



— Universidad —
Inca Garcilaso de la Vega
Nuevos Tiempos. Nuevas Ideas

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

TESIS

MECANISMOS DE PREVENCIÓN Y PROTECCIÓN DEL BIEN
JURÍDICO TUTELADO FRENTE A LA MODALIDAD DELICTIVA
PHISHING EN EL ORDENAMIENTO JURÍDICO PENAL PERUANO

PARA OBTENER EL TÍTULO DE

ABOGADO

LINEA DE INVESTIGACIÓN

DERECHO PENAL

AUTOR

ESPARTA CENTENO, MARITZA MARISOL

ASESOR

DRA. BARDALES BECERRA, KARINA KAROL

LIMA, PERÚ, MARZO DE 2022



DEDICATORIA

A Dios por ser mi fuerza de vida, que gracias a él logré culminar la presente tesis.

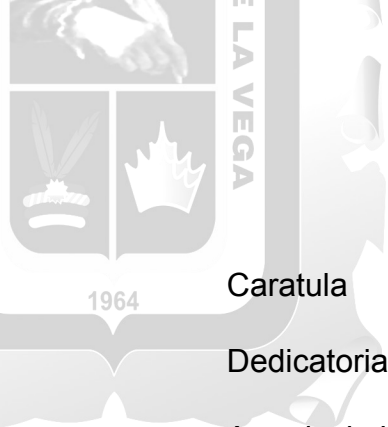
A mi familia, por el apoyo incondicional que me han brindado para hacer la presente tesis.



AGRADECIMIENTOS

Agradezco a mi alma mater, la Universidad Inca Garcilaso de la Vega; por acobijarme en sus aulas en todo este periodo de estudios superiores.

Agradezco a mi asesora de tesis la Dra. Karina Karol Bardales Becerra, por la paciencia, su dedicación, su apoyo incondicional y el respeto que tuvo en el asesoramiento de la presente tesis.



ÍNDICE

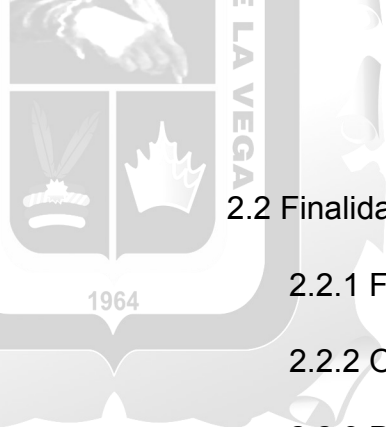
Caratula	
Dedicatoria.....	ii
Agradecimientos.....	iii
Índice.....	iv
Lista de Tablas.....	vii
Lista de Figuras.....	viii
Lista de Gráficos.....	x
Resumen.....	xv
Abstract.....	xvi
Introducción.....	xvii

CAPÍTULO I: FUNDAMENTOS TEÓRICOS DE LA INVESTIGACIÓN

1.1 Marco Teórico.....	18
1.1.1 Teoría del delito.....	18
1.1.2 Teoría del delito phishing	18
1.1.3 Teoría selecccionada.....	20
1.2 Investigaciones.....	21
1.2.1 Investigaciones internacionales.....	21
1.2.2 Investigaciones nacionales.....	28
1.3 Marco Conceptual.....	34

CAPÍTULO II: EL PROBLEMA, OBJETIVOS, HIPÓTESIS Y VARIABLES

2.1 Planteamiento del problema.....	37
2.1.1 Descripción de la realidad problemática.....	39
2.1.2 Antecedentes teóricos.....	39
2.1.3 Definición del problema.....	41



2.2 Finalidad y Objetivos de la investigación.....	41
2.2.1 Finalidad.....	
2.2.2 Objetivo general y específicos.....	41.
2.2.3 Delimitación del estudio.....	42
2.2.4 Justificación e importancia del estudio.....	42
2.3 Hipótesis y variables.....	43
2.3.1 Supuestos teóricos.....	43
2.3.2 Hipótesis Principal y Especificaciones.....	43.
2.3.3 Variables e indicadores.....	43.

CAPÍTULO III: MÉTODO, TÉCNICA E INSTRUMENTO

3.1 Población y muestra.....	45
3.2 Diseño (s) a utilizar en el estudio.....	45
3.2.1 Tipos de investigación.....	45
3.2.2 Métodos de la investigación.....	46
3.2.3 Enfoque y diseño de la investigación.....	47
3.3 Técnica (s) e instrumentos de Recolección de datos.....	47
3.3.1 Técnica de recolección de datos.....	47
3.3.2 Instrumento de recolección de datos.....	49.
3.4 Procesamiento de Datos.....	

CAPITULO IV: PRESENTACIÓN Y ANALISIS DE LOS RESULTADOS

4.1 Presentación de Resultados.....	
4.2 Contrastación de Hipótesis.....	
4.3 Discusión de Resultados.....	



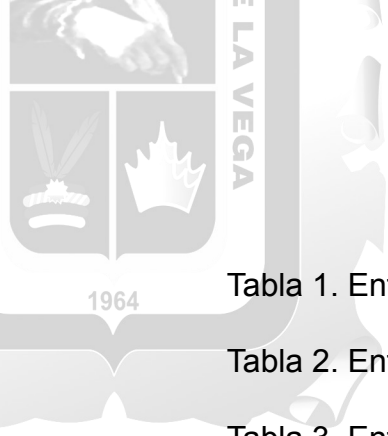
CAPITULO V: CONCLUSIÓN Y RECOMENDACIONES

5.1 Conclusión.....

5.2 Recomendaciones.....

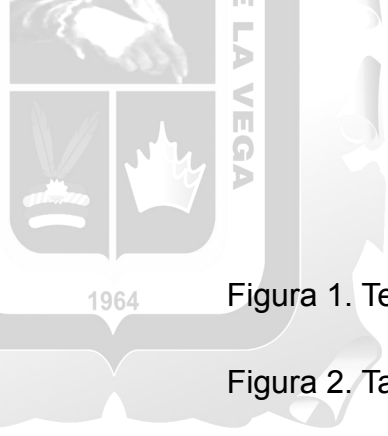
BIBLIOGRAFIA

ANEXOS



LISTA DE TABLAS

Tabla 1. Entrevistado 1.....	72
Tabla 2. Entrevistado 2.....	73
Tabla 3. Entrevistado 3.....	74
Tabla 4. Entrevistado 4.....	75
Tabla 5. Contrastación de la hipótesis principal.....	80
Tabla 6. Operacionalización de las variables.....	100



LISTA DE FIGURAS

Figura 1. Teoría del delito

Figura 2. Tareas de Phishing

21



LISTA DE GRÁFICOS

Gráfico 1 ¿Cuentan con sistema informáticos ante un eventual delito de phishing? De ser afirmativa la respuesta indique qué programas.....69

Gráfico 2 ¿Su entidad bancaria ha sido víctima de los hackers informáticos?.....70

Gráfico 3 ¿Cuándo acude la persona al banco se le brinda orientación sobre los peligros de los delitos informáticos y cómo prevenirlos? De ser afirmativa la respuesta indique qué actividades se ha desarrollado.....71

Gráfico 4 ¿Durante el primer trimestre del año 2022, se ha reportado víctimas de este delito? De ser afirmativa la respuesta indique un aproximado.....72

Gráfico 5 ¿Conoce de qué manera ha intervenido la SBS frente a los denominados hackers informáticos? Si la respuesta es afirmativa indique la forma de intervención..73

Gráfico 6 ¿Los usuarios qué actitudes han adoptado frente al delito del phishing? Puede marcar más de una opción.74

Gráfico 7 ¿Cuál de las siguientes opciones considera usted que se debe implantar en las agencias bancarias para evitar la comisión de delitos informativos phishing? De ser necesario puede marcar más de una opción.75



GLOSARIO

PHISHING:

Password Harvesting Fishing,

El término inglés phishing es un abreviado de password harvesting fishing, que son diferentes conceptos informáticos y traducen cosecha y pesca de contraseñas; su nombre se le atribuye a una modalidad delictiva conocida como “suplantación de sitios web para capturar datos personales”.

BACKUP:

Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

BIOMETRÍA:

La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.)

BULO:

También llamados hoax, son noticias falsas creadas para su reenvío masivo ya sea a través de redes sociales, mensajería instantánea o correo electrónico, con el fin de hacer creer al destinatario que algo es falso.

LAN:

Una LAN (del inglés Local Area Network) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc.



MALWARE:

Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.

KEYLOGGER:

Graba todo lo que hace el usuario en el teclado.

PENTEST:

Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades.



RESUMEN

La presente investigación denominada “Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano”, por lo cual se formuló la siguiente pregunta ¿De qué manera los mecanismos de prevención y protección del bien jurídico tutelado influyen a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano?

Teniendo como meta: Verificar la manera en que los mecanismos de prevención y protección del bien jurídico tutelado influye a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano.

El método de investigación aplicado fue dogmático, debido a que no se alteró la realidad para el estudio ni se propone modificaciones al ordenamiento jurídico.

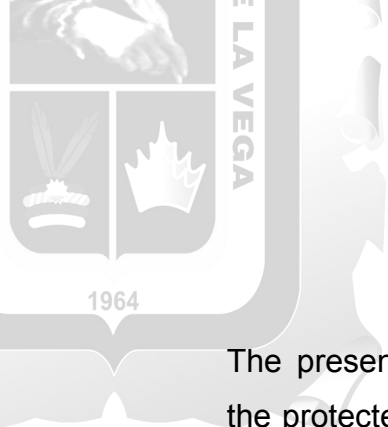
La presente investigación tiene enfoque mixto y como diseño de investigación es experimental, dado la manipulación de ambas variables para el análisis y el hallazgo de conclusiones.

La población es el conjunto de reclamos sobre modalidad delictiva phishing en el ordenamiento jurídico penal peruano, y mérito a la técnica de muestreo por no probabilística por conveniencia se analizó el 20% de nuestra población correspondiente a una cantidad de 10000 reclamos en su totalidad como objeto de estudio.

Para el procesamiento de datos se utilizó a estadística descriptiva mediante cuadros y gráficos estadísticos en Excel donde se expusieron los datos recopilados de cada sentencia analizada.

Los resultados de la hipótesis fueron validados pues se demostró que una campaña de información sobre el cómo prevenir este tipo de delitos tiene como resultado que existan menos víctimas por este delito.

PALABRAS CLAVES: mecanismos de prevención y protección, bien jurídico tutelado, modalidad delictiva phishing, ordenamiento jurídico, derecho penal



ABSTRACT

The present investigation called "Mechanisms of prevention and protection of the protected legal asset against the criminal modality phishing in the Peruvian criminal legal system", for which the following question was formulated: How do the mechanisms of prevention and protection of the protected legal asset Does it influence the criminal modality of phishing in the Peruvian criminal legal system?

Having as general goal: To determine the way in which the mechanisms of prevention and protection of the protected legal right influence the criminal modality phishing in the Peruvian penal system.

The applied research method was dogmatic, because reality was not altered for the study and no modifications to the legal system were proposed.

The present investigation has a mixed approach and as a research design it is experimental, given the manipulation of both variables for the analysis and the finding of conclusions.

The population is the set of claims on the criminal phishing modality in the Peruvian criminal legal system, and due to the technique demonstrated by non-probabilistic convenience, 20% of our population corresponding to an amount of 10,000 claims in its entirety was analyzed as object. study.

For data processing, descriptive statistics were produced using statistical charts and graphs in Excel where the data collected from each sentence analyzed was presented.

The results of the hypothesis were validated because they learned that an information campaign on how to prevent this type of crime results in fewer victims of this crime.

KEY WORDS: prevention and protection mechanisms, protected legal asset, phishing criminal modality, legal system, criminal law



INTRODUCCIÓN

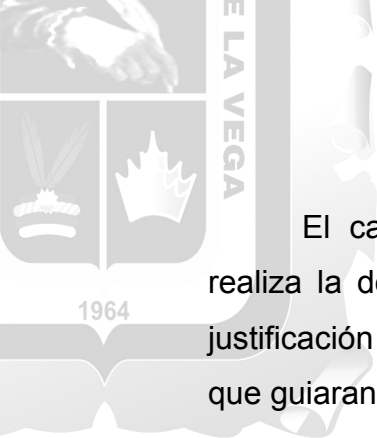
La actual investigación tiene como finalidad demostrar la influencia de los mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano. En el presente estudio, no solo se demuestra la ausencia de criterios objetivos por parte del estado, como ente regulador en el análisis de dicho bien jurídico tutelado dentro de un proceso penal, sino también la falta de nuevos incisos en los artículos del Código Penal que sean más severos contra las personas que cometen tal delito

Dentro de ese contexto de delito informático phishing, se estaría en constante amenaza a nuestro patrimonio por lo que se debe sancionar severamente con penas de cárcel a aquel o aquellas personas que cometan el delito informático phishing, dada la magnitud de la afectación de los datos personales y/o patrimoniales, pues en este primer semestre del año ya existe más de once mil denuncias ocasionadas por este delito.

Como sabemos el delito informático phishing es considerado originariamente como “la pesca” que se realiza, ya que, así como el pescador tiende la red para cazar muchos pescados el delito informático lo realizan enviando correos maliciosos y atractivos que te proponen ganar dinero de manera rápida y segura con solo llenar tus datos y cuya consecuencia es hackear la contraseña de las tarjetas bancarias y a través de ella ingresar a la esfera personal y patrimonial del sujeto agraviado.

Esta investigación está conformada por cinco capítulos:

En el capítulo I, denominado fundamentos teóricos de la investigación, se presentará antecedentes a nuestra investigación que son estudios anteriores al nuestro, las teorías imperantes y aplicables a la presente investigación, así como del desarrollo de un marco conceptual de las categorías relevantes conforme al objeto de estudio, entre otros del problema de la falta de criterios de los órganos jurisdiccionales para conceder el cambio de nombre, problemática antes descrita.



El capítulo II, considera el planteamiento del problema, en el cual se realiza la descripción de la realidad problemática, la definición del mismo, su justificación e importancia, así como su delimitación temporal, espacial y social, que guiaran el presente estudio.

En el capítulo III, comprenderá la metodología de la presente investigación, mediante la cual se presentará el tipo de investigación, el ámbito de estudio, las técnicas e instrumentos utilizados para el estudio de la presente investigación, entre otros.

En el capítulo IV, en base a los resultados obtenidos del estudio, se realizará la contrastación y presentación de los resultados, así como de su respectiva discusión conforme a lo planteado en los diversos objetivos de la investigación.

Finalmente, en el Capítulo V, se mostrarán las conclusiones y recomendaciones relativas a la hipótesis del estudio, bibliografía y anexos recogidas en base a ello.



CAPÍTULO I: FUNDAMENTOS TEÓRICOS DE LA INVESTIGACIÓN

1.1 Marco Teórico

En este apartado procederemos a describir y analizar tres diferentes teorías en las cuales se desarrollan distintos postulados que contribuirán al entendimiento del presente problema de investigación:

1.1.1 Teoría del delito

Explica el concepto de delito como una acción, típica, antijurídica, culpable y punible; asimismo, damos a conocer que para que exista acción esta, debe ser voluntaria y humana. Existe ausencia de acción cuando se cumple:

F = fuerza física irresistible Ej. Un hombre que empuja a otro al realizar un trabajo y el señor que fue empujado, provoco un accidente

E = Cuando la persona se encuentra en estado de inconsciencia Ej.

Un sonámbulo

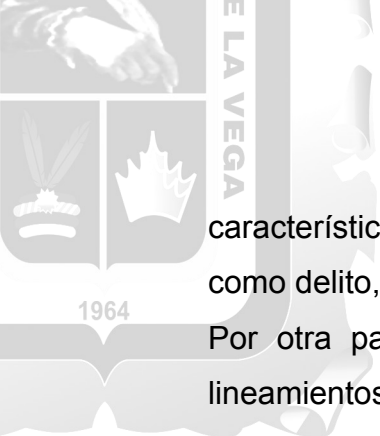
A = Acto reflejo (Kcomt, 2020, p. 1)

Figura 1

Teoría del delito

Nota: (Manzanosite,2021, p. s/n)

La teoría del delito, se ocupa del estudio de las características que debe reunir cualquier conducta para ser reconocida como tal; así, para el profesor Muñoz Conde, la teoría General del delito es aquella que se encarga de las



características comunes que debe poseer cualquier hecho para ser reconocido como delito, sea este una estafa, fraude, homicidio u otros.

Por otra parte, esta teoría, da seguridad jurídica al sujeto, pues facilita los lineamientos válidos de análisis de cada una de las partes contempladas en la parte especial.

Podemos mencionar algunas características que deben ser consideradas para que sea un delito:

El delito debe ser una acción u omisión

La omisión o acción deberá ser dolosa o culposa

La conducta que realice el sujeto debe ser penado por la ley

En realidad, esto es lo que nos resalta el Código Penal, más la doctrina agranda este contexto facilitándonos los elementos del delito como son:

Acción. - Entendemos por acción al comportamiento humano revelador en el mundo exterior, basada en la voluntad del individuo.

Tipicidad. – Consideramos que una acción es típica cuando cumple los requisitos que debe tener para ser considerado un delito.

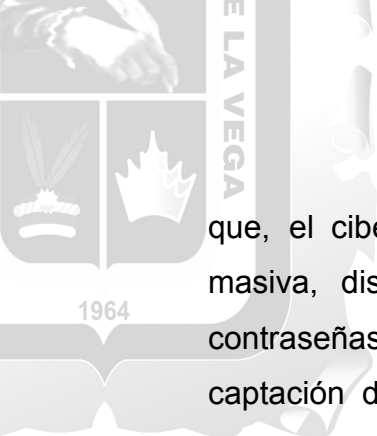
Antijurídica. - La acción típica es considerada antijurídica cuando está prohibida. Existen algunas excepciones como cuando: una conducta típica no es antijurídica si existiera una razón de justificación.

Culpabilidad. - finalmente, se considera culpable cuando se reúnen los dos fundamentos como son típica y antijurídica; es decir, se haga responsable del hecho al autor.

Otros presupuestos de Punibilidad. – para ser considerada punibles debe la acción ser típica, antijurídica y culpable, salvo algunas excepciones como cuando se adjunta otros presupuestos como son: las condiciones objetivas de punibilidad y la ausencia de causas de exclusión de la punibilidad. Así pues, el dolo se estimaba desde el punto de vista de esa teoría como forma de la culpabilidad (Bramont, 2002, p. 133)

Después de lo señalado, podemos sostener que la teoría del delito es la conducta humana en base a características que debe cumplirse para poder ser considerado un delito.

El phishing cumple con los fundamentos que debe tener un delito como son: acción, tipicidad, antijuricidad y culpabilidad; es considerado como acción ya



que, el ciberdelincuente realizó un acto que fue enviar los emails en forma masiva, diseñados estos con contenido malicioso donde busca robar las contraseñas de las tarjetas de débito/crédito lo que tendrá como consecuencia la captación de más víctimas. Es tipificada porque los hechos ocurridos (por el phishing), se adecuan a la conducta de tipo penal; es antijurídico por que los hechos realizados son contrarios al ordenamiento jurídico; es hallado culpable, desde el momento que es imputable por que el sujeto conoce la tipicidad de su conducta.

Figura 2

Tareas de Phishing

	Agentes	Tareas
Alta complejidad Baja participación	<ul style="list-style-type: none">• <i>Phisher</i> y colaboradores• Empresa atacada• Víctimas	<ul style="list-style-type: none">• A la espera de los datos• Ejecución de código malicioso
Media complejidad Media/Alta participación	<ul style="list-style-type: none">• <i>Phisher</i> y colaboradores• Víctimas• Empresa suplantada (si existe)	<ul style="list-style-type: none">• A la espera de datos (aplicaciones autónomas y <i>Phishing</i> de motor de búsqueda)• Ejecución de códigos maliciosos para la consecución de datos (robo de datos, <i>pharming</i>)
Baja complejidad Alta participación	<ul style="list-style-type: none">• <i>Phisher</i> y colaboradores• Víctimas• Empresa suplantada	<ul style="list-style-type: none">• A la espera de datos (vía respuesta correo electrónico o visita a la web fraudulenta)

Nota: (Leguizamón, 2021, p.17)

1.1.2. Teoría del delito informático phishing

Esta teoría se base en que el creador intelectual de la apropiación ilícita intenta u obtiene información confidencial como son las contraseñas, claves de las tarjetas, claves de las cuentas bancarias y otros, en ese sentido se ha intentado explicar la forma como se configura este delito, así se tiene que a través de este sistema, el estafador utiliza una página o envía correos de entidades con la cual mantenemos una relación donde nos anuncia que nuestra cuenta corriente ha sido cancelada, nosotros en



nuestra preocupación por ello, no discernimos en el momento y damos la información que nos solicita a veces sin darnos cuenta que hay datos que no se deben de dar a través de las páginas o correos, es allí cuando sucede la apropiación (Ruiz, 2020, p. 6)

Es en este delito que el sujeto activo delimita el iter criminis a seguir y un aspecto peculiar es que actúa en escenarios y horarios en donde hace incurrir a error al sujeto pasivo, quien valiéndose de los medios tecnológicos expresa la información que le es solicitada, entonces si se quiere establecer una conducta típica, puede ser mencionado como aquel sujeto que valiéndose de sistemas informáticos bancarios, emails masivos de publicidad induce al otro a llenar los datos que le solicitan, con la intención de obtener información personal, patrimonial, se debe tener en cuenta que es delito se consuma desde el momento que el sujeto activo toma conocimiento de los datos personales, entiéndase contraseñas del agraviado, no siendo necesario que haya existido un gasto o traslado de información para que se configure este tipo penal.

Continuando con nuestra investigación, Bramont-Arias sostiene que “la teoría del delito, se encarga del análisis particular que debe agrupar cualquier comportamiento para ser nombrada como delito” (Bramont, 2002, p. 130)

La teoría general del delito proporciona seguridad jurídica al sujeto, pues genera la directriz válida de análisis de cada una de las formas contenidas en la parte especial. Si bien es cierto, no existe un articulado que delimite la premisa fáctica y por ende la consecuencia jurídica, se ha creído conveniente en esta teoría desarrollar todos los elementos que comprende la teoría del delito, a la luz de esta modalidad informática delictiva.

En este tipo de delitos, la configuración se realiza de la siguiente manera:



1.1.2.1. Acción

El sujeto activo es el ciberdelincuente que tiene acceso ilegal a la base de datos del usuario, y lo configura a través del envío masivo de correos electrónicos donde incluyen diversos enlaces de entidades financieras simulando ser auténticas solicitando a la víctima registrar sus datos personales, código de tarjetas clave, DNI y otros dando lugar de esta forma a cometer tal delito.

1.1.2.2. Antijuricidad

Este delito lesiona el bien jurídico de patrimonio , el mismo que es entendido como la vulnerabilidad a nuestra información confidencial que utilizamos para tener acceso a nuestras cuentas bancarias, trayendo como consecuencia que los delincuentes usen esta información para fines ilícitos (retiro fraudulento de dinero); Asimismo, se lesiona el derecho a la intimidad , porque al sustraer nuestras claves y números de cuentas están vulnerando una información que solo nosotros debemos conocer (vulnera la privacidad).

1.1.2.3. Culpabilidad

Este delito será de resultado consumado cuando efectivamente haga el mal uso de las cuentas bancarias a través de sus claves generándose un perjuicio patrimonial; es decir en la disminución o variación negativa del patrimonio económico.

1.1.3. Teoría Punitiva del Estado

La teoría punitiva del Estado, es definida por López Pérez, quien señala sobre el particular que,

El Estado es el único que tiene potestad para aplicar las sanciones penales, previo al seguimiento de un debido proceso penal; siendo el que tiene el dominio del proceso de criminalización secundaria. Es el operador penal judicial quien, materializa las sanciones penales (López Pérez, 2020, p. 1)



Este poder sancionador que tiene únicamente el Poder Judicial órgano a quien se delega esta función, ejercerá dicha función sobre aquella nación jurídicamente organizada y sobre un territorio en concreto, y siguiendo esta línea de pensamiento, se tiene que,

La función sancionadora tiene por finalidad la protección de los diversos derechos fundamentales o como es denominado bien jurídico protegido, como lo es el honor, la propiedad, la integridad corporal, entre otros, pero en el caso del delito informático del phishing el bien jurídico será el patrimonio, puesto que, es el bien o interés que está protegido por el Derecho, lo que la norma, mediante la amenaza de la pena, tiende a tutelar, a proteger de posibles agresiones (Peña Gonzales, 2010, pp. 81-82)

Entonces, se puede señalar que el bien jurídico

es el interés jurídicamente protegido es lo que la comunidad colectiva fija como su principio básico para lograr el desarrollo armónico y pacífico. El delito debe contener una conducta humana que sea capaz de provocar la puesta en peligro, real claro e inminente o la lesión de un bien jurídico de conformidad con el artículo IV del TP del Código penal. La defensa del bien jurídico es lo que le da sentido a todo el ordenamiento jurídico penal (Bramont Arias, 2002, p. 173).

A nuestro entender el derecho penal se basa en la necesaria tutela de los bienes jurídicos como finalidad de cada ordenamiento. Protege y tiene en la pena el mecanismo eficaz y adecuado como consecuencia jurídica de posible aplicación para aquel que ha infringido las normas establecidas.



Asimismo, se requiere que tanto el estado como la tecnología estén siempre al mismo nivel pues a medida que la tecnología avanza, los mecanismos de protección a través del código penal también deben ser más severos contra el delito informático phishing.

El derecho de castigar del estado o ius Puniendi es la facultad que se le ha otorgado al estado para imponer una pena o una medida de seguridad y está integrada por un sistema de principios denominados delictivos al derecho a castigar, mediante los cuales se logra introducir un “límite” ante posibles excesos, así resulta necesario en los tiempos actuales la búsqueda de alternativas o la cárcel lo cual se encuentra entre los objetivos pendientes del derecho penal en cuanto a los delitos informáticos como es el phishing, donde existen vacíos legales. (Sánchez, 2015, p. 54)

Además, de acuerdo al profesor Rebollo Puig

la persecución y represión estatal de un Estado es la misma que detenta el juez y autoridad administrativa con competencia para sancionar, toda vez que la potestad sancionadora del Estado o ius puniendi estatal es una sola que emana del Estado y puede manifestarse a través de la responsabilidad civil, penal o administrativa sancionador (Puig, 2006, p. 93)

No menos importante, Luquin ubica los fundamentos dogmáticos que acreditan la aplicación de sanciones penales por parte del Estado, ya que, sin razones convincentes, opina, que “la legitimidad del ius puniendi depende de la legitimidad de la forma de Estado, y considera que sólo un Estado social y democrático de Derecho garantiza tal acción” (Luquin, 2006, p.113).

En el caso de los delitos informáticos, dada la globalización, el avance tecnológico para el Estado ha constituido un verdadero reto proteger a todos aquellos bienes que se ven vulnerados por el uso indebido de medios tecnológicos, cuya consecuencia lógica es que si el Estado quiere ejercer el



ius puniendi tiene que previamente tipificar este tipo de conductas delictiva, ello como parte del principio de legalidad que orienta a todo ordenamiento jurídico.

1.1.4. Teoría Seleccionada

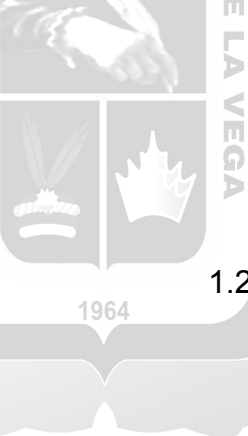
La presente tesis a través de su marco teórico, se encuentra respaldada por la teoría del delito de phishing, porque se considera que el Estado debe actuar a través del derecho penal haciendo cumplir los reglamentos y normas que se han regulado frente al delito informático del phishing y crear un nuevo inciso en el artículo 264 del Código Penal que aplique penas más severas frente a este delito, paralelamente a ello, antes de invocar la facultad sancionadora, el Estado como garante de los derechos debe promover campañas publicitarias a través de los medios de comunicación la forma de prevenir estos tipos de delitos como es el phishing.

Finalmente, sobre esta investigación acoge el marco teórico imperante para el desarrollo y comprobación de la hipótesis, sin desmerecer cada teoría desarrollada, pues todas estas aportan y contribuyen a la postura de la tesis, pero sí se ha creído conveniente escoger aquella teoría que es la guía principal de este trabajo de investigación.

El phishing es una de las estafas más antiguas y mejor conocidas de Internet. Podemos definirlo como un tipo de fraude en las telecomunicaciones que emplea trucos de ingeniería social para obtener datos privados de sus víctimas.

Un ataque de phishing tiene tres componentes:

1. El ataque se realiza mediante comunicaciones electrónicas, como un correo electrónico o una llamada de teléfono.
2. El atacante se hace pasar por una persona u organización de confianza.
3. El objetivo es obtener información personal confidencial, como credenciales de inicio de sesión o números de tarjeta de crédito (Avast phishing, 2022, p.1)



1.2. Investigaciones

Actualmente, se puede decir que existe gran variedad de investigaciones sobre los delitos informáticos en forma general, de todos ellos, en especial el phishing, ha logrado tener una figura importante dentro de los delitos de apropiación ilícita. Como es de suponerse, a medida que avanza la tecnología lo cual nos permite tener muchas facilidades, mayor comodidad, de la misma forma es una preocupación para el estado y por ende los usuarios porque estamos más expuestos al delito de apropiación ilícita a través de los correos electrónicos, violación de información como contraseña de las tarjetas, clonación de contraseñas en las cuentas bancarias y otros más.

Una de las tantas formas que utiliza el estafador para apropiarse de un bien ajeno es el envío masivo de correos electrónicos donde se muestran páginas que brindan oportunidades (aparentemente) para realizar un negocio, para poder conseguir trabajo, o para realizar estudios en otros países, etc. que a veces es tentativo y le piden sus datos entre ellos contraseñas y el usuario sin darse cuenta proporcionan tal información.

1.2.1. Antecedentes Internacionales

Se han encontrado Tesis Internacionales, entre ellos la tesis de maestría en derecho penal desarrollada por el Abogado Valle Matute, Juan Carlos presentado a la Universidad Regional autónoma de los Andes, de Quevedo – Ecuador, titulada “El Delito Informático de Phishing”, tesis que fue desarrollada en el año 2013 y que llega a las siguientes conclusiones:

1. Los sujetos o personas que efectúan o cometen los delitos informáticos, en este caso específico el delito de phishing, son los Hackers o criminales informáticos, que aprovechan sus conocimientos (experto) de la informática (redes, programación, etc.) para utilizar la vulnerabilidad de un sistema con un fin, obtener información privada.



2. De la investigación realizada con referencia a los diferentes tipos de delitos informáticos, debo mencionar que el delito de phishing es la modalidad más lucrativa, y en la gran mayoría de legislaciones internacionales se la considera ilegal, la misma que no se encuentra establecida en nuestra normativa penal.
3. En los últimos años, Ecuador ha tenido avances con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo cual es importante para el desarrollo tecnológico en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se comentan relacionados con las tecnologías.
4. Frente a esta falencia legal, hay que agregar que este tipo de infracciones son difíciles de descubrir o perseguir, debido a que los sujetos activos actúan sigilosamente con herramientas capaces de borrar toda huella de intrusión o de la consumación del delito; se debe ya impulsar estos avances tecnológicos que son realidades sociales y para las cuales los ecuatorianos estamos casi indefensos (Valle,2013, p.125)

Por otro lado, hemos encontrado el estudio en computación de los bachilleres Gonzales Juárez Diego y Peña Enríquez José, presentado en la Universidad Nacional Autónoma de México que lleva por título “Estudio del impacto de la ingeniería social – phishing”, 2013, donde sus conclusiones son:

1. Correos electrónicos. Usuarios atraídos por una serie de engaños muy simples para ingresar en diversos sitios y obtener su información personal.
2. Suplantación de páginas Web. Se basa en comprar el dominio de una página web que se parezca mucho a la página oficial y de esta forma cuando la gente intente acceder a este servicio la información se le proporcionara al administrador de esta página.



3. Instalación de malware. Al acceder a una página o descargar un archivo el equipo se infecta con un programa llamado keylogger| este graba todo lo que hace el usuario con el teclado y lo envía al correo de la persona que lo programo.

4. Familiarcita Exploit: Basado en la familiaridad y la confianza que las personas tenemos al reaccionar a peticiones de individuos que nos son relativamente conocidos.

5. Trashing: Revisar los desperdicios y la basura nos puede proporcionar información de los usuarios.

6. Robo de información de cuentas bancarias. Se obtiene la información como la clave del usuario y con diversos métodos se obtiene la tarjeta de crédito de la víctima o se clona esta misma después se vacía la cuenta. A base del estudio también podemos proveer que el siguiente blanco para los hackers son los dispositivos móviles, primeramente porque nadie espera un ataque en su Smartphone o en su Tablet pero sobre todo que no existen herramientas tan desarrolladas para la seguridad de dispositivos móviles que para computadoras personales, viendo esa deficiencia es importante aplicar buenas prácticas de seguridad en estos dispositivos y no dejar todo el cargo de la responsabilidad a los programas automáticos (Gonzáles, 2012, p. 109)

Siguiendo con nuestra investigación, hemos encontrado la tesis de Mayra Sheila Mariana Leguizamón quien pretende obtener el grado en criminología y seguridad por la universidad Jaume de España teniendo como título “El Phishing” para lo cual detalla sus conclusiones:

1. El avance de los medios informáticos y de la tecnología trajo consigo grandes ventajas en la vida de la población. Estos avances facilitan la realización de cosas cotidianas y es muy favorable en muchos aspectos en la vida de una persona. Pero no todo trajo beneficios. Estos avances también facilitan que los delitos comunes se trasladen a las redes. Como es el caso que hemos tratado: el



PHISHING. Como hemos visto es un tipo de estafa pero que se produce en la red. Al cobrar tanta importancia en los últimos años el uso de internet, se abrieron las puertas para que también sea un medio donde se pueden cometer diferentes delitos. Podríamos decir pues, que todas estas ventajas que nos trajo la evolución, también tiene su parte negativa, y es que en internet y en la red se producen casi tantos delitos como en la vida real.

2. Como ya hemos visto, las víctimas del phishing corresponden a un ámbito bastante amplio donde nos encontramos con personas individuales, como empresas o instituciones. No se centra en un tipo de víctima en concreto, sino que todos pueden ser víctimas del phishing. Por tanto, es necesario que se implementen medidas de lucha contra el fraude en España. Este delito va en aumento, como se ve en los últimos años que nacieron el smishing y el vishing, y es muy importante evitar la comisión de los mismos. Una forma que hoy en día poco se ve por España, pero puede resultar muy exitosa, es la realización de campañas de prevención contra el phishing. Advertir a la población de la existencia de este delito, que conozcan cuales son los riesgos de navegar por internet. Es necesario cambiarles un poco el pensamiento.

3. Para combatir el phishing, es necesaria una colaboración global e internacional. Este delito evoluciona de forma diferente en cada país. Si todos colaboran entre sí, se pueden conocer todos los tipos de phishing existentes y combatirlos con mayor eficacia. Cada país debería aportar toda la información necesaria para llegar a una conclusión conjunta que ofrezca resultados positivos. El impacto económico del phishing es bastante elevado, causa pérdidas de dinero en los países y esto es algo lo suficientemente negativo para que todos colaboren entre sí. Por tanto, la creación de legislación y directivas que traten el tema es primordial. La poca legislación existente deja espacios en blanco y muchos de estos delitos quedan totalmente impunes. Esto es así, porque el ataque se produce en un



país, pero los beneficios van a otros. Al no haber legislación que regule estos temas, el phishing va en aumento y los phishers se consideran inmunes. Ese sentimiento les lleva a seguir cometiendo estafas y mejorando sus técnicas.

4. Con referencia a la evolución del phishing, muchas personas coinciden en que llegó a su máxima evolución mientras que otro gran porcentaje considera que esto está recién empezando. Y de acuerdo con esta última idea, si tenemos en cuenta la evolución del mismo en los últimos años, es bastante probable que en los años que nos preceden las técnicas vayan aumentando considerablemente. Es más, los phishers cada día son más profesionales, utilizando esta técnica incluso en grupos u organizaciones criminales. Últimamente los emails eran más personalizados. Lo que queda es estar lo suficientemente preparados en un futuro para conocer estos ataques y su evolución y poder solucionarlo.

5. El phishing es un fenómeno actual y real. Utilizan la ingeniería social y por tanto es importante la concienciación del usuario. (Leguizamon, 2021, p. 45)

Encontramos también a través de nuestra investigación al abogado Castillo Rubiano, Oscar, quien en el al 2021 desarrollo la tesis en la Universidad Externado de Colombia, quien propone su tesis para alcanzar el grado de magister en derecho Informático a través de su investigación titulado “Phishing: día de Pesca”, veamos a continuación lo que nos manifiesta:

1. La ciberdelincuencia es un fenómeno global creciente que demanda soluciones globales inmediatas, en esa línea los Estados han venido adoptando decisiones de orden legislativo y de cooperación internacional, pero falta un largo camino por recorrer, los desafíos son titánicos y los esfuerzos multilaterales



deben continuar e intensificarse, so pena de incurrir en rezagos por tratarse de fenómenos criminales que están en constante evolución. Las medidas adoptadas por los Estados para hacer frente a la cibercriminalidad son de naturaleza represiva principalmente, y es meritorio, pero además resulta imperativo implementar acciones preventivas e intensificar las ya existentes.

2. La consolidación de una verdadera cultura de ciberseguridad se erige como un importante estandarte (primera línea de defensa) para evitar la consumación de fenómenos criminosos en el ciberespacio, en la medida en que se reduzca el analfabetismo digital, los índices delincuenciales también lo harán. Los avatares propios de la criminalidad cibernética, particularmente el acecho del phishing, en gran medida, se sortean promoviendo un comportamiento en línea más seguro y sensibilizando a los internautas sobre las consecuencias de no atender las buenas prácticas de la ciberseguridad.
3. En materia de ciberseguridad, los expertos coinciden en señalar que el factor humano es el eslabón más débil (errores de capa 8) del ecosistema digital. La mayoría de ataques de phishing tienen éxito no precisamente debido a las virtudes del atacante, sino a las debilidades de la víctima que interactúan sin medir las consecuencias económicas y sociales de sus actos, sumado a inexistentes o frágiles medidas de seguridad, (Castillo,2021, p.61)

1.2.2. Antecedentes Nacionales

Asimismo, Solano, en su tesis de Pregrado de la Universidad Nacional del Santa presenta su obra titulada “El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. propuesta de incorporación del artículo 7-a en la ley de delitos informáticos 30096”, en dicha tesis, se dio a conocer las siguientes confirmaciones:



1. Ninguno de los tipos penales regulados en el Código Penal permite subsumir adecuadamente los supuestos fácticos del phishing, lo que favorece la impunidad de la conducta.
2. Los tipos penales regulados en la Ley de Delitos Informáticos no permiten subsumir adecuadamente todas las modalidades de phishing, lo que ocasiona la impunidad de la conducta.
3. En el distrito fiscal del Santa, las denuncias por phishing son archivadas en su gran mayoría, siendo uno de los factores más determinantes para el archivo de los casos la deficiente redacción de los tipos penales regulados en la Ley de Delitos Informáticos.
4. Es necesaria la creación de un tipo penal específico, que regule adecuadamente el phishing, donde se establezca con precisión la conducta típica, el bien jurídico protegido, así como una pena en concordancia con la magnitud del daño causado a los bienes jurídicos (Solano, 2021, p. 116)

Seguidamente, se tiene la tesis de pregrado presentada por Mengoa Valdivia Mariel Melissa, titulada “Punibilidad del comportamiento de phisher -mule en el delito de fraude informático en el Perú” realizado en el año 2021, y que arriba a las siguientes conclusiones:

1. Se verifico que la conducta del phisher-mule no se logra tipificar por lo que se necesitaría hacer un estudio concienzudo para su correcta tipificación e introducción en el código penal o le ley especial, por lo que se recomienda hacer un estudio más afondo del comportamiento de este individuo.



2. El acceso ilícito en el sistema informático, es sancionado en el Perú, pero no hay un tratamiento claro del delito de estafa informática, el cual se reduce a la previsión del artículo 196-A, numeral 5, teniendo en consideración el Código Penal, que reporta como estafa agravada, lo cual es muy llamativo, sobre todo si tomamos en cuenta que el delito de fraude informático implica la conexión con otros comportamientos criminales como la de phisher - mule, quien colabora activamente en la consumación del acto delictivo y del daño al patrimonio de la víctima.
3. La ignorancia deliberada es recurrida por los encargados de la defensa, Esta doctrina en esencia se aparta de las exigencias para la imputación a título del dolo ofreciendo como solución la intencionalidad, que es relevante en el derecho penal peruano. (Mengo, 2021, p. 33)

También, en su tesis titulada “la tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en lima, 2020” de Ventura Quijano Mishel Alisson realizado en el año 2021, presenta la siguiente conclusión:

1. El sistema judicial penal tiene como una de sus prioridades de trabajo, subsanar las deficiencias legales que existen en el Perú para poder lograr identificar a los autores de la comisión de los delitos cibernéticos y la dificultad de los cortos plazos de investigación.



2. Uno de los retos para que el Perú realice una transformación digital conlleva a hacer una reflexión ante amenazas sobre la vulneración.
3. Para obtener seguridad informática; es necesario la protección de infraestructura de la información y establecer la conformación de un consejo sobre ciberseguridad, con el objetivo de generar una gestión en riesgos informáticos.
4. La contribucion de información tanto en sectores públicos y privados necesaria para denunciar ataques cibernéticos y brindar a los usuarios estabilidad informática. (Ventura,2021, p.77)

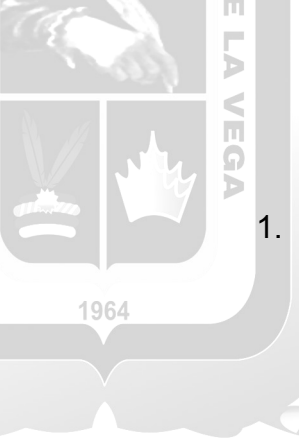
Asimismo, se tiene la tesis de pregrado presentada por Olivares y Ceras, titulada “Delitos informáticos y la evidencia digital en el proceso peruano del Distrito judicial de Junín” desarrollada en el año 2020, dichos autores llegan a las siguientes conclusiones:

1. Se determinó que los resultados del objetivo general muestran que No existe una relación directa y significativa entre los delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020. ($p=0,952>0.05$). Donde la mayoría de los operadores de derecho, consideran que el nivel en que se aplica la legislación para los delitos informáticos en el proceso peruano del distrito judicial de Junín, 2020 es medianamente suficiente (62.5%). Y la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%).



2. Se determinó que los resultados del objetivo específico 1 muestran que No existe una relación directa y significativa entre los delitos informáticos y el valor probatorio en el proceso peruano del Distrito Judicial de Junín, 2020. ($p=0,632>0.05$). Donde la mayoría de los operadores de derecho, consideran que el nivel de valor probatorio en el proceso peruano del distrito judicial de Junín, 2020 es alto (60.0%)
3. Se ha determinado que los resultados del objetivo específico 2 muestran que No existe una relación directa y significativa entre los delitos informáticos y los alcances de la regulación en el proceso peruano del Distrito Judicial de Junín, 2020. ($p=0,509>0.05$). Donde la mayoría de los operadores de derecho, consideran que el nivel de alcances de regulación en el proceso peruano del distrito judicial de Junín, 2020 es alto (37.5%)
4. Se estableció que los resultados del objetivo específico 3 muestran que No existe una relación directa y significativa entre los delitos informáticos y la Información digital en el proceso peruano del Distrito Judicial de Junín, 2020. ($p=0,884>0.05$). Donde la mayoría de los operadores de derecho, consideran que el nivel de evidencia digital en el proceso peruano del distrito judicial de Junín, 2020 es muy alto (40.0%) (Olivares, 2021, p. 139)

Por otro lado, se tiene la tesis de pregrado presentada por Vilca Aíra Gaby Lizet titulada “Los hackers: delito informático frente al código penal peruano” realizada en el año 2018, presentando las siguientes conclusiones:



1. La falta de una información adecuada sobre los límites de la tecnología informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.
2. Al hacer un análisis comparativo de legislación con otros países, se determinó que Perú es un país que ciertamente regula los delitos informáticos, sin embargo, lo hace de una forma deficiente ya que es de forma generalizada, lo que propicia algunos vacíos legales que imposibilitan una investigación forense en materia informática.
3. La comisión de delitos emergentes en la internet es un problema que afecta a la sociedad mundialmente, tanto niños como adultos, no importando edad ni género, se ven vulnerables a caer en las redes de algún delito o crimen cibernético, por lo que es necesaria la capacidad del perito o investigador en la escena del crimen y el correcto procedimiento en la misma para lograr la resolución óptima del caso.
4. La generalidad de los delitos informáticos en Perú únicamente provoca la ignorancia de la sociedad en el tema y es imperativa la existencia de normas que especifiquen los hechos o actos que se consideran como hackers para un mejor control del mismo.
5. Es indispensable y necesaria la correcta instrucción para agentes de investigación de crímenes informáticos, ya que son estos quienes tienen bajo su control los elementos o indicios que pueden ser considerados como evidencias y pruebas 91 durante el proceso penal, por lo que la manipulación de estos debe resguardar su contenido.

La evidencia digital debe ser meticulosamente recaudada y procesada para luego ser presentada en la corte cumpliendo los requisitos de admisibilidad.



Es esencial garantizar la veracidad de la evidencia digital durante el proceso de investigación, y para ello es indispensable contar con los conocimientos y habilidades especiales en la recaudación, embalaje y manipulación de este tipo de evidencia (Vilca, 2018, p. 90).

1.3. **Marco conceptual**

1.3.1. **Phishing**

Hidalgo y Solano, entienden, el phishing como “el envío masivo e indiscriminado de spam conteniendo información falsa, tendiente a la obtención de datos personales privados” (Hidalgo y Solano, 2021, p. 31)

En ese mismo orden de ideas, Acurio, explica que,

el phishing, se encuentra diseñada con la finalidad de robarle la identidad del usuario obteniendo información privada que es usada por medio de engaños, utilizando ventanas emergentes o mensajes de los correos electrónicos. En otras palabras, el phishing tiene como objeto buscar grupos vulnerables para inducirlos en error (Acurio, 2018, p. 35)

Finalmente, una de las aproximaciones del phishing, es que es una de las formas más clásicas de comisión de ilícitos penales, que con ánimo de lucro utilizan el engaño para inducir en error al usuario y provocar un perjuicio económico (ventura, 2021, p. 11)

1.3.2. **Bien jurídico**

Claus Roxin entiende como bien jurídico “a todas las circunstancias y finalidades que son necesarias para el libre desarrollo del individuo, la



realización de sus derechos fundamentales y el funcionamiento de un sistema estatal edificado sobre esa finalidad” (Roxin, 2013, p. 11)

Los bienes jurídicos son bienes vitales, fundamentales para la existencia en común, abarcan aspectos individuales, colectivos e institucionales que concurren en los procesos de relación del individuo dentro de su comunidad y del sistema social y del funcionamiento del mismo. El Derecho penal asume la tutela y ofrece una "concreción material" y no ideal o abstracta de los bienes jurídicos (Olaechea, 1998, p. 2)

El bien jurídico es el interés jurídicamente protegido, es aquello que la sociedad lo establece como su fundamento básico para lograr un desarrollo armónico y pacífico (es un valor de carácter inmaterial)

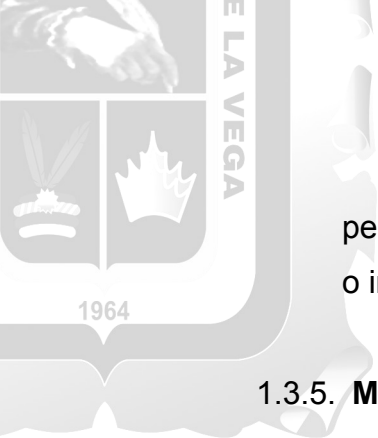
1.3.3. **Mecanismos prevención**

Los mecanismos de seguridad preventivos “son todas aquellas acciones que van encaminadas a prevenir cualquier amenaza a la confidencialidad, integridad y disponibilidad de los elementos críticos del sistema” (Bauer, 2001, párraf. 1)

Para la presente tesis, el mecanismos de prevención debe ser entendido como aquella implementación normativa y/o reglamentaria que tenga por objetivo evitar la comisión del acto delictivo.

1.3.4. **Mecanismos sancionatorios**

Son los que tienen como finalidad castigar al agente de la afectación de la libertad sindical, habría que buscar la implantación tanto de sanciones de carácter económico, cuanto, de carácter penal, según la gravedad y reiteración de la infracción y, para el caso de las sanciones



penales, cuando los demás medios de control social resulten ineficaces o insuficientes, como sostiene (Terradillos 2015, p. 35)

1.3.5. Mecanismo de protección

Según la RAE la palabra mecanismo es “un proceso y esta a su vez es el conjunto de actos que tienen por objeto la decisión de un conflicto o litigio que tienden a la aplicación de una ley general a un Caso concreto controvertido para solucionarlo o dirimirlo” (RAE, 2021 p.1150), en tanto debe entenderse que la palabra protección supone “Amparar, defender a alguien o algo” (RAE, 2021, s/n).

Para la presente investigación el mecanismo de protección es la utilización de los conocimientos necesarios y de los controles suficientes con la finalidad de no ser víctimas de los delitos informáticos.

1.3.6. Modalidad delictiva

Una modalidad delictiva puede definirse como aquella forma en la que puede manifestarse un delito.

Modus Operandi: Es un comportamiento aprendido que evoluciona con el tiempo, como delincuentes adquieren experiencia y confianza los



delincuentes remodelan continuamente sus modus operandi para satisfacer las demandas de delincuencia (Benavidez, 2014,p. 36).

Del mismo modo, el Diccionario de la Real Academia Española(2005) define el Modus Operandi como la manera especial de trabajar o actuar para alcanzar el fin propuesto. Policialmente es una expresión que define el método con el que se realiza el acto delictivo; es decir, la forma en la que un delincuente desarrolla sus actividades de acuerdo a su estilo personal (Bernal,2019,p. 25)

CAPÍTULO II: EL PROBLEMA, OBJETIVOS, HIPÓTESIS Y VARIABLES

2.1 Planteamiento del problema

2.1.1 Descripción de la Realidad Problemática

La globalización es una manifestación que se viene presentando en el siglo XXI a través del cual, ha permitido el avance o crecimiento y desarrollo de



las diversas empresas públicas y privadas en diversas áreas del estado; paralelamente a ello, la tecnología cumple un rol importante en este siglo XXI por que la mayoría de actividades bancarias, comerciales, contractuales, civiles y familiares se desarrolla a través del uso de esta tecnología, hecho que se evidencia aún más en el contexto sanitario actual en la que prácticamente es imposible concebir una actividad normal donde es indispensable contar con internet a través del computador.

A pesar que el internet y el uso de estos equipos tecnológicos son buenos y generan el desarrollo, la educación y otros avances, por otro lado también, se ha podido observar que se está haciendo un mal uso por parte de los sujetos que se valen de estos medios electrónicos para poder cometer los actos ilícitos a lo cual el derecho lo ha regulado, pero no es suficiente.

En el Perú, esta clase de delitos ha ido en aumento día a día donde surgen nuevas intervenciones es así como el Ministerio Público ha registrado más de 21,000 denuncias al año. Asimismo, la ciberdelincuencia se acrecentó en periodos de pandemia, porque los usuarios hicieron mayor uso de las plataformas virtuales (Diario Gestión, 2021, p. 1)

Es por ello que, “La fiscal de la Nación, Zoraida Ávalos, dispuso la creación de la Unidad Fiscal Especializada en Ciberdelincuencia para hacer frente al incremento en la incidencia criminal que se produce en internet (Diario Peru 21, 2021, p.16)

El Estado a través del derecho y sus manifestaciones, busca perseguir y sancionar el delito para proteger el bien jurídico tutelado; en el caso de los delitos informáticos aun no es suficiente, porque todavía no se supera las dificultades para su aplicación como son: las nuevas conductas delictivas del delito informático, los mismos que vienen lesionando derechos fundamentales contenidos no solo en documentos nacionales como es la carta magna, sino que tienen su respaldo y protección en tratados internacionales, uno de ello es el Convenio de Budapest, al que se encuentra ratificado nuestro país y por ende es de obligatorio cumplimiento;



y por lo tanto es a través de estos instrumentos que el Estado ejerce su *ius puniendi* para tutela el bien jurídico, que el caso de los ilícitos informáticos son la información, la ley de protección de los datos, la integridad de las personas, la integridad de los datos (artículo. 186º inciso 3 del código penal) y (en la ley 30016 y su modificación a la ley 30171).

La falta de los mecanismos de prevención y protección por parte del estado de los bienes jurídicos protegidos ha ocasionado que haya incremento de las nuevas formas de criminalidad como es el delito informático. El estado a través de la SBS tiene una función importante dentro del mecanismo de prevención y control

La doctrina ha advertido esta situación, pues “en relación a esta forma delictiva, la ley penal tiene por finalidad prevenir y sancionar las conductas que afectan los datos informáticos y bienes jurídicos que resulten afectados como son el patrimonio, la fe pública y la libertad sexual” (Villavicencio, 2014, p.17)

Villavicencio, refiriéndose a Klaus indica que considera respecto a la tarea del derecho que, “la misma no puede mantenerse en base a categorías, producto de teorías antiquísimas, que al día de hoy no responde a las formas de delito, para ser más específicos delitos informáticos” (ídem 2014, p.21)

Hoy en día, el incremento de nuevas formas de los delitos informáticos como el llamado *Phishing*, delito que es entendido como obtener información tal como el número de tarjetas de crédito, contraseñas, información de cuentas y otros datos personales por medio de engaños (conducta delictiva diseñado para robarle la identidad de los sujetos pasivos) por lo tanto, urge la intervención del estado de manera eficaz a través del derecho penal, todo esto se encuentra respaldado pues “los fraudes en línea se disparan en Perú ante mayor uso de internet donde agrega que en el primer trimestre del año ya van 1000 denuncias realizadas” (Diario Gestión, 2018,p.1)



Según la resolución N°930-2017 de la SBS en su artículo 9° inciso “c”, establece que “Contar con sistemas informáticos que soporten la administración, procesamiento y monitoreo de las operaciones con tarjetas de crédito” (SBS, 2020), a pesar de estos constante monitoreos, ha demostrado ser insuficiente frente a las distintas modalidades delictivas.

La Universidad Nacional de Ingeniería (UNI) podrá dictar el programa de estudio de pregrado de Ingeniero de Ciberseguridad en la modalidad presencial, tras la resolución de la Superintendencia Nacional de Educación Superior_Universitaria (Diario Gestion, 2022, p.1)

Como se advierte el problema de los delitos informáticos vienen incrementándose día a día, y que en la mayoría de los casos el Estado aún no ha encontrado formas de solucionar o prevenir este delito, donde los más perjudicados son aquellas personas que partiendo del principio de confianza, sus derechos son vulnerados.

2.1.2 Antecedentes teóricos

Partiendo desde la teoría punitiva del Estado, corresponde analizar cada una de la tesis citada anteriormente, en consecuencia, se tiene respecto a las investigaciones internacionales. La tesis de González y Peña (2012), México, titulada “El estudio del impacto de la ingeniería social- phishing” donde presta importancia al conocimiento de prevención que se debe tener frente a este tipo de delitos, partiendo de ciertas técnicas que utilizan como son a través de los correos electrónicos donde el usuario es atraído por una serie de engaños muy simple para ingresar a diferentes paginas obteniendo información personal, otra de las formas utilizadas es a través de la suplantación de las páginas webs donde el usuario creyendo que es una página de la entidad financiera, brinda sus datos y contraseñas de sus tarjetas de débito/crédito sin imaginar que consecuencia de ello serán víctimas de este tipo de delitos. Concuerdo con González y Peña en cuanto a la prevención que tenemos que tener frente a este tipo de delitos. Sin embargo, estaría por acotar que se debe culturizar a la gente a través de



espacios publicitarios mediante los medios de comunicación tanto públicos como privados, haciendo conocer este tipo de modalidad de fraude.

Una recomendación constructiva sería que los usuarios no se sientan confiados cuanto más avanza la tecnología porque los ciberdelincuentes también están maniobrando de que otra forma cometer este tipo de delito.

Los delitos informáticos de phishing están siendo muy utilizados en nuestro país, por lo que el estado como ente regulador debe incrementar leyes severas para este tipo de delitos, frente a este vacío legal, hay que adicionar que este tipo de infracciones son difíciles de descubrir o perseguir, debido a que los sujetos activos actúan sigilosamente con herramientas capaces de borrar toda huella de intrusión o de la consumación del delito; se debe ya impulsar estos avances tecnológicos que son realidades sociales y para las cuales los usuarios están casi indefensos.

El robo de información de cuentas bancarias. Se obtiene la información como la clave del usuario y con diversos métodos se obtiene la tarjeta de crédito de la víctima o se clona esta misma después se vacía la cuenta. A base del estudio también podemos proveer que el siguiente blanco para los hackers son los dispositivos móviles.

Existen muchas personas que concuerdan que la evolución del phishing, llegó a su máxima evolución mientras que otro gran porcentaje considera que esto está recién empezando. Analizando la evolución del mismo en los últimos años, es bastante probable que en los años que nos preceden las técnicas vayan aumentando considerablemente. Es más, los phishers cada día son más profesionales, utilizando esta técnica incluso en grupos u organizaciones criminales.

Coincidió con la investigación realizada por el abogado Castillo, previamente citado en el ítem anterior, al manifestar que la ciberdelincuencia es un fenómeno global que va en crecimiento y que debemos de tomar decisiones en la solución inmediata. Castillo menciona que, en Colombia, el Estado ha adoptado decisiones de orden legislativo y de cooperación internacional, sin embargo, sostiene que deberían intensificarse otra forma de prevenir este tipo de delitos. Además, estoy de acuerdo en cuanto a la consolidación de



una cultura de ciberseguridad pudiendo así evitar la consumación de fenómenos criminales quiero acotar que los sistemas financieros deben de capacitar al usuario el cómo deben de usar los medios tecnológicos a través de las paginas virtuales para realizar transferencias, depósitos, etc.

Por otra parte, con referencia a la tesista Ventura, coincido en todos los puntos mencionados en su tesis, sin embargo, quiero acotar que el Estado a través del código penal, debe incluir en uno de sus artículos un inciso donde la pena sea más severa para este tipo de delincuentes. Por otro lado, la SBS, debe estar facultada o una de sus funciones debería ser supervisar a las instituciones financieras en cuanto a la orientación que se le deba dar a cada usuario, podría ser mediante una declaración jurada donde acredite que ha tomado conocimientos sobre las medidas de prevención que debe tener frente a este tipo de delitos.

Coincido con la investigación realizada por el tesista Valle, previamente citado en el ítem anterior, en manifestar que los sujetos o personas que realizan o cometen los delitos informáticos como el delito de phishing, son los Hackers o criminales informáticos, que aprovechan sus conocimientos (experto) de la informática para utilizar la vulnerabilidad de un sistema con un fin, obtener información privada.

Coincido con la investigación realizada por el tesis de Gonzales y Peña previamente citado en el ítem anterior, al referir que los delitos cibernéticos como el phishing a veces llega mediante correos electrónicos y los usuarios atraídos por una serie de engaños muy simples para ingresar en diversos sitios y obtener su información personal caen en esta trampa, tambien ocurre una suplantación de páginas Web la cual se basa en comprar el dominio de una página web que se parezca mucho a la página oficial y de esta forma cuando la gente intente acceder a este servicio la información se le proporcionara al administrador de esta página.

Coincido con la investigación realizada por el tesista Leguizamón, previamente citado en el ítem anterior, cuando reporta que la tecnología trajo



consigo grandes ventajas y es muy favorable en muchos aspectos en la vida de una persona, pero no todo trajo beneficios.

Coincido con la investigación realizada por el tesista Solano, previamente citado en el ítem anterior que reporta que ninguno de los tipos penales regulados en el Código Penal permite subsumir adecuadamente los supuestos fácticos del phishing, lo que favorece la impunidad de la conducta.

Coincido con la investigación realizada por el tesista Mengoa, previamente citada en el ítem anterior quien establece que el avance tecnológico ha incrementado delitos como sabotaje informático, lavado de activos y fraudes.

Coincido con la investigación realizada por el tesista Olivares y Ceras, previamente citados en el ítem anterior, pues consideran que el nivel en que se aplica la legislación para los delitos informáticos es muy lento.

Coincido con la investigación realizada por el tesista Vilca, previamente citado en el ítem anterior, por la falta de una información adecuada sobre los límites de la tecnología informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

Finalmente, considero que para poder evitar que se consume el delito informático phishing debemos de hacer campañas publicitarias, sea por medio de comunicación, en las entidades financieras y otros dando a conocer cómo prevenir y de qué forma protegernos dado que la confianza depositada en las entidades financieras a través de nuestros ahorros no se deteriore al ser víctima de este delito. Asimismo, se debe proponer que las penas condenatorias sean más severas a través del Código Penal Peruano

2.2. Formulación del problema



2.2.1. Problema General

¿Cuáles son los mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva del phishing?

2.3. Objetivos

2.3.1. Objetivo General

Establecer los mecanismos de prevención y protección del bien jurídico tutelados por el estado a través del derecho penal en el delito informático phishing.

2.3.2. Objetivos Específicos

- a) **Analizar** el delito de fraude informático bajo la modalidad del phishing
- b) Sistematizar la protección de los sistemas de información del delito informático phishing
- c) Establecer el tratamiento legislativo en el derecho comparado respecto del phishing
- d) Identificar, reportar cuantas denuncias han sido registradas por este tipo de delito phishing
- e) Proponer la SBS – directiva

2.4. Delimitación del estudio

2.4.1. Delimitación Temporal

La presente investigación fue realizada en el año 2021.



2.4.2 Delimitación Espacial

Atendiendo a que la presente tesis es dogmática y busca establecer los fundamentos prevención y protección, la investigación se realizó en la provincia de Lima, de manera concreta en el Cercado de Lima – Breña, Departamento de Lima.

2.4.3 Delimitación Social

Este estudio se pudo realizar con la colaboración de las autoridades financieras y las denuncias fiscales y policiales.

2.5. Justificación e importancia del estudio

2.5.1. Importancia

La importancia se sustenta en que en los últimos años ha incrementado el delito informático phishing dado los avances tecnológicos y la crisis sanitaria por la que atravesó el país, lo cual generó que muchas más personas usaran las plataformas virtuales., porque dado el avance en la comisión de este tipo de delito, es importante proponer medidas de prevención y protección.

2.5.2. Justificación

2.5.2.1. Justificación Teórica

El presente trabajo de investigación se justifica en dar a conocer en qué medida las víctimas del delito informático phishing tiende a incidir en la búsqueda de la incorporación de nuevos mecanismos de protección frente al avance tecnológico lo cual genera que el estado este siempre a la altura de los avances tecnológicos pues a medida que este avanza, también los que dan mal uso de esta tecnología lo hacen lo cual conlleva a incorporar nuevos mecanismos



de control en el código penal y esta a su vez al convenio internacional.

2.5.2.2. Justificación Práctica

En los resultados se obtuvieron que el estado a través del código penal debe mejorar los procedimientos penales y tener un mayor alcance sancionador para contrarrestar el delito informático phishing en concordancia con los convenios internacionales lo cual permitirá la uniformidad de nuestras leyes, busca implementar los mecanismos de prevención y protección.

Que debe ser reforzado en estas nuevas modalidades que se incrementan

2.5.2.3. Justificación Social

La justificación social se sustenta en que se requiere solucionar este problema actual para el bien de la sociedad que confía en que las entidades bancarias protejan mejor sus fondos, construye a la sociedad en general, de manera concreta esta tesis permite que futuros legisladores puedan proponer nuevas medidas destinadas a la protección del bien jurídico colectivo en los delitos informáticos.

2.6. Hipótesis

Los mecanismos de prevención y protección del bien jurídico tutelados frente a la modalidad delictiva del phishing, son: la cultura jurídica de prevención y plan estratégico conjunta entre la SBS y bancos.



2.7. Variables

Variable dependiente

Prevención y protección del bien jurídico en el delito informático phishing

Variable independiente

- Cultura jurídica de prevención
- Plan estratégico conjunta entre la SBS y bancos



CAPÍTULO III

METODOS, TÉCNICAS E INSTRUMENTOS

3.1. Población y muestra

3.1.1 Población

Para la presente investigación la población está conformada por los funcionarios de las principales entidades bancarias ubicadas en el distrito de Breña como es: BCP, BBVA, BANCO DE LA NACION, INTERBANK, SCOTIABANK. Asimismo, se ha optado por considerar dentro de la población a la totalidad de usuarios de estas entidades bancarias que representan el 100%; y finalmente forma parte de la población la totalidad de los efectivos policiales especialistas de la división de alta tecnología que laboran en las comisarías del distrito de Breña.

3.1.2 Muestra

Para la presente investigación valiéndose como técnica de muestreo no probabilística por conveniencia y a elección del investigador, la muestra queda reducida de la siguiente manera:

- Jefe de la agencia (funcionario) de las siguientes entidades bancarias: BCP, BBVA, SCOTIABANK, que hacen un total de 3 funcionarios.
- En cuanto a los usuarios de estas entidades bancarias, se ha tomado como criterio aquellos que vienen siendo clientes desde aproximadamente 15 años, siendo un total de 500
- Respecto a los efectivos policiales, únicamente existe un especialista de la división de alta tecnología, en ese sentido la muestra son los 3 principales integrantes de esta división.

3.2 Diseño(os) a utilizar en el estudio



3.2.1 Tipo

Esta investigación es básica pues brinda herramientas de carácter doctrinario, las analiza, propone ciertos mecanismos que puedan darse para prevenir y proteger al usuario del delito de phishing.

3.2.2 Métodos de la investigación

3.2.2.1 Métodos generales

a) Método hipotético deductivo

Este método fue aplicado en la presente investigación pues se tomó en cuenta, la observación del problema a estudiar, creando hipótesis para explicar dicho problema, deduciendo consecuencias de la hipótesis y culminando con la comprobación

b) Método Inductivo

A través de este método se llegó a conclusiones generales, partiendo de premisas específicas

c) Método Analítico

Por medio de este método, la presente investigación analiza las normas jurídicas desde una forma general para llegar a lo específico como lo observaremos en la presente tesis.

3.2.2.2 Específicos

a) Exegético

Es exegético pues se ha hecho un análisis literal de las normas que se han visto incluidos en la presente investigación.

b) Hermenéutico

Plantea la interpretación que se le da a cada una de las normas jurídicas que se han utilizado para la presente investigación, llegando así a una consolidada hipótesis.



c) Dogmático:

El método utilizado es dogmático pues en nuestra disciplina la norma jurídica es considerada un dogma (Díaz, 1998, p.159), este patrón de estudio se enlaza con el tema de la validez de las normas jurídicas (tal y como se labora en la construcción del fenómeno jurídico).

Incidimos en un estudio dogmático circunstanciado en lo referente a los delitos informáticos en sus variadas modalidades básicas y formas agravadas (Serrano, 2021, p. 33)

Finalmente el trabajo de investigación se ubica dentro del método del derecho dogmático puesto que analiza las normas jurídicas relacionadas a la teoría del delito como base para reconocer el delito informático del phishing, asimismo, cabe resaltar que es argumentativa.

3.2.3 Enfoque de la investigación

En el enfoque utilizado en esta investigación es el Mixto pues a través del proceso, los datos obtenidos fueron agrupados, analizados y vinculados en forma cualitativa y cuantitativa para llegar a una proposición.

3.2.4 Diseño de la investigación

El tipo de diseño utilizado es no experimental pues se estudia la realidad tal cual sin alterarla.

3.3 Técnicas e instrumentos de Recolección de datos

3.3.1. Técnicas

a) Análisis documental

La información y la integración de tecnología para su transformación, hacen profundizar en el análisis



documental como mediador. El objetivo general de este proceso y estudio es enfatizar en las dimensiones lingüísticas y psicológicas. El objetivo específico busca profundizar y puntualizar sus aspectos característicos (Johann, 2012, p. 16). Se aplicó esta técnica toda vez que ha sido necesario a la revisión bibliográfica sobre el delito informático del phishing.

b) Entrevista

A través de este instrumento, se ha recolectado datos por medio de cuestionarios donde una persona calificada en el tema, absolvió las preguntas; muy en particular en esta investigación, se entrevisto a personal del DIVINDAT quienes tienen mucho conocimiento y experiencia en esta modalidad de delitos como es el phishing. Así pues, este tipo de instrumento permite una interacción entre el entrevistado y el entrevistador.

c) Encuesta:

Es una de ellas técnicas de investigación social mas usado en la ciencia sociológica que ha avanzado un estricto ámbito en la investigación científica convirtiéndose en una actividad cotidiana de la que todos participamos en algún momento ((Fachelli, 2015,p.3).

Se realizó la encuesta a los administradores de las agencias bancarias como BCP, SCOTIABANK, BANCO DE LA NACION; BBVA y personal civil.

3.3.2 Instrumentos

1. Ficha de análisis documental
2. Guía de encuestas
- 3.. Guía de entrevistas

3.4 Procesamiento de Datos



Es todo desarrollo que sigue el observador desde que reúne información, hasta la presentación del mismo; sin embargo, este proceso para por tres periodos como son: recolección de datos y/o entrada, procesamiento y presentación; Asimismo,

. En la presente investigación se utilizó:

- a) Ordenamiento y Clasificación: Se halló información en las diferentes tesis relacionadas a esta modalidad de delitos como es el phishing tanto de tesis nacionales como internacionales, lo cual nos permitió seleccionar la opinión que tiene cada uno de ellos con referencia a como poder prevenir este delito. Finalmente se ha clasificado también los mecanismos de protección que debe considerarse.
- b) Encuestas: A través de las encuestas se hizo la recopilación de datos como por ejemplo si los sistemas financieros cuentan con sistemas informáticos que puedan garantizar la no ocurrencia del delito del phishing. O tal vez para saber el aproximado de cuantas personas que son clientes de una entidad financiera por 5 años aprox. han sido víctimas del mencionado delito. Finalmente, las encuestas son anónimas.
- c) Entrevistas: Esta técnica esta básicamente respaldada por la guía de entrevistas.
- d) Digitalización y Proceso en Excel y Work: Se aplicó cuadros en Excel y work para poder hacer la presentación de los gráficos que se obtuvieron después de haber planteado la hipótesis.

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

4.1 Presentación de Resultados

4.1.1 El delito de fraude informático bajo la modalidad del phishing

En este trabajo de investigación, se ha seleccionado la teoría



del delito phishing por ser la guía o base de esta tesis.

Como tenemos conocimiento, el delito de phishing, es considerado uno de los fraudes mas antiguos que conocemos a través del internet; tuvo su origen en a mediados de los años 90 y este término fue dirigido por vez primera a América online(AOL). Manifestamos que el objetivo principal del phishing es obtener información confidencial a través de los correos electrónicos, páginas web, clonación de contraseñas de las tarjetas y/o de las cuentas bancarias. Podemos comentar una forma de haber sido víctima de este delito como cuando el usuario usa su computador donde ha observado que ha recibido un correo donde le proponen un negocio y/o trabajo donde le ofrecen un sueldo atractivo; el usuario muestra interés y continua leyendo el correo, llega un momento donde le solicitan su información confidencial como son las contraseñas de su tarjeta, y otros es allí cuando involuntariamente el usuario digita sus datos lo cual el ciberdelincuente esta listo a cometer su delito luego de haber recibido la información.

Son varias las formas que se están usando para poder luchar contra este tipo de delitos no solo en nuestro país, internacionalmente también tienen esta preocupación por ello en el año 2004 entro en vigencia los acuerdos que se dieron en el tratado de Budapest lo cual pretende uniformizar entre los países que conforman este tratado para que haya uniformidad en cuanto a las penas que se le dan a los ciberdelincuentes



En la presente investigación se determinó que La Cultura jurídica de prevención y un Plan estratégico conjunta entre la SBS y bancos inciden positivamente en la prevención del delito de phishing por correo electrónico, habiendo sido respaldado dado que la mayoría de los operadores respaldaron la afirmación en un 59%.

Los resultados armonizan con lo señalado por Mengoa (2021), quien señala que el incremento del avance tecnológico a traído como consecuencia delitos como sabotaje informático, fraude, y lavado de activos,

Lo expuesto se refiere que el Estado es el único que está facultado para aplicar las sanciones penales, previo al seguimiento de un debido proceso penal; siendo el que tiene el dominio del proceso de criminalización secundaria. Esta función la ejerce, dentro del control penal, a través de los operadores penales judiciales, quienes son los únicos que tienen la potestad de administrar justicia en los conflictos de naturaleza penal. Es el operador penal judicial, materializa las sanciones penales. En ese sentido, este poder sancionador que tiene únicamente el Poder Judicial órgano a quien se delega esta función, ejercerá dicha función sobre aquella nación jurídicamente organizada y sobre un territorio en concreto.

La función sancionadora tiene por objetivo la protección de los diversos derechos fundamentales o como es denominado bien jurídico protegido, como lo es el honor, la propiedad, la integridad corporal, entre otros, pero en el caso del delito informático del phishing el bien jurídico será el patrimonio, puesto que, es el bien o interés que está protegido por el Derecho, lo que la norma, mediante la amenaza de la pena, tiende a tutelar, a proteger de posibles agresiones.

En consecuencia, el bien jurídico es el interés jurídicamente protegido es lo que la comunidad colectiva fija como su principio básico para lograr el desarrollo armónico y pacífico. El delito debe



contener una conducta humana que sea capaz de provocar la puesta en peligro, real claro e inminente o la lesión de un bien jurídico de conformidad con el artículo IV del TP del Código penal. La defensa del bien jurídico es lo que le da sentido a todo el ordenamiento jurídico penal (Bramont Arias, 2002, p. 173).

En ese sentido a nuestro entender el derecho penal se basa en la necesaria tutela de los bienes jurídicos como finalidad de cada ordenamiento. Protege y tiene en la pena el mecanismo eficaz y adecuado como consecuencia jurídica de posible aplicación para aquel que ha infringido las normas establecidas. En otras palabras, se requiere que tanto el estado como la tecnología estén siempre al mismo nivel pues a medida que la tecnología avanza, los mecanismos de protección a través del código penal también deben ser más severos contra el delito informático phishing. El derecho de castigar del estado o *ius Puniendi* es la facultad que se le ha otorgado al estado para imponer una pena o una medida de seguridad y está integrada por un sistema de principios denominados delictivos al derecho a castigar, mediante los cuales se logra introducir un “límite” ante posibles excesos.

En la actualidad tenemos un gran objetivo que es contrarrestar esta modalidad de delito informático y lo debemos hacer primeramente a través de la prevención lo cual lo lograremos a través de información brindada por campañas publicitarias que deben ser dirigidas en coordinación entre la SBS y las entidades financieras.

4.1.2 La protección de los sistemas de información del delito informático phishing

Los sistemas informáticos están conformados por computadoras y sus suministros o llamados también ordenadores que constan de una parte física llamada hardware y una parte lógica denominada software lo cual es funcional para un usuario. Asimismo, el componente humano es el personal técnico que le da mantenimiento



al sistema, entre ellos podemos mencionar al digitador, programador, analista y otros.

El Ministerio del interior posee un sistema informático general donde se encuentra información de diferentes entidades públicas entre ellos el de la DIVINDAT, que es el encargado de combatir el crimen organizado, pero su sede donde se recepcionan este tipo de denuncias como es el fraude o estafa, lo ubicamos en la Av. España. Cabe señalar que existe una gran diferencia entre sistema informático y dato informático. El primero aborda todo un sistema con servidores de gran capacidad mientras que un dato informático es específico con relación a un determinado tema.

En la presente investigación se estableció que la cultura jurídica de prevención y un plan estratégico conjunta entre la SBS y bancos, inciden positivamente en la prevención del delito de phishing, habiendo sido respaldados por la mayoría de los operadores.

Los resultados guardan relación con lo sostenido por Ventura (2021) quien señala que una de las prioridades del sistema judicial penal es poder subsanar las deficiencias legales que existen en el Perú para poder lograr identificar a los autores de la comisión de los delitos cibernéticos y la dificultad de los cortos plazos de investigación.

Asimismo, uno de los retos para que el Perú realice una transformación digital conlleva a hacer una reflexión ante amenazas sobre la vulneración.

Es menester señalar que los fundamentos dogmáticos acreditan la aplicación de sanciones penales por parte del Estado ya que, sin razones convincentes, opina, que la legitimidad del ius puniendi depende de la legitimidad de la forma de Estado, y considera que solo un Estado social y democrático de Derecho garantiza tal acción.



Es por ello que los delitos informáticos, dada la globalización, el avance tecnológico para el Estado ha constituido un verdadero reto proteger a todos aquellos bienes que se ven vulnerados por el uso indebido de medios tecnológicos, cuya consecuencia lógica es que si el Estado quiere ejercer el *ius puniendi* tiene que previamente tipificar este tipo de conductas delictivas, ello como parte del principio de legalidad que orienta a todo ordenamiento jurídico.

Para la sistematización de la protección de los sistemas informáticos, es menester precisar que las empresas consideran incontrollable poder enfrentar a este tipo de delito y de determinada forma siempre derivan a la ayuda de la autoridad judicial competente con el debido apoyo de las autoridades policiales para las investigaciones necesarias con la intención de dar con la central de operaciones y cabezas de estas organizaciones criminales.

Ante el incremento del delito de phishing en el Perú también salió a relucir la deficiente estructuras de las empresas y sus mecanismos para hacer frente este tipo de delitos informáticos y solo el 9% se preocupó por implementar estas medidas preventivas y coincidentemente se traduce en entidades bancarias grandes como el banco de crédito, el banco interbank y el banco BBVA, y mostrando la dejadez del estado en proteger las acciones de su principal banco, el de la nación.

Es por ello que las organizaciones criminales, deciden operar a otras entidades financieras de menor categoría, esto pues las principales antes mencionadas proporcionan herramientas como comunicados, emisión de correos electrónicos, mensajes confiables con números identificables y cortos que solo son de acceso para entidades de estado y financieras.

Existe también datos estadísticos de cuáles son los países que generan más software maliciosos países como reino unido y china lideran esta lista con un aproximado de 25 y 30% respectivamente y



eso por ser pioneros en cibernética y digitalización. Es por eso que, en el año 2019, a nivel mundial Google y Microsoft cerraron mas de 20 millones de correos electrónicos que tenían la condición de inoperativos o con características de sospechosas que eran utilizadas para engañar a los usuarios y utilizar métodos de phishing, esto con la intención de prevenir e ir erradicando desde su frontera este problema cibernético.

En ase a ello es que se requiere, sistematizar todos los sistemas informáticos para una mejor prevención de dicha modalidad delictiva

4.1.3 Tratamiento legislativo en el derecho comparado respecto del phishing

Al respecto en países como **Ecuador**, no se han visto avances en cuanto a la legislación como nos menciona Valle (2013), donde manifiesta que existe un gran perjuicio social al no encontrar una tipificación específica y adecuada en el código integral penal, y mucho menos en reconocimiento o mención constitucional la libertad de acceso a la información digital permite el descontrol en este delito, ya que la forma de sanción y tipificación de estos delitos es de forma genérica y no particular con respecto al phishing, penas mínimas como de 5 a 10 años para quienes que cometen delitos que generan pérdidas de hasta millones en cuentas

Mientras que por el lado de la legislación **colombiana**, Castillo (2021), menciona que si existe una regulación dentro del código penal con respecto al delito informático de phishing pero sin embargo no existe una actualización adecuada del mismo y con ello la transmisión de información para la planificación de herramientas y mecanismos de prevención por parte de las empresas, además de no establecer de manera constante mediante jurisprudencia adecuada estableciendo hitos y formas de defensa ante el



reconocimiento de la comisión del delito de phishing y las organizaciones criminales que las cometen.

Los países europeos como España, Francia y Alemania han regularizado el fraude y estafa informativa a través del Convenio de Budapest en el año 2001 lo cual entro en vigencia internacionalmente en el año 2004.

En el año 2013, en nuestro país se aprobó la ley Nª 30096, con la finalidad de prevenir y sancionar las conductas ilícitas y posteriormente fue modificado mediante ley N° 30171 la que fue publicada en el año 2014, donde se agregó a los tipos penales varios de estos delitos; sin embargo, para los tesisistas Hidalgo y Solano, no es suficiente pues plantean que se incorpore en el Artículo 7-A de la ley de delitos informáticos 30096 penas más severas.

4.14 Reporte de denuncias registradas por este tipo de delito phishing

Al respecto es de precisar que conforme información brindada por personal de la divindat se ha registrado mas de 2,000 denuncias interpuestas en dicha unidad especializada de la policía a nivel local.

Sin embargo, ante la implementación de las conocidas bancas móviles por parte de las agencias bancarias a partir del año 2016 en adelante se han ido conociendo métodos nuevos para engañar a los clientes, en cifras representadas y proporcionadas por la DIRINCRI se sabe que en ese mismo año hubo pérdidas muy elevadas, esto debido a que la gente no desconfiaba de los métodos de engaño y proporcionaban sus datos personales, usuarios y clave de las entidades bancarias, llegando a vaciar cuentas enteras de clientes frecuentes, en estos primeros años como en el 2016, 2017 y hasta



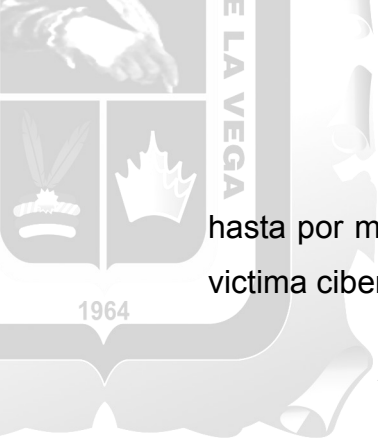
en el 2018 se utilizaban formas de engañar como correos electrónicos o la redirección a paginas falsas con las mismas características de la entidad bancaria.

El ingenio de estas organizaciones criminales ha ido evolucionando tanto que han llegado hasta mandar mensajes a los móviles personales de las personas, que con tan solo presionar el enlace ya se exponen al conocimiento de todos sus datos privados.

Asimismo, en un pronunciamiento internacional demás países del mundo han sufrido por estos delitos informáticos, países latinoamericanos como Brasil, Ecuador lideran el mayor índice de ataque cibernético mediante la modalidad de phishing con un ponderado anual de 65% de robos y estafas bancarias.

En países europeos como Reino Unido y España las estafas se dan en un ponderado del (46%) aproximadamente, aunque eso no es lo que preocupa a la población y autoridades competentes, el problema es el porcentaje anual con el que se incrementa estos delitos. México es un país en donde el phishing se incrementa anualmente entre un 14 al 22% anual y esto debido también al gran manejo informal de las cuentas bancarias y métodos de obtención del dinero.

En el Perú, en el presente año, en cuanto delitos informáticos ha sido el phishing el de mayor incidencia, hasta marzo del 2022 se incrementó en un 21% las denuncias por ingeniería social o también conocido como phishing, la división de investigación de delitos en alta tecnología registra más de 9000 casos anuales, un aproximado y más de 500 casos mensuales, eso sin contar con que desde el año 2020 y con la pandemia el delito que más se incremento fue el de phishing pues al pasar todos al confinamiento y al conocido ya trabajo remoto en donde los usuarios y cantidad de datos personales que se encontraban en las redes eran masivos, es por eso que las organizaciones criminales se infiltraban



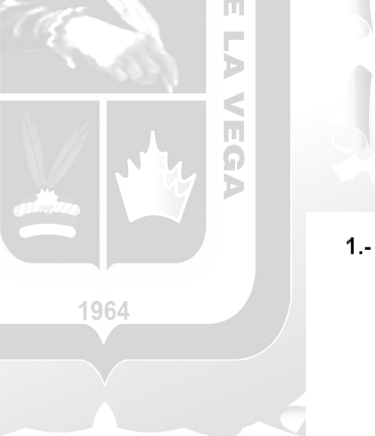
hasta por medio de WhatsApp con la intención de generar más confianza con la víctima cibernética.

Asimismo, se ha creído conveniente aplicar entrevistas a la Policía Nacional, Personal de la DIVINDAT, así como también encuestas/cuestionarios a funcionarios de las entidades bancarias, clientes/usuarios que tienen cuentas en las mencionadas entidades financieras cuyos resultados se muestran a continuación:

4.1.1 Cuadros de las entrevistas realizadas a 50 usuarios

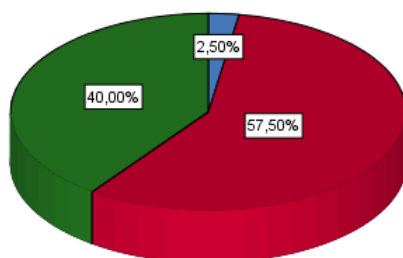
Gráfico 1

1.- ¿Cuentan con sistemas informáticos ante un eventual delito de phishing? De ser afirmativa la respuesta indique que programas.



1.- ¿Cuentan con sistemas informáticos ante un eventual delito de phishing? De ser afirmativa la respuesta indique que programas.

SI
NO
DESCONOCE



Fuente: propia

Se obtuvieron las siguientes respuestas:

SI	: 2.50%
NO	: 57.50%
DESCONOCE	: 40%

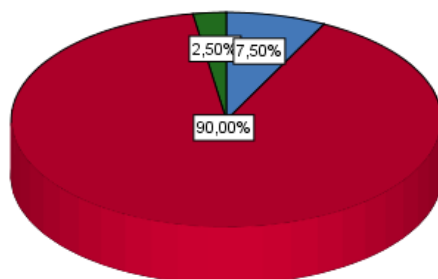
Gráfico 2

2.- Esta entidad bancaria ha sido víctimas de los hackers informáticos



2.- Su entidad bancaria ha sido víctimas de los hackers informáticos:

SI
NO
DESCONOCE



Se obtuvieron las siguientes respuestas:

SI	: 2,50%
NO	: 90%
DESCONOCE	: 7,50%

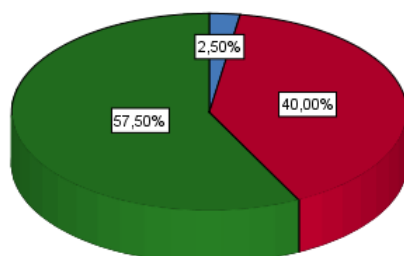
Gráfico 3

3.-Cuando acude la persona al banco se le brinda orientación sobre los peligros de los delitos informáticos y cómo prevenirlos. De ser afirmativa la respuesta indique que actividades se ha desarrollado



3.-Cuando acude la persona al banco se le brinda orientación sobre los peligros de los delitos informáticos y como prevenirlos. De ser afirmativa la respuesta indique que actividades se ha desarrollado

SI
NO
DESCONOCE



Se obtuvieron las siguientes respuestas frente a estas interrogantes:

SI : 2.50%
NO : 40%
DESCONOCE : 57,50%

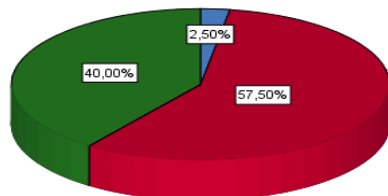
Gráfico 4

4.- ¿Durante el primer trimestre del año 2022, se ha reportado víctimas de este delito? De ser afirmativa la respuesta indique un aproximado.



4.-¿Durante el primer trimestre del año 2022, se ha reportado víctimas de este delito? De ser afirmativa la respuesta indique un aproximado.

SI
NO
DESCONOCE



Se obtuvieron las siguientes respuestas:

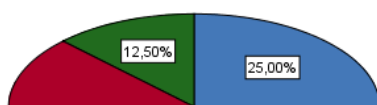
SI : 2,50%
NO : 57.50%
DESCONOCE : 40%

Gráfico 5

5.- Conoce de qué manera ha intervenido la SBS frente a los denominados hackers informáticos. Si la respuesta es afirmativa indique la forma de intervención

5.-Conoce de qué manera ha intervenido la SBS frente a los denominados hackers informáticos. Si la respuesta es afirmativa indique la forma que intervención.

SI
NO
DESCONOCE



Se obtuvieron las siguientes respuestas:

- a) Han perdido confianza en las entidades financiera y ahora no guardan su dinero en ellas 20%
- b) Utilizan menos aplicativos en su celular 30%
- c) Borrar/Bloquean los correos electrónicos de la entidad bancaria. 12,50%
- d) Cambian constantemente las contraseñas 12,50

Se obtuvieron las siguientes respuestas:

- SI : 12.50%
- NO : 62.50%
- DESCONOCE : 25%

Gráfico 6

*6.- Los usuarios que actitudes han adoptado frente al delito del pshiging:
Puede marcar más de una opción*

6.- Los usuarios que actitudes han adoptado frente al delito del pshiging: Puede marcar más de una opción.

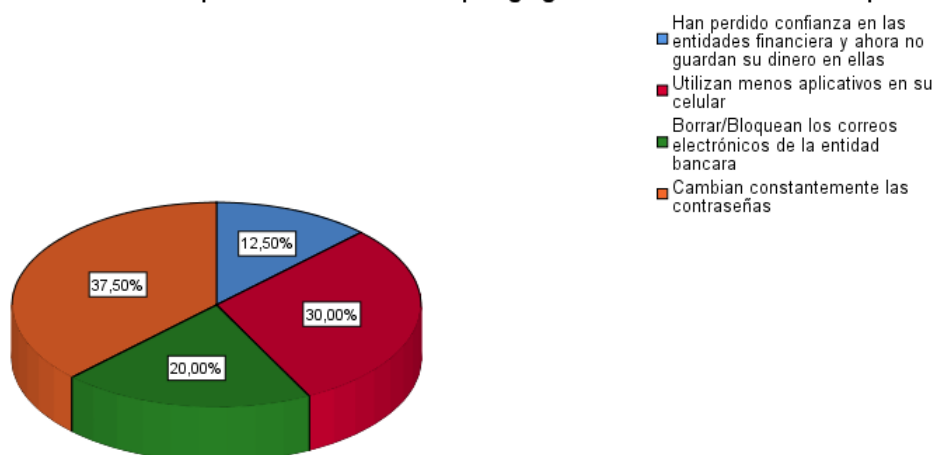
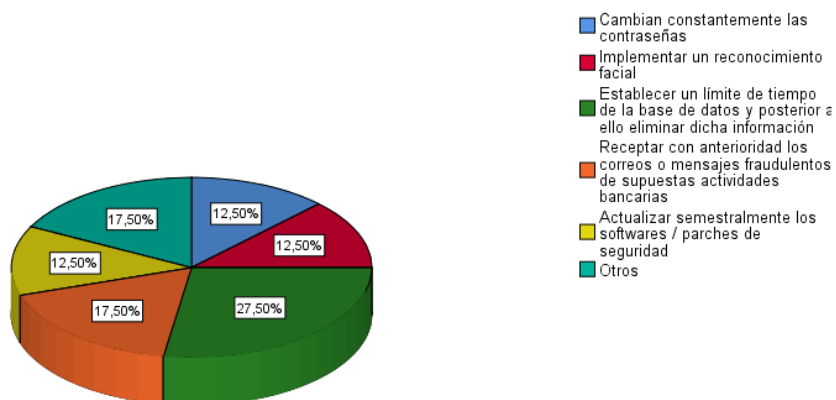




Gráfico 7

7.- ¿Cuáles de las siguientes opciones considera usted que se debe implantar en las agencias bancarias para evitar la comisión de delitos informáticos phishing? De ser necesario puede marcar más de una opción





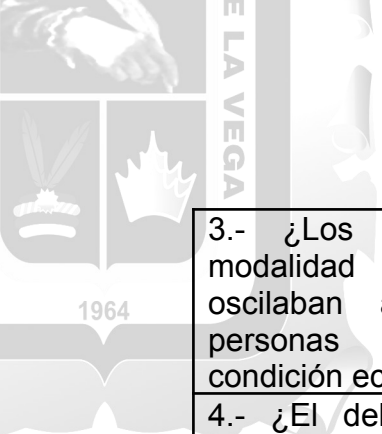
Se obtuvieron los siguientes resultados frente a esta interrogante:

- a) Las contraseñas sean reemplazadas por identificador biométrico 12,50
- b) Implementar un reconocimiento facial 12,50
- c) Establecer un límite de tiempo de la base de datos y posterior a ello eliminar dicha información 12,50
- d) Receptar con anterioridad los correos o mensajes fraudulentos de supuestas actividades bancarias 17,50
- e) Actualizar semestralmente los softwares / parches de seguridad
- f) Otros..... 17,50

Tabla 1

Entrevistado 1

TÍTULO	Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano
CARGO	Investigador I
1.- ¿Qué función desempeña actualmente y cuánto tiempo tiene el cargo?	Investigador, labora en la DIVINDAT –PNP DIRINCRI – PNP.
2.- ¿Se han reportado denuncias bajo la modalidad informática del phishing en el año 2020, puede indicar aproximadamente cuantos se han denunciado?	Sí, se han reportado un aproximado de 1800 casos.



3.- ¿Los denunciante de esta modalidad delictiva, que edad oscilaban aproximadamente, eran personas con estudios y que condición económica social tenían?	En su mayoría, eran personas que tenían secundaria completa.
4.- ¿El delito informático phishing esta direccionado mayormente a empresas o a personas naturales?	No, considero un delito informático la modalidad phishing, a mi criterio es una estafa agravada en el artículo 196 numeral 05.
5.- ¿Las personas acreedoras de los bonos otorgados por el gobierno, han reportado denuncias sobre este tipo de delitos por ser víctimas de ellos? Explique.	Sí, se han reportado, en especial en la época de inicios de pandemia, donde hubo un alto índice.
6.- Los ciberdelincuentes, después de haber cometido el delito. ¿Cuántos de ellos fueron judicializados y cuál fue la pena impuesta?	Sí se han capturado, siendo ellos judicializados.
7.- ¿Qué medidas y/o acciones se han adoptado para prevenir este tipo de delitos? Explique.	Se han impartido charlas dirigidas a la población a través de los medios de comunicación.



Tabla 2

Entrevistado 2

TÍTULO	Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano
CARGO	Investigador II
1.- ¿Qué función desempeña actualmente y cuánto tiempo tiene el cargo?	Soy efectivo investigador de la DIVINDAT, desde hace 7 años.
2.- ¿Se han reportado denuncias bajo la modalidad informática del phishing en el año 2020, puede indicar aproximadamente cuantos se han denunciado?	En la DIVINDAT, se tuvo como registro, las denuncias de 2000 personas aproximadamente.
3.- ¿Los denunciantes de esta modalidad delictiva, que edad oscilaban aproximadamente, eran personas con estudios y que condición económica social tenían?	Las edades son entre los 21 a 35 años sin estudios, clase media.
4.- ¿El delito informático phishing esta direccionado mayormente a empresas o a personas naturales?	A ambos.
5.- ¿Las personas acreedoras de los bonos otorgados por el gobierno, han reportado denuncias sobre este tipo de delitos por ser víctimas de ellos? Explique.	Sí, tenemos denuncias en el 2021 y todos ellos fueron suplantados para cobrar su bono.
6.- Los ciberdelincuentes, después de haber cometido el delito. ¿Cuántos de ellos fueron	Hasta la fecha, no tienen condena sobre ello, pero si tienen prisiones preventivas.

judicializados y cuál fue la pena impuesta?

7.- ¿Qué medidas y/o acciones se han adoptado para prevenir este tipo de delitos? Explique.

Campañas de concientización
Comunicación con los bancos para compartir información
Coordinación con las empresas o comercios virtuales para identificar las incidencias sobre fraudes
Operativos en lugares de venta de artefactos utilizados para ello.



Tabla 3

Entrevistado 3

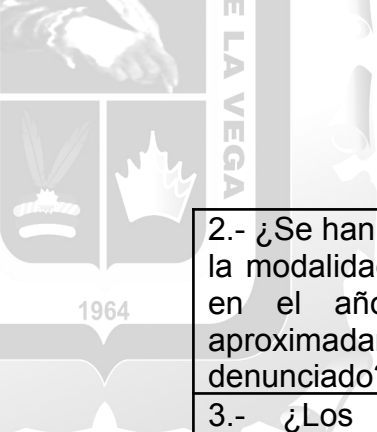
TÍTULO	Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano
CARGO	Investigador III
1.- ¿Qué función desempeña actualmente y cuánto tiempo tiene el cargo?	La función que realizo es investigar delitos, faltas y combatir la delincuencia en todas sus modalidades.
2.- ¿Se han reportado denuncias bajo la modalidad informática del phishing en el año 2020, puede indicar aproximadamente cuantos se han denunciado?	Este tipo de denuncias está encargado la Unidad especializada de Alta Tecnología DIVINDAT.
3.- ¿Los denunciantes de esta modalidad delictiva, que edad oscilaban aproximadamente, eran personas con estudios y que condición económica social tenían?	Acuden personas de distintas edades y de diferentes niveles de estudio como son de secundaria y nivel superior.
4.- ¿El delito informático phishing esta direccionado mayormente a empresas o a personas naturales?	Se da en los dos tipos: empresas y personas naturales.
5.- ¿Las personas acreedoras de los bonos otorgados por el gobierno, han reportado denuncias sobre este tipo de delitos por ser víctimas de ellos? Explique.	Se sabe que, si se han reportado este tipo de denuncias, pero es la DIVINDAT, encargada de ello.
6.- Los ciberdelincuentes, después de haber cometido el delito. ¿Cuántos de ellos fueron judicializados y cuál fue la pena impuesta?	Los delincuentes han sido juzgados por las fiscalías, y utilizan la modalidad de phishing y smishing.
7.- ¿Qué medidas y/o acciones se han adoptado para prevenir este tipo de delitos? Explique.	En las unidades policiales especializadas mediante medios informáticos televisivos.



Tabla 4

Entrevistado 4

TÍTULO	Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano
CARGO	Investigador IV
1.- ¿Qué función desempeña actualmente y cuánto tiempo tiene el cargo?	Actualmente me desempeño como superior PNP, cumpliendo la función de investigador en el departamento de adulteración de teléfonos celulares - DIVINDAT aproximadamente 10 años.



2.- ¿Se han reportado denuncias bajo la modalidad informática del phishing en el año 2020, puede indicar aproximadamente cuantos se han denunciado?	Que si se han reportado denuncias de delitos informáticos en la modalidad de phishing en el 2021 un aproximado de 200 en la indicada modalidad.
3.- ¿Los denunciantes de esta modalidad delictiva, que edad oscilaban aproximadamente, eran personas con estudios y que condición económica social tenían?	Las edades de los denunciantes son de 26 años aproximadamente, son personas que cuentan con solvencia económica, con estudios superiores y algunos sin estudios.
4.- ¿El delito informático phishing esta direccionado mayormente a empresas o a personas naturales?	A todas las personas que tienen una cuenta bancaria tanto natural como jurídica.
5.- ¿Las personas acreedoras de los bonos otorgados por el gobierno, han reportado denuncias sobre este tipo de delitos por ser víctimas de ellos? Explique.	Que, si se han reportado denuncias sobre los bonos otorgados por el gobierno, cabe mencionar que luego de vulnerar la base de datos del MINDIS y tener la información de los beneficiarios usaban la modalidad del phishing para suplantar la identidad.
6.- Los ciberdelincuentes, después de haber cometido el delito. ¿Cuántos de ellos fueron judicializados y cuál fue la pena impuesta?	Un 50% de las personas que han cometido el delito han sido judicializados por el delito de estafa agravado y su sentencia ha sido por 4 a 8 años.
7.- ¿Qué medidas y/o acciones se han adoptado para prevenir este tipo de delitos? Explique.	La DIVINDAT –DIRINCRI-PNP como unidad Especializada en la lucha frontal a los delitos informáticos, está orientando a la población a través de entrevista televisado el uso de las tarjetas de crédito y/o débito realizando operativos, patrullajes virtuales y coordinaciones con las entidades financieras para que difundan a sus clientes sobre la seguridad que deben dar a su información personal (número de DNI, tarjeta, contraseña).



4.2 Contrastación de Hipótesis

La Cultura jurídica de prevención y un Plan estratégico conjunta entre la SBS y bancos resultan ser los mecanismos de prevención y protección del bien jurídico tutelados frente a la modalidad delictiva del phishing.

4.3 Discusión de Resultados

4.3.1 Discusión de la hipótesis principal

En la presente investigación se afirmó que La Cultura jurídica de prevención y un Plan estratégico conjunta entre la SBS y bancos resultan ser los mecanismos de prevención y protección del bien jurídico tutelados frente a la modalidad delictiva del phishing, habiendo sido respaldado dado que la mayoría de los operadores respaldaron la afirmación en un 61%.

Los resultados guardan relación con lo señalado por Hidalgo y Solano (2021, p. 56), quien señala que, en el distrito fiscal del Santa, las denuncias por phishing son archivadas en su gran mayoría, siendo uno de los factores más determinantes para el archivo de los casos la deficiente redacción de los tipos penales regulados en la Ley de Delitos Informáticos.

Asimismo, guarda relación con lo señalado en el marco teórico al precisar que el phishing tiene tres fases para concretarse, los cuales son la fase de acercamiento, la fase de alerta y la fase de distracción. En la primera mencionada se trata de hacer el seguimiento, seleccionar a la víctima y acercarse a ella y a sus datos afectando debilidades mediante la comunicación cibernética. La siguiente fase se da con la interacción directa con su víctima ya



seleccionada aquí el ciberdelincuente ya identifico que información específica necesita que la víctima le revele. Finalmente, la última etapa consiste en, la concertación del delito pues la victima al ya sentirse en confianza con la proporción de mecanismos de la página o directamente con el delincuente le proporciona de forma fácil o le da alcance a lo que quiere el delincuente, que por lo general es el acceso a las cuentas bancarias de la víctima.

Es necesario describir las principales formas en las que se presenta el phishing, una de ellas es mediante las páginas de pago, en donde se manifiesta mediante la clonación de la paginas de pago y manera idéntica por lo que realmente son formas difíciles de identificar al hacker detrás de esas acciones, aquí se ve paginas como PayPal o safetypay. Otra forme en donde se evidencia el phishing es en las páginas de aerolínea, en los famosos check out en línea ya que estas páginas solicitan datos personalísimos como fecha de nacimiento y todos los datos registrados en los documentos de identidad.

Otra forma es el alojamiento del phishing en el sistema del computador, este se da mediante la llegada de los virus que pueden ser trasmitidos al momento de abrir las páginas, al momento de alojarse en la computadora tienen el acceso total de la información que se realiza dentro de ella, esta es una forma altamente peligrosa. Finalmente, el ya conocido como redireccionamiento malicioso, en donde te dirigen a una página falsa o de validez ficticia y que una forma fácil de identificar es fijándose el comienzo y final de las direcciones de URL.

Remontándonos históricamente brevemente a los 70 empezó una nueva era, la era digital con la revolución industrial el ciberespacio fue naciendo y con ello facilidades en las comunicaciones. Estados Unidos fue uno de los países en implementar y evolucionar cibernéticamente de ahí que naciera paginas como Messenger,



Hotmail, Gmail y demás medios de interrelaciones públicas, además de las ya conocidas y determinadas redes sociales. Sin embargo, también se dio inicio al anonimato dificultando la actividad de rastrear a la persona detrás de un computador y con ello el ingenio por organizaciones criminales de idearse métodos perjudiciales en contra de los usuarios.

Por lo que las empresas consideran incontrolable poder enfrentar a este tipo de delito y de determinada forma siempre derivan a la ayuda de la autoridad judicial competente con el debido apoyo de las autoridades policiales para las investigaciones necesarias con la intención de dar con la central de operaciones y cabezas de estas organizaciones criminales.

Finalmente planteamos los siguientes mecanismos de prevención y protección frente a este tipo de delitos:

a) Mecanismos de prevención:

No enviar información personal por medio de correos electrónicos más aún si son correos que tengan dudoso origen

Se debe evitar ingresar a un sitio web de una entidad financiera cuando estemos en lugares públicos como por ejemplo un locutorio

No responder correos donde les soliciten información personal o financiera

Se debe verificar los indicadores del sitio web. Por seguridad cuando deseamos ingresar a la web de una institución financiera de preferencia lo debemos hacer nosotros mismos.

Se debe realizar la visualización diaria de los movimientos o transacciones efectuadas.

b) Mecanismos de protección:



Usar Software originales

Estar atento a la evolución de este tipo de modalidad delictiva

No descargar archivos de procedencia dudosa

CAPÍTULO V: CONCLUSIÓN Y RECOMENDACIONES

5.1 Conclusiones

5.1.1. Se analizó el delito de fraude informático bajo la modalidad del phishing en el sentido que es una modalidad delictiva que tiene como propósito extraer datos del usuario, empujando para ello paginas clonadas que tienen a causar una apariencia real de las paginas reales, de tal manera que induce al error a los usuarios con el objeto de extraer sus datos, teniendo para ello la emisión de correos electrónicos, que



contienen mensajes maliciosos que buscan extraer información privada del usuario.

5.1.2. Se estableció que la sistematización de la protección de los sistemas de información del delito informático phishing pasa por un Plan estratégico conjunta entre la SBS y bancos a efectos detectar la prevención del delito de phishing por sitio web e identificar a los ciberdelincuentes.

Además, el sistema informático de este delito, parte únicamente del sistema DIVINDAT a través del Ministerio del Interior; asimismo, los bancos han implementado su sistema, pero aún no hay mayor mecanismo de prevención que ayude a que los usuarios víctimas de este delito disminuyan, pues esto no está regulado.

5.1.3. Se determinó que el tratamiento legislativo en el derecho comparado respecto del phishing tal como los países de México y Colombia, cuentan con una legislación adecuada, ya que tipifican el delito de manera específica, de tal manera que permite una persecución eficaz dicha modalidad delictiva; sin embargo, cabe precisar que en el caso de Ecuador no está tipificado lo cual permite que no hay un avance en cuanto a la severidad de la pena.

5.1.4. Se estableció que son 2,000 las denuncias policiales que obran en las DIVINDAT, sobre delitos informáticos registradas por este tipo de delito phishing, las mismas que son objeto de investigación por parte de la fiscalía especializada en a la ciberdelincuencia. Por otro lado, se encuestó a 50 usuarios, quienes manifestaron en su mayoría su desconocimiento sobre este tipo de delitos lo que nos hace concluir afirmando que existe una falencia en cuanto a la información brindada al usuario.

5.1.5 Con referencia a la hipótesis, se determinó que los mecanismos de prevención y protección del bien jurídico tutelado por el Estado a través del derecho penal a una cultura jurídica de prevención y plan estratégico conjunta entre la SBS y las entidades financieras , resultan ser los



mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva del phishing debido a que resulta la medida más idónea de afrontar el elevado índice delictivo que padecen los ciudadanos que utilizan la web para hacer sus transacciones.

5.2 Recomendaciones

5.2.1. A la superintendencia de banca y seguro

Crear plataformas informáticas de prevención, en donde puedan cruzar información con los bancos y usuarios a efectos de prevenir la comisión delictiva del smishing de tal manera que se pueda evitar la consumación del citado evento delictivo.

5.2.2. Al ministerio publico

Realizar coordinaciones con la policía a efectos de realizar acciones preventivas, de tal manera que se haga seguimiento y búsquedas en la web, así como un patrullaje informativo con la finalidad de identificar a los ciberdelincuentes y la creación de páginas falsa y clonadas.

5.2.3. A los bancos

Efectuar una intensa campaña dirigido a los Bancos a efectos de incrementar una mayor difusión de medidas preventivas para evitar el phishing que atenta contra los intereses de los usuarios



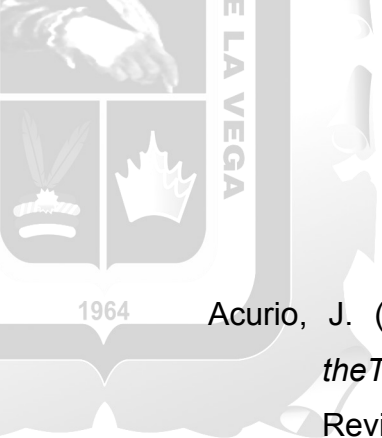
CAPITULO VI: PROPONER A LA SBS - DIRECTIVAS

Se propone directiva de protección basada en los lineamientos de la hipótesis.

Es necesario en base a una cultura jurídica de prevención y un plan estratégico conjunta entre la SBS y bancos a efectos de prevenir el delito de phishing por sitio web, paginas falsas creadas por ciberdelincuentes con el objeto de captar los datos personales e información de tarjetas de los usuarios para efectuar operaciones bancarias maliciosas, asi también debemos proponer la cultura digital en cuanto a las redes sociales. En los últimos años el crecimiento de los delitos informáticos se ha despuntado a nivel nacional, pues el implemento progresivo de nuevas tecnologías con ella el uso excesivo del teléfono y la forma como se confía datos personales en él, han permitido que con tan solo un clic puedan generarse cuantiosas



pérdidas. Por lo mismo que las empresas han ido implementando mecanismo de reconocimiento de la autenticidad de sus canales digitales, así como la propagación de la forma de cómo se actúan e intervienen mediante los delitos informáticos por parte de grandes y muy bien estructuradas organizaciones criminales.



REFERENCIAS

- Acurio, J. (2018). *Open-Source tools: Incidence in the wireless security of the Technical University of Babahoyo*. Journal of Science and Research: Revista Ciencia e Investigación.
- Aula virtual derecho. (2021). *Guía estudiantil*.
- Avast. (2022). *¿Qué estafas de phishing son tendencia en 2022?*
- Bauer, F. (2016). *Los delitos de pornografía infantil como paradigma del moderno Derecho Penal (estudio del artículo 189 cp)*.
- Benavides, E., Fuertes, W., Sánchez, S. y Nuñez-Agurto, D. (2020). *Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura*. Ciencia y Tecnología.
- Benavides, J. y Cárdenas, J. (2015). *Factores sociales y económicos que determinan el perfil delictivo de las personas privadas de libertad que se encuentran en el Centro de Rehabilitación Social de la ciudad de Tulcán en el periodo Septiembre 2014-Marzo 2015*.
- Castillo, O. (2021). *Phishing: día de Pesca*. Tesis para obtener el grado de magister en derecho informático. Universidad Externado de Colombia.
- Castro, C. (2002). *La tutela cautelar de las consecuencias jurídicas económicas del delito*. Ius et veritas.
- Chiew, K., Yong, K. y Tan, C. (2018). *A survey of phishing attacks: Their types, vectors and technical approaches*. Expert Systems with Applications.
- Dominguez, A. (2021). *Principales mecanismos para el enfrentamiento al phishing en las redes de datos*. Revista Cubana de Ciencias Informáticas.
- El Comercio. (2021). *Ministerio Público crea una unidad especializada en ciberdelincuencia para atender delitos informáticos*.
- Europol. (2020). *8ª Conferencia de INTERPOL y Europol sobre Ciberdelincuencia: "Media humanidad está en peligro"*.



García, D. (2018). *El Phishing como delito de estafa informática*. Iuris Tantum Revista Boliviana de Derecho.

Gonzales, J. y Peña, J. (2013). *Estudio del impacto de la ingeniería social – phishing. Tesis para obtener el grado*. Universidad Nacional Autónoma de México

González, J., Bermeo, J., Villacreses, E. y Guerrero, J. (2018). *Delitos informáticos: una revisión en Latinoamérica*. UTMACH.

González, J. (2010). *Compendio de Derecho penal*. Parte general.

Hidalgo, C. y Solano G. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. propuesta de incorporación del artículo 7-a en la ley de delitos informáticos 30096*. Tesis. Universidad Nacional del Santa.

Hidalgo, C. y Solano, G. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096*.

Kcomt, R. (2020). *Función constitucional asignada a la pena: bases para un plan de política criminal*. Derecho PUCP.

Leal, J. (2012). *El impacto del phishing en el desempeño y el perfil de riesgo*. Evidencia de Credit Unión Australiano.

Leguizamon, J. (2021). *Propuesta para establecer una correcta recolección de evidencia digital, de acuerdo con la normatividad colombiana, enfocado a pequeñas y medianas empresas*.

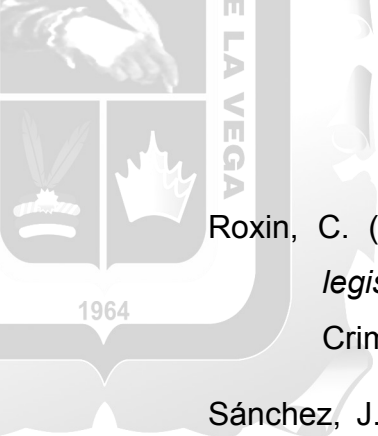
López, B. J. (2020). *La creación de las normas jurídico-penales en Colombia y su relación con los medios masivos de comunicación*. Doctoral dissertation. Universitat Autònoma de Barcelona.

Lozano, A. (2019). *La importancia del sistema de gestión de la seguridad de la Información en el comercio electrónico empresarial*. Doctoral dissertation. Universidad Santiago de Cali.

Luquin, E. (2007). *Repensando el ius puniendi*.



- Mariana, A. (2015). *El phishing. Proyecto de grado en Criminología*. Universidad Jaume.
- Mengo, M. (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú*.
- Messina, A. (2021). *Diseño e implementación de una extensión de Chrome para la detección de sitios web de Phishing utilizando aprendizaje automático*. Bachelor's thesis.
- Ministerio Publico. (2021). *Ministerio Público registró más de 21 mil denuncias por delitos informáticos en los últimos años*.
- Olaechea, J. (1998). *El bien jurídico*. Rev. Peruana de Ciencias Penales.
- Olivares, A. y Ceras, K. (2020). *Delitos informáticos y la evidencia digital en el proceso peruano del Distrito judicial de Junín*. Tesis. Universidad Peruana Los Andes.
- Paredes, J. (2013). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el periodo 2009-2010*. Tesis para optar el grado académico de magíster en derecho con mención en Cienas Penales. Universidad Mayor de San Marcos.
- Paypal. (2020). *Declaración de Privacidad*.
- Penal, D. (2002). *Parte general*. Fundamentos y teoría de la imputación.
- Peña, D. y Cañadillas, R. (2010). *La administración desleal societaria en el derecho penal español*. InDret.
- Puig, M. (2004). *Derecho penal. Parte general*. UNC.
- Ríos, A. V. (1999). *La protección de la libertad sindical y su regulación (limitada y simbólica) en el Perú*. IUS ET VERITAS.
- Rodríguez, G. (2019). *Phishing Attacks: Detecting and Preventing Infected E-mails Using Machine Learning Methods*. Cyber Security in Networking Conference.



Roxin, C. (2013). *El concepto de bien jurídico como instrumento de crítica legislativa sometido a examen*. Revista Electrónica de Ciencia Penal y Criminología.

Sánchez, J. (2020). *Delincuencia empresarial, derechos humanos y seguridad humana: reflexiones desde el Derecho penal económico y de la empresa*. Revista Criminalia Nueva Época.

Superintendencia de banca, seguros y AFP. (2015). *Fraudes financieros*.

Terradillos, J. (2015). *Derecho penal económico. Lineamientos de política penal*. Revista IUS.

Universidad Libre (2021). *Nuevo Concepto de Delito*.

Universitat Jaume (2021). *La edad de responsabilidad penal en los diferentes países europeos*. UJI

Valle, C. (2013) *Manejo que se le ha dado al delito informático jurisprudencialmente en Colombia en los últimos 10 años a nivel probatorio*.

Valle, J. (2013). *El Delito Informático de Phishing*. Tesis para obtener el grado de maestro. Universidad Regional Autónoma de los Andes.

Ventura, M. (2021). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima*.

Vilca, G. (2018). *Los hackers: delito informático frente al código penal peruano*. Tesis. Universidad Nacional Santiago Antúnez de Mayolo.

Giraldo. M., Jenny y Duarte. P., Iban. (2018). *Ingeniería Social: Técnica de ataque phishing y su impacto en las empresas colombianas*. Tesis de grado, título profesional. Universidad nacional abierta y a distancia. Salamina, Colombia.

Herrera, C., Edwin. (2016). *El phishing como delito informático y su falta de tipificación en el código orgánico integral penal*. Tesis de grado, título



profesional de abogado. Universidad Central del Ecuador. Quito, Ecuador.

Meléndez. M., Jhon. (2020). Software opelect en máquina virtual y la prevención del riesgo de fraude electrónico en operaciones bancarias de los clientes de lima metropolitana. Tesis de posgrado, maestría. Universidad Nacional Federico Villarreal. Lima, Perú.

Olivares, R. Bruno y Ceras, R. Maribel. (2022). Delitos informáticos y la incidencia en el proceso penal peruano en el distrito judicial de Junín. Tesis de grado, título profesional de abogado. Universidad Peruana Los Andes. Junín, Perú.

Ventura. Q., Mishell (2021). Lima, Perú. La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020. Tesis de grado, título profesional. Universidad Privada del Norte.



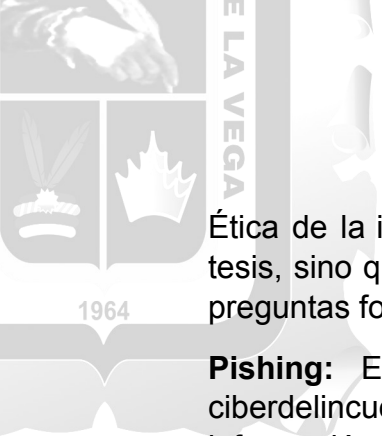
ANEXOS

UNIVERSIDAD INCA GARCILASO DE LA VEGA

BACHILLER EN DERECHO Y CIENCIAS POLITICAS

ENTREVISTA

**TITULO: “MECANISMOS DE PREVENCION Y PROTECION DEL BIEN JURIDICO TUTELADO
FRENTE A LA MODALIDAD DELICTIVA PHISHING EN EL ORDENAMIENTO JURIDICO
PENAL PERUANO”**



Ética de la investigación, los nombres no serán revelados en el desarrollo de la tesis, sino que únicamente se va a recopilar la información sobre la base de las preguntas formuladas.

Pishing: Es una modalidad delictiva informática, a través del cual, el ciberdelincuente roba su dinero o su identidad haciendo que divulgue su información personal a través de correos electrónicos donde fingen haciéndose pasar por una entidad bancaria

APELLIDOS Y NOMBRES:

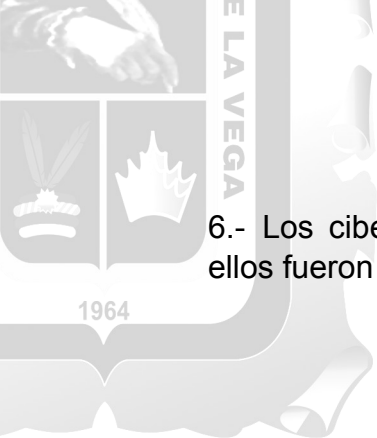
- 1.- ¿Qué función desempeña actualmente y cuánto tiempo tiene el cargo?

- 2.- ¿Se han reportado denuncias bajo la modalidad informática del phishing en el año 2020, puede indicar aproximadamente cuantos se han denunciado?

3. Los denunciantes de esta modalidad delictiva, que edad oscilaban aproximadamente, eran personas con estudios y que condición económica social tenían?

- 4.- El delito informático phishing esta direccionado mayormente a empresas o ha personas naturales

- 5.- ¿Las personas acreedoras de los bonos otorgados por el gobierno, han reportado denuncias sobre este tipo de delitos por ser víctimas de ellos? Explique



6.- Los ciberdelincuentes, después de haber cometido el delito. ¿Cuántos de ellos fueron judicializados y cuál fue la pena impuesta?

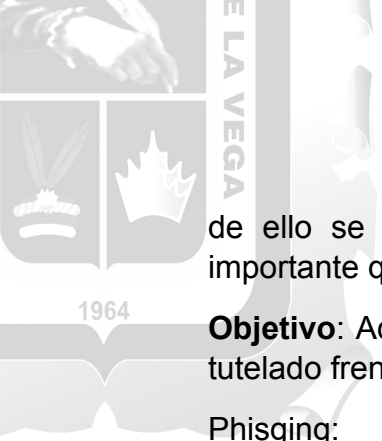
7.- ¿Qué medidas y/o acciones se han adoptado para prevenir este tipo de delitos? Explique

UNIVERSIDAD INCA GARCILASO DE LA VEGA
BACHILLER EN DERECHO Y CIENCIAS POLITICAS
ENCUESTA

SEÑOR (A) :

Con la finalidad de desarrollar la tesis para obtener el título profesional de Abogado con el tema “MECANISMOS DE PREVENCIÓN Y PROTECCIÓN DEL BIEN JURÍDICO TUTELADO FRENTE A LA MODALIDAD DELICTIVA PHISHING EN EL ORDENAMIENTO JURÍDICO PENAL PERUANO”

Se le solicita y agradece anticipadamente su contribución, asimismo le indicamos que la presente encuesta es totalmente confidencial y consecuencia



de ello se dará a conocer únicamente en forma tabulada e impersonal. Es importante que sus respuestas sean sostenidas con la verdad.

Objetivo: Adquirir información necesaria para prevenir y proteger el bien jurídico tutelado frente a la modalidad delictiva del phishing.

Phishing:

INFORMACION GENERAL:

Instrucciones: Por favor marque con una (X), en la alternativa propia de su desempeño:

Gerente () Cliente () personal en ventanilla () ~~Otros ()~~

Sexo: Masculino () Femenino ()

INSTRUCCIONES: Lea las preguntas que se citan a continuación y marque (X), el casillero de su preferencia.

1. ¿Cuentan con sistemas informáticos ante un eventual delito de phishing? De ser afirmativa la respuesta indique que programas.

Si / No / Desconoce (Cuáles)

2. Esta entidad bancaria ha sido víctimas de los hackers informáticos:
Si / No/ Desconoce

3. Cuando acude la persona al banco se le brinda orientación sobre los peligros de los delitos informáticos y como prevenirlos. De ser afirmativa la respuesta indique que actividades se ha desarrollado

Si

No

4. ¿Durante el primer trimestre del año 2022, se ha reportado víctimas de este delito? De ser afirmativa la respuesta indique un aproximado.

Si / No (Indica)

5. Conoce de qué manera ha intervenido la SBS frente a los denominados hackers informáticos. Si la respuesta es afirmativa indique la forma que intervención.

Si

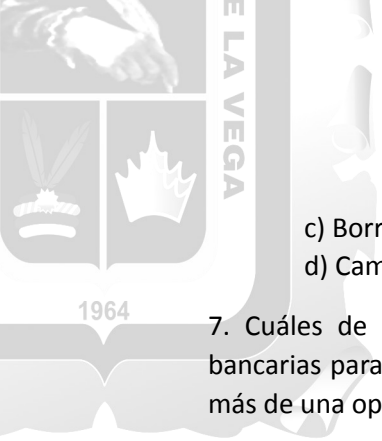
No

Desconoce

6. Los usuarios que actitudes han adoptado frente al delito del phishing: Puede marcar más de una opción.

a) Han perdido confianza en las entidades financiera y ahora no guardan su dinero en ellas

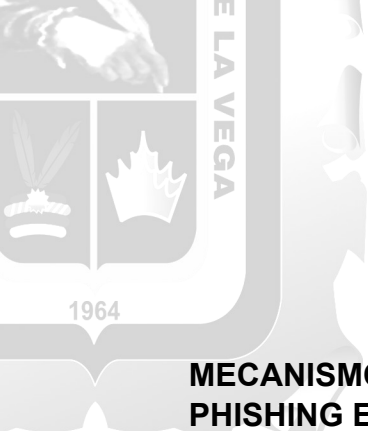
b) Utilizan menos aplicativos en su celular



- c) Borrar/Bloquean los correos electrónicos de la entidad bancaria.
- d) Cambian constantemente las contraseñas

7. Cuáles de las siguientes opciones considera Ud. que se debe implementar en las agencias bancarias para evitar la comisión de delitos informáticos phishing. De ser necesario puede marcar más de una opción.

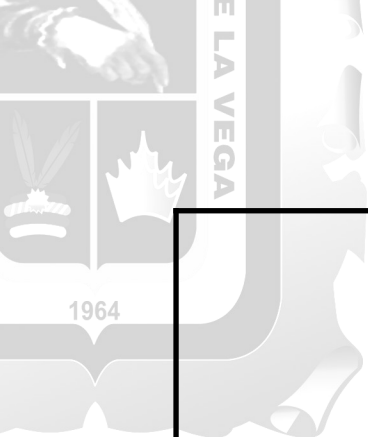
- a) Las contraseñas sean reemplazadas por identificador biométrico
- b) Implementar un reconocimiento facial
- c) Establecer un límite de tiempo de la base de datos y posterior a ello eliminar dicha información
- d) Receptar con anterioridad los correos o mensajes fraudulentos de supuestas actividades bancarias
- e) Actualizar semestralmente los softwares / parches de seguridad
- f) Otros.....



a) MATRIZ DE COHERENCIA

MECANISMOS DE PREVENCIÓN Y PROTECCIÓN DEL BIEN JURÍDICO TUTELADO FRENTE A LA MODALIDAD DELICTIVA PHISHING EN EL ORDENAMIENTO JURÍDICO PENAL PERUANO

PROBLEMA	OBJETIVOS	HIPÓTESIS Y VARIABLES	METODOLOGIA
<p><u>Problema General</u></p> <p>¿Cuáles son los mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva del phishing?</p>	<p><u>Objetivo general:</u></p> <p>Establecer los mecanismos de prevención y protección del bien jurídico tutelado por el estado a través del derecho penal en el delito informático phishing</p> <p><u>Primer Objetivo específico</u></p> <p>Analizar el delito de fraude informático bajo la modalidad del phishing</p> <p><u>Segundo objetivo específico</u></p> <p>Sistematizar la protección de los sistemas de información del delito</p>	<p><u>Hipótesis Principal</u></p> <p>La Cultura jurídica de prevención y un Plan estratégico conjunta entre la SBS y bancos resultan ser los mecanismos de prevención y protección del bien jurídico tutelados frente a la modalidad delictiva del phishing</p>	<p>Tipo: Básica</p> <p>Diseño: No experimental</p> <p>Población:</p> <p>Muestra:</p> <p>Métodos:</p> <p>General: Analítico, Deductivo e Inductivo</p> <p>Específicos: Exegético, Hermenéutico y Dogmático</p> <p>Técnicas:</p> <ul style="list-style-type: none"> -Análisis documental -Encuesta a funcionarios a especialistas en derecho penal -Entrevista a policías



<p>informático phishing</p> <p><u>Tercer objetivo específico</u></p> <p>Establecer el tratamiento legislativo en el derecho comparado respecto del phishing</p> <p><u>Cuarto objetivo específico</u></p> <p>Identificar, reportar cuantas denuncias han sido registradas por este tipo de delito phishing</p> <p><u>Quinto objetivo específico</u></p> <p>Proponer a la SBS - Directiva</p>		<p>Instrumentos</p> <ul style="list-style-type: none"> -Guía de Análisis documental -Cuestionario escala Likert - Guía de entrevistas <p>Procesamiento de Datos</p> <p>El nivel de investigación: es Descriptiva porque busca describir el fenómeno objeto de estudio</p>
--	--	--

Tabla 6*Operacionalización de las variables*

Variables	CONCEPTO	DIMENSIONES	INDICADORES
La Cultura jurídica de prevención y un Plan estratégico conjunta entre la SBS y bancos	La Cultura jurídica de prevención y un Plan estratégico conjunta entre la SBS y bancos resultan ser acciones preventivas para delitos informáticos	La Cultura jurídica de prevención	<ul style="list-style-type: none">• Informarse sobre modalidad delictiva• Abstención de manipulación
		Plan estratégico conjunta entre la SBS y bancos	<ul style="list-style-type: none">• Comunicación oportuna con bancos• Cruzamiento de información
la modalidad delictiva del phishing,	Modalidad de delito informático		<ul style="list-style-type: none">• enlaces que llevan hasta sitios web maliciosos• archivos adjuntos infectados con malware
			<ul style="list-style-type: none">• copias falsas de sitios web• introduzcan sus datos• conectarse a todas sus cuentas.
			<ul style="list-style-type: none">• mediante SMS.• descargue una aplicación.• descarga un malware en su celular.