen para la prevención de los

delitos informáticos. Desde luego, deben existir procedimientos para el resarcimiento de daños y perjuicios, los cuales son causados por la violación de un derecho que se encuentra protegido constitucionalmente.

En el año 2019 se presentó ante el honorable pleno del Congreso de la República de Guatemala la iniciativa legislativa número 5601, que proponía la aprobación la ley de prevención y protección contra la ciberdelincuencia. Desde luego, esta iniciativa generaba gran expectación, ya que contaba con los delitos informáticos que durante años no tuvieron una tipificación adecuada. Vale indicar que esta iniciativa fue desarrollada de una forma muy detallada, por medio de estudios y con la ayuda de instrucciones del Ministerio de Gobernación y el Consejo de Europa, así como de entidades del sector justicia de Guatemala, esto se realizó con el objetivo de cumplir con lo establecido por el convenio contra la ciberdelincuencia suscrito en Budapest. La legislación penal guatemalteca con la aprobación de la mencionada ley daría un avance importante a su modernización, y de esa forma buscaría suscribirse al mencionado convenio.

Guatemala un año después de la presentación de la iniciativa legislativa 5601, solicito acceder a la convención de Budapest, la cual fue aprobada y se envió la invitación formal por medio del ministerio de Relaciones Exteriores para formar parte del mismo. El convenio de Budapest, fue suscrito en el año 2001 y entro en vigor en el año 2004, este fue el primer

tratado que protege a la sociedad de los delitos informáticos. Por lo cual, desarrolla medios de elaboración de políticas penales comunes entre los países, así como la creación de técnicas cuyo objetivo es la investigación y cooperación entre los países que lo integran. Sin duda esto facilita de gran forma la persecución penal en contra de los ciberdelincuentes, así como su extradición en caso que estos se encuentren fuera de las fronteras del país de la víctima. En consecuencia, al integrar dicho convenio los países se obligan a desarrollar leyes para la protección contra los delitos informáticos.

Cabe mencionar que el 4 de agosto del año 2022, se aprobó por el Congreso de la República de Guatemala con 100 votos a favor, la ley de prevención y protección contra la ciberdelincuencia, Decreto número 39-2022. Ahora bien, dicha norma jurídica era considerada de gran importancia para el desarrollo de la legislación guatemalteca, ya que se incluían en ella una variedad muy importante de delitos informáticos. Así mismo, contaban con una tipificación completa para establecer si los actos realizados por los individuos de forma ilícita podían ser considerados como delitos. De esta manera, al constatar la existencia del acto ilícito, debía imponerles las sanciones que dicho cuerpo legal contenía para cada caso.

Sin embargo, el 1 de septiembre del año 2022 se publicó en el diario de Centro América el Acuerdo número 14-2022 del Congreso de la República, el cual contenía la decisión del honorable pleno, de suspender en definitiva el procedimiento de formación de la Ley del Decreto número 39-2022. En el mismo acuerdo se ordenaba el traslado de este al archivo de la Dirección Legislativa, poniendo fin inmediato y en definitiva al procedimiento, por lo cual la norma que por un momento se consideró como un avance para la legislación penal guatemalteca, no entraría en vigencia. Dicho de otra manera, se tiene como un retroceso en la modernización de la ley penal, por lo cual los delitos informáticos siguen sin tener una tipificación jurídica, que encuadre todos los elementos de realización para ser considerada como un ilícito.

Regulación de delitos informáticos en Colombia

En Colombia surgió la necesidad de formular una norma legal en la cual se tipificarían los delitos que violaran los derechos de los ciudadanos que trabajaban de forma honrada, quienes eran constantemente afectados por delitos cometidos a través de la informática. Por lo cual los ciberdelincuentes haciendo uso de los avances tecnológicos, robaban números de tarjetas de crédito y débito para apropiarse de forma ilícita del patrimonio de sus víctimas. Así mismo se realizaban vulneraciones y alteraciones a equipos de cómputo, para realizar transferencias y mediante programas afectaban la seguridad de los cajeros para sacar provecho de

sus actos ilícitos. En consecuencia, en Colombia durante el año 2007, empresas y particulares perdieron cerca de 6 billones de pesos, que equivalen 11 mil millones de quetzales, esto gracias a los delitos informáticos.

Es de esa forma que el 5 de enero del año 2009 entro en vigencia la Ley número 1273, del Congreso de la República de Colombia, la cual se refiere a las reformas que modifican el Código Penal colombiano vigente. Además, con la promulgación de dicha norma, se tiene como novedad la incorporación de un nuevo bien jurídico tutelado el cual se denominó, de la protección de la información y de los datos. Por lo cual, los ciudadanos ya contaban con un cuerpo legal que protegía sus derechos, información y patrimonio, tenían la seguridad que al momento de ser víctimas de algún delito informático contenido en la nueva ley se castigaría al infractor colocándole una pena y multa para resarcir el daño causado a los ciudadanos. Y de esta forma se lograría una prevención de los delitos informáticos.

La Ley número 1273 tipifico como delitos las conductas que tenían relación con el uso de datos personales, ya que con los avances tecnológicos al aplicarse estos pueden ser fácilmente utilizados para la realización de actos ilícitos. De esta manera algunos de los delitos tipificados son, el acceso abusivo a un sistema informático, interceptación de datos informáticos, uso de *software* malicioso, la violación de datos

personales, suplantación de sitios web para capturar datos personales siendo este ultimo de gran importancia para el presente trabajo. A pesar que la ley número 1273 contiene tan solo cuatro artículos en los cuales se adicionan al Código Penal colombiano diez nuevas figuras delictivas, todas ellas realizadas por medio de los sistemas informáticos.

La Ley número 1273 contiene diez nuevas figuras delictivas, que fueron adicionadas al Código Penal colombiano, estas regulan de una forma muy adecuada los actos ilícitos informáticos. De esta manera se pueden establecer los hechos y la forma en que un individuo debe de actuar para que se pueda indicar que realizo un ilícito penal, ya que al transgredir la norma el sujeto deberá ser sometido ante los tribunales de justicia para que sea juzgado según el delito cometido y para que le sea impuesta la pena correspondiente. En consecuencia, en Colombia se aplican penas desde 36 meses de prisión hasta un máximo de 120 meses en los casos más graves, con multas que van desde los 100 hasta los 1500 salarios legales vigentes.

Se puede establecer que el artículo 269F, de la ley 1273, del Congreso de Colombia (2009), contiene una tipificación bastante completa en la regulación de este delito y establece que:

> VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique *p* [*sic*] emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de

> cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Ley 1273, del Congreso de Colombia, 2009 artículo 269F)

Según lo establecido en anterior artículo se puede establecer que el contenido del mismo tiene gran importancia ya que tiene un mayor alcance al momento de una investigación penal. Por lo cual al analizar la ley colombiana abarca una serie de actos que pueden ser realizados por los ciberdelincuentes quienes obtienen, almacenan, sustraen, venden, intercepten y divulgan información de terceras personas obteniendo ganancias económicas. Por lo cual, para el investigador del presente trabajo, el artículo 269F de la ley 1273, tipifica de buena manera este ilícito, ya que regula la forma de adquirir y distribuir los datos obtenidos ilegalmente. Por lo cual las penas establecidas en la presente ley, son muy acertadas para quienes realicen estos delitos.

Es importante observar el texto original del artículo 269G. de la ley 1273, del Congreso de Colombia (2009), que ayudara a la observación en la redacción y los aspectos regulados dentro de esta norma jurídica la cual establece que:

> SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos

> anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito (Ley 1273, del Congreso de Colombia, 2009 artículo 269G)

Desde luego, del artículo anterior, se establece que se considerara como delito, la suplantación de sitios web para capturar datos personales. Por lo cual se regula este ilícito de buena forma ya que contiene los elementos básicos para la realización de este acto por medio de los medios informáticos. De este modo se sancionará a quienes de forma consciente diseñe, desarrolle y venda programas que generen paginas emergentes o anuncios para caer en error al usuario y robar su información. En consecuencia, para los infractores se les impondrá una pena justa al daño causado que puede ser desde 48 a 96 meses de prisión y una multa económica que sus extremos tanto mínimo y como el máximo se encuentran muy bien reguladas junto a la pena que se verá agravada en una tercera parte a la mitad, esto en casos que los delitos cumplan con los elementos de su tipificación.

Colombia el día 16 de marzo del año 2020, entrego ante el Consejo de Europa, el instrumento legal con el cual se adhiere al convenio de Budapest. Desde luego, ya se mencionó con anterioridad que es el único tratado que busca la protección de los ciudadanos ante los ataques de delitos informáticos, y que sirve como estándar a nivel global para la lucha contra la ciberdelincuencia. Por tal motivo, Colombia al tener la necesidad de mejorar la cooperación entre estados, y fortalecer su capacidad de prevenir, detectar, investigar, imponer multas y penas acordes a los

delincuentes que actúan en el ciberespacio se suscribe al mencionado convenio. Es necesario establecer que ya había 65 países suscritos, los cuales actuaban de forma conjunta.

Colombia el 16 de marzo de 2020, se adhiere al convenio de Budapest, realizando así un paso importante en la lucha contra los delitos informáticos. Por lo cual se tenían las siguientes expectativas que son de gran importancia su conocimiento y que según el Ministerio de Relaciones Exteriores colombiano en su página web, https://www.cancilleria.gov.co indica:

> - Actualizar y complementar la legislación nacional a los estándares internacionales contra la ciberdelincuencia.- Formalizar y dinamizar los canales de intercambio de información con los países miembros del Convenio, para facilitar las investigaciones judiciales sobre hechos delictivos de carácter transnacional.- Acceder a proyectos y programas para la transferencia de conocimientos, apoyo investigativo, soporte tecnológico y acciones conjuntas bilaterales y multilaterales.- Mejorar la cooperación judicial internacional, avanzar en los temas de evidencia digital, y participar en las estrategias conjuntas en materia de ciberdelincuencia.

De lo anterior se puede establecer que gracias a las políticas de seguridad implementadas por el estado colombiano y a la ley que modifica su Código Penal, cuya reforma tipifica los delitos informáticos de igual forma la adhesión al convenio de Budapest que se realizó en el año 2020. Por lo tanto, se ha alcanzado un gran avance en la modernización de las leyes que protegen de los ciberdelincuentes, las cuales no solo castigan al infractor estas también luchan por restablecer a su estado natural los derechos violados. Desde luego, las normas velan por lograr

investigaciones precisas y justas, buscan la prevención de los actos ilícitos realizados por los medios informáticos. En consecuencia, los usuarios de todos los dispositivos inteligentes y sitios web tienen mayor confianza al utilizar los mismos, en Colombia desde la adopción de todas estas medidas de seguridad en todo el país se ha logrado reducir considerablemente los ataques informáticos.

Regulación de delitos informáticos en República Dominicana

República Dominicana en la actualidad posee una ley específica, en la cual se encuadran los delitos informáticos. Es decir, la Ley número 53-07, que se refiere a los crímenes y delitos de alta tecnología, esta fue promulgada el día 23 de abril del año 2007, por el Congreso Nacional de República Dominicana. Por lo cual, esta norma fue emitida para la protección de la persona, su libertad de expresión, la integridad y sobre todo la inviolabilidad de la correspondencia y demás documentos privados. De este modo, el estado cumpliendo con uno de sus fines, vela por el respeto de los derechos que se encuentran plasmados dentro de la Constitución Política de República Dominicana.

Para la creación de la presente ley se observaron varios aspectos que motivaron la promulgación de dicha norma, es por esa razón que es importante conocerlo y citarlo dentro del presente trabajo y se encuentra plasmado en el tercer considerando de la Ley número 53-07 del Congreso Nacional que establece:

> Que las tecnologías de la información y de la comunicación han experimentado un desarrollo impresionante, con lo que brindan un nuevo soporte para la comisión de delitos tradicionales y crean nuevas modalidades de infracciones y hechos no incriminados, afectando los intereses patrimoniales y extrapatrimoniales de las personas físicas y morales, así como del Estado y las instituciones que lo representan (Ley número 53-07 del Congreso Nacional, 2007, tercer considerando).

De lo anterior se puede comentar que en República Dominicana se llevó a cabo el auge tecnológico con lo que se inició a utilizar con mayor frecuencia los medios informáticos. Por lo cual, por medio de investigaciones, análisis de denuncias se observó que los criminales realizaban actos ilícitos por estos sistemas informáticos. Ciertamente en el momento que se cometían estos actos ilícitos no se contaba con una legislación que tipificara los delitos informáticos lo cual entorpecía la persecución penal para dar con los responsables. Por este motivo los ataques fueron en aumento y el estado siendo el encargado de velar por el bien común de su población, creo la ley número 53-07 para realizar una lucha contra la ciberdelincuencia y de esa forma proteger el patrimonio, de las personas física y morales, así como del estado.

Al no contar con una ley que tipificara todos los delitos informáticos, dentro de la legislación penal de la República Dominicana, en su momento era casi imposible que los delincuentes recibieran una sanción adecuada. Por lo cual no se castigaba al infractor de manera que pagara por el delito cometido y de esa forma realizar un resarcimiento adecuado hacia las víctimas. En consecuencia, para lograr una investigación adecuada se

necesitaba de forma urgente la creación de una norma que cubriera todos estos elementos. Al momento de entrar en vigencia se crearon medios adecuados para lograr una lucha efectiva, que facilita la cooperación entre estados para la detección e investigación de estos delitos, esta norma fue considerada como un gran avance a la modernización de la legislación dominicana, ya que vela por la protección de sus pobladores frente a los ciberdelitos.

En la siguiente cita se observa la importancia que tiene la nueva norma jurídica que regula los delitos informáticos, así como el objeto de la misma y se encuentra establecido en el artículo 1 de la Ley número 53-07 (2007) del Congreso Nacional, y establece que:

> La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos (Ley número 53-07, 2007, Congreso Nacional, 2007, artículo 1).

Como se observa al momento de la creación de la mencionada norma jurídica el cual regula los delitos informáticos o como lo manifiesta esta ley delitos de alta tecnología. Así mismo los legisladores quienes tienen un compromiso con la población de velar que las leyes sean acordes a la realidad actual de la sociedad, tenían el objetivo de este cuerpo legal muy

claro. Siendo este la protección de los datos personales de los usuarios de los sistemas tecnológicos. Por lo cual, se realizó la tipificación de delitos cometidos por medio de la informática que causara perjuicio a personas físicas o morales en su patrimonio. De la misma forma, la protección de todos los sistemas informáticos que contienen información sensible.

La Ley número 53-07 que está compuesta por 67 artículos, en donde se tipifican los delitos informáticos y sus elementos junto a sus sanciones y penas a aplicar. Así mismo, se pueden observar distintos actos ilícitos como lo puede ser el acceso ilícito para servicios a terceros, dispositivos fraudulentos, el sabotaje, el robo mediante la utilización de alta tecnología, la estafa el chantaje y el robo de identidad entre muchos. Esto muestra que el objetivo de la creación de esta ley especial en materia penal es generar la protección adecuada a las personas que utilizan los sistemas informáticos. En consecuencia, con dicha normativa se busca realizar investigaciones penales más eficaces y la colaboración entre estados para imponer sanciones a los infractores que estén dentro de su territorio o fuera de él.

Entre los artículos de mayor importancia para la presente investigación se puede mencionar el artículo 9, de la ley número 53-07 del Congreso Nacional de la República Dominicana, y establece,

> Interceptación e Intervención de Datos o Señales. El hecho de interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales (Ley número 53-07 del Congreso Nacional, 2007, artículo 9).

Como se puede observar en el artículo citado, se regula el delito de la interceptación de datos o señales, de esta manera se busca la protección de esta información que se transmiten por medio de la red. Ciertamente se tipifica la interceptación, el espiar, escuchar, grabar u observar datos sin la debida autorización. Así mismo se regula una característica importante y es que el delincuente debe materializar sus actos de forma voluntaria e intencionadamente, dañando el derecho de privacidad de los usuarios. Esta norma jurídica contiene una pena que, en la opinión del investigador, los legisladores fueron benevolentes al colocar de 1 a 3 años de prisión, y una multa de 20 a 100 salarios mínimos vigentes. En consecuencia, las sanciones que se podrán imponer al delincuente son considerablemente bajas, teniendo en cuenta el daño que pueden causar en el patrimonio de las víctimas.

También se pueden mencionar otro delito tipificado siendo este el robo de identidad, el cual es de gran importancia por el valor normativo que contiene, estando regulado en el artículo 17 de la ley 53-07 del Congreso

Nacional de la República Dominicana y establece.

> Robo de Identidad. El hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con penas de tres meses a siete años de prisión y multa de dos a doscientas veces el salario mínimo. (Ley 53-07 del Congreso Nacional, 2007, artículo 17).

En este artículo se puede observar, que se regula el robo de identidad, que se puede establecer que es la forma de operar de la suplantación de identidad o *phishing*. Como se muestra en la anterior cita se encuentra regulado, pero de una forma muy sencilla sin llegar a profundizar mucho en cuanto a la forma de realización de este ilícito penal. Ahora bien, dentro de la norma jurídica establece que comete el robo de identidad quien use datos ajenos a través de los medios informáticos. En consecuencia, a los infractores de este delito les será impuesta una pena de prisión de 3 meses a 7 años y una multa de 2 a 200 salarios mínimos vigentes, por lo cual son sanciones certeras desde el punto de vista del daño causado a las víctimas.

Cabe resaltar que la ley establecida anteriormente, contiene diversos delitos que se realizan por medio de la informática. Por lo cual también cuenta con una regulación de las penas y multas que incurren los ciberdelincuentes que trasgredan dicha normativa, siendo penas desde un mínimo de 2 meses de prisión hasta un máximo de 10 años, según sea el caso de gravedad del delito cometido. No obstante, como se puede observar en otro apartado de dicha ley, impone penas mayores por cometer actos contra la nación y estas pueden ser de 15 hasta 30 años de

prisión. En consecuencia, con estas penas mencionadas se busca que los delincuentes analicen bien sus actos antes de cometer los mismos, con ello se previene la realización de estos delitos, también se regulan multas económicas que pueden ser de 5 salarios mínimos vigentes hasta un máximo de 2000, todas las sanciones mencionadas son para proteger a la población dominicana.

Regulación de delitos informáticos en Costa Rica

En la legislación costarricense se puede observar que han luchado para ir junto a los avances tecnológicos, pero esto no se ha logrado con mucho éxito. Desde luego, Costa Rica cuenta con la Ley número 4573 el cual es el Código Penal, que entró en vigencia el 4 de mayo de 1970, como se observa esta norma jurídica ya tiene casi 53 años de antigüedad, con lo cual tiende a quedarse casi obsoleta en ciertos asuntos del mundo moderno. Obviamente carece de la tipificación de los delitos informáticos que han incrementado dentro del territorio costarricense, por lo cual se ha generado una serie de reformas que modifican y adhieren nuevos artículos al Código Penal. Siendo el caso de la Ley número 8148 de la Asamblea Legislativa, que fue promulgada el 24 de octubre del año 2001, dicho cuerpo legal agrega los artículos 196 bis, 217bis, 229bis, con lo que se pretendía reprimir y castigar los delios informáticos.

En el año 2012 se promulgo la Ley número 9048 de la Asamblea Legislativa, con la cual se realizaba una nueva reforma al Código Penal costarricense. De esta forma se adicionaron 12 artículos que contienen figuras delictivas tales como la extorsión, la estafa informática, daño informático, suplantación de identidad, espionaje informático, instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas. Por lo cual, como se observa son delitos cometidos por cualquier medio informático, con esta adición al Código Penal se intentaba realizar una modernización de la legislación costarricense. Cabe mencionar que dicha norma se utilizaría para la lucha contra los ataques informáticos a los que se encontraban expuestos todos los ciudadanos al hacer uso de los dispositivos electrónicos.

Dentro de la Ley número 9048 se pueden observar los elementos que constituyen como delito las violaciones a dicha norma, también se observan las sanciones que serán aplicadas a las personas que cometan los delitos establecidos dentro de la misma. De esta manera, pueden recibir una sanción de 6 meses como mínimo y un máximo de 10 años de prisión como máximo según la gravedad del acto delictivo realizado por determinada persona. Esto muestra que el objetivo de estas penas es castigar al infractor y prevenir que se sigan realizando dichos ilícitos. Así mismo, algo a resaltar y que llama mucho la atención es que este cuerpo legal no cuenta con sanciones económicas que deban imponerse a los

ciberdelincuentes, algo que se puede considerar como un punto débil en la legislación.

Dentro de los artículos que conforman la Ley número 9048 de la Asamblea Legislativa de la República de Costa Rica, es importante citar el artículo 230, el cual es de gran relevancia para la presente investigación y establece que.

> Suplantación de identidad. Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero. La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz (Ley número 9048 de la Asamblea Legislativa, 2012, Artículo 230).

Con el anterior artículo, se observa que si se tiene regulado el delito de suplantación de identidad dentro de la legislación costarricense. De esta manera se busca la prevención para que los delincuentes no realicen este acto ilícito a través de los medios electrónicos. Dentro la tipificación mencionada indica que cualquier persona que utilice la identidad de persona ajena o una ficticia dentro de redes sociales o sitios web, comete este delito. Por lo cual al analizar la estructura de este articulo esta normado de una forma muy básica sin ser amplia lo cual limita de cierta forma la aplicación de la misma en los actos ilícitos, este mismo contiene una pena de prisión de 3 a 6 años según sea el caso.

Otro artículo que es de gran importancia es el 233, Ley número 9048 de la Asamblea Legislativa de la República de Costa Rica, que se refiere a la suplantación de páginas electrónicas, siendo este una forma de actuar de la suplantación de identidad o *phishing* y el mismo establece que.

> Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet. La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero (Ley número 9048 de la Asamblea Legislativa, 2012, Artículo 233).

Como se observa en el anterior artículo, nuevamente la redacción que se realizó de esta norma jurídica es muy básica sin tener una interpretación extensiva lo cual dificulta una investigación de la realización del delito. Ciertamente se tipifico la suplantación de sitios legítimos de la red de internet, que es básicamente el modo de operar del *phishing* que está siendo estudiado en este trabajo. En este artículo se regula que el delincuente debe inducir a error para capturar información privada, para beneficio propio o de un tercero. En consecuencia, es una norma muy sencilla sin abarcar mucho, que contiene una pena de prisión de 1 a 3 años, algo que resalta es que no contiene una sanción de multa.

Costa Rica el día 23 de julio del año 2017, se adhiere formalmente al convenio de Budapest, el cual se refiere a la ciberdelincuencia. Ciertamente, tiene como objetivo el velar por de la protección de la sociedad contra los ataques informáticos, que se realizan todos los días

por los medios informáticos. Por lo cual, esta incorporación a dicho convenio se realizó casi 10 años después de la invitación que se realizó al país costarricense, con ello se adquieren los objetivos fundamentales como lo son el mejoramiento de leyes que desarrollen cooperación a nivel internacional. De igual forma a la creación de legislaciones acordes para el combate a los delitos informáticos y la instauración de una red, que debe trabajar de forma permanente sin interrupción.

A pesar de los esfuerzos de Costa Rica por realizar mejoras a su legislación, para crear métodos de protección cibernética. Ciertamente, esto ha sido muy poco en comparación a los avances tecnológicos y a los nuevos medios de cometer actos delictivos, cabe resaltar que, al momento de la creación de la ley mencionada y la incorporación al convenio de Budapest, tuvo una buena aceptación y se realizó una baja considerable en los ataques informáticos, teniendo así medios de prevención de la realización de estos actos ilegales. Sin embargo, del año 2017 al año 2020 se multiplicaron las denuncias por haber sido víctimas de ciberdelincuentes, lo que deja saturadas las instituciones que son las encargadas de realizar las investigaciones. En consecuencia, entorpece las investigaciones y la población nuevamente queda vulnerable ante los ciberdelincuentes que siguen apropiándose indebidamente del patrimonio de los particulares.

Incorporación del delito de suplantación de identidad en la legislación guatemalteca

Como se ha establecido anteriormente en Guatemala no se cuenta actualmente con una regulación que tipifique todos los delitos informáticos, lo cual hace que la población sea vulnerable a sufrir alguno de estos actos ilícitos que afectan gravemente su patrimonio. Sin embargo, la mejor forma para velar por la protección, de los usuarios de los medios tecnológicos es con la creación de una norma especial que contenga todos los ilícitos que se realizan a través de la informática. Desde luego que la creación de dicho cuerpo legal tomara un largo tiempo, ya que se puede considerar como una ley que no tiene prioridad dentro del territorio, lo cual atrasaría grandemente la modernización de la ciencia penal guatemalteca.

De lo anteriormente establecido, observando y analizando la forma de incorporar ciertos delitos nuevos a los ordenamientos jurídicos extranjeros han tomado como referencia algunos aspectos. El presente trabajo se propone realizar una reforma al Código Penal guatemalteco, el cual se ha quedado atrasado en cuanto a la tipificación de los delitos informáticos, dejando de esa forma muchas personas afectadas sin la esperanza de que se haga justicia por el daño causado a su patrimonio. Por tal motivo se propone una reforma de ley, para la adhesión del delito de suplantación de identidad o también llamado *phishing*, dicho ilícito

deberá contener una pena justa para el delincuente y una multa para resarcir el daño causado a la víctima, de esa forma se busca la prevención de la realización del delito. Dicha propuesta queda de la siguiente forma:

Congreso de la República de Guatemala

Considerando:

Que es deber del Estado velar por la realización del bien común, así como garantizar un desarrollo integral de la persona, protegiendo el derecho de libertad y de la propiedad privada.

Considerando:

Que se necesita de forma urgente la reforma del Código Penal, para cumplir con las necesidades de seguridad que se tiene en la actual realidad del país por los avances tecnológicos.

Considerando:

Que los delitos informáticos no están previstos dentro de la regulación penal guatemalteca, lo cual hace que dichas acciones no puedan ser sancionadas, por lo que se entiende que la reforma para la adición del delito de suplantación de identidad dentro del Código Penal vigente se debe realizar de forma urgente para realizar avances de la ley penal.

Por tanto:

En uso de las facultades que le otorga la literal a) del artículo 171 de la Constitución Política de la República,

Decreta:

Las siguientes Reformas al Decreto número 17-73 del Congreso de la República, Código Penal.

Artículo 1.- Se adiciona el artículo 274 I el cual queda como sigue:

Artículo 274 I.- Suplantación de identidad. Comete el delito de suplantación de identidad:

a) Quien utilizare cualquier medio informático, con el objetivo de inducir a error a tercero mediante engaños, para revelar y apropiarse de información privada.

b) Quien valiéndose de ingeniería social modifique páginas web, haciéndose pasar por páginas legitimas para obtener de forma ilegal información privada de terceros.

c) Quien utilizare nombre ajeno, contraseñas, números de tarjetas de crédito o débito de terceros obtenidos de forma ilegitima, con el ánimo de causar daños morales, físicos y patrimoniales.

d) Quien, utilizando información de terceros obtenida de forma indebida, ingrese a cuentas bancarias para sustraer total o parcialmente dinero ajeno.

e) Quien habiendo obtenido información personal y privada por cualquier medio informático de forma ilegitima, venda, comparta, revele, publique datos personales, fotografías, videos, audios, mensajes o secretos corporativos de forma que busquen dañar a terceros la integridad física y psíquica.

Los responsables de la comisión de este delito, serán sancionados con una pena de prisión de tres a seis años, y será sancionado con el pago de multa de veinte hasta ciento cincuenta salarios mínimos vigentes para actividades no agrícolas.

Artículo 2.- Agravación de la pena. La pena a imponer por el delito de Suplantación de identidad, será aumentada en dos terceras partes, en los siguientes casos:

a) Cuando se realice el ingreso ilegitimo a sistemas de instituciones estatales, con el objetivo de adquirir datos privados de funcionarios y empleados públicos.

b) Cuando el delito sea cometido en contra del Estado de Guatemala para la interceptación, revelación y publicación de información confidencial de carácter estatal.

c) Cuando la información revelada o publicada sean secretos estatales que afecten la soberanía del estado de Guatemala.

Artículo 3.- Vigencia: El presente decreto entrara en vigencia ocho días después de su publicación en el diario oficial. Pase al organismo ejecutivo para su sanción, promulgación y publicación.

La anterior propuesta se refiere a una reforma del Código Penal guatemalteco donde se incorpora una nueva figura delictiva. Esta se realizó conforme al análisis de las legislaciones extranjeras, en donde se observaron dentro de los cuerpos jurídicos de Colombia, República Dominicana, penas de prisión y multas económicas. Sin embargo, dentro de la norma legal de Costa Rica únicamente se establecen sanciones relativas a la privación de libertad y no contiene multas que deban pagar los ciberdelincuentes declarados culpables de la realización de este delito. Por lo cual se tomó como base las tres legislaciones, para la implementación de la tipificación de este delito dentro del ordenamiento jurídico de Guatemala.

Por lo cual, la respectiva propuesta que contiene la tipificación del delito de suplantación de identidad, la cual incorpora su respectiva pena y sanción. Por lo cual, se deberá presentar ante el Congreso de la República de Guatemala, ya que dicho organismo es el encargado de legislar y promulgar las leyes dentro del territorio nacional. En consecuencia, con la regulación del delito de suplantación de identidad tiene el objetivo de lograr un avance en cuanto a la tipificación, de los delitos informáticos que atentan contra la sociedad en general que hacen uso de los medios

informáticos. De esta manera se obtendrá una prevención para que los ciberdelincuentes no realicen este ilícito penal, ya que serán sancionados por el daño causado en caso de vulnerar los derechos de los usuarios de distintos sistemas informáticos.

Conclusiones

En relación con el objetivo general, que se refiere a comparar la regulación extranjera contra el delito de la suplantación de identidad, para determinar los aspectos que pueden ser utilizados en la legislación guatemalteca, se concluye que el estado de Guatemala necesita realizar de manera urgente acciones para la tipificación del delito de suplantación de identidad. Ya que en la actualidad no cuenta con una norma que lo tipifique y sancione a los que cometan este ilícito, con lo cual se hace casi imposible la investigación y persecución penal de los ciberdelincuentes. Desde luego, en la legislación extranjera se observan penas y multas que se pueden considerar adecuadas para castigar al infractor. Por lo cual se determina que puede realizarse la incorporación de esta figura delictiva por medio de una reforma al Código Penal, el cual deberá contener una pena de prisión justa y una multa para resarcir el daño causado.

En el primer objetivo específico que consiste en describir la suplantación de identidad y los demás delitos informáticos, se arribó a la conclusión que existe gran variedad de formas en que puede operar la suplantación de identidad. Así mismo, con los avances tecnológicos han desarrollado nuevos medios para realizar actos de ilícitos, los cuales afectan el patrimonio de sus víctimas, como lo realiza la suplantación de identidad o *phishing*. Ciertamente, este delito se realiza por lo general por medio de mensajes privados enviando vínculos que redirigen a páginas web

maliciosas las cuales tienen por objeto adquirir información de forma ilegitima, para posteriormente buscar un beneficio económico para si o para terceros.

Con relación al segundo objetivo específico que consiste en examinar la vulnerabilidad que existe en Guatemala ante los ataques de la suplantación de identidad se concluye que el país tiene un punto vulnerable en su legislación con relación a los delitos informáticos. Es decir, no tipifica la suplantación de identidad como ilícito penal al no contar con una norma moderna, con esto deja sin protección a los bienes jurídicos, que son tutelados por la Constitución Política de la República. En consecuencia, a lo establecido en Guatemala se tiene un porcentaje alto en relación a ataques de suplantación de identidad, el mismo que cada año incrementa siendo uno de los países con mayor riesgo de ataques de *phishing*, al no poder investigar ni castigar a los delincuentes que realizan estos actos ilegales.

Referencias

Centro estadístico de observación y monitoreo de ciberdelitos, (s.f.), *Estadísticas.* Cengage Learning. https://ogdi.org/estadisticas

Cáceres Diaz, I.F. (2015), *Análisis sistémico de ataques de spear phishing utilizando inspección profunda de paquetes*. Cengage Learning. https://bibdigital.epn.edu.ec/handle/15000/21670

Cancilleria.gov.co. (2020) *Colombia se adhiere al convenio de Budapest*. Cengage Learning. https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

Camille Jauffret-spinosi, R.D. Morineau, M. (S.F). *Evolución de la familia jurídica romano-canónica, el derecho comparado.* Cengage Learning.https://www.uazuay.edu.ec/sites/default/files/public/VII_derecho_comparado.pdf

Constantinescu R.M. (2020), *Análisis del delito de stalking del artículo 172 ter del Código Penal, su perspectiva penal*. Cengage Learning. https://repositori.uji.es/xmlui/bitstream/handle/10234/188938/TFM_2020_Constantinescu_RalucaMaria.pdf?sequence=1

De Mata Vela, J.F. (2011). *Derecho penal guatemalteco.* (11a. ed.). Magna Terra Editores.

Del Pino, S. Miguel Angel Davara Rodríguez, (S.F.) *Delitos informáticos*. Cengage Learning. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Fernández Tomé A. (2015), *Bullying y Ciberbullying, prevalencia en adolescentes y jóvenes de Cantabria*. Cengage Learning. https://addi.ehu.es/bitstream/handle/10810/22185/TESIS_FERNANDEZ_TOME_M%C2%AAAIDA.pdf?sequence=1

Gonzales Juárez D.D. (2012), *Estudio del impacto de la Ingeniería Social Phishing*. Cengage Learning. http://132.248.9.195/ptd2013/Presenciales/0689984/Index.html

Gutteridge H.C. Marta Morineau. (S.F.). *Evolución de la familia jurídica romano-canónica, el derecho comparado.* Cengage Learning.https://www.uazuay.edu.ec/sites/default/files/public/VII_derecho_comparado.pdf

Organización de los Estados Americanos, (2020), *Observatorio de la Ciberseguridad en América Latina y el Caribe*. Recuperado el 14 de junio de 2023 de https://observatoriociberseguridad.org/#/home

Superintendencia de Bancos de Guatemala, (s.f.), *Desafíos de la seguridad tecnológica cibercrimen.* [Diapositivas de PowerPoint]. PowerPoint. https://www.sib.gob.gt/c/document_library/get_file?folderId=3960235&name=DLFE-27231.pdf&__cf_chl_tk=yO0rbrHR4uBRy.nINLERYIcId.r1YatEo.esrQSFcLc-1687032081-0-gaNycGzNDKU

Sánchez Bernal, J. (2009). *El bien jurídico protegido en el delito de estafa informática*. Cengage Learning. https://dialnet.unirioja.es/servlet/articulo?codigo=3760666

Usaid, Superintendencia de Bancos de Guatemala, (2020), *Guatemala Ciberdelito 2020*. Cengage Learning. https://infosegura.org/sites/default/files/2023-02/CiberdelitoGT2020.pdf

Legislación nacional

Asamblea Nacional Constituyente. (1985). *Constitución Política de la República de Guatemala.*

Congreso de la República de Guatemala. (1973). *Código Penal.* Decreto número 17-73.

Congreso de la República de Guatemala. (2022). *Ley de prevención y protección contra la ciberdelincuencia*. Decreto archivado número 39-2022.

Congreso de la República de Guatemala. (2022). Acuerdo número 14-2022.

Legislación internacional

Asamblea legislativa de la República de Costa Rica. (2012). *Reforma de la sección VII, Delitos informáticos y conexos, del título VII del Código Penal.* Ley número 9048.

Congreso de la República de Colombia. (2009). *Reformas al código Penal de Colombia*. Ley número 1273.

Congreso Nacional de la República Dominicana. (2007). *Ley sobre crímenes y delitos de alta Tecnología.* Ley número 53-07.