Universidad Nacional de Loja

Facultad Jurídica, Social y Administrativa

Carrera de Derecho

“El phishing como medio de disposición patrimonial fraudulenta”

Trabajo de Integración Curricular previo a la obtención del título de Abogada.

AUTOR:

Valeria Alejandra Campoverde Salas

DIRECTOR:

Dr. Servio Patricio González Chamba Mg. Sc.

LOJA – ECUADOR

2023

Loja, 12 de mayo de 2023

Dr. Servio Patricio González Chamba Mg. Sc.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: **"El phishing como medio de disposición patrimonial fraudulenta"** previo a la obtención del título de **Abogada,** de la autoría de la estudiante **Valeria Alejandra Campoverde Salas,** con cédula de identidad **Nro. 1105658619**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

Dr. Servio Patricio González Chamba Mg. Sc.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Autoría

Yo, **Valeria Alejandra Campoverde Salas**, declaro ser autora del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Integración Curricular en el Repositorio Digital Institucional-Biblioteca Virtual.

Firma: 

Cédula de identidad: 1105658619

Fecha: 16/05/2023

Correo Electrónico: valeria.compoverde@unl.edu.ec

Teléfono: 0959520249

Carta de autorización del trabajo de integración curricular por parte del autor (a) para la consulta de producción parcial o total, y publicación electrónica de texto completo.

Yo, **Valeria Alejandra Campoverde Salas,** declaro ser autora del Trabajo de Integración Curricular denominado: **"El phishing como medio de disposición patrimonial fraudulenta",** como requisito para optar al título de: **Abogada**, autorizo al sistema Bibliotecario de la Universidad de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los Usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dieciséis días del mes de mayo del dos mil veintitrés.

Firma: Firmado electrónicamente por: VALERIA ALEJANDRA CAMPOVERDE SALAS

Autor/a: Valeria Alejandra Campoverde Salas

Cédula: 1105658619

Dirección: Barrio "El Dorado"

Correo electrónico: valeria.compoverde@unl.edu.ec

Teléfono: 0959520249

DATOS COMPLEMENTARIOS

Director/a del Trabajo de Integración Curricular: Dr. Servio Patricio González Chamba, Mg.Sc.

Dedicatoria

Quiero dedicarlo con mucho cariño y respeto a mis padres Fanny e Ilmo, a mis hermanos Karina, Miguel y Luis, a Bryan, a toda mi familia, y a mis valiosos amigos por brindarme todo su amor y apoyo que fueron de gran ayuda para que pueda alcanzar este gran logro.

Valeria Alejandra Campoverde Salas

Agradecimiento

Agradezco a Dios por haberme otorgado una familia maravillosa, la cual me ha inculcado los valores de honestidad, superación y sacrificio, lo que me ha permitido cumplir mis metas y culminar con éxito este arduo trabajo.

Mi agradecimiento a la Universidad Nacional de Loja, Facultad Jurídica, Social y Administrativa, de manera especial a la Carrera de Derecho y a su personal docente por brindarme todos los conocimientos que se necesitan para mi formación profesional.

De igual forma, expreso mi sincero agradecimiento a mi madre por cada día hacerme ver la vida de una forma diferente y real. A mi padre por estar presente y por enseñarme que nada es fácil. A mis hermanos por enseñarme que con constancia y sacrificio se logra lo que se propone.

A mi pareja por acompañarme siempre en este proceso, por apoyarme en todo momento y nunca dejar que me rindiera.

A mis amigos y compañeros de clase con quienes he compartido grandes y hermosos momentos.

Al Dr. Servio Patricio González, que con su inmensa ayuda y sabios conocimientos del bien me han permitido culminar mi trabajo.

Y a todos quienes están a mi alrededor, que siguen estando cerca de mí y me regalan momentos llenos de sabiduría y felicidad para recordarlos con gran amor en mi vida.

Valeria Alejandra Campoverde Salas

Índice de contenidos

Índice de tablas

Índice de figuras

Índice de anexos

1. Título

“El phishing como medio de disposición patrimonial fraudulenta”

2. Resumen

Hoy en día los avances de la tecnología de la información y comunicación evolucionan con el pasar del tiempo dando muchas facilidades en diferentes aspectos o ámbitos de la vida, sobre todo en cómo se desenvuelven las personas dentro de la sociedad, además, presentan algunas consecuencias o desventajas como por ejemplo: la característica del libre acceso a cualquier usuario; no tiene un límite de edad; muchas de las veces estos usuarios dan un sin número de información personal en distintas plataformas que existen hoy en día como son las redes sociales o las llamativas compras en línea. Aun así, nadie está a salvo de la gran influencia de estos avances ya que han dado surgimiento a una serie de comportamientos o modalidades ilícitas a los cuales se los ha denominado "delitos informáticos".

Es así, que existen varias formas en que los ciudadanos de cualquier país pueden ser víctimas de un fraude o engaño a través de las plataformas virtuales, por lo que se observa la necesidad de dar a conocer el tipo de delito que está teniendo mayor concurrencia en la actualidad, el cual es el delito informático de Phishing, se informará la forma de como lo ejecutan, la finalidad que tienen los infractores para realizarlo o el motivo que los llevó a cometer el hecho delictivo.

Durante el desarrollo del presente trabajo investigativo abordaré y desenvolveré temas que ayuden a identificar las implicaciones y perjuicios que se ocasionan al realizar este delito, demostrar cómo se vulneran los derechos económicos y patrimoniales de las personas; ya que se considera al phishing como un producto de la tecnología que avanza con mayor intensidad.

Para lograr una completa investigación de esta temática se establece una respectiva conceptualización acerca de algunos términos que se relacionan con el tema para comprenderlo de mejor manera; además, se menciona una breve reseña histórica acerca de la Tecnología de la Información y Comunicación (TIC) con sus características, ventajas y desventajas correspondientes, a continuación se aborda el tema de delitos informáticos definiendo los sujetos que intervienen dentro de este y la repercusión social que se está produciendo en la actualidad; seguidamente se da a manifiesto de lo que significa hoy en día las redes sociales con sus respectivas características, ventajas y desventajas; finalmente, se aborda en manera general el origen y definición del delito informático del phishing, cuáles

son los tipos que existen, las fases que se establecen para lograr el objetivo de los ciberdelincuentes, el gran impacto que tiene ese delito en la sociedad y algunas recomendaciones que deberían seguirse para no ser víctimas de este o así mismo evitar a esta clase de infractores.

Se incluye de igual forma a nuestra legislación constitucional y penal para identificar los bienes económicos y patrimoniales que son protegidos. Así mismo, se menciona los recursos normativos internacionales que son otorgados por el Derecho, mismos que tienen un valor elevado en esta investigación, se aporta de manera referencial el Convenio sobre Ciberdelincuencia celebrado en Budapest que es una fuente de guía para las legislaciones de los distintos países europeos que si tienen tipificado el delito de phishing de una forma más autónoma e independiente.

De esta manera concluyo esta investigación con el planteamiento de una propuesta jurídica de reforma que se adapta a la realidad por la que está pasando la sociedad, principalmente se basa en los fundamentos o argumentos que son extraídos del estudio jurídico que se realiza. Por lo tanto, se hace mención del principio de legalidad, es cual es fundamental para que se pueda sancionar a una persona y que se realice una interpretación literal de la norma. Con esto se verifica la necesidad de integrar el delito informático de phishing al Código Orgánico Integral Penal para que de esta forma no se vulnere el patrimonio y propiedad de las personas.

2.1 Abstract

Nowadays the advances in information and communication technology growth with the time giving many facilities in different aspects of life, above all how the people develop into society. Furthermore, it presents some consequences or disadvantage, as for example: The characteristic of free access to any person: It does not have a limit of age. Sometimes these users give a number of personal information in any platforms that exists: for instant the social media or shopping in line. Even, nobody is out of the big influence of these advances because these have done an emergent of a serial behaviour or ilicit forms which are called: "cybercrime".

So. There are various forms in which cityzenships of any country can be victims of fraud and deceit through the virtual platforms, hence, it is observed the necesity to give the kind of crine which is having the most attendance in the actuality, which is the cybercrime "Phishing".It will inform the form of development, the finality that have the infractors to do or the motive they have to commit the criminal act.

During the development of the research work I will develop and approach topics that help to identify the implications and damage caused by this crime, showing how are vulnerable the economic and patrimonial rights of people; so that, phishing is considered as a product of technology which advances with a major intensity.

For achieving a complete researching of this thematic, it is established a respective conceptualization about some terms which are related with the topic to understand in a best way; furthermore, it is mentioned a history review about the technology of information and communication (TIC) with its characteristics, advantage, and disadvantage. It is adressed the cybercrime define the human being that intervene into it and the social repercussion which is produced in the actuality; Next it is given, what does it mean nowadays in the social media with its respective characteristics, advantage and disadvantage; finally it is adressed in a general way the origin and definition of cybercrime of phishing, which are the types that exists, the phases which to get the objective of the cyber delinquents, the big impact that this crime has into society and some recommendations that should follow to do not be victims of it or avoid this class of infractors.

It is included our constitutional criminal law to identify the economic and patrimonial properties protected. In addition. It is mentioned the normative international resources given by law, which have a high investigation. It is contributed an agreement of cybercrime

celebrated in Budapest that is a source and guide for the legislations of the different Europe countries that they have typified the crime of phishing in an autonomun and independent way.

I conclude this investigation with the approach of a legal porposing adapted to the reality of the society, principally it is based in the fundaments or arguments which are extracted of a legal study that is developed.

Therefore, it is mentioned the legality beginning, which is fundamental for sanction a person and make a literal interpretation of the norm.

With this. It is verified the necesity to integrate the cybercrime of phyishing to the Integral Organic Legal Code in order to it does not vulnerable the patrimonial and property of people.

3. Introducción

El presente trabajo de investigación tiene como objetivo principal brindar una visión específica de la nueva forma de delinquir que ha surgido por los grandes avances de la tecnología de la información y la comunicación (TIC) ya que casi todo el mundo está siendo globalizado por las herramientas tecnológicas; de esta forma se da a origen al delito informático de phishing, que se constituye principalmente en la inserción de enlaces ilícitos en cualquier red social y por correos electrónicos que tienen por finalidad la obtención de información íntima y confidencial ya sea de alguien especial o de terceras personas para obtener beneficio propio lucrativo.

A continuación, la metodología de este trabajo se representó cualitativamente, por los métodos: científico, inductivo, deductivo, analítico, comparativo y estadístico; por ende, recurrí a bibliografía necesaria para recolectar información verídica para que me permita fundamentar y posteriormente poder sustentarla de manera eficaz, conceptual, doctrinaria y jurídicamente. Para lograr obtener esta investigación apliqué los dos objetivos específicos que definí para su desarrollo.

En el estudio del marco teórico se plantea el primer objetivo específico, en el cual se presentan algunas definiciones básicas de algunos términos, temas y subtemas que se relacionan con la problemática de esta investigación que han permitido contrastar los modos o formas de esta. En otras legislaciones y normas penales de varios países esta conducta ilícita del phishing ya se encuentra tipificada con la sanción que le corresponde de manera autónoma; mientras que en nuestra legislación no se encuentra tipificado ni sancionado, motivo por el cual los legisladores adecuan el hecho delictivo a otro tipo penal que no cumple con las características y factores de la conducta delictiva descrita.

Con el planteamiento de la metodología ya mencionada ha sido de gran ayuda para plantear algunas interrogantes descritas en un modelo de encuesta y entrevista que fueron dirigidas únicamente a profesiones del Derecho en la ciudad de Loja, ellos han facilitado grandes conocimientos y opiniones, con el fin de examinar o analizar la veracidad de mi investigación y de esta manera proteger el tema objeto de esta.

Finalmente, mi estudio busca aportar con una propuesta de reforma jurídica al Código Orgánico Integral Penal, para resarcir la ausencia que se presenta en la realidad, incorporando

como delito autónomo al delito informático de Phishing con sus modalidades, sus elementos y formas propias de esta conducta para que no sea confuso con otro tipo penal; si se da esta modificación a la legislación penal ya no se verían vulnerados los derechos económicos y patrimoniales de los ciudadanos.

4. Marco teórico

4.1 Definición de Términos Básicos

4.1.1 Delito

Es de suma importancia iniciar por este concepto ya que el delito es la principal razón de la existencia del Derecho Penal, dado que la finalidad de esta rama del Derecho es el controlar de alguna forma todos los comportamientos que son malignos o que pueden dañar a la sociedad en general.

Es decir, delito es aquella conducta que lesiona un bien jurídico que ya está protegido, por ello en nuestro Código Orgánico Integral Penal se pueden encontrar una gran serie de tipos penales que son la descripción exacta de las omisiones o acciones que son consideradas como delitos, como, por ejemplo: el robo, la estafa, homicidio, violaciones, entre otros.

Según palabras de algunos tratadistas muy importantes dentro del Derecho, delito es:

> "La acción típicamente antijuridica y culpable, la cual es imputable a quien cometió el injusto penal y por lo tanto sometido a sanción penal». (Carranca Trujillo, 1991, pág. 223)

Se puede extraer de este concepto que el delito es una acción ilícita la cual imputa a la persona quien realizó dicha acción con gran libertad lesionando de manera intencional los intereses de sus semejantes.

4.1.1.1 Elementos del Delito

En palabras del tratadista Edmundo Mezger:

> "cuando se infringe el supuesto hipotético presente en la norma jurídica penal, esta acción debe ajustarse dentro de lo descrito por la legislación como delito, es decir, que la infracción que se haya cometido debe siempre encajar con el tipo penal tipificado",

(Tratado de Derecho Penal, 1935, pág. 54).

Por lo que plantea los siguientes elementos:

Conducta. - Es el comportamiento voluntario de los humanos, ya sea positivo o negativo, para lograr un propósito; esta conducta se puede caracterizar por la acción, la actividad o la inactividad. Se lo define como voluntario porque se lo realiza de acuerdo si la persona lo quiere realizar o no. En esta existen tres elementos: Un acto positivo o negativo (con una acción u omisión). Un resultado. Una relación de causa-efecto entre acto-resultado.

Tipicidad. - Es aquella que se refiere a la adecuación de una conducta al tipo penal. La acción típica es la que se acomoda a la descripción, es decir, que lo que se hizo o no se debe relacionar en un cien por ciento con lo que se establece en las leyes penales. Lo negativo de la tipicidad es la atipicidad, donde falta esa adecuación de la conducta.

Antijuricidad. - Si una conducta se considera antijurídica, entonces es un delito. La conducta de los seres humanos debe estar en contra de las normas jurídicas establecidas. Puede existir una justificación cuando se considere que hay una determinada actuación delictiva sin ánimo de contravenir la ley, en ese caso se excluye la antijuricidad en laconducta.

Culpabilidad. - En términos jurídicos se refiere a la reprochabilidad de un acto; es el nexo intelectual y emocional que liga al sujeto con el acto delictivo. En distintas palabras la culpabilidad se da cuando el sujeto conoce y comprende lo que está sucediendo, pero decidió seguir adelante aun cuando podía realizar algo distinto que no afectara al bien jurídico de la manera que ya lo afecto. Por ende, es un juicio de imputación de porque se condujo de esa manera el sujeto que realizó la conduta. Sus elementos son: imputabilidad, dolo o culpa, exigibilidad de la conducta.

Punibilidad. - Es el merecimiento de determinada pena ante un delito. Las penas se tipifican en el Código Penal, donde se verifican un conjunto de presupuestos normativos a esa pena. En el aspecto negativo de la punibilidad, se habla de excusa absolutoria.

4.1.2 Tipo

Se conceptualiza por la gran relevancia dentro del ámbito penal y por su estrecha relación con el tema del cual trata esta investigación. Por ello, dentro de la doctrina se lo puede

encontrar como:

> "La descripción hecha por el legislador, de una conducta antijurídica, plasmada en una ley. Se lo ha considerado como un instrumento legal necesario y de naturaleza descriptiva. Es importante manifestar que también se conforma de las modalidades de la conducta, como pueden ser el tiempo, lugar, referencia legal a otro ilícito, así como de los medios empleados, que, de no darse, tampoco será posible se dé la tipicidad". (Betancourt, 2007, págs. 149-174)

Con lo citado anteriormente puedo manifestar que el tipo es una serie de hechos o acciones a las cuales el derecho le va a imponer una ley o una sanción para que así se pueda dar una o varias soluciones a los conflictos que se generan en nuestra sociedad día tras día.

Así mismo, el tipo es el cual establece todas aquellas conductas que son consideradas antijuridicas, es decir, que son sancionables porque al final perjudican a alguien o a algo. Presenta una gran garantía ya que es aquel que elije lo que puede ser objeto de sanción y lo que no; es motivador porque al establecer las sanciones significa que las personas no tienen que hacerlo porque se les aplicará alguna o todas ellas.

Según las palabras de los escritores Francisco Muñoz Conde y Mercedes García Arán, Tipo, es, por tanto:

> "la descripción de la conducta prohibida que lleva a cabo el legislador en el supuesto de hecho de una norma penal". (Derecho Penal, Parte General, 2010, pág. 254)

Con lo dicho manifiesto que Tipo es aquella descripción que el legislador necesita para que la norma penal sancione a la infracción de una manera adecuada según lo que se haya cometido.

En Derecho Penal, Tipo contiene una triple función, de acuerdo con el jurista Sainz Cantero las cuales se detallan a continuación:

La función seleccionadora de todos aquellos comportamientos de los seres humanos penalmente destacados. Es decir, se debe tomar en cuenta simplemente las conductas que se relacionan con la infracción cometida y lo que está escrito en la ley.

La función de garantía para que solo las conductas que se integren en él puedan ser

sancionados penalmente. Sirve de gran ayuda, ya que con esta función no se podrán sancionar hechos que no estén dentro del tipo penal que se fue encontrado.

La función motivadora, es donde se describen los comportamientos en el tipo penal, por ende, el legislador da a conocer a los todos los ciudadanos que conductas están prohibidas y cuales no, esperando que estos se limiten de cometer las mismas. (Lecciones de Derecho Penal, 1990, pág. 95),

4.1.3 Tipicidad

Tanto el tipo como la tipicidad se enmarcan en toda acción u omisión que pone en peligro a un bien jurídico.

A la tipicidad se la utiliza dentro del ámbito de derecho para nombrar a aquello que siempre va a constituir un delito porque se va a adecuar a una figura que se describirá en la ley. Dicho de otro modo: la tipicidad supone la adecuación de una conducta a los presupuestos que detalla la legislación sobre un delito. Si la acción que ejecuta una persona de forma voluntaria encaja con la figura que describen las leyes como delito, se habla de la tipicidad del hecho cometido.

Por ello, cuando una conducta se adecua a la descripción de la ley, puede afirmarse que el acto constituye un delito. En cambio, cuando la adecuación no se produce en totalidad, la acción no supone un delito, es decir, que esta adecuación está vinculada a la tipicidad de los hechos. Esta tipicidad es indispensable para que un juez pueda evaluar los hechos concretos de acuerdo con los tipos fijados por la ley.

Doy mención a los catedráticos Francisco Muñoz Conde y Mercedes García Arán, los cuales definen a la tipicidad como:

> "aquella cualidad que se atribuye a un comportamiento cuando es subsumible en el supuesto de hecho de una norma penal" (Derecho Penal, Parte General, 2010, pág. 251).

A mi criterio, dan a conocer que la tipicidad es la característica que se incorpora al comportamiento de una norma, es decir, que la inflación o delito que se cometió se va a adecuar a lo que se este escrito en la norma o ley.

4.1.4 Fraude

Es una de las formas más antiguas que se han conocido para la corrupción, es un acto ilegal, principalmente utiliza el engaño ya que se lo realiza por una o varias personas para obtener algún provecho personal o general perjudicando los intereses de los demás. Existen varios tipos de fraudes en función del ámbito al que afecta. Siendo así, no se debe confundir el fraude con la estafa ya que esto es muy común.

Cabe mencionar el concepto que da el tratadista Andrew Nelson acerca del fraude:

> "Consiste en alguna práctica engañosa, plan preconcebido con la intención dolosa de privar a otro de sus derechos, o en alguna forma causarle perjuicios. Se distingue de la diligencia en que, siempre es positivo e intencional". (Introducción a la intervención de cuentas, 1942).

Por ende, el fraude es un hábito o habilidad que tienen los infractores para causar un daño a la víctima, la mayoría de las veces se lo realiza de manera intensional para obtener un beneficio propio o para terceros.

De igual manera cito al tratadista Rodrigo de León, quien manifiesta que el fraude es:

> "El aprovechamiento ilegal de bienes, con enriquecimiento sin causas, de un funcionario público, gerente, administrador o cualquier persona de una empresa, con perjuicio para terceras personas, haciendo mal uso de la confianza conferida". (Algunos fraudes no detectables en libros (tesis de graduación), 1970, pág. 35).

Los conceptos citados anteriormente ponen en conocimiento que los dos elementos más relevantes y constitutivos del fraude son: la malicia o la intención de perjudicar mediante el engaño y el daño que siempre va a ocasionar ya sea de manera inmediata o posteriori.

4.1.5 Falsificación

La falsificación supone crear o alterar un producto o un documento con la intención de hacerlo pasar como real. De este modo, la acción apunta a generar un engaño: la intención es que las personas piensen que el elemento falsificado es el bien original o verdadero.

Cabanellas, afirma que la falsificación es:

> "adulteración, corrupción, cambio o imitación para perjudicar a otro u obtener ilícito provecho" (Diccionario Enciclopédico de Derecho Usual, 1997)

En tal caso es cuando se da el plagio o simulación de lo que desea para así causar daño y conseguir lo que desde un principio quiso.

Así mismo, es importante recalcar que la falsificación constituye obviamente en un delito, es decir, se lo puede considerar como un fraude o como una violación de la propiedad intelectual o patrimonial.

Con respecto a la falsificación de documentos Ossorio declara que es:

> "un delito que se configura por la imitación fraudulenta de ellos, o por la adulteración de uno verdadero, siempre que de tales actos pueda resultar perjuicio. Este delito varía en su gravedad según se haya cometido en documento público o en documento privado". (Diccionario de Ciencias Jurídicas, Políticas y Sociales. 1era. Edición Electrónica., 1998).

De la cita anterior puedo exponer que el delito de falsificación de documentos tiene una gran pesadez o así mismo puede ser poca, porque siempre va a depender del documento que se haya encontrado falsificado o se quiera falsificar.

En la actualidad en las plataformas de venta por medio de internet son muy reconocidas, pero no siempre los compradores están amparados y resulta casi imposible estar seguros en caso de falsificación.

4.1.6 Estafa

La palabra estafa se remonta de la palabra italiana *"staffa"* que significa estribo, subirse a algo que era ajeno. Es decir, originalmente estafa o estafar significaba pedir prestado algo, pero no existía la intención de devolver dicho objeto.

Como es de conocimiento a la estafa hoy en día se la considera como un delito contra la propiedad, que consiste en provocar un deterioro patrimonial a cualquier persona mediante el engaño siempre con la finalidad de obtener un beneficio lucrativo, siendo así que a la víctima la traicionan de la buena fe que tiene. Por ello se puede manifestar que la estafa tiene dos figuras representativas, como es el engaño y el daño al bien patrimonial.

La estafa está siendo reconocida como la promesa de entregar algo que no existe o que no se lo quiere dar, pero antes de realizar la entrega se pide una garantía, pero la persona que dio dicha garantía nunca recibe lo que se le había prometido. En especial, las personas mayores están más expuestas a las estafas porque suelen confiar en la gente. Deben, por tanto, ser objeto de mayor protección por parte de la sociedad.

4.1.6.1 Elementos de la Estafa

El distinguido catedrático Edgardo Alberto Donna y Javier Esteban de la Fuente, dan a conocer que los elementos de la estafa se los divide en dos clases, subjetivos y objetivos, dentro de los cuales encontramos:

4.1.6.1.1 Elementos Subjetivos

Ánimo de lucro. – es el único fin que persigue el autor del delito de estafa, por lo que, forma un escenario falso e idóneo para obtener un beneficio propio o para terceros.

Dolo. – en nuestra legislación es el conocimiento y la voluntad de realizar elementos objetivos del tipo, es decir, este debe incluir el error, el engaño, la disposición patrimonial y el perjuicio económico.

4.1.6.1.2 Elementos Objetivos

Sujetos. – el sujeto activo no siempre va a realizar la conducta delictiva, ya que puede ser la idea de uno y ejecutado por otro. Se debe identificar quien es el sujeto con quien recibió el daño del delito. Por otro lado, el sujeto pasivo es la víctima, quien fue engañada, esta debe tener una inteligencia sutil y una capacidad mínima.

Conducta engañosa. – el engaño debe ser idóneo, para que la situación que crea el infractor logre su objetivo, es decir, que la víctima acepte voluntariamente el desplazamiento de su patrimonio.

Proceder errado de la víctima. – se considera que es errado porque la victima tiene un juicio errado o una apreciación falsa, un concepto erróneo sobre algo, por lo que el agente delictivo se aprovecha para engañar a la víctima.

Disposición patrimonial. – es el fin que persigue el autor del acto para producir el perjuicio económico en la victima y obtener un lucro ilícito.

Perjuicio económico. – es el daño que se da al patrimonio de la víctima, se produce cuando se entrega voluntariamente una cosa, un bien o un servicio sin que exista una causa legal. Aquí, el engaño es la razón del perjuicio, no existe uno sin el otro. (Aspectos generales del tipo penal de estafa, 2004, pág. 9)

4.1.7 Estafa Informática

Según el diccionario de la Real Academia Española, al respecto de la estafa informática otorga la definición más sencilla acerca de este delito declarando que:

> "es el delito de estafa que se comete por medios informáticos". (2019)

Dicho de una manera diferente, Romeo Casabona, describe el fraude informático (que inicialmente denomina «manipulación de datos informatizados») como:

> "la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero". (Poder informático y seguridad jurídica, 1987)

De lo expuesto me permito a realizar una definición más amplia acerca de la estafa informática: es aquella alteración, eliminación o supresión indebida de los datos informáticos por medio de una computadora, celular, Tablet o cualquier herramienta tecnológica, de las personas como es principalmente los datos de identidad, los datos de las cuentas bancarias y la transferencia no consentida de uno o varios activos patrimoniales en perjuicio de estas personas. Así también, se ven afectadas las empresas o entidades bancarias ya que sus datos son interceptados de manera fraudulenta lo que los perjudica gravemente. De igual manera el propósito de quienes realizan esta infracción de estafa informática es con la intención de obtener un beneficio con ánimo de lucro.

4.1.7.1 Elementos para que se Configure la Estafa Informática

Por todo el deterioro que la estafa informática está causando dentro de muchos países ricos y muy desarrollados como lo son Alemania, Francia, España; en sus ordenamientos jurídicos han tipificado la estafa informática mediante el manejo de datos o por medio de la alteración de programas que son utilizados para solucionar los actos ilícitos que causan los

desarrollos informáticos.

Para que exista el delito de estafa informática existen algunos requisitos que nos presenta el abogado Marlon Ron, como:

Obtener un resultado. – Obviamente en esta clase de delitos se obtiene un beneficio económico, pero no es inevitable que este resultado sea falso, es decir, se puede tener un resultado verdadero porque estos delincuentes reemplazan los datos con otros que los beneficie.

Datos. – Se trata de hechos que manejan dato para perjudicar el patrimonio de los individuos ya sea el titular o de terceros, o en su momento utilizar datos que son falsos. Por lo tanto, se da la introducción, alteración o eliminación de datos. Estos incidentes siempre son los más comunes en los delitos de phishing.

Lucro. – En la estafa informática se debe obligatoriamente existir un lucro, dado que, si no existe este tipo penal se hablaría de un sabotaje informático. De igual manera, siempre existirá un lucro porque el delincuente busca ganancias económicas.

Bien jurídico. – En la materia de Derecho Penal los bienes jurídicos son aquellos que demuestran los intereses que tiene la sociedad de manera colectiva, así mismo, tienen un valor importante por lo que el legislador va a considerar indispensable la protección de estos a través de la norma. Además, es necesario recalcar que el bien jurídico que se quiere precautelar en los delitos informáticos es sin duda la información considerada un bien intangible protegido constitucionalmente.

Es por lo que la información debe ser vista desde distintas perspectivas, como: un valor económico, valor intrínseco de la persona, por los sistemas que la automatizan.

Tecnología de la Información y Comunicación. – El acto de la estafa informática debe ser señalado por el inicio, medio y final y evidentemente utilizar las herramientas de la información y comunicación. (Estafa Informática, 2019)

4.1.7.2 Diferencias entre Estafa Informática y Estafa

Hay que tener presente las diferencias que existen entre estos dos tipos de estafas para determinar el tipo penal de cada uno de estos delitos.

Por lo mencionado anteriormente la estafa informática se da por la utilización de las herramientas tecnológicas y no se requiere que la víctima se encuentre físicamente, sino que con el simple hecho de un contacto personal es suficiente para ejecutar el acto ilícito, asimismo es donde e introduce, altera o elimina a información de todos los datos informáticos de las personas, enfocándose principalmente en los datos de identidad, el sistema de un programa o de un sistema. Los infractores pretenden obtener un beneficio por medio de la manipulación de las TIC para ellos o terceras personas.

En cambio, la estafa común su principal elemento que destaca es el engaño o el comportamiento engañoso que debe ser utilizado con una gran precisión para poder influir en las personas y producir un acto indebido, se necesita que la víctima se encuentre en forma física para usar el engaño con el fin de hacer que esta se desapropie de uno o varios de sus patrimonios y se le entregue por voluntad propia para el beneficio de los delincuentes.

4.1.8 Daño

La definición técnica que se puede desprender de este tema es que, daño es el perjuicio o deterioro que sufren los intereses o patrimonios de una persona o empresa en específica. Dicho de otra forma, si el daño se da en un bien, mueble o inmueble, el daño es patrimonial, porque afecta el patrimonio del dueño de los bienes dañados.

Es por lo que Francisco Muñoz y Mercedes García mencionan que se deben diferenciar los tipos de daño que existen según la intencionalidad:

Daño doloso. - es cuando se realiza la acción de manera intencional de producir un deterioro en la persona; también

Daño culposo. - es cuando no existe la intención de producir un perjuicio, pero de igual forma se da por alguna negligencia o descuido que haya existido. (Derecho Penal, Parte General, 2010, pág. 268)

Es importante para la investigación conocer los daños que se pueden dar al patrimonio, por lo cual se los puede diferenciar en dos tipos: el daño emergente, se da cuando la consecuencia es directa de la acción del agente que quiere producir el daño; y el lucro cesante, es cuando no se utiliza de la manera correcta el bien dañado y este produce pérdidas económicas sobrevinientes.

4.1.9 Patrimonio

Es de conocimiento que todos los delitos informáticos afectan al patrimonio de las personas que se ven afectadas, por lo tanto, veo conveniente tratar diferentes definiciones acerca de este tema.

Por primera definición tenemos al jurista Viladevall que define patrimonio como:

> "aquel aspecto cultural al cual la sociedad le atribuye ciertos valores específicos los cuales, a grandes rasgos podrían resumirse en históricos, estéticos y de uso". (El Patrimonio, 2003, pág. 17)

Hace hincapié que el patrimonio tiene un significado particular para las personas que son dueñas de este y de aquellas que lo van a heredar, ya que con los cambios que se pueden dar este va perdiendo o aumentando el valor.

El patrimonio también,

> "registra y expresa procesos largos de la evolución histórica, constituyendo la esencia de muy diversas entidades nacionales, regionales, locales, indígenas y gran parte de la vida moderna". (ICOMOS, 1999)

Al patrimonio desde mucho tiempo atrás se lo ha considerado como el alma de distintas etnias o nacionalidades en todo el mundo, de modo que, se lo protege en gran medida que no sea lesionado por ningún ámbito. También es, todo el conjunto considerado de bienes muebles e inmuebles, de derechos y obligaciones que son propiedad de una o varias personas ya sean naturales o jurídicas a los cuales siempre se los va a proteger de una manera muy especial paraque no se vean afectados por los delitos informáticos o más delitos que se conocen hoy en día.

4.1.10 Datos Privados Personales

De acuerdo con la definición del Reglamento Europeo de Protección de Datos, un dato de carácter personal es:

> "toda información sobre una persona física identificada o identificable". (2016, pág. 2)

Es decir, desde el momento en el que nacemos y nos registramos en el Registro Civil de

cada país ya estamos siendo una persona identificada con la respectiva cédula o el documento que avale nuestra identidad.

De igual forma los datos de las personas son privados, pero también son capaces de determinar qué datos de un sistema informático si pueden ser compartidos con terceros y cuales no, pero siempre teniendo una gran responsabilidad respecto al control de acceso.

El Reglamento Europeo de Protección de Datos (RGPD) ha realizado varias categorías para diferenciar los datos privados de las personas, de los cuales pueden ser: datos personales especialmente protegidos, categorías especiales de datos, los datos genéticos, los datos biométricos, los datos médicos, datos de carácter penal, datos no personales (públicos, comunitarios, privados no personales).

Actualmente el uso de todos los sistemas informáticos va en un gran aumento ya que no solo los adolescentes que son los principales consumidores las utilizan, sino que se ha demostrado que tanto las personas de tercera y mediana a edad han empezado a utilizarlas, pero no la mayoría del tiempo. Según encuestas realizadas en la realizada por el grupo CPP Group Spain refleja un hecho algo alarmante y es que más de la mitad de la población española no considera como datos de carácter personal los almacenados en distintas plataformas de redes sociales, ya sean fotografías, vídeos, etc.; porque creen que al estar en un sitio publico ya no son de carácter personal, sino que todo el mundo puede observar esto.

Referente al tema de investigación es necesario dar a conocer que en cuanto a los datos personales de las cuentas bancarias o identificaciones fiscales es muy diferente a lo mencionado anteriormente ya que en cualquier momento se pueden estar dando los ciberdelitos, como, por ejemplo: los fraudes bancarios, robo digital de tarjetas de débitos, suplantación de identidad, etc.

Existe una gran preocupación y cada día, mejor dicho, cada minuto, se hace más evidente que tanto entidades privadas como públicas deben invertir y hacer todo lo posible por garantizar un tráfico seguro de nuestros datos de carácter personal.

4.1.11 Sanción

La palabra proviene del vocablo latino sanctio, llegando a nuestro idioma como sanción, haciendo referencia a que se va a aplicar un castigo a la persona que no lleva a cabo una norma o regla ya establecida.

El diccionario de la Real Academia Española da un concepto acerca de sanción, mencionando que es:

> "una pena, una ley o un reglamento establecido para sus infractores". (2019)

Según los factores de jerarquía las sanciones se van a expresar en diferentes grados de intensidad, ya sean positivas o negativas para las personas. Este término puede ser considerado de dos formas que son distintas de acuerdo en el ámbito que vaya a emplearse, pero que pueden llegar a conectarse entre sí, es decir, la forma jurídica y la forma social.

Por la forma jurídica es cuando se busca que se represente el castigo o la pena que reciben las personas cuando cometen una infracción, un delito o un acto ilegal y siempre se regirán por el hecho particular.

En cambio, por la forma social, son cuando se basan principalmente por las tradiciones, costumbres, conductas o comportamientos que tienen las personas que forman parte de alguna comunidad o tienen una cultura distinta, es decir, se refieren más en lo ético y lo moral.

4.2 Antecedentes Investigativos

Al realizar una investigación previa en respectivos repositorios de algunas universidades del país he concluido que no existen varios trabajos sobre los delitos informáticos que se están cometiendo en la actualidad, en general más con el tema que trata esta investigación que es sobre el phishing, siendo este una nueva modalidad de estafa o apropiación indebida de los recursos de las personas.

Los países que están más desarrollados alertan a las personas y previenen este tipo de delitos informáticos, por ejemplo, en la legislación española ya está tipificado el delito informático phishing; esto es de gran ayuda o una alerta para nuestro país y países que no tipifican este delito, nos hace reflexionar acerca de lo que pasa hoy en día con la tecnología y los riesgos que trae consigo.

Serrahima Joaquim, en su obra "La Amenaza Digital", analiza y previene al mundo sobre una nueva forma de apropiación indebida de los recursos en red, la tecnología avanza tan acelerada y junto con ello el delito. (2010).

4.2.1 Tecnología de la Información y Comunicación

Es necesario conocer y especificar dicho tema a tratar para comprender de mejor manera la importancia de esta investigación. Para ello he de referirme en primera instancia al término tecnología que proviene del término griego τέχνη (se pronuncia "téchnē") lo que quiere decir arte, oficio o destreza; por tal, es la suma de métodos, técnicas o procesos que son utilizados en la producción de bienes o servicios para obtener logros en alguna investigación científica o darle una nueva función a algo.

En cuanto a la información, es un término que va a variar según el enfoque o la disciplina en la cual vaya a ser tratado. Dicho esto, la información es un conjunto de datos que ya han sido organizados o planeados para que puedan dar un mensaje concreto y eficaz basado en una cierta figura. El autor Idalberto Chiavenato afirmaba que:

> "la información consiste en un conjunto de datos que poseen un significado, de modo tal que reducen la incertidumbre y aumentan el conocimiento de quien se acerca a contemplarlos. Estos datos se encuentran disponibles para su uso inmediato y sirven para clarificar incertidumbres sobre determinados temas". (Introducción a la Teoría General de la Administración., 2007, pág. 110)

Finalmente tenemos a la comunicación, se la puede definir como la habilidad que todo ser humano posee para entenderse con los demás; procedimiento que es utilizado para la distribución de ideas, mensajes o información.

Por lo tanto, la tecnología de la información y comunicación es el resultado de colocar en interacción las telecomunicaciones e informática, con el único fin de obtener, almacenar y dar una buena información. Con las TIC se puede transmitir y procesar información de forma inmediata presentada de diferentes maneras como textos, imágenes, vídeos o sonido.

El objetivo principal de estas es el de mejorar la calidad de vida y reducir los esfuerzos y el tiempo necesario para realizar procesos de trabajo y comunicación, es por ello que algunas de estas tecnologías se han convertido en algo indispensable para las personas, como son las computadoras, teléfonos móviles, televisiones, tabletas, tarjetas de memorias o flash, discos en DVD.

Se pueden encontrar distintas definiciones acerca de las TIC, a continuación: El tratadista Cabero las define como:

> "En líneas generales podríamos decir que las nuevas tecnologías de la información y

> comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e Inter conexionadas, lo que permite conseguir nuevas realidades comunicativas." (Un nuevo sujeto para la sociedad de la información, 2005, pág. 56)

Dicho tratadista da a conocer que las TIC van a utilizar específicamente tres medios que serán básicos para interactuar en las realidades actuales para poder comunicarnos con las demás personas de diferentes partes del mundo.

La Unesco por su parte define a estas como:

> "disciplinas científicas, de ingeniería y de técnicas de gestión utilizadas en el manejo y procesamiento de la información: sus aplicaciones; las computadoras y su interacción con hombres y máquinas; y los contenidos asociados de carácter social, económico y cultura". (Documents General Conference., 2022)

Las TIC Son aquellas conductas que se las manejan para asociar las distintas culturas dentro del ámbito social y económico para que obtengan un buen encausamiento de la información.

La definición que es de mayor relevancia es la del jurista Cobo Romaní, ya que define a las tecnologías de la información y la comunicación como:

> "Dispositivos tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información con protocolos comunes. Integran medios de informática, telecomunicaciones y redes, posibilitan la comunicación y colaboración interpersonal y la multidireccional (uno a muchos o muchos a muchos). Desempeñan un papel sustantivo en la generación, intercambio, difusión, gestión y acceso al conocimiento". (El concepto de tecnologías dela información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento., 2011)

El uso de las TIC es creciente y se extiende de una manera tan significativa, principalmente en los países que son considerados ricos y con un gran desarrollo; así mismo, muchos temen que este desarrollo sea el origen de un nuevo paradigma que puede provocar grandes cambios en la sociedad.

4.2.1.1 Características

Existen diferentes características generales dentro de algunos contextos, fundamentalmente en el educativo porque es más relevante para la educación de las personas.

Es por lo que las características más elocuentes en los últimos años son las que menciona el tratadista Cabero:

Inmaterialidad. - Las TIC realizan la creación, el proceso y la comunicación de la información, que puede ser llevada de forma transparente e instantánea a lugares lejanos (internet o la nube).

Interactividad. - Característica más importante de las TIC para su aplicación en el campo educativo; se consigue un intercambio de información entre el usuario y el ordenador.

Interconexión. - Hace referencia a la creación de nuevas posibilidades tecnológicas a partir de la conexión entre dos tecnologías.

Instantaneidad. - Permiten la comunicación y transmisión de la información, entre lugares de larga distancia, de una forma rápida y eficaz.

Elevados parámetros de calidad de imagen y sonido. - El proceso y transmisión de la información abarca todo tipo de información, por lo que los avances han ido encaminados a conseguir transmisiones multimedia de gran calidad.

Digitalización. – a la información se la representa en un formato único universal, lo cual hace que sea transmitida a través de los mismos medios.

Innovación. - Las TIC están produciendo una innovación y cambio constante en todos los ámbitos sociales, dando lugar a una nueva fundación de medios para impulsar las comunicaciones.

Diversidad. – Tienen varios propósitos, es decir, no solo cumplen el propósito de comunicarse entre las personas, sino también de crear nueva información, buscar información.

Amplio alcance. – Las TIC no solo se enfocan en un mismo grupo de personas, sino que han llegado a extenderse y a penetrar áreas como la medicina, economía, casos militares, educación privilegiada, entre otros a nivel mundial. (Ciber sociedad y juventud: la cara oculta

(buena) de la luna., 2005, pág. 56)

4.2.1.2 Ventajas

Han hecho más fácil el acceso a la información y comunicación a larga distancia por la diversidad de medios que existen.

Las personas tienen motivación e interés para realizar cualquier tipo de actividad dentro de las tecnologías, especialmente dedican tiempo al trabajar desde casa, siendo notorio que aprenden más.

Proporcionan nuevos puestos de trabajo en las industrias que día a día van iniciando dentro de las tecnologías.

Brindan un rápido y libre acceso a la mayoría de la información para obtener un mejor conocimiento.

Las herramientas que proporcionan las TIC realizan el cultivo de actitudes sociales, es decir, que se trabaje en equipo, que se intercambien ideas, que desarrollen su personalidad, que tengan facilidad de palabra o escritura y que vayan descubriendo soluciones para algún problema.

Ayudan a las personas que sufren algún tipo de deficiencia en el ámbito audiovisual o alfabetización, es decir, generan nuevas experiencias y facilitan el aprendizaje.

Generan que exista competencias de expresión y creatividad entre las personas porque ayudan al desarrollo de distintas habilidades como la expresión oral, expresión escrita, gráfica, visual y auditiva.

Ayudan a los docentes con material de trabajo para los estudiantes que sin duda pueden mejorar su aprendizaje.

En la actualidad existen simulaciones en realidad virtual para que las personas puedan tener otras experiencias fuera de su cotidianidad con fenómenos inexistentes.

4.2.1.3 Desventajas

Son una distracción para las personas, especialmente para los adolescentes ya que en lugar de estudiar se dedican a jugar videojuegos o ver videos no relacionados a sus estudios.

Al existir un sin número de información dentro de las tecnologías por el motivo del internet la mayoría de las veces se pierde el tiempo por exagerar la búsqueda de esta.

La sociedad al exagerar el uso de las TIC puede llegar a volverse adictas a estas y no saber utilizarlas de la manera adecuada.

Los usuarios estarán expuestos a varios peligros dentro de las TIC, como son los delitos informáticos.

En el internet existe información que no siempre va a ser fiable, muchas veces las personas utilizan este medio en forma de gracia.

Muchas personas se acostumbran al uso de estas y obtienen un aprendizaje incompleto y superficial.

A veces los programas presentar una visión muy irregular acerca de la realidad que existe, es decir, presentan lo que no es.

Pueden provocar ansiedad o depresión en las personas.

Existe un cansancio virtual y otros problemas físicos o psicológicos.

No todas las personas saben utilizarlas y esto genera que se produzca estrés y agotamiento emocional.

4.2.1.4 Tipos

4.2.1.4.1 Redes

En las últimas décadas los avances científicos han sufrido un gran desarrollo dentro de la tecnología, información y comunicación, especialmente lo que son las redes.

Se las puede definir como los sistemas de comunicación que conectan varios equipos entre sí a través de la cual circulan todos los datos y se componen básicamente de usuarios, software y hardware; esta conexión puede ser por medio de un cable, vía satélite o por frecuencias de radio.

> "Las redes así constituidas, no son sólo una estrategia para la cooperación y construcción del conocimiento, sino que son el modelo organizativo que puede

> contribuir al fortalecimiento institucional al integrarse como redes generadoras de conocimiento y que parten de la unidad que conforma un cuerpo". (La integración de redes de colaboración entre cuerpos académicos., 2012)

En distintas palabras se denomina red a todo sistema de comunicación que enlaza a dos o más equipos, los cuales ayudan al desarrollo de las personas para que obtengan mucho más conocimiento a través de estas, pero teniendo en cuenta que desde el principio hay que saber utilizarlas para que luego no existan consecuencias para uno mismo o para los demás.

La gran ventaja que otorgan las redes hoy en día es la que se puede compartir todos los recursos que normalmente son muy poco utilizados o que tienen un alto costo por lo cual algunas personas de baja economía no pueden darse el gusto de utilizar, como son las impresoras o copiadoras.

Otra ventaja que se puede observar de las redes es la efectividad que tienen al organizar varios medios que son óptimos para realizar un buen desempeño, como, por ejemplo, en los presupuestos de las empresas, presupuestos de las escuelas y colegios.

Entre las distintas redes que se existen se diferencian algunos tipos según su tamaño, su velocidad de transferencia y el gran alcance que tienen.

4.2.1.4.2 Terminales

Son conocidos como consolas, es decir, un dispositivo electrónico que se lo utiliza para la función de introducir datos que serán mostrados en una computadora, un móvil, las tabletas, las laptops, los televisores y las consolas de videojuegos, siendo todos estos elementos un punto de acceso a la información ya que continuamente van evolucionando.

Para muchas personas que tienen conocimiento acerca de los terminales consideran que son como una entrada y salida de la información, que se utilizan para transmitir todos los datos a cualquiera de los dispositivos ya mencionados anteriormente.

La científica Roig manifiesta que es:

> "Un terminal está formado por un teclado y una pantalla: el teclado permite introducir programas o datos al ordenador". (Tecnología de la Información. Conceptos Básicos., 2008, pág. 16).

La única finalidad de estos terminales es que se enfocan en expandir sus funciones para que se puedan mejorar las actividades diarias como la búsqueda de información de los temas que les parecen más importantes a las personas. También existen los terminales modernos porque pueden emular hasta 40 o 50 máquinas simultáneamente, utilizados especialmente dentro de los sitios de trabajo.

4.2.1.4.3 Servicios

Al principio los servicios estaban centrados en la difusión de información estática y algunas otras herramientas. Luego apareció un segundo grupo de servicios como el comercio electrónico, la banda online, el acceso a contenidos informativos, de ocio y el acceso a la administración pública. (Romero, 2012, pág. 4). En la actualidad los servicios siempre se van a ir transformando o van a sufrir cambios para poder utilizarlos de la mejor manera.

Este tipo de servicios ofrecen distintos servicios a los usuarios o consumidores entre los que se destacan principalmente el correo electrónico, la banca en línea, la administración electrónica, el gobierno electrónico, aprendizaje electrónico, el GPS, la nube, la educación, el cine, videos, audio y música, etc.

Finalmente hay que considerar también a un software como un servicio que sea utilizado para hacer todo tipo de actividad dentro de las TIC, es decir, pagos en línea, compras virtuales, enviar paquetes a diferentes lugares ya sea a corta o larga distancia; así mismo son de gran ayuda para verificar el registro y estado del envío.

4.3 Delitos Informáticos

4.3.1 Definición y Generalidades

En nuestro país los fenómenos de la criminalidad por medio de las herramientas tecnológicas o mayormente conocidos como los delitos informáticos, no han alcanzado la importancia que realmente se merecen, motivo por el cual no se tiene un conocimiento amplio dentro del entorno de los ciudadanos a pesar del efecto tan global en el que estamos viviendo, razón por la que existe esta nueva modalidad de estafa que no es tomada en cuenta; se lo puede considerar un gran problema no solo dentro del ámbito penal sino dentro de todo el ordenamiento jurídico nacional.

Hoy en día no se encuentra una definición que sea aceptable por todos los juristas y

estudiosos del derecho, pero de igual forma, se han dado definiciones funcionales que atiendena las verdades concretas por las que cada país pasa.

Es por lo que doy mención al tratadista Téllez que conceptualiza al delito informático como:

> "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". (Los delitos informáticos. Situación en México, 1996)

Señalando que el delito supone una multiplicidad de modalidades consideradas delictivas que están vinculadas en cierto modo a los ordenadores o conocidos cotidianamente como computadoras, porque en la actualidad es cotidiano que utilicen los dispositivos electrónicos a cualquier hora del día sin un tiempo limitado.

De igual forma, los autores chilenos Huerta y Líbano definen los delitos informáticos como:

> "[…] todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro". (Los delitos informáticos, 1996)

Con todo lo mencionado anteriormente es importante establecer que los delitos informáticos son aquellas conductas dolosas o criminógenas que están encaminadas a la alteración o violación de todos los bienes jurídicos protegidas de las personas, afectando a la integridad personal o psicológica, ya que estos delitos son los que más han ido evolucionado; por ello, todos los organismos legales de los países deben estar incluso hasta adelantados con las sanciones que deben tener las personas que comentan estos delitos.

Gracias a la información que existe se deduce que existe un gran número de delitos informáticos siendo su única limitación la imaginación y capacidad que tenga el autor de

estos. La revista digital Parlar publicó el 22 de diciembre del 2019 todos los datos estadísticos de las infracciones informáticas que se dan dentro de nuestro país. Las primeras cifras más comunes que son de mayor relevancia son las modalidades de acceder al sistema informático de una persona por algún dispositivo con información peculiar y el segundo es cuando se aceptan a personas desconocidas en nuestras redes sociales (a veces son los mismos delincuentes) que quieren aprovecharse del poco conocimiento que tiene la sociedad; así mismo, se mencionan las ciudades donde se registran más este tipo de infracciones, siendo estas: Guayaquil, Pichincha y Azuay.

Cabe mencionar que el escritos Luis Azaola Calderón deduce las formas más comunes para la comisión de los denominados delitos informáticos como son:

> "el sabotaje, espionaje, fraude, robo, el acceso no autorizado a servicios informáticos y últimamente acoso escolar, acoso, injurias, calumnias entre otros; mismos que trasgreden la seguridad de los sistemas de información y comunicación; y, vulneran incluso los derechos de los seres humanos". (Delitos Informáticos y Derecho Penal, 2010, pág. 85).

Dicho esto, considero que en nuestro país hace falta algunos técnicos que asuman el trabajo de realizar peritajes dentro de la red para descubrir a los autores de los delitos, conocidos como "piratas cibernéticos" y que se pueda vincular dichos delitos a algunas sanciones que tiene nuestro Código Orgánico Integral Penal, así sea que nuestro código mantenga vacíos en cuanto a delitos informáticos.

4.3.2 Sujetos del Delito Informático

Dentro del delito informático es de suma importancia la presencia de dos personas, es decir, el sujeto activo que va a cometer la infracción y el sujeto pasivo quien será considerado como víctima; estas dos personas son de gran ayuda para el estudio de un tipo penal.

4.3.2.1 Sujeto Activo

Es la persona o individuo que contienen características especiales, es decir, que los delincuentes tradicionales no tienen, ya que se conoce que existe complejidad en la mayoría de los casos al realizar algún tipo de delito informático, estas personas deben tener un alto conocimiento o habilidades superiores para el manejo de las herramientas tecnológicas y así cometer el ilícito fácilmente sin dejar huellas o rastro para la persecución de estos.

Además, el sujeto activo siempre va a estar ubicado en sitios o lugares estratégicos en donde se encontrará información perceptible, no hay que utilizar mal esta información porque traerá consigo varios problemas y no se podrá realizar al cien por ciento el delito.

Estos sujetos cuentan con algunas características, entre ellas están la alta condición socioeconómica, porque se sabe que necesitan de buenas herramientas tecnológicas para ejercer su daño a la o las personas; de igual forma, son sujetos listos, inteligentes, motivadas para crear o descubrir cualquier desafío tecnológico que se les presente, por todo lo mencionado es casi imposible descubrirlos gracias al poder económico y la gran habilidad que poseen.

A la persona que se le considera sujeto activo también se lo distingue o nombra por diferentes términos porque en el tiempo actual se conciben como las nuevas modalidades delictivas que están revolucionando dentro del internet u otras plataformas.

Por ende, es importante reconocer las denominaciones que el escritor Castro ha diferenciado, a continuación:

Hacker. - Son los individuos que gozan de tener la experiencia necesaria para poder acceder a los sistemas tecnológicos sin alguna autorización, su finalidad es la de obtener información y de perjudicar dichos sistemas.

Es muy extraño conocer o averiguar los nombres verdaderos de estas personas y en algunas ocasiones hasta son parte de grupos o asociaciones que se dedican a delinquir de esta forma. Pero llegando a los años 80 estos hackers deciden diferenciarse de otros individuos que solo desean el beneficio propio para destruir.

Cracker. - Este es quien crea y modifica el software y hardware de todas las computadoras para poder desarrollar las modificaciones que desea a su gusto, es decir, descomponen aquellos programas de protección de seguridad de los sistemas y logran producir el perjuicio que desean. En definitiva, son aquellos programadores que tienen el único fin de destruir todo lo que ellos quieren en las redes de forma no autorizada e ilegal.

Phreaker. - Es aquella persona que tiene una gran inclinación hacia los sistemas telefónicos, es decir, conoce el funcionamiento de las redes de la telefonía. Su motivo es obtener llamadas ilimitadas, realizar espionaje a cualquier persona, poder grabar conversaciones ajenas de otros teléfonos para luego sacar información y en algunos casos

producir un chantaje, en general, destruir todo lo que tiene que ver con las líneas telefónicas.

Carding. - La finalidad de estas personas es obtener un beneficio económico ilegal, utilizan números de tarjetas de crédito para traspasar el dinero directamente a otras cuentas ilícitas, dicha actividad está relacionada con el tema de investigación que es el delito del phishing, el delincuente origina páginas web falsas induciendo a la víctima ingresar sus datos.

Thrashers. - Son etiquetados como las entidades o sociedades más peligrosos dentro de los delincuentes informáticos. Esta palabra traducida al idioma español significa basurero, puesto que ellos buscan y rebuscan en todas las papeleras de los cajeros automáticos bancarios, con el propósito de obtener las contraseñas de las tarjetas de débito o crédito de los usuarios. (Tipos de Sujetos Activos en Delitos Informáticos, 2015)

Con lo expuesto se puede determinar que hoy por hoy el mundo de la tecnología, información y comunicación ha dado espacio para el origen de este tipo de delincuentes, muchos de estos hasta llegan a integrar pandillas a fin de realizar un atraco cibernético lo cual crea que los usuarios tengan miedo o incertidumbre al utilizar cualquier herramienta tecnológica ya sea desde su hogar o su lugar de trabajo, no se sienten seguros porque estos delincuentes operan con tanta frecuencia que ningún usuario podría percatarse de lo que le esté sucediendo.

4.3.2.2 Sujeto Pasivo

Sujeto pasivo se refiere al individuo sobre quien reincide la conducta delictiva, se explica que es la víctima del delito (persona natural o jurídica), entidades financieras o hasta los gobiernos que sufren un perjuicio en su patrimonio por el hecho que utilizan las herramientas tecnológicas.

Como bien es cierto en esta clase de delitos no se produce la fuerza física o violencia en las personas ni en las cosas, aquí se especifica que existe simplemente la manipulación por la informática y como inferencia se produce una transacción, sustracción o apoderamiento en los bienes muebles o inmuebles sin el consentimiento.

Ahora es muy difícil que las personas denuncien este tipo de delitos porque tienen el pensar de que las autoridades no son lo suficientemente buenas para encontrar a estos piratas informáticos. De igual forma no existe una correcta tipificación de estos delitos por ende se da la desconfianza de las víctimas y deciden dejar el ilícito en la impunidad porque no desean

perder su tiempo, sus energías e incluso sus propios recursos ya que consideran que no tendrán éxito para encontrar a la persona que le produjo el daño.

4.3.3 Repercusión en la Sociedad Actual

Gracias a la evolución que se da día tras día el desarrollo de la sociedad ha sido indispensable para relacionarse uno con otro, razón por la que la tecnología no se queda atrás y va evolucionando incluso mucho más, siendo una herramienta utilizada dentro de la vida cotidiana para realizar tareas importantes dentro de la comunicación.

Es increíble la forma en que son empleadas las herramientas tecnológicas, las utilizan para traspasar información y también realizar transferencias bancarias, además para enviar acuerdos sociales y que tengan que ver con temas políticos.

Sabemos que el avance de la tecnología y todos los medios que dentro de ella existen son muy importantes a nivel mundial porque son de gran ayuda para todos los seres humanos que, en la actualidad, hasta las usan en el interior del ámbito laboral, familiar, económico, escolar, bancario, entre otras.

No obstante, la evolución de estas herramientas tecnológicas no es siempre tan buenas como lo parecen, es decir, hoy por hoy estas son utilizadas para el surgimiento de nuevos delitos informáticos, que se los denomina "delitos de cuello blanco"; las personas al proporcionar su información personal en cualquier tecnología, ya sea un celular, una computadora, una Tablet, etc., pueden ser violentadas por estos infractores que no realizan ni mucho esfuerzo para logar su beneficio.

Por todo lo descrito es obvio que hay que luchar con todas estas conductas delictivas, se contempla la necesidad que existe de que se tipifique esta clase de delitos dentro de nuestro Código Orgánico Integral Penal o incluso reformar algunas maneras, para que exista la sanción que se adecue al tipo penal.

4.4 Las Redes Sociales

4.4.1 Historia

Las redes sociales son un acontecimiento motivado por grandes avances tecnológicos, entre los cuales tenemos el de Estados Unidos que creó la *Advanced Research Projects*

Agency (ARPA) que permitía el intercambio de información entre instituciones; con el paso del tiempo gracias a este avance muchas personas empezaron a estar en constante comunicación, ya que el primer email que se envió fue en 1971, es decir, han ido evolucionando según la demanda de los usuarios y con las herramientas tecnológicas que día a día son mucho más avanzadas.

Al pasar de los años nuevas plataformas siguieron surgiendo, pero con algunos ajustes que no estaban del todo correctos, en el año 2005 las redes sociales empezaron a crecer en el mercado, pero sin tener un dominio global. En Latinoamérica la plataforma *Hi5* se convirtió en la red con mayor crecimiento; en este mismo año la plataforma Facebook permitió el ingreso de bastantes personas siendo así que se crearon un billón de usuarios.

En la actualidad existe una diversidad de plataformas como YouTube, Instagram, Twitter, Pinterest, WhatsApp, Tiktok, Google, Twicth, entre otras, con una audiencia única u otras que son utilizadas por todos los seres humanos.

Son una forma de sentir a las personas que se encuentran lejos más cerca, dan la oportunidad de cortar la distancia y no simplemente eso, sino que ayudan a estar en constante movimiento realizando actividades como deporte, trabajo, leyendo, entre otros.

4.4.2 Definición

Gracias a la aparición de la informática se dio origen a las redes sociales, las cuales son utilizadas por las personas a través de un medio virtual, siendo una forma muy distinta a la realidad, por medio de estas existe la posibilidad de interactuar entre nosotros, conocer gente nueva, experimentar actividades de acuerdo con nuestros propios gustos sin limitaciones de tiempo ni de espacio.

Los tratadistas Martínez & Lomarte, afirman que se conoce como redes sociales a:

> "[…] aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través del internet para que estos generen un perfil con sus datos personales facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su interacción." (Derecho y Redes Sociales, 2010, pág. 6).

Con lo mencionado nos ayuda a identificar que las redes sociales son un conjunto de

personas por lo que ellos mismo crean sus perfiles u usuarios para poder tener algunos vínculos entre sí, ya sea por temas musicales, educativos, comerciales, parentesco, etc.

Sin embargo, también se menciona que los usuarios deben compartir criterios comunes pero lo que sin duda no va a suceder, ya que cada persona tiene su propia personalidad y su distinto pensar, es posible que, si tengan ideas parecidas, pero no siempre van a ser las mismas, lo que si se espere es que exista el respeto y responsabilidad al compartir todos los pensamientos en las redes sociales.

Adicionalmente, Jaramillo considera que estas redes son:

> "[…] estructuras sociales compuestas de personas, organizaciones u entidades, que están conectadas por uno o varios tipos de relaciones, […] o comparten creencias, conocimientos, etc." (Twitter para todos, 2010, pág. 22)

Como es de conocimiento la principal razón de las redes sociales es conectar a las personas dentro del mundo virtual ya sea para compartir los gustos o disgustos, crecencias, cultura; es innegable el éxito que hoy por hoy viven estas y sin duda las ganancias que tienen van en aumento.

4.4.3 Características

Las redes sociales son de fácil acceso ya que disminuyen la barrera de distancia, tiempo entre dos o más personas siendo fácil su comunicación con distintas personas de diferentes razas, etnias, nacionalidades.

Estas son herramientas donde la información se publica de manera instantánea, a veces perjudica el derecho de los individuos porque al compartir un video, una foto o comentario no se tiene todo el control, llegando hasta violentar o agredir la intimidad de estos.

De igual manera estas redes tienen características con gran peculiaridad ya que son el punto de encuentro de millones de usuarios de partes de todo el mundo, a continuación, se presentan algunas de ellas que son descritas por la escritora Romina Aguilar:

Interacción. – Se interactúa con diferentes usuarios por medio de estas, ya que nos podemos expresar y establecer conversaciones para mejorar dentro del aspecto en las que se estén utilizando las redes.

Creación de comunidades virtuales. – Se pueden crear diferentes comunidades virtuales de usuarios para recopilar información sobre alguna marca en específico, de productos o servicios.

Atractividad para jóvenes. – Estas se dividen en base a la edad que tengan los usuarios ya que no en todas las redes tienen el mismo contenido. Un ejemplo es el uso de la plataforma Tiktok que está dirigido para un público menor de 40 años y Facebook que es para todo tipo de edad, excepto los niños que deben estar bajo supervisión.

Contenido Viral. – Se encuentra todo el contenido que haya sido viral hace algunos años o en la actualidad. Son una puerta de conexión para consumir todo lo que nos interese.

Información real instantánea. – Es obvio que a todas las redes las tenemos a nuestro alcance por lo que significa que podemos enviar toda la información que deseemos en el instante que queramos, evitando que las personas se aburran o dentro del ámbito comercial no se arrepientan de comprar.

Masivas. – Son plataformas que no optan por tener capacidad de limite, los usuarios siempre van a ir en aumento y así mismo la información ira evolucionando. (Redes Sociales: ¿Cuáles son sus principales características para el 2021?, 2020)

4.4.4 Ventajas y Desventajas

Estas herramientas tecnológicas tienen un gran potencial positivo siempre y cuando se dé el uso adecuado, algunas ventajas que presentan son las siguientes:

Conexión a nivel mundial. – Se puede conectar con personas que hace años no se ven o conocer nuevas personas y verse por medio de las cámaras.

Grupos. - Se consideran lo mejor porque por medios de ellos existe una llamada "inteligencia conectiva" donde conecta a usuarios de todo el mundo. Existen grupos públicos oprivados, en algunos se preguntan las dudas que se tiene de un tema determinado.

Denuncia social. – Es de gran ayuda que las noticias de algunos crímenes, delitos, corrupciones se hagan públicos o inclusive virales para poder llegar con los actores de estos y que obtengan la sanción que les corresponde.

Aprender idiomas. – Gracias al fácil acceso a las redes ya no existen excusas para no

aprender nuevos idiomas porque se lo puede realizar desde la comodidad de tu hogar y en cualquier momento que deseemos. Si se busca en internet se encuentran demasiadas plataformas.

Ampliar tu negocio. – Dentro del ámbito comercial y administrativo si se tiene un negocio es muy fácil hacer conocer el mismo, también se localiza de forma rápida a los clientes y hasta se lleva a domicilio lo que adquieran.

Entretenimiento. – Se las usa para la diversión y desconectarse de la realidad cuando las personas están cansadas o aburridas.

Diversidad de empleos. – Dentro de las redes sociales hay que posicionarnos de una manera adecuada y profesional, ya que no siempre vamos a encontrar un empleo, sino que tenemos que nosotros mismos ayudarnos para hacernos más visibles hacia la sociedad.

Si no se gestiona de manera adecuada a las redes sociales pueden provocar incidentes en todos los ámbitos en que nos relacionemos, he aquí algunas desventajas que esto produce:

No existe contacto físico. – Muchas de las personas usan las redes sociales todo el día y no se relacionan con el mundo exterior. El uso excesivo de las mismas es muy malo.

Posibilidad de fraude o robo de identidad. – Se debe tener un límite para publicar información nuestra en las redes, hay que ser cauteloso cambiando las contraseñas a menudo.

Pérdida de tiempo y productividad. – Esta mal visto que en horas de trabajo o dentro de tu jornada laboral se utilicen las redes sociales porque se desconcentran y no realizan al cien por ciento lo que deben hacer.

Creer información falsa. – En la actualidad hay un sin número de información falsa que circula por las redes, algunas son utilizadas como bromas que, si pueden ser graciosas, pero en muchos casos provocan problemas.

Cyberbullying. - Algunos infractores utilizan las redes para aprovecharse de los niños, niñas o adolescentes. En el ámbito educativo existen comportamientos inadecuados, es por ello, que las instituciones tienen que realizar un gran hincapié en la educación sobre el buen uso que deben darle a las mismas.

Adicción. – Se produce por el uso descontrolado de las redes cuando se presentan

síntomas de ansiedad, depresión, intranquilidad, por eso las personas quieren perderse en el mundo de las redes para no aceptar su realidad. (44 Ventajas y desventajas de las redes sociales, 2019)

4.5 El Delito Informático de Phishing

4.5.1 Origen

Este término proviene de la palabra inglesa "fishing" que significa pesca porque hacen la alusión al intento de que los usuarios como se dice comúnmente "muerdan el anzuelo" y por eso al infractor que practica este método se lo llama phisher.

Se dio la primera mención de este término en el año 1996 en el mes de enero, por medio de un grupo de noticias de hackers, aunque según la información es posible que años atrás ya se hubiera utilizado en la edición impresa del boletín de noticias hacker 2600 Magazine. (Ollmann, 2006)

4.5.2 Definición

Por la velocidad que tiene el mundo electrónico para evolucionar a gran escala los delincuentes se han dado cuenta que la Red es un modo para realizar de manera más eficiente y practica las llamadas estafas tradicionales informáticas.

Es por lo que no se puede dar una definición precisa de lo que se entiende por el delito de phishing porque se trata de un fenómeno que va evolucionando día tras día.

Sin embargo, el Phishing es una conducta informática que distingue un modelo de abuso informático que se da por medio del uso de un tipo de informática o ingeniería social caracterizado por pretender obtener información de forma fraudulenta. De este modo el infractor o phisher como ya lo manifesté, se esconde debajo de una identidad falsa, ya sea de una persona o empresa; por lo común se envían correos electrónicos u otro sistema de mensajería instantánea y también por las llamadas telefónicas.

Otra definición, que contiene la idea básica que subyace tras el Phishing, lo define como:

> "[…] una forma de ingeniería social en la cual un atacante intenta de forma fraudulenta adquirir información confidencial de una víctima, haciéndose pasar por un tercero de confianza". (González, 2007)

Efectivamente, no se trata de algo reciente, es decir, es la suplantación de empresas o personas que tienen el único fin de robar información personal de diferente tipo para defraudar y obtener un beneficio propio o para terceros, con el motivo principal que es hacer uso de las herramientas tecnológicas para poder realizar ese delito en forma masiva y en periodo de tiempo demasiado corto.

El espacio del Phishing por lo común está relacionado con la facultad de duplicar una página web para hacer creer a la víctima que se encuentra en el sitio original y no en el falso. En ello se produce el engaño a través de un correo electrónico que se da por medio de spam (correo no deseado) invitando a acceder a una página que tienen la apariencia casi idéntica a un sitio verdadero, una vez que las victimas ingresen son engañados para que pongan sus datos personales confidenciales como número de cédula, de pasaporte, tarjetas de crédito o débito, datos financieros y bancarios, proporcionando así a los delincuentes un margen extenso para realizar las estafas y fraudes a su patrimonio.

Una medida más para que se de este tipo de delito, aunque no es muy común son cuando se da por medio de fax y los mensajes SMS a través de los teléfonos móviles. En ciertos casos estos mensajes son genéricos porque son enviados en forma abundante para alcanzar que exista una gran cantidad de usuarios sabiendo que por lo menos algunos caerán en la trampa e ingresarán al sitio falso para robarse la información. También envían mensajes proclamando grandes premios y descuentos en la venta de productos.

Las características que se exhiben más frecuentes en este tipo de mensajes son:

Utilizar el nombre de un empleado o trabajador real de alguna empresa como remitente del correo falso. Por esta forma si se intenta verificar que este correo es cierto llaman a la empresa y le informaran que esa persona si trabaja ahí.

El manejo de nombres de compañías que ya existen. Aquí los infractores no crean desde cero una página para poder delinquir, sino que adoptan la imagen de alguna cooperativa y funcionalidad de la página web, con el fin de desconcentrar al receptor del mensaje.

Páginas web con un aspecto idóneo. Como he mencionado estos correos electrónicos suelen llevar al lector hacia sitios que parecen ser el sitio original, pero sin duda son falsos y están siendo utilizados para robar la información. Incluso la información legal y otros enlaces no vitales pueden redirigir al confiado usuario a la página web real

Los infractores tienen un límite de tiempo muy breve para delinquir, porque las victimas informan a las empresas que están siento objeto de algún tipo de delito porque el servidor alojan un sitio web fraudulento y que sirve para recoger información, es ahí donde se cierra esta página. (Belcic, 2020)

4.5.3 Tipos de Phishing

Se diferencian varios tipos de phishing, pero van a depender en la forma que se de este fraude. Es necesario saber que el mayor número de estos tipos se pueden evitar por un poco de sentido común, ya que siempre hay que ver lo que se nos ofrece.

No todo el tiempo se debe confiar en los mensajes que llegan al correo electrónico que ofrecen acceder a grandes cantidades de dinero, ni tampoco en aquellos mensajes que piden nuestros datos personales o de cuentas bancarias, hay que saber ignorar para evitar cualquier problema.

Principalmente se pueden diferenciar los siguientes tipos de phishing según el modus operandi, es lo que menciona en el escritor Miguel Salas en su artículo:

Estafa Piramidal. – en la actualidad este tipo de estafa está muy de moda, es en el cual, llega una oferta de empleo al correo electrónico de cualquier usuario que se basa en la promoción de algún producto y la captación de nuevos empleados. Estos empleados tendrán que abonar un poco de dinero para iniciar a trabajar, lo que es muy obvio que nunca podrán recuperar, sino que se darán cuenta que las ganancias que van a obtener se van a generar por captar a nuevos empleados cada vez y no por la venta del producto que se les mostró inicialmente.

Phishing engañoso. – consiste básicamente en el envío de correos electrónicos en general, para que alguno de los usuarios caiga en la trampa, este correo suplanta a una entidad o institución legitima y quiere dar confianza a la víctima, ella dará clic en el enlace siendo desviado de manera inconsciente a un sitio falso, en el que se requiere la información personal del usuario, si este da la información el phisher ya podrá realizar el fraude que quiere para obtener un beneficio.

Smishing. - este tipo utiliza el teléfono móvil como herramienta, en donde los usuarios reciben un SMS en el que les manifiesta que llamen a un número que les salga en pantalla para recibir algún tipo de regalo, recompensa o para saber es quieren; cuando el usuario llama

accede sin conocer a un servicio telefónico en el que se pide información personal que serán utilizados para el fraude.

Pharming. – el atacante modifica los mecanismos de resolución de nombres sobre los que el usuario accede a las diferentes páginas web tecleando la dirección en su navegador. Esta modificación provoca que cuando el usuario introduce en el navegador la dirección del sitio web legítimo, automáticamente es dirigido hacia una página web fraudulenta que suplanta a la oficial.

Mulas. – se trata de un blanqueo de dinero, es decir, el usuario recibe un correo electrónico donde se le dice que tiene la posibilidad de quedarse con un cierto porcentaje de dinero de alguna transacción electrónica por el simple hecho de realizar una transferencia del importe recibido menos la comisión a otra cuenta que se le indica en dicho correo.

Malvertising. – es en aquel que los ciberdelincuentes realizan un pago a las páginas de anuncios legítimos para que muestren anuncios en las páginas web donde trabajen o paginas relaciones a las redes sociales para persuadir a las víctimas a que accedan a los enlaces o naveguen hacia las páginas web fraudulentas por la cual se descarga el programa maligno en sus dispositivos y les permite obtener la información que deseaban. (Tipos de Phishing, 2019)

Por otro lado, se dan los tipos de phishing según el servicio que ataquen:

Redes sociales. – es en la cual se pretende suplantar la identidad de las personas y obtener información privada. Esta forma es muy utilizada hoy en día porque la mayoría de los seres humanos se comunican por las redes sociales, no cabe duda de que los usuarios se van incrementando conforme pasa el tiempo y es mucho más probable que sufran estos ataques.

Bancos y cajas. – los phishers envían correos donde solicitan los datos de la cuenta bancaria o la tarjeta de crédito porque manifiestan que es por motivos de seguridad ya que la cuenta fue bloqueada o porque cambio la normativa en el banco del que sea parte, etc. El objetivo es robar la contraseña de la tarjeta de crédito para obtener beneficio lucrativo.

Juegos online. - los motivos de este tipo son: robar los datos bancarios, robar la identidad del jugador, suplantar la identidad; el juego en el que más ha existido este fraude es en "WorldWarcraft".

Falsas ofertas de trabajo. – se dan diferentes tipos de ofertas con las cuales quieren

engañar a los usuarios, por ejemplo: trabajar desde casa haciendo labores manuales por lo que piden dinero para guardar su puesto; cuando llaman al número del anuncio que vieron y piden sus datos para tener el trabajo; al entrar al enlace de un anuncio ficticio ya se instala un programa maligno fraudulento. (La guía definitiva sobre el phishing: qué es el phishing y cómo evitar las estafas, 2020)

4.5.4 Fases del Phishing

Gracias a las investigaciones que se han realizado se ha podido observar que existe un grupo de normas que se ajusta a los ataques que realizan los ciberdelincuentes. Pero hay que tomar en cuenta que no siempre van a ser las mismas, porque en algunas ocasiones estas normas pueden cambiar dependiendo del ataque y su escala, es decir, si es profundo, extenso o difícil, de igual forma con los agentes que intervienen y que papel deben seguir.

A continuación, las fases que se pueden registrar cuando se dé un tipo de phishing, reconocidas por la escritora Mayra Leguizamón:

Planificación. – en esta etapa el phisher toma las principales iniciativas con las que va a llevar a cabo el ataque; quien va a hacer la víctima, donde y como lo va a realizar, que tipo de herramienta tecnológica va a usar, que beneficio podrá obtener, entre otros. Es una etapa común para todos los tipos de phishing.

Preparación. – los ciberdelincuentes a su manera muy lógica deben conseguir los datos de la víctima, el destino del ataque, el software que van a utilizar, los equipos, diseñar y construir desde cero la página web para producir el fraude, se toma en cuenta las necesidades de cada tipo de ataque. Además, en algunas ocasiones estos ciberdelincuentes realizan ataques muy específicos a personas u organizaciones muy concretas, es por ello que los correos electrónicos son más elaborados.

Ataque. – aquí se involucran los usuarios, depende de su participación que puede ser media o alta, es decir, mientras ellos abran el correo electrónico, visiten la página web o realicen la búsqueda el ataque llega a consumirse.

Recolección de datos. – en esta fase hay que esperar a que la víctima ingrese sus datos personales para así poder obtenerlos.

Ejecución del fraude. – cuando se hayan obtenido los datos que se esperaba, el

ciberdelincuente los utiliza para obtener un beneficio propio o para terceros, así mismo, puede vender esta información a personas que les interese para que estas ejecuten el delito.

Post-ataque. – el phisher elimina todo rastro que pudiera dejar luego de realizar este delito, de tal sentido que todas las personas que están implicadas en el ataque pueden ser susceptibles de formar parte del acto. (El Phishing, 2015, págs. 15-18)

4.5.5 Impacto del Phishing

Si este tipo de delito informático no tuviera ningún impacto sería innecesario utilizarlo para conseguir algún beneficio. Por ende, se ha evidenciado los grandes impactos sociales y económicos que se han presentado.

4.5.5.1 Impacto Social

El phishing perjudica especialmente la confianza de los usuarios al realizar operaciones por medio del internet, pero ante, al ejecutar transferencias, transacciones bancarias o patrimoniales. Este es un fenómeno que crece desmesuradamente al igual que la tecnología, por ello es que los usuarios de las herramientas tecnológicas ya no efectúan operaciones como lo solían hacer.

Además, tienen miedo en convertirse en víctimas de estafa por este delito, especialmente en las plataformas que son de venta y compra online, muchos usuarios se sientes más seguros y tranquilos en las páginas web que ya son de su conocimiento. Así pues, se han realizado varios estudios para verificar en que afecta principalmente este delito, y una de la cuestión que tiene mayor intensidad, es que violan el derecho de intimidad de la persona.

Por otra parte, existe una gran desconfianza de las personas al creer que una empresa puede ser suplantada, pero en la actualidad esto ya es real; la perdida de seguridad que esto presenta causa grandes perjuicios para la imagen de la empresa y por tal modo, los usuarios se retiraran constantemente.

4.5.5.2 Impacto Económico

Muchas empresas como particulares han sido víctimas del phishing a través del correo electrónico, lo que provoca pérdida de información personal, ya que extraen credenciales y contraseñas.

Durante años en países como España, Estados Unidos, Argentina y Ecuador, se han ido incrementando los ataques a servicios financieros, echando mano al dinero y negocios de personas, por ello, las pérdidas económicas que presentan producidas por esto son mayor que por cualquier otro tipo de delito.

Es así, que se ve la necesidad de tener un sistema anti-phishing adecuado para prevenir estos ataques, ya que una responsabilidad muy grande que tienen las empresas o entidades bancarias es garantizar la seguridad, tanto de sus empleados como clientes, a fin de evitar la pérdida de información y datos personales.

4.5.6 ¿Como Protegerse de Estos Ataques?

Es evidente que hoy en día los delitos informáticos tienen más concurrencia. Como lo mencioné anteriormente, el delito informático de phishing es una técnica que consiste en robar la información confidencial del usuario utilizando las herramientas tecnológicas por medio de un correo electrónico engañoso, por llamadas o mensajes a través de un celular, haciéndole creer que está en un sitio confiable. Es importante destacar que las entidades y organismos financieros no solicitan esta clase de información utilizando estos medios.

Muchas personas se ven afectadas por esta clase de delito, una razón es por la crisis económica que por desgracia está azotando a varios países, es decir, estos correos son masivos y tienen como gancho la promesa para obtener un gran empleo o una vía sencilla para conseguir dinero.

Ahora bien, a continuación, se presentan algunas consejos o recomendaciones para prevenir el ataque del delito informático de phishing.

Aprender a identificar los correos electrónicos que son sospechosos, ya que utilizan nombres y adoptan una imagen de ser reales; tienen como remitente el nombre de alguna empresa verdadera o el nombre de un usuario de esta; ofrecen regalos o dan como perdida la cuenta para que ingresen sus nuevos datos. Además, es necesario que se identifique la fuente de información de los correos electrónicos que se encuentren en la bandeja de entrada.

Nunca se debe entrar a la página web de un banco pulsando en los enlaces que existan en los correos electrónicos, ya que de forma fraudulenta u oculta pueden dirigir a otro lado perjudicial.

Las herramientas tecnológicas que se utilice deben tener de manera indispensable un buen antivirus para que bloquee este tipo de ataque, siempre hay que tener actualizado el sistema operativo de las mismas.

Esta clase de delito no siempre va a ser en el idioma natal del usuario, sino puede llegar en cualquier idioma para engañar y obtener lo deseado.

Si una persona o usuario abrió este tipo de página y cree ser víctima del phishing, es fundamental que cambie los datos personales con la mayor brevedad posible.

4.6 Normas Jurídicas del Ecuador

4.6.1 La Constitución del Ecuador

Art. 1.- El Ecuador es un estado social de derecho, soberano, unitario, independiente, democrático, pluricultural y multiétnico. Su gobierno es republicano, presidencial, electivo, representativo, responsable, alternativo, participativo y de administración descentralizada. (Constitución de la República del Ecuador, 2008)

Se menciona que nuestra constitución es la fuente y órgano principal del derecho constitucional, porque es quien regula toda figura de organización y funcionamiento del poder que tiene el Estado; de igual forma, dentro de esta, se reconocen todos los derechos fundamentales de los ciudadanos y garantías constitucionales.

En la sección tercera, se manifiesta sobre la comunicación e información, a continuación:

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación. (Constitución de la República del Ecuador, 2008)

Dando coherencia al Art. 16, se destaca que todos los ciudadanos tienen el mismo derecho a tener un acceso a la información libre y voluntaria, comunicación participativa, al espacio para que puedan crear medios de comunicación dentro de los diferentes ámbitos que existen como la radio, la televisión, periódicos, entre otros; todo ello para que las personas se integren en el campo de la comunicación y todos se puedan relacionar, dando sus opiniones y criterios desde su perspectiva.

Art. 17.- El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto:

1. Garantizará la asignación, a través de métodos transparentes y en igualdad de condiciones, de las frecuencias del espectro radioeléctrico, para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelará que en su utilización prevalezca el interés colectivo.

2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.

3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias. (Constitución de la República del Ecuador, 2008)

Conforme a lo indicado en el Art. 17 el Estado es quien impulsará de manera respetuosa para que exista la pluralidad y la diversidad dentro de la comunicación, de tal forma que garantiza el uso del acceso a bandas libres de los distintes medios de información, especialmente con las personas que carecen de tener el posible acceso a estos medios o que incluso los tengas de forman limitada, así mismo, no se permite que exista una o varias personas que dominen los medios de comunicación sino que es para todos.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadasque manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información. (Constitución de la República del Ecuador, 2008)

En el Art. 18 se hace mención que los ciudadanos del Ecuador tienen derecho ya sea solos o en grupo a acceder, buscar, dar, intercambiar, toda la información que ellos deseen siempre ycuando se de manera decente, responsable y que dicha información sea verdadera, eficiente, contextualizada y sin censura. En los casos especiales de violación de derechos humanos nadie dentro de las instituciones públicas podrá negar la información.

Art. 19.- La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente. Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos. (Constitución de la República del Ecuador, 2008)

Mediante lo tipificado en el Art. 19 se priorizará la aplicación necesaria de todo el contenido que sea informativo, educativo y cultural en los medios de comunicación del país para que existan espacios donde se pueda difundir la información sin discriminar a nadie, sin violentar a nadie ni a nadie, es decir, evitar todo lo negativo que atente contra los derechos de las personas.

En el Título VII nos menciona acerca del Buen Vivir, se divide en secciones, principalmente en la sección octava se ha tipificado la Ciencia, tecnología, innovación y saberes ancestrales, a continuación:

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá

como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir. (Constitución de la República del Ecuador, 2008)

En el Art. 385, se determina que gracias al sistema de ciencia, tecnología, innovación y saberes ancestrales que existe en nuestro país, se consigue que las personas se adapten, difundan, fortalezcan, promuevan todos los conocimientos acerca de saberes ancestrales, científicos y tecnológicos para que la calidad de vida mejore siempre que se dé el respeto al medio ambiente, las etnias, entre otros.

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumak kawsay.

3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales. 5. Reconocer la condición de investigador de acuerdo con la Ley. (Constitución de la República del Ecuador, 2008)

En congruencia a lo indicado en el Art. 387 se manifiesta que el Estado es quien tiene la responsabilidad de garantizar que exista la libertad de creación en todos los ámbitos que existen, así mismo, es quien asegura que se dé el acceso y difusión de todos los trabajos

científicos que se realicen siempre que estén establecidos en la ley y como lo manifesté en páginas anteriores, impulsa a los ciudadanos para que contribuyan en realizar todo lo bueno para que se dé cumplimiento al buen vivir.

4.6.2 Legislación en Ecuador

En nuestra Legislación, la información es considerada un bien jurídico que se debe proteger, es por lo que se mantienen leyes y decretos en donde se establecen apartados y especificaciones que van acorde a con la importancia de las herramientas tecnológicas, así como:

4.6.2.1 Ley Orgánica de Transparencia y Acceso a la Información Pública.

En esta ley se tipifica que todas las instituciones del ámbito público deben poner a disposición de todos los ciudadanos el libre acceso a la información institucional refiriéndose todo lo que ellos pidan o necesitan en ese momento. Lo realizan por medio de sus páginas web y bajo este mismo entorno las 70 disposiciones que están dentro de la Constitución Política del Ecuador, misma que se encuentra vigente en el capítulo tercero de las Garantías Jurisdiccionales de las secciones cuarta y quinta de los Arts. 91 y 92 que nos hablan sobre el acceso a la información pública y acción de Habeas Data en las cuales también se encuentra tipificado dichas garantías.

Realizando una investigación previa, se concluye que todos los ministerios de Ecuador no cumplen con el 100% que dispone la Ley Orgánica de Transparencia y Acceso a la Información, sino que simplemente dan cumplimiento al 49% de las mismas.

En el año 2008 el día 27 de octubre se puede observar un informe que se publicómediante el medio de información Diario El Telégrafo, en el cual, La Defensoría del Pueblo dio revelación a algunos datos que tienen relación con el monitoreo de la Ley:

1. De 380 instituciones públicas, 291 cumplen publicando su información de acuerdo con lo dispuesto en la Ley.
2. A 89 instituciones se les notificó para que cumplan con la Ley.
3. 72 instituciones solicitaron una prórroga para completar y cumplir con las disposiciones de la Ley.

4. 70 instituciones cumplieron luego de haber recibido la notificación.

5. 17 instituciones no remitieron ninguna respuesta acerca de la notificación.

6. 12 instituciones respondieron la notificación indicando que las páginas se encuentran en fase de construcción.

7. Por último 7 instituciones no cumplen con las disposiciones de la Ley.

De este mismo informe podemos rescatar el caso que existió en la Provincia del Guayas, donde la Defensoría del Pueblo asignó un convenio con la Participación Ciudadana, en la que se espera promover el cumplimiento de lo establecido en la Ley.

4.6.2.2 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (Reglamento Hábeas Data).

Esta Ley fue publicada en el año de 1997 mediante el Registro Oficial N° 99, misma que fue calificada con gran jerarquía, convirtiéndole a considerarse Ley Orgánica, y con el pasar del tiempo en el año 2001 fue dada por resolución Legislativa.

La Ley Orgánica de Control Constitucional en su Capítulo VI nos da mención a todo lo relacionado con Hábeas Data:

Art. 49.- Objeto. - La acción de hábeas data tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos.

El titular de los datos podrá solicitar al responsable del archivo o banco de datos, el acceso sin costo a la información antes referida, así como la actualización de los datos, su rectificación, eliminación o anulación. No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos. Las personas responsables de los bancos o archivos de datos personales únicamente podrán difundir la información archivada con autorización del titular o de la ley. Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de

conformidad con la Constitución. (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009, pág. 17)

Lo tipificado en el Art. 49 señala que todas las personas tienen derecho a acceder a la información que se encuentre en manos de entidades públicas, de personas naturales o jurídicas, ya sea en soporte tecnológico o físico. Además, los ciudadanos tienen el derecho de saber el uso que se le dará a dicha información y siempre se la puede utilizar, pero cuando exista autorización del titular o lo manifieste la ley. Es por lo que toda persona por sus propios derechos o como representante legitimado para el efecto, podrá interponer una acción de hábeas data.

De igual manera en la Constitución del Ecuador año 2008 nos presenta en su capítulo tercero las Garantías Jurisdiccionales, en el Art. 92 sobre la acción de Habeas Data, estableciendo un recurso para la misma.

4.6.2.3 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.

Esta Ley se publicó en el Registro Oficial N° 320 del 19 de mayo de 1998, siendo utilizada para brindar por parte del Estado una conveniente protección de todos los derechos intelectuales para hacerse cargo de la defensa de estos, ya que sirven, como un componente fundamental para el desarrollo económico y tecnológico del país.

El Instituto Ecuatoriano de Propiedad Intelectual es el encargado para que difunda y de una correcta aplicación de esta ley, su sede se encuentra en la ciudad de Quito, pero de igual forma, cuenta con oficinas en la ciudad de Guayaquil y Cuenca. Se la considera una persona jurídica con un derecho público, misma que cuenta con patrimonio individual, y con una gran autonomía.

Es de vital importancia la Propiedad Intelectual que existe en nuestro país porque se debe dar una correcta aplicación en los sectores industriales, económicos, intelectuales y sobre todo el de investigación, ya que considero que todas las personas que trabajan en estos ámbitos y las de entidades públicas y privadas deben informar a la ciudadanía el gran significado que tiene esta ley.

Hoy en día esta ramificación del derecho es considerada moderno, ya que uno de los principales problemas a los que se enfrenta es la piratería y falsificación de las obras de la

inteligencia humana; por ello, se dan muchas consecuencias sociales y económicas. Además, esto no afecta solo a estas personas, sino que se produce un acortamiento de ingresos tributarios, incluso la pérdida de empleos, producto de la mano de obra clandestina.

De igual forma se debe distinguir la codificación que existe en esta ley, que se trata de la protección que tienen las bases de datos ya sean impresos o que estén dentro de las herramientas tecnológicas.

El estudio de piratería mundial de software 19, que corresponde al año 2007, realizado por la International Data Corporation (IDC), publicado por la Business Software Alliance, establece que Ecuador mantiene una tasa de piratería de un 66%, que constituyen pérdidas por aproximadamente 33 millones de dólares y representan un incremento del 10% con respecto a la última medición (30 millones de dólares).

4.6.2.4 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Esta ley fue publicada en el Registro Oficial N° 557 del 17 de abril del 2002, mediante esta se dispone que los mensajes de datos tienen el mismo valor jurídico al igual que los documentos escritos.

La interpretación de la ley y el ejercicio de la propiedad intelectual rigen por medio de la legislación ecuatoriana y por los tratados internacionales que también forman parte de esta. También, existe la confidencialidad de estos mensajes en las diferentes maneras que existen.

Contiene todos los principios jurídicos que van a regir las transmisiones de los mensajes de los datos, es por lo que la firma electrónica tiene la validez siempre y cuando conste como un requisito de legalidad documental. De igual forma, se cuida la base de datos, porque el titular es quien debe autorizar si se puede disponer de su información o no.

Se indaga que los negocios que se relacionen con el comercio electrónico deben tener todas las notificaciones de manera obligatoria sean por medio del correo electrónico, ya que el documento electrónico puede y será considerado como un medio de prueba con todos los efectos legales, pero debe cumplir con el principio de integridad e identidad.

Según lo dispuesto en esta Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos y el Reglamento que se expidió por el Presidente de la República, Rafael Correa, mediante dos Decretos Ejecutivos se establece que el organismo autorizado para facultar a las

entidades de certificación de información y servicios relacionados es el Consejo Nacional de Telecomunicaciones; dichas entidades son las encargadas de la gestión, administración, generación, cuidado de las claves y los certificados de firma electrónica, además pueden validar la identidad o información de los usuarios que desean obtener su firma electrónica.

El Consejo Nacional de Telecomunicaciones dio autorización al Banco Central del Ecuador para que sea una Entidad de Certificación, para que emita certificados a cualquier persona ya sea natural, jurídica, o funcionarios públicos.

4.6.2.5 Ley Orgánica de Telecomunicaciones.

Dicha Ley se la publico en el Registro Oficial N° 996 del 10 de agosto de 1992, siendo su función principal, que es atribución del Estado regular, controlar, poner en marcha todas las actividades de telecomunicaciones, de igual forma, vigilará y contratará los servicios de estas telecomunicaciones para el país.

Art. 1.- Objeto. - Esta Ley tiene por objeto desarrollar, el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos. (Ley Orgánica de Telecomunicaciones, 2015)

En referencia al Art. 1, se nos presenta el objeto que tiene esta ley para que exista una inigualable comunicación dentro del entorno territorial para con todos los ciudadanos.

4.7 Tratados Internacionales

En el ámbito internacional tenemos el primer tratado internacional que buscó afrontar a aquellos delitos informáticos y las infracciones que se cometen por medio de internet, es El Convenio sobre la Cibercriminalidad, conocido especialmente como el Convenio de Budapest, mediante el cual se pretende la armonización de las leyes nacionales para que mejoren todas las técnicas de investigación y que exista una perfecta cooperación entre las naciones.

Podemos encontrar en este Convenio en su Capitulo II todos los tipos penales que pueden ser aplicados a nivel nacional, a todos los delitos que se relacionan con la confidencialidad de los sistemas o redes informáticas, la alteración de datos, la integridad y la disposición de todos

los datos por medio de sistemas informáticos. Además, el propósito de este Convenio es que la seguridad de la información sea protegida y confiable, para que se priorice una política penal común con el objetivo de salvaguardar a los ciudadanos frente a este tipo de delitos e infracciones, se motiva a que las naciones adopten un modelo de legislación adecuada.

La Organización de Estados Americanos (OEA) manifiesta que durante los últimos años con la ciberdelincuencia las amenazas y maneras de cometer todos los delitos informáticos se van haciendo más peligrosas para las herramientas tecnológicas, para la integridad de los usuarios y para los mensajes de datos; es por ello, que mediante el Comité Interamericano contra el Terrorismo (CICTE) y el Programa de Seguridad Cibernética se han dispuesto a contrarrestar el crimen cibernético, una agenda que sea empleada para la seguridad cibernética en América.

La OEA refuerza las acciones que se relacionan con estos delitos, impulsando las actividades de seguridad cibernética a través de ejercicios, mesas redondas, intercambio de prácticas para el uso de los medios tecnológicos, asistencia técnica, entre otros.

4.8 Derecho Comparado

Todos los ciudadanos tenemos una serie de derecho y deberes, por eso se da paso a los fundamentos de Derecho porque es necesario que se dé una construcción de normas de forma obligatoria ya que son el sustento jurídico de este proyecto, de igual forma son el acceso que tenemos para las Tecnologías de la Información y Comunicación.

Desde hace muchos años las Naciones Unidas por medio de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional han incentivado a las legislaciones de todo el mundo para que inserten en sus leyes modelos sobre el Comercio Electrónico y sobre las Firmas Electrónicas.

Por otro lado, en Sudamérica, Colombia fue el primer país que se inquietó por este tema de delitos informáticos, por ende, en el año 2009 se promulgó la “Ley de Delitos Informáticos”; es ahí donde impulsa a que más países incluyan esta ley en sus diferentes legislaciones, siguiendo Perú, Argentina, Venezuela, Chile y Ecuador.

4.8.1 Delitos Informáticos y Legislación en Colombia

En el año 1989 Colombia empezó a legislar distintos temas relacionados con los delitos cibernéticos mediante el decreto 1360 publicado en el Diario Oficial de la República de Colombia, esto sirvió de fundamento normativo para proteger la violación de algunos derechos. Es entonces, que en el año 2009 se promulga la "Ley de Delitos Informáticos", por ende, se modifica el Código Penal Colombiano del año 2000.

Se adicionó el Titulo VII BIS que se denomina "De la protección de la información y de los datos", siendo los tipos de delitos informáticos tipificados, los siguientes:

Art. 269A.- Acceso abusivo a un sistema informático. – El que acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, 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. (De la Protección de la información y de los datos, 2009)

El artículo anterior hace mención que es un delito en el que una persona accede ilegalmente a un sistema informático ya sea que este protegido o no por medidas de seguridad, o se mantiene dentro de él en contra de la voluntad de la persona con derecho legítimo a eliminarlo, dicha conducta es castigada con una pena de prisión de 48 a 96 meses y con una multa correspondiente.

Art. 269B.- Obstaculización ilegitima de sistema informático o red de telecomunicación. - El que impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, 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 una pena mayor. (De la Protección de la información y de los datos, 2009)

Se hace mención en el artículo descrito anteriormente que es un delito en el que un individuo impide el funcionamiento normal de un sistema informático, de los datos contenidos dentro de este o de una red de telecomunicaciones; esta conducta es castigada con una pena privativa de libertad con su respectiva multa, siempre y cuando no constituya un delito con una pena mayor.

Art. 269C.- Interceptación de datos informáticos. – El que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. (De la Protección de la información y de los datos, 2009).

Se nos manifiesta en el articulado anterior que la persona o personas que accedan e intercepten sin autorización previa a los datos informáticos sean de poco o gran interés y que estén siendo redireccionados a otro destino si el infractor por propias razones evita o lo envía a otro lugar, tendrá su respectiva sanción.

Art. 269D.- Daño informático. – El que destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, 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. (De la Protección de la información y de los datos, 2009)

En el artículo anterior se nos manifiesta que un individuo que realice un daño informático deformando todo o en partes a los datos de una persona o empresa sin autorización de estos y lo realice de una manera grave, será condenado con una pena privativa de libertad y de igual forma pagará su respectiva multa.

Art. 269E.- Uso de software malicioso. – El que produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, 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. (De la Protección de la información y de los datos, 2009)

Se nos hace mención que el sujeto que robe datos confidenciales de cualquier computadora, y asuma el control de todos los sistemas informáticos como las redes, tabletas y dispositivos móviles que perjudique parcial o gravemente al propietario, será privado de su libertad y sancionado con una multa que de alguna forma pueda reparar lo que hizo.

Art. 269F.- Violación de datos personales. – El que con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o 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. (De la Protección de la información y de los datos, 2009)

Del artículo descrito anteriormente podemos extraer que la violación de datos personales se produce cuando una persona desea obtener beneficio propio para si o para terceros, es decir, los datos del propietario sufren un incidente de seguridad, dando origen a la violación de confidencialidad, poniendo en riesgo los derechos y libertades de este, deberá notificar y el infractor será privado de la libertad, pagando la multa correspondiente.

Art. 269G.- Suplantación de sitios web para capturar datos personales. – El que con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o 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. 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. (De la Protección de la información y de los datos, 2009)

Se entiende del artículo anterior que el ciberdelincuente que ejecute un fraude para obtener información de la base de datos de cualquier empresa pública o privada, o también suplante el sitio web de la entidad bancaria cambiando la dirección IP para generar un engaño a los consumidores financieros que utilizan las aplicaciones virtuales, tendrán una pena privativa de libertad, y así mismo se les acarreara una multa correspondiente para dicho delito.

4.8.2 Delitos Informáticos y Legislación en Chile

Se da por primera vez la tipificación de los delitos informáticos el 7 de junio de 1993 con la Ley N° 19.223 publicada en el Boletín Oficial Chileno, señalando que si se da la destrucción o inutilización de un sistema de tratamiento de información será castigado.

Actualmente, el 20 de junio de 2022 se publicó la Ley N° 21.459 sobre delitos informáticos teniendo un gran significado para la legislación chilena, en la cual aborda temas que no habían sido considerados en la ley anterior (derogada).

En esta normativa se mencionan algunas definiciones acerca de “datos informáticos”, “sistema informático”, “prestador de servicios” e incorpora algunos ilícitos informáticos que no eran contemplados hasta ahora. Entre ellos, tenemos:

Art. 1.- Ataque a la integridad de un sistema informático. – El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo. (De los delitos informáticos y sus sanciones, 2022)

Del articulado anterior se puede extraer que los ataques a la integridad de un sistema informático consisten en que la persona modifique o impida el funcionamiento de un sistema informático sin autorización alguna del propietario y será sancionado con una pena privativa de libertad.

Art. 2.- Acceso ilícito. – El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo. (De los delitos informáticos y sus sanciones, 2022)

En el artículo anterior se menciona que el sujeto que acceda con o sin autorización a los datos informáticos y se exceda en la vulneración de estos, como, por ejemplo, se apodere de la información, la extraiga para venderla y obtener un beneficio lucrativo o que la divulgue y transfiera a otra persona será castigada con pena privativa de libertad de menor grado a medio o máximo

Art. 3.- Interceptación ilícita. – El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio. El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en

sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo. (De los delitos informáticos y sus sanciones, 2022)

El presente artículo nos menciona que la interceptación ilícita es una infracción en el que la persona interfiere la transmisión no pública de información en un sistema informático o de varios sistemas sin tener una autorización previa para poder hacerlo, lo cual será castigado con una pena de presidio menor en su grado medio; por otro lado, si una persona capta datos en sistemas informáticos sin tener así mismo la autorización también será considerada un delito y será castigada con una pena de presidio menor en sus grados medio y máximo.

Art. 4.- Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos. (De los delitos informáticos y sus sanciones, 2022)

Se entiende del artículo anterior que un ataque a la integridad de los datos informáticos es un delito en el que una persona o individuo injustamente altera, elimina o daña datos informáticos provocando un gran daño al titular de estos, por ende, será castigado con una respectiva pena privativa de libertad.

Art. 5.- Falsificación informática. – El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo. Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo. (De los delitos informáticos y sus sanciones, 2022)

Se puede entender que la falsificación informática es un delito en el que una persona sustrae o elimina datos informáticos con la gran intención de que se hagan pasar por auténticos o utilizarlos para poder falsificar lo que quieran y obtener un beneficio. Esta conducta es castigada con una pena de presidio menor en sus grados medio a máximo; si la falsificación es ocasionada por un empleado público que ha abusado de su cargo, la pena que recibirá será más severa.

Art. 6. Receptación de datos informáticos. – El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado. (De los delitos informáticos y sus sanciones, 2022)

El artículo anterior nos menciona que la receptación de datos informáticos en un delito en donde un sujeto comercializa pierde o almacena datos informáticos de origen ilícito, ya sea conociendo o no su origen ilegal, con un objeto o fin ilícito. Esta conducta debe ser castigada con la pena destacada a los delitos correspondientes descritos en los artículos 2, 3 y 5, pero conla diferencia que es con una rebaja en un grado.

Art. 7.- Fraude informático. – El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado: 1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales. 2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales. 3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales. Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

El presente artículo nos hace referencia a que el fraude informático es una acción que consiste en manipular un sistema informático con la intención de causar daño a alguien y así lograr un beneficio económico, dicha acción puede realizarse a través de la introducción, daño o eliminación de datos informáticos o cualquier otra interferencia en el funcionamiento de un sistema informático; la persona que cometa dicha acción será penalizada.

5. Metodología

Con la finalidad de realizar la investigación de forma eficiente, se procederá a aplicar los siguientes métodos:

5.1 Métodos

5.1.1 Método Científico

En mi presente trabajo de investigación se me permitió utilizar este método que me sirvió como instrumento más idóneo, por lo que fue aplicado al razonar desde una perspectiva lógica y científica para dar algunas posibles soluciones al problema planteado, y poder verificar si es necesario que se tipifique el delito de phishing en nuestro Código Orgánico Integral Penal.

5.1.2 Método Deductivo

Este método me dio la posibilidad de realizar un análisis partiendo desde el tema planteado, se lo descompuso en diferentes categorías principales para desarrollarlas una por una dentro de la investigación, hasta que se llegó a concluir en la situación específica del tema. Fue de utilidad para lograr deducir que camino se puede tomar para dar una solución en general para el problema.

5.1.3 Método Analítico

Este método igual al anterior me permitió descomponer temas generales en distintas partes o fragmentos que están dentro de este trabajo investigativo, los cuales están propuestos de forma separada para identificar las causas, los efectos de estos temas; de igual forma para establecer analogías o teorías nuevas para lograr entender al cien por ciento el objeto de estudio y obtener el fin que se quiere.

5.1.4 Método Comparativo

Dicho método me permitió distinguir las diferentes realidades jurídicas que existen hoy en día por medio del Derecho Comparado, me dio la posibilidad de realizar un estudio a diferentes legislaciones de España, Colombia, Chile, que tipifican y sancionan diferentes tipos de delitos informáticos.

5.1.5 Método Estadístico

Consiste en aplicar la estadística para la contabilización de información numérica, por lo que se empleará en el conteo de los datos obtenidos al aplicar la encuesta, mismos que serán tabulados y procesados con la estadística descriptiva para su mejor interpretación.

5.2 Técnicas

5.2.1 La Encuesta

Esta técnica fue de gran ayuda para poder realizar la investigación de campo y obtener la información subjetiva sobre el tema de este trabajo investigativo, la cual fue aplicada de forma directa a cuarenta profesionales de diferentes ámbitos, situados en la ciudad de Loja, mediante un cuestionario de seis preguntas, todas relacionadas con el tema de esta investigación.

La información que se recolectó fue de ayuda en la contribución de reunir datos y saber que conocimiento tiene el encuestado acerca de la problemática planteada; así mismo, la necesidad que existe de tipificar y sancionar al delito informático de phishing como una nueva modalidad de estafa con sus propias características.

5.2.2 La Entrevista

La entrevista al igual que la técnica anterior mencionada, constó en la elaboración de tres preguntas todas muy puntuales referentes al tema investigativo, la misma fue aplicada personalmente mediante un dialogo con el entrevistado; la realice a distintos profesionales especializados dentro del ámbito jurídico situados en la ciudad de Loja.

Todas las respuestas con los grandes criterios y sugerencias de estos profesionales fueron de vital importancia dentro de la trascendencia jurídica y social del tema planteado para lograr obtener una solución a este problema planteado.

6. Resultados

6.1 Resultados de las Encuestas

Para obtener los resultados de este trabajo investigativo se aplicó una encuesta, la cual fue aplicada de forma directa a sesenta profesionales del Derecho situados en la ciudad de Loja, mediante un cuestionario de seis preguntas, todas relacionadas con el tema, obteniendo los siguientes resultados:

Pregunta #1

¿Conoce usted lo que es el delito informático de phishing?

Indicadores	Variables	Porcentaje
SI	32	54%
NO	28	46%

Tabla 1. Conocimiento del delito informático de phishing
Fuente: Encuestasrealizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

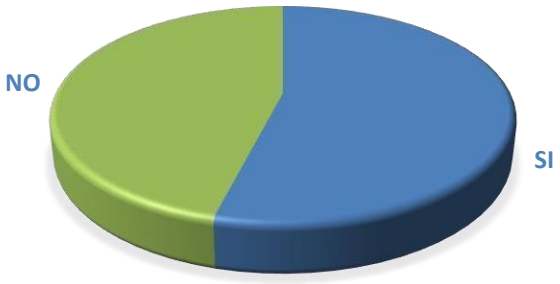


Figura 1. Conocimiento del delito informático del phishing
Fuente: Encuestasrealizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

Interpretación:

Como se observa los datos de la tabla n°1, gráfica n°1, la población se despliega de sesenta profesionales del Derecho encuestados, en donde, 32 profesionales que representan el 54% respondieron que SI conocen lo que es el delito informático de phishing. Por otro lado, 28 profesionales que representan el 46% respondieron que NO conocen el delito informático de phishing.

Análisis:

Por las respuestas que se obtuvo en el primer interrogante de esta encuesta se deduce que casi la mitad de los profesionales del derecho si tienen conocimiento de lo que es el delito informático de phishing, mientras que los demás no, es por ello, que esta propuesta es viable para que se tipifique en nuestro Código Orgánico Integral Penal el delito informático de phishing como una nueva modalidad de estafa.

Pregunta #2

¿Ha sido usted víctima de alguna situación en la cual le hayan enviado un correo electrónico y se hayan apropiado de sus datos personales, claves o contraseñas de forma

ilícita para acceder a diferentes sistemas informáticos, haciéndose pasar por personas de confianza para obtener beneficio propio o para terceros?

Indicadores	Variables	Porcentaje
SI	10	17%
NO	50	83%

Tabla 2. ¿Ha sido víctima del phishing?
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

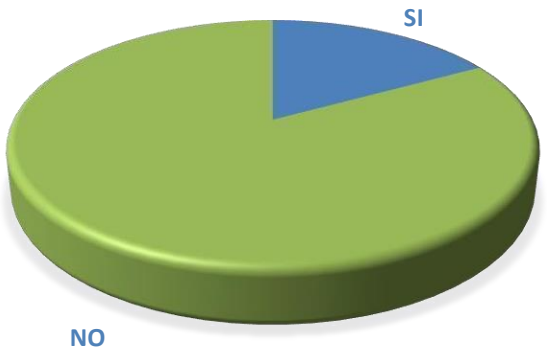


Figura 2. ¿Ha sido víctima del phishing?
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

Interpretación:

En cuanto a esta interrogante se puede observar en la tabla n°2, gráfica n°2, 10 profesionales del derecho que representan el 17% de los encuestados SI han sido víctimas de que se hayan apropiado sus datos personales, claves o contraseñas de forma ilícita a través de un correo electrónico; mientras que demás 50 profesionales que representan el 83% de los encuestados NO han sido víctimas de que se hayan apropiado sus datos personales, claves o contraseñas de forma ilícita a través de un correo electrónico.

Análisis:

Por las respuestas obtenidas en esta segunda interrogante de la encuesta es sencillo deducir que la mayoría de los profesionales que dieron respuesta no han sido víctimas del delito informático de phishing, puesto que algunos de ellos han tenido un conocimiento previo acerca del mismo ya sea por investigaciones que han realizado o por la pluralidad de casos que se denuncian día tras día en las diferentes fiscalías de nuestro país, otros son muy

precavidos al abrir este tipo de correos ya que no confían plenamente en ellos y tienen miedo a ser víctimas de los ciberdelincuentes. En cambio, muy pocos de los profesionales encuestados si han sido perjudicados en situaciones en las cuales les han enviado un correo electrónico y se han apropiado de forma ilícita de sus datos personales tanto como contraseñas de alguna red social, cuenta bancaria o el número de tarjetas de crédito, por esta razón han tenido que crear nuevas cuentas dentro de las redes sociales y en empresas bancarias; o tan solo algunos de ellos han cambiado sus contraseñas y ahora tienen más precaución para no volver a servíctimas del phishing.

Pregunta #3

¿Conoce usted si alguna o algunas otras personas hayan sido víctimas de este tipo de delito informático de phishing?

Indicadores	Variables	Porcentaje
SI	38	64%
NO	22	36%

Tabla 3.¿Conocea alguna víctima del phishing?
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

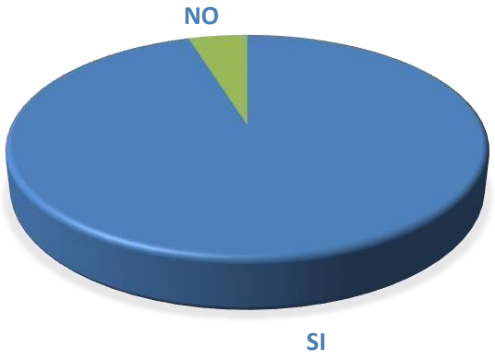


Figura 3.¿Conoce a alguna víctima del phishing?
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

Interpretación:

En los resultados de esta pregunta en la tabla n°3, ilustración n°3, se verifica que: de los sesenta profesionales del Derecho, 38 de ellos que representan el 64% SI conocen a distintas personas que hayan sido víctimas del delito informático de phishing; por otro lado, los 22 restantes que representan el 36% NO conocen a personas que hayan sido víctimas del delito

informático de phishing.

Análisis:

En base a las respuestas de esta pregunta se puede identificar que gran parte de los profesionales del Derecho encuestados efectivamente conocen a varias personas que han sido víctimas del delito informático de phishing, mencionan que algunas de ellas son cercanas a los encuestados las cuales les han manifestado que los ciberdelincuentes han robado sus contraseñas de las redes sociales o en algunos casos las claves y usuarios de las cuentas bancarias porque han creído que el correo electrónico que recibieron era real ya que así lo parecía. Por otro lado, se observó que varias de las respuestas que se obtuvieron no conocen a personas que hayan sido víctimas de este delito puesto que ya tienen una intuición previa de que los correos electrónicos que reciben son falsos; desde otro punto de vista, a pocos individuos les genera desconfianza de los correos que observan en su bandeja de entrada y prefieren no abrirlo.

Pregunta #4

¿Considera usted que debería existir mucha más información por parte de las autoridades para poder prevenir este tipo de delito informático de phishing?

Indicadores	Variables	Porcentaje
SI	59	99%
NO	1	1%

Tabla 4. Prevenir el phishing.
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

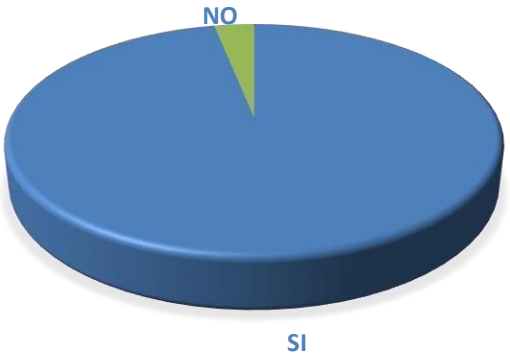


Figura 4. Prevenir el phishing.
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

Interpretación:

Los resultados que se obtuvieron por la investigación de campo que se realizó se muestran en la tabla n°4 e gráfica n°4, los cuales arrojan como evidencia que 59 profesionales del Derecho que representan el 99% SI consideran que debería existir mucha más informaciónpor parte de las autoridades acerca de este delito para poder prevenirlo;1 profesional que representa al 1% considera que NO debería existir más información del delito informático del phishing.

Análisis:

Con las opiniones y resultados que se adquirieron por parte de los profesionales del Derecho que fueron encuestados, se demuestra que es evidente que debe existir más información acerca del delito informático de phishing por parte de las autoridades; se verifica la necesidad que tienen los ciudadanos de tener algún conocimiento o criterio acerca del mismo porque en la actualidad existen muchas denuncias recibidas en las distintas fiscalías del Ecuador en las cuales se demuestran los daños y perjuicios ocasionados en las cuentas, tarjetas bancarias o redes sociales por los ciberdelincuentes, en donde han tenido que de forma urgente eliminar, cerrar, cambiar las claves o contraseñas de las mismas; por ello, las autoridades deben tomar conciencia e informar de los nuevos delitos que día a día van apareciendo por la facilidad y variedad de herramientas tecnológicas que existen para realizarlos. Por el contrario el único encuestado que manifestó que no, fue por la razón que cree que las personas deben tener el interés para informarse de todo lo que se comete en la actualidad; claro que se es consciente que cada uno tiene la obligación de informarse pero hay que tomar en cuenta que la mayor parte de estos individuos no cuentan en algunos casos con los servicios necesarios para observar noticias o averiguar lo que está sucediendo día tras día, es por esta manera que es indispensable que las autoridades de nuestro país realicen campañas educativas, sociales, publicitarias con el fin de dar toda la información posible a los ecuatorianos y que no sean víctimas de esta clase o clases de delitos.

Pregunta #5

¿Considera usted que la falta de tipificación del delito informático de phishing es la causa directa por lo que se sigue produciendo en la actualidad?

Indicadores	Variables	Porcentaje
SI	54	90%
NO	6	10%

Tabla 5. Tipificar y sancionar el delito informático de phishing.
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

Figura 5. *Tipificar y sancionar el delito informático de phishing.*
Fuente: Encuestas realizadas a profesionales del derecho
Autora: Valeria Alejandra Campoverde Salas

Interpretación:

Como se demuestra en los datos de la tabla n°6 e gráfica n°6, de los sesenta profesionales del Derecho encuestados, 54 de ellos dieron como respuesta SI a esta interrogante, es decir, consideran que por la falta de tipificación del delito informático de phishing es la causa directa por lo que se sigue cometiendo este delito con más concurrencia en la actualidad; por otro lado, los 6 profesionales restantes dan como respuesta NO, es decir, ellos no consideran que la falta de tipificación de este delito sea la causa directa para que se siga cometiendo, consideran que existen diferentes causas.

Análisis:

Al ser el phishing un delito informático que produce grandes implicaciones y afectaciones en el patrimonio de las víctimas, concuerdo con las respuestas mayoritarias emitidas por los encuestados, razón por la que se considera importante tipificar este delito en nuestro Código Orgánico Integral Penal para proteger el patrimonio de todos los ciudadanos pues se debe considerar que las posibles víctimas tendrán el conocimiento acerca de esta nueva modalidad de estafa y tendrán mayor cuidado al instante de entrar en los correos electrónicos que

observen de dudosa procedencia, aunque parezcan verdaderos, así los phishers no conseguirán la información personal o reservada de los usuarios; siendo de gran ayuda para dichos usuarios porque tendrán la seguridad que están siendo amparados por una respectiva legislación penal y en los casos que sean víctimas de este delito se procederá a realizar una correspondiente administración de justicia. De esta manera se dará paso para crear una posibilidad de que todos los ecuatorianos que alguna vez han sido víctimas de este delito o lo lleguen a ser puedan recurrir a un sistema penal adecuado para que el derecho que ha sido vulnerado sea restituido y el ciberdelincuente considerado como el sujeto activo reciba la sanción que le corresponde.

Desde mi perspectiva no comparto la postura de los profesionales que expresaron su respuesta de forma negativa porque es evidente que la causa directa por la que se sigue produciendo este tipo de delito informático es la falta de tipificar y sancionar de la manera correcta este delito, ya que dentro del Derecho Penal se establece que la norma será interpretada en forma literal a lo que estipule, tampoco se debe adecuarlo o modificarlo a otro tipo penal ya que cada tipo emplea un verbo rector característico y especial.

6.2 Resultados de las Entrevistas

Con el fin de comprobar la realidad socio-jurídica que se presenta por la problemática que se planteó dentro de este trabajo investigativo y para obtener diferentes criterios que permitan comprobar los objetivos descritos inicialmente, se aplicó una entrevista siguiendo los lineamientos metodológicos de la investigación de campo, en la cual se elaboró preguntas de carácter abierto relacionadas al tema, estas interrogantes fueron dirigidas a cinco profesionales del ámbito jurídico, obteniendo los siguientes resultados.

Pregunta #1

El delito informático de phishing producido por los ciberdelincuentes hacia la victima presenta aspectos fundamentales como es el engaño, el daño al bien patrimonial y específicamente a la alteración o modificación de las claves, datos personales o dispositivos de la banca online. Tomando en cuenta esto, ¿Según su criterio profesional, piensa usted que es necesario que al delito informático de phishing se lo considere como una nueva modalidad de estafa y se lo tipifique en nuestro Código Orgánico Integral Penal?

Entrevistado Nro. 1.- La abogada manifiesta en palabras textuales: Según mi opinión considero importante que al delito informático de phishing se lo tipifique e incorpore al Código Orgánico Integral Penal, pues es en la actualidad que a través de las redes sociales es donde más las personas están siendo víctimas de estafas.

Entrevistado Nro. 2.- El abogado manifiesta en palabras textuales: Si es necesario considerarlo al phishing como un delito, ya que muchas de las personas han sido víctimas del mismo, lo que ha afectado tanto a su patrimonio familiar como a sus finanzas, por lo que muchas de las veces son derechos vulnerados por la falta de conocimiento de cómo se debe manejar este tipo de delitos porque las personas utilizan la plataforma virtual o cualquier otra herramienta tecnológica en la cual este inmerso un bien económico.

Entrevistado Nro. 3.- La abogada manifiesta en palabras textuales: Primeramente hay que identificar que este es un tipo de delito informático o estafa informática que se da a través de los medios digitales pero no es el único, es decir, existen varias modalidades de diferentes tipos de delitos relacionados con estas estafas por vía web o virtual; evidente es necesario que sea incorporado en el Código Orgánico Integral Penal porque en el momento que se desarrolló la normativa como tal no se tenía en consideración este tipo de delitos informáticos, si bien algo se habla dentro del COIP sobre este tema no se legisla de una manera adecuada ni se regula cada uno de estos delitos en específico, entonces obviamente es necesario que se incluya este tipo de delito para singularizar los casos y poder diferenciarlos de los distintos delitos informáticos, para no incluir o abarcar a todos como si fueran lo mismo en un solo delito, no se debe considerar como una generalidad cuando cada uno de estos delitos son distintos.

Entrevistado Nro. 4.- Hoy en día las estafas que se dan por medio de las herramientas tecnológicas son más comunes por la confianza que generan a las personas o por la falta de información que tienen, en especial, aquellas que no pueden utilizarlas al cien por ciento. Como profesional en libre ejercicio he tenido varios casos en los que muchos usuarios han sido engañados por la red social más conocida que es Facebook, en esta se ofertan productos que son de agrado para los usuarios y por eso deciden comprar, pero se les pide que paguen antes para realizar la respectiva entrega del producto, pero esta nunca llega. Por ello si creo necesario tipificar al delito de phishing como una nueva modalidad de estafa para poder sancionar a las personas que realizan este hecho delictivo y poder frenar un poco el número de casos.

Entrevistado Nro. 5.- Si se debiese tipificar a este delito como una nueva modalidad de estafa por el incremento de víctimas que está produciendo ya que estos infractores no tienen miedo de realizarlo por el motivo que no existe una adecuada sanción que los castigue de la forma que merecen.

Comentario:

De todas las entrevistas que se realizó a los distintos profesionales del Derecho se puede determinar que es necesario la tipificación del delito informático de phishing en el Código Orgánico Integral Penal ya que se debe tomar en consideración los avances tecnológicos que se presentan en la actualidad, de igual forma considerar las siguientes razones: en realidad muchas personas están siendo víctimas de esta clase de delito por medio de las redes sociales; afecta al patrimonio familiar o individual lo que genera grandes pérdidas económicas; sería de gran ayuda para poder singularizar los distintos casos que se presenten y no incluirlos a todos en un solo tipo penal porque existen diferentes modalidades para dañar o perjudicar a alguien por medio de la informática; para evitar que los ciberdelincuentes sigan realizando esta clase de delitos puesto que si habría una sanción con su respectiva pena privada de libertad tendrían miedo de ser encontrados y ya no los realizarían más.

Además, se toma en cuenta el principio de legalidad considerando que si este tipo de delito informático no se encuentra tipificado en la respectiva norma penal una persona no puede ser responsable del hecho delictivo, es decir, si no se encuentra una sanción correspondiente no se puede sancionar a una persona. Finalmente, la tipificación de este delito se debe tomar en cuenta como carácter urgente dado que los avances tecnológicos crecen a una velocidad increíble y así mismo los casos delictivos; entonces gracias al amparo de la ley se lograría determinar la infracción penal y como se la puede sancionar sin problema alguno.

Pregunta #2

En este tipo de delito informático de phishing se trata con personas muy especialistas, es decir, pueden cometer el delito y eliminar todo dato o huella de lo que han realizado, ¿Cómo cree usted que se podría identificar la identidad de la persona que cometió el delito?

Entrevistado Nro. 1.- Se podría identificar a través de pericias de los IP donde salió la información, solicitar a que personas están asignadas los números de teléfonos por lo que se

comunicó y diferentes mecanismos para determinar quien cometió el hecho delictivo.

Entrevistado Nro. 2.- Este tipo de delitos siempre será cometido por una persona que conoce y sabe de la materia, ya que para eliminar tanto una huella o el dato de la cuenta y poder acceder fácilmente se necesita tener un conocimiento bastante avanzado para obtener lo que ellos requieran, por lo tanto considero que se podría identificar a estas personas por las direcciones IP porque así como existen los especialistas para cometer esta clase de delitos también existe la fiscalía y policía judicial que trabajan en conjunto y a través de sus peritos se podría determinar el lugar exacto donde se emitió el delito, por lo tanto se reconocería a quien perteneció el computador o herramienta tecnológica que se utilizó.

Entrevistado Nro. 3.- Es muy difícil poder identificar a las personas que cometan esta clase de delito del phishing, lo que sí se puede realizar según se ha podido determinar por especialistas peritos que trabajan en investigación de estos delitos es identificar el IP de donde provienen dichas acciones, es decir, la computadora donde se realizaron; ahora bien, no se determina exclusivamente cual fue la persona que lo hizo pero ya nos puede dar un indicio que si es una computadora en específico de determinada persona entonces ya puede ser parte de unproceso investigativo, repito, no es fácil conocer al individuo que comete el delito, lo más próximo para poder investigar responsabilidades es identificar el IP de la computadora donde se realizó este delitos.

Entrevistado Nro. 4.- Como usted lo menciona estos ciberdelincuentes son especialistas, pueden eliminar todo acto delictivo que realizaron para obtener el beneficio esperado; pero, aun así, no se dan cuenta que dentro de nuestro país también existen autoridades especialistas en esta materia que ayudan a identificar a los infractores por medio de la dirección IP que, aunque elimine todo esta sigue siendo visible.

Entrevistado Nro. 5.- Por lo que tengo conocimiento a estos infractores se los puede identificar por medio de la dirección IP que dejan las computadoras, pero esto no siempre va a ser de beneficio para las autoridades ya que muchas de las veces estas computadoras son robadas para cometer la estafa a través de esta y luego desechadas; dejando libre al infractor.

Comentario:

Gracias a todas las respuestas obtenidas por los entrevistados se puede verificar que es un poco difícil encontrar a los infractores que realizan estos engaños o estafas por medio de la

tecnología, ya que se desconoce que herramienta utilizó; es claro que por el IP que dejan las computadoras ayudan a los especialistas peritos de la fiscalía o policía para poder identificarlos, pero en algunos casos estos ordenadores llegan a ser incluso hasta robados para cometer dicho delito. Por lo que día tras día se presentan más casos de personas que han sido víctimas del phishing.

Pregunta #3

Según la fiscalía general de nuestro país los casos respecto a delitos informáticos han ido incrementando desmesuradamente, ¿Cree usted que a estos delitos informáticos no se los puede prevenir por la falta de capacitación o información que tienen las personas tanto naturales como jurídicas?

Entrevistado Nro. 1.- Estos delitos se los puede prevenir haciendo conocer a las personas que si solicitan números de cedulas, claves u otra información que llega a sus correos electrónicos deben eliminarlos y que es importante indicarles que si llegan mensajes de chats desconocidos no deben abrir estos correos y eliminarlos.

Entrevistado Nro. 2.- Efectivamente muchos de estos delitos se han incrementado actualmente ya que muchas de las personas consideran este modo operandi como nuevo, los ciberdelincuentes se encuentran sumamente capacitados para realizar dichas acciones, por lo tanto, considero que debe existir una capacitación mayor por parte de las entidades bancarias ya sea para las personas naturales como jurídicas para que conozcan las distintas consecuencias que se darían por el mal uso o manejo de este tipo de sistemas y así logren obtener la información necesaria principalmente aquellos individuos que no utilizan con frecuencia la tecnología, un ejemplo seria que las personas consideran raro realizar una transacción o transferencia bancaria porque no tienen la confianza o en algunas ocasiones no la reciben.

Entrevistado Nro. 3.- No necesariamente tiene que ver con una falta de capacitación sino con una falta de implementación de medidas de seguridad para prevenir este tipo de delitos, si bien se tiene claro el tema de las capacitaciones o sobre el conocimiento de estas modalidades de estafa que es necesario conocerla; lo más importante para las empresas es que implementen medidas de seguridad mejores, es decir que constantemente mantengan a sus sistemas resguardados con mejor seguridad. Un ejemplo es el hackeo que se realizó al Banco del Pichincha o el hackeo que se hizo a CNT, entonces claro no necesariamente se relaciona

con la falta de capacitación a su personal sino con reforzar las medidas de seguridad en sus sistemas para evitar este tipo de fraudes.

Entrevistado Nro. 4.- Obviamente las autoridades en conjunto con la policía nacional deberían dar más capacitaciones para informar a la ciudadanía de los nuevos delitos que se están presentando en la actualidad, pero de igual forma son los ciudadanos quienes también deben mostrar interés en lo que está sucediendo dentro del país, no limitarse a lo que ya conocen.

Entrevistado Nro. 5.- Si es necesario que se presenten campañas de concientización por parte de las empresas públicas y privadas para que los ciudadanos se informen y no sigan confiando en mensajes o correos electrónicos que les llegan. No solo que la policía haga frecuentemente estas campañas por las redes sociales, dando a conocer las medidas de seguridad que deben ser tomadas en cuenta. Pero aun así es la sociedad quien debería cambiar su propia mentalidad y abrirse a la realidad por la que se está pasando no solo quedarse en el pasado.

Comentario:

Desde otra perspectiva de las diferentes opiniones se logró determinar que debería existir más información del delito informático de phishing, tanto de las entidades bancarias como dela prensa del país, ya sea por medio de noticias, radio, periódicos, entre otros., para que las personas tengan el conocimiento necesario y puedan evitar ser víctimas del mismo; por otra parte, son las empresas o compañías quienes a más de dar capacitaciones a sus empleados deberían de implementar medidas de seguridad a los sistemas que tengan mayor uso dentro de la misma para evitar estas modalidades delictivas.

7. Discusión

7.1 Verificación de los objetivos

Con el único fin de verificar si se dio el respectico cumplimiento de los objetivos planteados dentro de esta investigación, sobre la temática "EL PHISHING COMO MEDIO DE DISPOSICIÓN PATRIMONIAL FRAUDULENTA", por objetivo general se estableció uno que tiene un valor fundamental y dos objetivos específicos con igualdad de importancia.

Es por lo que gracias al estudio teórico-normativo que se realizó y en conjunto con todos

los datos que se adquirieron gracias a la investigación de campo que realicé, he obtenido muy buenos resultados, los cuales exponen la necesidad de tipificar al delito informático de phishing como una nueva modalidad de estafa; es así como, para que se dé una correcta verificación de todo lo comprobado realizo los respectivos análisis y contrastes:

7.1.1 Objetivo General

"Analizar el Phishing en su contexto jurídico y las implicaciones y afectaciones que produce al patrimonio de sus víctimas".

Por medio de revisión de la literatura este objetivo pudo ser verificado, he realizado una recopilación selectiva de fuentes de información para obtener el marco teórico de una forma explícita o entendible, así mismo, pude verificar las normativas vigentes que existen dentro del Ecuador para luego efectuar una comparación con legislaciones penales de otros países, de igual forma con algunos convenios y tratados internacionales que se han ejecutado, con los cuales puedo demostrar de manera especial que el delito informático de phishing no está contemplado en la legislación penal vigente de nuestro país; se concluye que por la carencia de tipificación se permite que se sigan dando actos o situaciones de índole delictivo a través de las herramientas tecnológicas produciendo grandes daños al patrimonio de las víctimas.

Por otro lado, con la investigación de campo realizada, en base a las respuestas que logré obtener por parte de los diferentes profesionales del Derecho tanto en las encuestas como entrevistas se verifica que cuentan con el conocimiento de las consecuencias y afectaciones que el phishing produce, que no existe como tal y de manera autónoma dentro de los diferentes delitos que se encuentran tipificados y sancionados en el Código Orgánico Integral Penal del Ecuador.

7.1.2 Objetivos Específicos

"Conocer las modalidades participes y consecuencias que se presentan medianteun ataque de Phishing y la respuesta jurídica que se obtiene ante estos hechos".

El presente objetivo se logró cumplir por completo ya que gracias a una profunda investigación realizada previamente se pudo reconocer todas las modalidades participes que el delito de phishing presenta en la actualidad y así mismo las consecuencias que este produce, perjudicando principalmente la economía y patrimonio de las personas; dando como respuesta jurídica a esta problemática que son las autoridades quienes deben reformar el Código

Orgánico Integral Penal para que este delito tenga la sanción correspondiente y así lograr que no se sigan vulnerando estos derechos.

"Establecer la necesidad de tipificar el delito de phishing en la legislación penal ecuatoriana para evitar la vulneración de los derechos económicos y patrimoniales de los ciudadanos".

Este objetivo se cumple a toda cabalidad ya que gracias a la mayoría de la población por parte de la investigación de campo que se realizó, coinciden en todas sus respuestas referentes a la necesidad de tipificar el delito de phishing en el Código Orgánico Integral Penal, manifestando que debería ser de carácter urgente para que no se sigan produciendo perjuicios ni vulnerando los derechos económicos y patrimoniales de las personas. A parte de dichas afirmaciones, con el estudio teórico que realicé, el sustento legal, la recopilación de información de fuentes confiables y la representación de los datos obtenidos por la encuesta y entrevista, arrojan como principal consecuencia al problema planteado dentro de esta investigación, la cual es que se debe tipificar al phishing en la legislación penal ecuatoriana.

7.2 Fundamentación Jurídica de la Propuesta de Reforma Legal

Como es de conocimiento nuestro país es un Estado Constitucional de Derechos y busca que se dé la Justicia Social, por lo cual, posiciona a la Constitución de la Republica como la norma suprema, es decir, esta se establece ante cualquier ordenamiento jurídico interno que rige dentro del país.

En la Constitución de la República, específicamente en su Artículo 66, inciso 26, manifiesta que se reconoce y garantiza el Derecho a la propiedad de todas las formas, y obviamente el Derecho al acceso de la propiedad, por ello, es obligación del Estado adoptar medidas públicas que sean necesarias para garantizar y proteger dichos derechos que tienen todos los ciudadanos ecuatorianos.

De igual forma, en su Artículo 75 se describe que todas las personas tienen Derecho al acceso a una justicia gratuita y una tutela efectiva, que es neutral y libre de sus derechos e intereses, las cuales están ligadas a los principios de inmediación y celeridad; de ninguna forma alguna persona puede quedarse en indefensión y si se da el incumplimiento de estas resoluciones jurídicas son sancionados por la ley.

Es pertinente acogerse al Código Orgánico Integral Penal, ya que es el elemento

sistematizado de normas punitivas con sus respectivas sanciones, por este medio se establecen los diferentes procedimientos que deben seguirse para que se dé un buen juzgamiento de las personas con el respectivo Debido Proceso, con los derechos y garantías que nos establece la Constitución de la Republica y otras leyes que fuesen necesarias.

Por ende, en el Artículo 2 del Código Orgánico Integral Penal, se encuentran los principios generales afines al debido proceso, en el cual se informa que en todo lo que se refiera al ámbito penal se aplicaran los principios emanados de nuestra Constitución de la República, de aquellos instrumentos internacionales de Derechos Humanos y los que se encuentran en este código. De todos los principios que se pueden encontrar, se debe puntualizar al más importante, el principio de legalidad, dentro de este se manifiesta que no existe una infracción penal sin que no exista una ley anterior al hecho.

También cabe mencionar al Artículo 13 del mismo Código, en donde se presentan las normas de interpretación, en las cuales, se tiene que dar un sentido idóneo conforme a las siguientes reglas: 1. La interpretación en el ámbito penal se realiza con el significado que más se ajuste a la Constitución de la República, y a los instrumentos internacionales de derechos humanos. 2. Se deben interpretar de forma estricta todos los tipos penales y las penas, siempre respetando el sentido literal de la norma. 3. Se prohíbe profundamente que se utilice la analogía para crear infracciones penales, de igual forma, se prohíbe que se amplíen los límites de los presupuestos legales que permiten la aplicación de las sanciones o para instaurar excepciones o restricciones de derechos.

Por tal motivo, considero que la falta de tipificación del delito informático de phishing produce que los operadores de justicia puedan cometer un error en cuanto a la adecuación al tipo penal. Por lo que nuestro Código Orgánico Integral Penal es insuficiente jurídicamente porque como lo dije anteriormente este no se presta para analogías o interpretaciones que tengan alguna relación con un delito ya tipificado con su respectiva sanción, por cuanto esta ausencia afecta a los derechos de protección y seguridad que el Estado garantiza porque están siendo vulnerados.

8. Conclusiones

Concluida la presente investigación, tanto su parte teórica como el respectivo análisis de campo, referente al tema denominado: “EL PHISHING COMO MEDIO DE DISPOSICIÓN PATRIMONIAL FRAUDULENTA”, he llegado a las siguientes conclusiones:

En la actualidad el delito informático de phishing es muy perjudicial para todos los seres humanos, ya que violenta profundamente el derecho a la economía y el derecho al patrimonio, derechos que están protegidos por nuestro país, es sus respectivas legislaciones, tanto en la Constitución de la República, en el Código Orgánico Integral Penal y en el Código Civil, por tal motivo este delito debería ser tipificado en el Código Orgánico Integral Penal.

Hoy en día con los grandes avances de la tecnología de la información y comunicación, se han observado nuevas medidas o formas para cometer delitos, mediante el uso de las herramientas tecnológicas, siendo su finalidad eliminar, copiar, modificar, o transferir en poco tiempo la información personal de la víctima, perjudicar a los sistemas informáticos o incluso también afectar a los sistemas informáticos de grandes empresas.

En Ecuador es complicado determinar un número preciso de ciudadanos que hayan sido víctimas del delito informático de phishing, ya que la mayoría no denuncian estos casos porque piensan que las autoridades lo dejaran en el olvido; en cambio, cuando si denuncian a los funcionarios judiciales, estos adecuan este delito a otro tipo penal; o a su vez, la investigación queda en auge por motivo que los facultados no cuentan con el equipo especializado para este tipo de casos. Además, es nocivo que nuestro país no forme parte de algún convenio internacional para poder combatir todo lo referente a delitos informáticos, por ende, no le permite tener cooperación internacional para dar solución a estos casos.

Para que se ejecute el delito informático de phishing es necesario que los ciberdelincuentes tengan un alto conocimiento y sobre todo experiencia para que puedan manipular todos los medios y herramientas tecnológicas, logrando así que su víctima entregue sus datos confidenciales de una forma voluntaria.

Todos los individuos al darse cuenta de la facilidad que proporcionan los medios tecnológicos, día a día se observa que el número de usuarios va incrementando, por lo cual hanllegado a ser utilizadas para violentar a las personas y a la ley.

La deficiencia que existe en la falta de información por parte de las autoridades y ciudadanos en general es muy visible, ya que por la investigación de campo realizada se puede apreciar que la mayoría de encuestados desconoce lo que es este tipo de delito informático, porlo tanto, no se pueden tomar las medidas preventivas que son necesarias.

Es evidente que se debe tipificar como una nueva modalidad de estafa al delito

informático de phishing, con sus respectivas características en el Código Orgánico Integral Penal, basado jurídicamente en el principio de legalidad y seguridad jurídica; ya que se estaría protegiendo, previniendo, y cumpliendo todos los derechos que deben garantizarse a los ciudadanos y a su patrimonio.

9. Recomendaciones

Considero de manera oportuna poner a conocimiento las siguientes recomendaciones para lograr dar solución a la problemática que se planteó desde un inicio en la presente investigación:

Ecuador es una nación independiente, se debería unir a convenios internacionales contra los delitos informáticos o ciberdelincuencias para obtener una mayor cooperación internacional, así mismo, lograr capacitarnos de las nuevas modalidades que van surgiendo con el pasar del tiempo y obviamente con el avance de la tecnología.

Se observa la necesidad de que la Asamblea Nacional incorpore dentro del Código Orgánico Integral Penal, el delito informático de phishing como una nueva modalidad de estafa a fin de que mediante su tipificación se pueda establecer una regulación completa sobre todas las distintas clases de delitos informáticos que son auge a nivel mundial; se pondría al Ecuador como un país mucho más desarrollado respecto a este tema e iría al par con la evolución de la tecnología y categorías delictivas con el uso de las TIC.

El Estado a través del Ministerio de Educación podría implementar campañas o capacitaciones de educación y prevención con respecto al uso de las Redes Sociales para evitarque en futuro estos individuos sean víctimas respecto al delito informático de phishing.

Aquellas personas encargadas de administrar justicia deben tener cuidado y diligencia en todos los procesos que se dan por motivo del delito informático de phishing, con la finalidad de no caer en el error para adecuarlo al tipo penal que corresponde y no a otro similar.

A las empresas financieras o entidades bancarias no solo dar capacitaciones a sus empleados para que eviten este tipo de delito, sino más bien implementar distintas medidas de seguridad que refuercen de mejor manera los sistemas que utilizan y así no puedan ser hackeados fácilmente.

Las distintas fiscalías de nuestro país y la policía judicial pueden dar a conocer más casos de las victimas que pasan por este tipo de engaño o estafa para que los ciudadanos recurran a denunciar sus circunstancias para que no queden a la deriva, sino que se realice lo necesario para verificar a aquellos ciberdelincuentes que abusan de la tecnología para obtener beneficio propio o para terceros.

9.1 Proyecto de Reforma Legal

REPÚBLICA DEL ECUADORASAMBLEA NACIONAL

CONSIDERANDO

Que, el Artículo 1, de la Constitución de la República establece que el Ecuador es un Estado Constitucional de Derechos y Justicia, se ve la necesidad de poder realizar cambios en el ordenamiento jurídico nacional para que se dé una respuesta al cumplimiento del más alto deber que es respetar y hacer respetar los derechos que se garantizan para todos los ciudadanos ecuatorianos.

Que, el Artículo 3, de la Constitución de la República, manifiesta que el Estado tiene deberes primordiales, como garantizar sin discriminación alguna el efectivo goce de los derechos que se establecen en la misma y en los instrumentos internacionales.

Que, el Artículo 16 en su inciso 2, de la Constitución de la República del Ecuador, se refiere al derecho que tienen todos los ciudadanos tanto individual como colectivamente a "El acceso universal a las tecnologías de información y comunicación".

Que, el artículo 18, de la Constitución de la República, establece el derecho a la información, de que todas las personas, en forma individual o colectiva, tienen derecho a acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas […].

Que, el Artículo 30, de la Constitución de la República del Ecuador establece que "Las

personas tienen derecho a un hábitat seguro y saludable y a una vivienda adecuada y digna, con independencia de su situación social y económica.

Que el Artículo 66, en su inciso 19, de la Constitución de la República, establece el derecho a la protección de datos de carácter personal, que incluya el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Que, el Articulo 66, en su inciso 26, de la Constitución de la República del Ecuador se reconoce el Derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El Derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas.

Que, el Articulo 75, de la Constitución de la República, contempla que toda persona tiene Derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley.

Que, el Artículo 76 en su inciso 6, de la Constitución de la República del Ecuador, establece que en todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso, garantizando la debida proporcionalidad entre las infracciones y las sanciones penales, administrativas o de otra naturaleza.

Que, el Artículo 82 de la Constitución de la República del Ecuador, establece que "El derecho a la seguridad jurídica que se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes".

Que, el Artículo 84 de la Constitución de la República del Ecuador, establece que "La Asamblea Nacional y todo Órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público

atentarán contra los derechos que reconoce la Constitución".

Que, el Articulo 132, de la Constitución de la República del Ecuador, regula que la Asamblea Nacional aprobará como leyes las normas generales de interés común. Las atribuciones de la Asamblea Nacional que no requieran de la expedición de una ley se ejercerán a través de acuerdos o resoluciones […].

Que, el Artículo 321, de la Constitución de la República, reconoce y garantiza el Derecho a la propiedad en sus formas pública, privada, comunitaria, estatal, asociativa, cooperativa, mixta, y que deberá cumplir su función social y ambiental.

Que, el Artículo 424, primer inciso, ordena que la Constitución es la Norma Suprema del Estado y prevalece sobre cualquier otra del ordenamiento jurídico, y, por lo tanto, todas las normas de menor jerarquía deben mantener conformidad con las disposiciones constitucionales.

Que, el Articulo 1, del Código Orgánico Integral Penal, manifiesta que tiene por finalidad normar el poder punitivo, tipificar infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas.

Que, el Artículo 2, del Código Orgánico Integral Penal referente a los principios generales afines al debido proceso refiere que en materia penal se aplican todos los principios que emanan de la Constitución de la República, instrumentos internacionales de derechos humanos y los desarrollados en este mismo código.

Que, el Artículo 5, inciso 1, Código Orgánico Integral Penal, sobre el principio de legalidad manifiesta que no existirá una infracción penal sin una ley anterior al hecho.

Que, el Artículo 13, del Código Orgánico Integral Penal sobre las normas de interpretación establece: 1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de Derechos Humanos. 2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma. 3. Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos.

Que se ve la necesidad de manera urgente establecer un respectivo tipo penal, el cual se adecue a la realidad del Estado, principalmente relacionado con aquellas conductas perjudiciales que se las efectúa a través del uso de las Tecnologías de la Información y Comunicación.

En ejercicio de sus atribuciones constitucionales y legales la Asamblea Nacional Expide la presente reforma:

LEYREFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)

Artículo. 1.- Incorpórese como articulo innumerado antes del Art. 187 lo siguiente:

Articulo iin…1.- Delito Informático. – Se debe considerar delito informático a la conducta que se efectúa a través del manejo de las Tecnologías de la Información y Comunicación (TIC) destinada a generar perjuicio a una o varias personas para obtener beneficio patrimonial propio o para terceros.

Artículo. 2.- Incorpórese a continuación del Artículo 187 el siguiente Artículo innumerado.

Articulo inn…2.- Phishing. – La persona o personas que obtengan de forma fraudulenta datos íntimos o personales, ya sean claves o contraseñas para acceder a diferentes redes sociales, empresas bancarias, haciéndose pasar por un individuo de confianza mediante el uso frecuente y masivo de correos electrónicos, mensajería fugaz o inclusive utilizando llamadas telefónicas será sancionada con una pena privativa de libertad de uno a tres años.

Será sancionada con igualdad de pena, la persona que:

1. Cuando se envíe un correo electrónico que tenga fin de lucro, que ofrezca a un usuario o individuo una respectiva cantidad de dinero que se encuentra en moneda extranjera y para poder liberar aquel dinero obligue al usuario un anticipo o solicite datos personas para que este lo reciba en el menor tiempo posible.

2. Se envíe un correo electrónico con ánimo de lucro que oferte una oportunidad de trabajo a un usuario, la cual se base en promoción de algún producto o en la captación de más personas para nuevos empleos pero que dentro de este se exige una cantidad de dinero para empezar a trabajar.

3. Cuando un correo electrónico de forma ilícita pida a un usuario realizar una transferencia electrónica teniendo la posibilidad de quedarse con cierto porcentaje, por el simple hecho de realizar una transferencia del importe recibido menos la comisión de este que es destinada a otra cuenta.

4. Se utilice las herramientas tecnológicas con fin lucrativo, cuando se aproveche de un usuario que esté pasando por catástrofes naturales; cadenas de ayuda, de la suerte; diferentes métodos para hacerse millonario en tan poco tiempo; regalos que ofrecen compañías multinacionales o mensajes con temática religiosa, todos ellos que pidan realizar aportaciones económicas para poder empezar.

5. Envíe un correo electrónico o SMS para obtener beneficio lucrativo, en el cual se pida realizar una llamada a un número de celular para recibir información, un obsequio o para saber lo que la gente dice o piensa de este. Este correo o SMS lo redirigirá a un servicio de telefonía especial en la cual se le pedirá información personal, contraseñas, claves, número de tarjeta de crédito o débito, cuentas bancarias.

6. Cuando se envíe un mensaje a diferente red social que manifieste que el usuario se encuentra saliendo en un video y tiene que abrir el enlace que este contiene para poder verlo, con la finalidad de obtener sus contraseñas o mensajes que estén dentro de las mismas.

Disposición General. – Refórmese el Código Orgánico Integral Penal (COIP), con la finalidad de que se adecue las disposiciones mencionadas a través de los artículos presentes en esta reforma jurídica.

Disposición Final. – La presente reforma jurídica entrará en vigor a partir de su promulgación en el Registro Oficial.

Supuesto y suscrito, en el Distrito Metropolitano de San Francisco de Quito, en la sede de sesiones de la Asamblea Nacional del Ecuador, el 02 de febrero del 2023.

Presidente de la Asamblea Nacional del Ecuador

Secretario General

10. Bibliografía

Aguilar, R. (miércoles de noviembre de 2020). *Redes Sociales: ¿Cuáles son susprincipales características para el 2021?* Obtenido de Digital Business Academy: https://atrevete.academy/blog/redes-sociales-cuales-son-sus-principales-caracteristicas- para-el-2021/

Arán, F. M. (2010). *Derecho Penal, Parte General.* Valencia: Tirant Lo Blanch. Arán, F. M. (2010). *Derecho Penal, Parte General.* Valencia: Tirant Lo Blanch.

Belcic, I. (miercoles de febrero de 2020). *Guía esencial del phishing: cómo funciona, caracteristicas y cómo defenderse*. Obtenido de Avas, Academy: https://www.avast.com/es-es/c-phishing#:~:text=El%20ataque%20se%20realiza%20mediante,n%C3%BAmeros%20de% 20tarjeta%20de%20cr%C3%A9dito.

Beltran, S. &. (2012). *La integración de redes de colaboración entre cuerpos académicos.* Alternativas en Psicología.

Betancourt, E. L. (2007). *Módulo V La Antijuricidad y su Ausencia en Teoría del Delito.* Mexico, Porrua .

Blogspot, S. (2012). *Tegnologías de la Información y la Comunicación.* Obtenido de Clasificación de las TICS: http://informacioncomunicacion3.blogspot.com/p/clasificacion-de-las-tics.html

C. P. (2009). De la Protección de la información y de los datos.

Cabanellas, G. (1997). *Diccionario Enciclopédico de Derecho Usual.* Editorial Heliasta S.R.L.

Cabero, J. (2005). *Cibersociedad y juventud: la cara oculta (buena) de la luna.* Obtenido de Un nuevo sujeto para la sociedad de la información.: http://tecnologiaedu.us.es/cuestionario/bibliovir/ciberjuve.pdf

Cabero, J. (2005). *Un nuevo sujeto para la sociedad de la información.* Obtenido de Cibersociedad y Juventud: La cara oculta de la luna.: https://dialnet.unirioja.es/servlet/libro?codigo=270989

Calderón, L. (2010). *Delitos Informáticos y Derecho Penal.* Editorial UBIJUS. Carranca Trujillo, R. y. (1991). *Derecho Penal Mexicano.* México.

Casabona, R. (1987). *Poder informático y seguridad jurídica.* Madrid: Fundesco.

Castro, L. (2015). *Tipos de Sujetos Activos en Delitos Informáticos*. Obtenido de Delitos Informáticos: http://aprenderinternet.about.com/od/ConceptosBasico/g/Que-Es-Hacker.htm

Chiavenato, I. (2007). *Introducción a la Teoría General de la Administración.* . Séptima Edición, McGraw-Hill Interamericana.

Constitución de la República del Ecuador. (2008). Asamblea Nacional.

DICCIONARIO DE LA REAL ACADEMIA ESPAÑOLA. (2019).

Donna, E. y. (2004). *Aspectos generales del tipo penal de estafa.* Obtenido de Revista Latinoamericana de Derecho: https://revistas-colaboracion.juridicas.unam.mx/index.php/latinoamericana-derecho/article/view/21276/18950

García Sanz, N. (jueves de abril de 2019). *44 ventajas y desventajas de las redes sociales*. Obtenido de Comunicación y Estrategia Digital: https://nagoregarciasanz.com/ventajas-desventajas-redes-sociales/

González, P. (2007). *Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta PHISHING.* Obtenido de INTECO: www.inteco.es

Huerta Miranda, M. y. (1996). *Los delitos informáticos.* Chile: Editorial Jurídica ConoSur.

ICOMOS. (1999). *CARTA INTERNACIONAL SOBRE TURISMO CULTURAL.* Obtenido de: La Gestion del Turismo con Patrimonio Significativo: https://www.iaph.es/export/sites/default/galerias/patrimonio-cultural/documentos/gestion-informacion/icomoscartainternacionalsobreturismocultural.pdf

Jaramillo, A. (2010). *Twiter para todos.* Bogotá: Editorial Vergara.

La guía definitiva sobre el phishing: qué es el phishing y cómo evitar las estafas. (jueves de

agosto de 2020). Obtenido de KEEPER: https://www.keepersecurity.com/es_ES/threats/what-is-phishing.html

Leguizamón, M. (2015). *El Phishing.* Obtenido de Universitat Jaume: https://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizam%C3%B3n_Mayra.pdf?sequence=1

León, R. d. (1970). *Algunos fraudes no detectables en libros (tesis de graduación).* Santiago de León: USAC.

Lomarte, M. y. (2010). *Derecho y Redes Sociales.* Pamplona, España: Civitas. Ministerio de Justicia. (2022). De los delitos informáticos y sus sanciones.

Mezger, E. (1935). *Tratado de Derecho Penal.* Buenos Aires, Argentina: Edición Hammurabi.

Muñoz Conde, F. y. (2010). *Derecho Penal, Parte General.* Valencia: Tirant lo blanch.

Asamblea Nacional. (2009). Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

Asamblea Nacional. (2015). Ley Orgánica de Telecomunicaciones.

Nelson, A. (1942). *Introducción a la intervención de cuentas.* Unión Tipográfica Hispanoamericana.

Ollmann. (2006). *Understanding and Preventing Phishing Attacks*. Obtenido de TechnicalInfo Making sense of security: http://www.technicalinfo.net/papers/Phishing.html

Ossorio, M. (1998). *Diccionario de Ciencias Jurídicas, Políticas y Sociales. 1era. Edición Electrónica.* Guatemala, C. A.: Datascan, S. A. *Reglamento Europeo de Protección de Datos.* (27 de abril de 2016). Obtenido de Diario Oficial de la Unión Europea: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Roing, C. (2008). *Tecnología de la Información. Conceptos Básicos.* Obtenido de DOCPLAYER: https://docplayer.es/1825590-Tecnologia-de-la-informacion-conceptos- basicos.html

Romaní Cobo, J. C. (lunes de septiembre de 2011). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. *ZER: Revista De Estudios De Comunicación.*, pág. https://ojs.ehu.eus/index.php/Zer/article/view/2636.

Romero, A. S. (01 de febrero de 2012). *Clasificación de las TICS.* Obtenido de Slidesharea Scribd company: https://es.slideshare.net/AleksNet/clasificacin-de-las-tics

Ron, M. (21 de octubre de 2019). *Estafa Informática*. Obtenido de Derechoecuador.com: https://derechoecuador.com/estafa-informatica/

Sáinz Cantero, J. A. (1990). *Lecciones de Derecho Penal.* Barcelona: Bosch, Casa Editorial, S. A.

Salas, M. (marzo de 2019). *Tipos de Phishing*. Obtenido de Dirección de Tecnologías de Información: https://www.uach.cl/direccion-de-tecnologias-de-información/seguridad/tipos-de-phishing

Serrahima, J. (2010). *La amenaza digital.* Barcelona, España: Bresca Editorial. ISBN.

Téllez Valdés, J. (1996). *Los delitos informáticos. Situación en México.* Mérida: Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura.

UNESCO. (2022). *Documents General Conference.* Paris: Executive Board.

Viladevall, M. y. (2003). *El Patrimonio.* Puebla, México: Dirección General de Fomento Editorial.

11. Anexos

11.1 Formato de Encuesta, Entrevista y Certificación del Abstrac

11.1.1 Encuesta

UNIVERSIDAD NACIONAL DE LOJA FACULTAD JÚRIDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

Abogado (a): Con la finalidad de obtener los datos que sustenten mi trabajo de investigación realizado bajo el tema: "EL PHISHING COMO MEDIO DE DISPOSICIÓN PATRIMONIAL FRAUDULENTA" respetuosamente solicito a usted se digne a contestar demanera clara y precisa las siguientes interrogantes:

1. **¿Conoce usted lo que es el delito informático de phishing?**

Si ( ) No ( )

¿Por qué?

……
……
……

2. **¿Ha sido usted víctima de alguna situación en la cual le hayan enviado un correo electrónico y se hayan apropiado de sus datos personales, claves o contraseñas de forma ilícita para acceder a diferentes sistemas informáticos, haciéndose pasar por personas de confianza para obtener beneficio propio o para terceros?**

Si ( ) No ( )

¿Por qué?

……
……
……

3. **¿Conoce usted si alguna o algunas otras personas hayan sido víctimas de este tipo de delito informático de phishing?**

Si ( ) No ( )

¿Por qué?

……
……

……

4. **¿Considera usted que debería existir mucha más información por parte de las autoridades para poder prevenir este tipo de delito informático de phishing?**

Si ( ) No ( )

¿Por qué?

……
……
……

5. **¿Considera usted que la falta de tipificación del delito informático de phishing es lacausa directa por lo que se sigue produciendo en la actualidad?**

Si ( ) No ( )

¿Por qué?

……
……
……

11.1.2 Entrevista

UNIVERSIDAD NACIONAL DE LOJA FACULTAD JÚRIDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

Abogado (a): Con la finalidad de obtener los datos que sustenten mi trabajo de investigación realizado bajo el tema: "EL PHISHING COMO MEDIO DE DISPOSICIÓN PATRIMONIAL FRAUDULENTA" respetuosamente solicito a usted se digne a contestar de manera clara y precisa las siguientes interrogantes:

Pregunta #1

El delito informático de phishing producido por los ciberdelincuentes hacia la victima presenta aspectos fundamentales como es el engaño, el daño al bien patrimonial y específicamente a la alteración o modificación de las claves, datos personales o dispositivos de la banca online. Tomando en cuenta esto, ¿Según su criterio profesional, piensa usted que es necesario que al delito informático de phishing se lo considere como una nueva modalidad de estafa y se lo tipifique en nuestro Código Orgánico Integral Penal?

……
……
……
……
……

Pregunta #2

En este tipo de delito informático de phishing se trata con personas muy especialistas, es decir, pueden cometer el delito y eliminar todo dato o huella de lo que han realizado, ¿Cómo cree usted que se podría identificar la identidad de la persona que cometió el delito?

……
……
……
……
……

Pregunta #3

Según la fiscalía general de nuestro país los casos respecto a delitos informáticos han ido incrementando desmesuradamente, ¿Cree usted que a estos delitos informáticos no se los puede prevenir por la falta de capacitación o información que tienen las personas tanto naturales como jurídicas?

……

.....

.....

.....

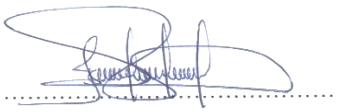
.....

11.1.3 Certificado de traducción del Abstrac

Loja, 04 de febrero de 2023

Julio Cesar Garnica Narváez, con cédula de identidad 1104170889, Licenciado en Ciencias de la Educación, certifico: Qué tengo el conocimiento y dominio del Idioma Inglés y que la traducción del resumen del trabajo titulado: **"El phishing como medio de disposición patrimonial fraudulenta"**, cuya autoría es de la estudiante **Valeria Alejandra Campoverde Salas**, con cédula de identidad **1105658619,** es verdadero y correcto a mi mejor saber y entender.

Atentamente:



Lcdo. Julio Cesar Garnica Narváez

Docente del Colegio Fiscomisional "Nuestra Señora del Rosario"